Труды лаборатории криптографии

2020 - 2021 учебный год

Новосибирск, 2021

Состав лаборатории:

- Токарева Наталья Николаевна,
  к.ф.-м.н., с.н.с. Института математики им. С.Л.Соболева СО РАН, доцент каф. комп.систем ФИТ НГУ, каф. теор.киб. ММФ НГУ, каф. дискр.мат.и инф. СУНЦ НГУ, руководитель группы

- Коломеец Николай Александрович,
  к.ф.-м.н., н.с. Института математики им. С.Л.Соболева СО РАН, ассистент кафедры параллельных вычислений ФИТ НГУ и кафедры теоретической кибернетики ММФ НГУ

- Городилова Анастасия Александровна
  к.ф.-м.н., н.с. Института математики им. С.Л.Соболева СО РАН, старший преподаватель кафедры теоретической кибернетики ММФ НГУ и кафедры дискретной математики и информатики СУНЦ НГУ

- Калгин Константин Викторович
  к.ф.-м.н., н.с. Института вычислительной математики и математической геофизики СО РАН, старший преподаватель кафедры параллельных вычислений ФИТ НГУ

- Идрисова Валерия Александровна
  к.ф.-м.н., н.с. Института математики им. С.Л.Соболева СО РАН, ассистент кафедры теоретической кибернетики ММФ НГУ

- Куценко Александр Владимирович
  к.ф.-м.н., аспирант ММФ НГУ, ассистент кафедры теоретической кибернетики ММФ НГУ, м.н.с. Института математики им. С.Л. Соболева СО РАН

- Кондырев Дмитрий Олегович
  Аспирант ФИТ НГУ, преподаватель НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН

- Ткачев Александр Витальевич
  Аспирант ФИТ НГУ, преподаватель ФИТ НГУ

- Доронин Артемий Евгеньевич
  Аспирант ФИТ НГУ, м.н.с. Института математики им.С.Л.Соболева

- Шапоренко Александр Сергеевич,
  Аспирант ММФ НГУ, м.н.с. Института математики им.С.Л.Соболева

- Максимлюк Юлия Павловна
  Аспирантка ММФ НГУ, м.н.с. Института математики им.С.Л.Соболева

- Номонде Шарон Маланда, аспирантка НГУ
  Аспирантка ММФ НГУ

- Бонич Татьяна Андреевна
  Магистрантка 2-го курса ММФ НГУ

- Завалишина Елена Владимировна
  Магистрантка 2-го курса ФИТ НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН, преподаватель кафедры дискретной математики и информатики СУНЦ НГУ

- Панферов Матвей Андреевич
  Магистрант 2-го курса ММФ НГУ

- Сутормин Иван Александрович
  Магистрант 1-го курса ММФ НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН

- Зюбина Дарья Александровна
  Студентка 4-го курса ФИТ НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН

- Атутова Наталья Дмитриевна
  Студентка 3-го курса ММФ НГУ

- Бахарев Александр Олегович
  Студент 3-го курса ММФ НГУ

- Быков Денис Александрович
  Студент 3-го курса ММФ НГУ

- Лаханский Алексей Адреевич
  Студент 3-го курса ФИТ НГУ

- Сафенрейтер Дмитрий Алексеевич
  Студент 3-го курса ФИТ НГУ

- Парфенов Денис Романович
  Студент 4-го курса ФИТ НГУ

Избранные научные направления лаборатории

Криптографические булевы функции (бент-функции, APN-функции, и т.д.).

Самое широкое направление и наиболее представленное в лаборатории. Вопросы изучения и построения булевых функций со специальными криптографическими свойствами широко исследуются в криптографии. Такие функции непосредственно используются для конструирования шифра с секретным ключом. Мы исследуем

- функции, максимально отклоняющиеся от линейных (бент-функции),
- функции, наиболее равномерные по парам разностей вход и выход (APN-функции)
- функции, затрудняющие проведение алгебраического криптоанализа (алгебраически иммунные функции)

К данному направлению относится большая часть наших публикаций – монографии, научные статьи, кандидатские диссертации.

Криптоанализ симметричных шифров.

В этом направлении мы исследуем стойкость шифров с секретным ключом по отношению к современным методам анализа, таким как линейный, дифференциальный, алгебраический, криптоанализ по сторонним каналам. Исследуются дифференциальные и алгебраические характеристики как отдельных компонент шифров (S-блоков), так и шифров в целом, таких как ARX-шифры, шифры Simon и Speck – стандарты для шифрования в RFID-метках и другие. Задачи интересны тем, что одновременно содержат интересную математику и близки к приложениям.

Блокчейн-технологии и их приложения.

В данном направлении мы решаем задачи, связанные с разработкой и реализацией алгоритмов сокрытия информации о транзакциях в открытых распределенных реестрах (в том числе, блокчейн-системах). Исследуются криптографические алгоритмы доказательства с нулевым разглашением, их модификации и реализации.

Квантовая и постквантовая криптография.

Одним из перспективных направлений постквантовой криптографии является разработка и анализ систем шифрования, основанных на использовании кодов, исправляющих ошибки. В данном направлении мы занимаемся изучением подкодов кода Рида-Маллера и других кодов, подходящих для построения стойких криптосистем.

Международная олимпиада по криптографии Non-stop University CRYPTO 2020

Наша команда выступает основным организатором международной олимпиады NSUCRYPTO.
NSUCRYPTO – единственная международная олимпиада по криптографии, которая объединяет как школьников и студентов, так и профессионалов. За время существования олимпиады (с 2014 года) в ней приняли участие более 1600 участников из 56 стран мира (среди них – страны ЕС, страны СНГ, Канада, Китай, Индия, ЮАР, Иран, Индонезия, Вьетнам и др.). По итогам каждой олимпиады публикуются научные статьи с разбором проблем, предложенных участникам, в том числе – нерешенных, требующих отдельного научного исследования. Отличительная черта олимпиады – включение в число ее задач нерешенных проблем криптографии и информационной безопасности, предложенных ведущими специалистами в данной области. Это как раз соответствует цели олимпиады – привлечь молодых исследователей к современным вопросам криптографии и помочь им сделать свой профессиональный выбор.

Олимпиада NSUCRYPTO – Non Stop University Crypto – проходит ежегодно, принять в ней участие может любой желающий. Официальный язык олимпиады – английский. Сайт – https://nsucrypto.nsu.ru.
Олимпиада зародилась в Новосибирском Академгородке. В 2020 году она проходила с 17 по 25 октября в два независимых этапа: личный и командный. Школьники Академгородка и студенты НГУ приняли в ней активное участие.

Больше ста участников и команд заслуженно получили призы и дипломы. Вручаются также благодарственные письма руководителям и учителям призеров.

Защиты выпускных работ студентов и аспирантов лаборатории в 2021 году:

Кандидатские диссертации:

- Куценко Александр Владимирович (рук. - Токарева Н.Н.)
  Самодуальные бент-функции и их метрические свойства // диссертация на соискание степени кандидата физ.-мат. наук по специальности 01.01.09. Защита состоялась 24.03.2021.

- Облаухов Алексей Константинович (рук. - Токарева Н.Н.)
  Метрически регулярные множества в булевом кубе: конструкции и свойства // диссертация на соискание степени кандидата физ.-мат. наук по специальности 01.01.09. Защита состоялась 24.03.2021.

Магистерские диссертации:

- Бонич Татьяна Андреевна (рук. - Токарева Н.Н.)
  Periodic properties of the sequence generated by the filter generator - Периодические свойства последовательности, порождаемой фильтрующим генератором (Премия Ляпунова I степени)

- Завалишина Елена Владимировна (рук. - Токарева Н.Н.)
  Post-quantum cryptosystem with a public key - Постквантовая криптосистема с открытым ключом (диплом II степени МНСК)

- Панферов Матвей Андреевич (рук. - Токарева Н.Н.)
  Analysis of the gamma generated by the combining generator - Анализ гаммы, порождаемой комбинирующим генератором

Бакалаврские диссертации:

- Зюбина Дарья Александровна (рук. - Токарева Н.Н.)
  Криптографические свойства S-блока, построенного на основе булевой функции и перестановки (диплом I степени МНСК)

Учебные курсы, проводимые в учебном году:

1) "Криптография и криптоанализ" (Спецсеминар)

Семинар о новых событиях и результатах в области криптографии. Он всегда проходит с объявлениями. Мы можем заслушать и новый результат с доказательством в некотором узком направлении, и послушать рассказы ребят о поездке на научную конференцию или стажировку. У нас выступают преподаватели, студенты, приглашенные докладчики. Темы семинаров никогда не повторяются вот уже девять лет)) Семинар для тех, кто хотел бы связать свою научную активность с криптографией.

Руководитель: Токарева Н. Н.

2) "Математические основы и приложения квантовой информатики: криптография и вычисления" (Спецкурс)

В курсе будут приведены математические основы квантовой информатики – научной дисциплины, изучающей закономерности передачи информации, базирующиеся на законах квантовой механики. Подробно будет рассмотрен ряд квантовых алгоритмов и протоколов квантовой криптографии. Также в курсе будут представлены основы постквантовой криптографии.

Руководитель: Куценко А. В., Токарева Н. Н.

3) "Основы теории информации и криптографии" (Основной курс)

Руководитель: Токарева Н.Н.
Семинаристы: Н.А.Коломеец, А.Е.Доронин, А.С.Шапоренко

Курс посвящен основам современной теории информации и криптографии. В него входят такие направления, как

- обработка непрерывной информации; методы дискретизации;
- основы теории информации (измерения количества информации, сложности сообщений, особенности источников данных);
- методы помехоустойчивого кодирования (особенно исследующиеся в последние, 2000-е, годы методы линейного кодирования, достигающие оптимальной оценки по скорости);
- методы сжатия информации (без потерь и с потерями; изложение теоретических основ и разбор современных архиваторов);
- задачи хранения информации (надежность и отказоустойчивость, RAID-массивы);
- криптография и криптоанализ (теоретические и практические результаты, новые направления исследований последнего десятилетия);

- псевдослучайные последовательности; статистические методы их анализа;
- методы хранения, обработки и передачи информации в цифровой сотовой связи, беспроводных сетях; представление информации на различных уровнях сетевых протоколов.

Курс совмещает изложение строгих математических результатов (и их доказательств) с практическими результатами внедрения методов теории информации в конкретные системы и протоколы. Цель курса – дать студентам базовые знания по основным направлениям современной теории информации. В состав курса кроме лекций входят семинарские занятия (с решением теоретических задач) и лабораторные работы в компьютерном классе. Будет сформулирован также ряд исследовательских задач студентам, интересующимся специализацией в данной области.

4) "Криптография в задачах" (Спецсеминар)

Курс позволяет погрузиться в математику, которая используется в криптографии. Алгоритмы шифрования, основные методы криптоанализа, связь с теорией информации, криптографические функции: разобраться во всем этом поможет решение задач.

Руководитель: Коломеец Н.А.

5) "Криптография и криптоанализ. Современные методы" (Спецкурс)
Вводный курс в основы криптографии. Если вы думаете, с чего начать в этой области, то, да, именно с него.

Руководитель: Идрисова В.А., Токарева Н.Н.

6) "Булевы функции в криптографии" (Спецкурс)

В курсе рассматриваются булевы функции, представляющие интерес для криптографических приложений. Цель курса – основательное знакомство слушателей с основными криптографическими свойствами булевых функций и методами их анализа, с последними математическими результатами в этой области и современными открытыми проблемами.

Руководитель: Городилова А. А.

7) "Олимпиадные задачи по криптографии" (Спецкурс СУНЦ НГУ)

Незаменимый спецкурс для подготовки ко всероссийской олимпиаде по математике и криптографии от ИКСИ и к международной олимпиаде по

криптографии NSUCRYPTO. Хочешь подготовиться к олимпиадам в интересной соревновательной форме - тебе сюда!

Руководитель: Городилова А.А., Бонич Т.А., Панферов М.А.

8) "Математические методы в криптографии" (Спецкурс СУНЦ НГУ)
Основные методы шифрования и базовые алгоритмы криптографии рассматриваются в этом вводном курсе для школьников.

Руководитель: Завалишина Е.В., Городилова А.А.

9) «Криптография» (Основной курс ГФ НГУ)

Руководитель: Максимлюк Ю.П.

Заседания семинара «Криптография и криптоанализ»

15 июня 2021 г.
А.В.Куценко, А.С.Шапоренко, Н.Д.Атутова
Об участии в X симпозиуме «Современные тенденции в криптографии» CTCrypt 2021 (1-4 июня 2021, Москва)

04 мая 2021 г.
А. В. Куценко, Н. Д. Атутова, Д. А. Зюбина
О поездке на всероссийскую научно-техническую конференцию «Состояние и перспективы развития современной науки по направлению «Информационная безопасность» (Анапа, 21-22 апреля 2021).
Н. Д. Атутова
О поездке на саммит молодых учёных и инженеров "Большие вызовы для общества, государства и науки" (Сочи, 26-30 апреля 2021).

13 апреля 2021 г.
Выступления студентов перед МНСК:
Н. Д. Атутова
Применение эвристических методов для поиска булевых функций с высокой алгебраической иммунностью.
Н. Д. Атутова, Д. А. Зюбина, С. Д. Филиппов
Разработка автоматизированного анализа шифров на алгебраическую криптоустойчивость.
А. О. Бахарев

Реализация и анализ гибридной атаки на криптографическую систему NTRU при малых значениях параметров с использованием алгоритма квантового поиска.
Т. А. Бонич
Свойства функции в регистре сдвига с нелинейной обратной связью.
Е. В. Завалишина
Об эквивалентных ключах. Анализ криптосистемы с открытым ключом, основанной на сложности решения системы полиномиальных уравнений в целых числах.
Д. А. Зюбина
S-блоки с высокой компонентной алгебраической иммунностью.
А. А. Лаханский, Д. А. Сафенрейтер
Интеграция алгоритмов доказательства с нулевым разглашением в смарт-контракты Ethereum.
М. А. Панферов
Построение функций изменения состояний в нелинейном регистре сдвига с обратной связью.
И. А. Сутормин
Рекуррентные формулы для разностной характеристики XOR относительно сложения по модулю 2^n.

30 марта 2021 г.
Коломеец Н. А.
Реферат статьи J. Daemen, V. Rijmen, "The Wide Trail Design Strategy".

25 марта 2021 г.
И. А. Панкратова (зав. лаборатории компьютерной криптографии ТГУ)
Криптосистемы с функциональными ключами.

9 марта 2021 г.
А. Куценко, Н. Атутова, Д. Зюбина, Е. Маро (ЮФУ), С. Филиппов (СПбГУ)
Алгебраический криптоанализ шифров Simon и Speck.

2 марта 2021 г.
А. Доронин, К. Калгин
Применение SAT-решателей в задаче поиска APN-функций с помощью итеративных конструкций.

16 февраля 2021 г.
А. Шапоренко
О производных булевых бент-функций.

9 февраля 2021 г.
Н. Н. Токарева

Встреча лаборатории: отчёт и планы.

27 октября 2020 г.
Д. Кондырев, А. Лаханский, Д. Сафенрейтер
Алгоритмы доказательства с нулевым разглашением в блокчейн-системах: принципы работы и примеры реализаций.

19 октября 2020 г.
И. Сутормин
Нелинейность сбалансированных булевых функций. Обзор.

29 сентября 2020 г.
Н. Коломеец, А. Куценко, К. Калгин, А. Облаухов, В. Идрисова
Об участии в международных конференциях BFA (Норвегия, 15-17 сентября 2020) и SETA (Санкт-Петербург, 22-25 сентября 2020).

22 сентября 2020 г.
А. Куценко
О поездке на IX симпозиум «Современные тенденции в криптографии» CTCrypt 2020 (Московская область, 15-17 сентября 2020).

15 сентября 2020 г. А. Облаухов
Метрически регулярные множества в булевом кубе: конструкции и свойства (кандидатская диссертация).

10 сентября 2020 г. А. Куценко
Самодуальные бент-функции и их метрические свойства (кандидатская диссертация).

Новые учебные курсы для ФИТ (разработаны программы, набраны студенты):

1) Введение в распределенные реестры и технологию блокчейн (Д.О.Кондырев, П.А.Сазонова)

2) Криптографические проекты (Н.А.Коломеец, Д.О.Кондырев, Ю.П.Максимлюк)

3) Криптография и криптоанализ (Н.Н.Токарева, А.В.Куценко)

4) Современные вычислительные системы для решения задач криптографии и информационной безопасности (К.В.Калгин, А.Е.Доронин)

Сотрудничество (участие в Летней школе по криптографии и информационной безопасности, совместные научные исследования):

Лаборатория криптографии НПК "Криптонит" (г. Москва)

Центр безопасности коммуникаций им. Селмера Бергенского университета (г. Берген, Норвегия)

Лаборатория блокчейн, ПАО «Сбербанк» (г. Москва)

Российский квантовый центр (г. Москва)

Лаборатория проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики Белорусского государственного университета (г.Минск)

Планы по сотрудничеству:

- Сотрудничество с Балтийским университетом им. И.Канта (Калининград)
- Проведение симпозиума по криптографии 2022.
  Сотрудничество с министерством цифрового развития, связи и массовых коммуникаций Российской Федерации.

Летняя школа-конференция «Криптография и информационная безопасность» 2021

Летняя школа-конференция с международным участием «Криптография и информационная безопасность – 2021» памяти профессора С. Ф. Кренделева — традиционное мероприятие, проходящее в стенах НГУ каждый год. Организаторами выступают Криптографический центр (Новосибирск), лаборатория криптографии JetBrains Research, Факультет информационных технологий, Международный математический Центр в Академгородке, организаторы международной олимпиады NSUCRYPTO и Механико-математический факультет.

Участие в школе-конференции принимали студенты, выпускники школ и школьники 11 классов. Школа проходила с 5 по 19 июля в очном формате.

В течение двух недель с участниками школы работали 20 преподавателей. Это кураторы проектов и лекторы из Новосибирска, Томска, Москвы (Российский квантовый центр, МГУ, лаборатория блокчейн ПАО «Сбербанк»), Бергена (Норвегия), Минска (Беларусь), Ларго (США). Часть школы-конференции проходила на английском языке. Прочитана 31 лекция, проведён круглый стол, а самое главное – проведены исследования малыми группами под руководством кураторов. Темы проектов были связаны с актуальными вопросами симметричной криптографии, криптоанализа, постквантовой криптографии, блокчейн-технологий и информационной безопасности. По ряду направлений группами участников школы получены результаты, которые лягут в основу научных публикаций, их планируется доработать в течение осени. Чтобы студенты и школьники развивали не только свои интеллектуальные способности, но и не забывали о здоровье, традиционно проводились спортивные занятия под руководством тренера из Новосибирска.

Школу успешно окончил 31 участник. Это студенты НГУ (ФИТ, ММФ, ФФ), Балтийского университета им. Канта (Калининград), ТГУ (Томск), ЮФУ (Таганрог) и школьники гимназии «Горностай» (Новосибирск), Лицея информационных технологий (Новосибирск), Лицея № 6 (Бердск). Все они получили памятные сертификаты и стипендии от JetBrains Foundation.

На сайте летней школы доступно расписание лекций и сборник трудов школы – тезисы, подготовленные участниками вместе с кураторами по результатам исследований, проводившихся в рамках школы.

— В этом году нам удалось провести школу очно, комбинируя обычный формат проведения лекций с видео-форматом, когда студенты и школьники находятся в аудитории, а лектор общается с ними через экран. Получилось,

на мой взгляд, продуктивно. Очный формат, конечно, плодотворный: то, что рядом с тобой, за соседним столом и в соседних комнатах, каждый день активно работают участники школы, спорят, увлеченно что-то обсуждают, программируют, пишут на доске – очень вдохновляет на работу. Я заметила, что многие ранее не знакомые между собой ребята сдружились, и это очень хорошо, — отметила Наталья Токарева, руководитель школы, доцент кафедры компьютерных систем ФИТ НГУ и заведующая лабораторией криптографии JetBrains Research.

— It was really a pleasure to take part in the summer school. I got the impression that everything was running very smoothly both from the technical and organizational side (which is no small feat for such a big event, especially when remote and physical lectures have to be combined), so I also want to congratulate you (and the entire team) with the successful event! – комментирует своё участие в качестве лектора Николай Калейский, криптограф из Бергенского университета (Норвегия).

— Мне было очень интересно познакомиться с совершенно новой для себя сферой. Программа летней школы очень насыщенная. Лекции от ведущих специалистов, которые находятся на передовой науки и рассказывают не по книжкам, а из собственного опыта и своих исследований, которыми они занимаются каждый день. Очень понравился преподавательский состав, это отзывчивые и увлечённые своим делом люди. Также мне выпала возможность познакомиться и работать в одной команде с ребятами из других университетов и регионов. От летней школы у меня остались только положительные эмоции и новые знания, – пишет Владислав Шапаренко, выпускник школы-конференции, студент ММФ НГУ.

— Летняя школа традиционно приносит много новых знакомств и интересных проектов. Список лекторов с каждым годом пополняется, расширяется география, становится разнообразнее материал. Не стал исключением и этот год. Команде нашего проекта удалось разработать оптимизацию алгоритма поиска гарантированного числа активаций [S-блоков при проведении разностного криптоанализа], которая позволяет значительно ускорить вычисление данной характеристики, что выглядит многообещающе. Также, нельзя забывать и о других традиционных активностях, которые являются интересными — волейбольный матч, круглый стол и криптоквест, – отмечает Денис Парфёнов, студент ФИТ НГУ.

— Летняя школа – это способ найти единомышленников, с которыми можно будет реализовать проект и получить опыт выступления перед аудиторией, – считает Александр Бахарев, студент ММФ НГУ, а Наталья Атутова, студентка ММФ НГУ отмечает: «Возможность непосредственного взаимодействия с людьми, которые горят своим делом, – очень ценный опыт.

Помимо лекций и групповых занятий мне запомнился крипто-квест и матч по волейболу среди преподавателей и участников».

Организаторы школы-конференции готовы продолжить работу со студентами-участниками школы в лаборатории криптографии JetBrains Research на базе ФИТ НГУ.

Лекторы и преподаватели школы:

1) Nicky Mouha (USA) - PhD, научный сотрудник отдела компьютерной безопасности Национального института стандартов и технологий США (NIST);
2) Nikolay Kaleyski (Болгария) - научный сотрудник Центр безопасности коммуникаций им. Селмера Бергенского университета (г. Берген, Норвегия);
3) Агиевич Сергей Валерьевич (республика Беларусь) - к.ф.-м.н., заведующий НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики Белорусского государственного университета (г. Минск, Беларусь);
4) Валиахметов Илья Вадимович - магистрант 1-го курса ФИТ НГУ;
5) Высоцкая Виктория Владимировна – аспирантка ВМК МГУ им. М.В. Ломоносова, специалист-исследователь лаборатории криптографии НПК "Криптонит" (г. Москва);
6) Городилова Анастасия Александровна - к.ф.-м.н., старший преподаватель кафедры теоретической кибернетики ММФ НГУ, н.с. ИМ СО РАН;
7) Гребнев Сергей Владимирович - ведущий криптограф-исследователь QApp, Российский квантовый центр (г. Москва);
8) Идрисова Валерия Александровна - к.ф.-м.н., н.с. Института математики им. С.Л.Соболева СО РАН, ассистент кафедры теоретической кибернетики ММФ НГУ;
9) Калгин Константин Викторович - к.ф.-м.н., старший преподаватель кафедры параллельного программирования ФИТ НГУ, м.н.с. ИВМиМГ, н.с. ИМ СО РАН;
10) Колегов Денис Николаевич - к.т.н., доцент кафедры компьютерной безопасности ТГУ, главный разработчик облачной платформы кибербезопасности компании Bi.Zone (г. Томск);
11) Коломеец Николай Александрович - к.ф.-м.н., ассистент кафедры теоретической кибернетики ММФ НГУ, н.с. ИМ СО РАН;
12) Кондырев Дмитрий Олегович - аспирант ФИТ НГУ, ассистент кафедры систем информатики ФИТ НГУ, м.н.с. ИМ СО РАН;
13) Косточка Светлана Владимировна – м.н.с. ИМ СО РАН, тренер ММФ и ФИТ;

14) Куценко Александр Владимирович - аспирант ММФ НГУ, ассистент кафедры теоретической кибернетики ММФ НГУ, м.н.с. ИМ СО РАН;
15) Кяжин Сергей Николаевич - к.ф.-м.н., руководитель проектов Лаборатории блокчейн, ПАО «Сбербанк» (г. Москва);
16) Николаев Антон Анатольевич - студент кафедры компьютерной безопасности ТГУ, разработчик сервисов анализа защищенности Bi.Zone, главный разработчик фрэймворка Grinder (Томск);
17) Максимлюк Юлия Павловна - аспирантка ММФ НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН;
18) Сазонова Полина Андреевна - аспирантка ФИТ НГУ, ассистент кафедры общей информатики ФИТ НГУ, м.н.с. ИМ СО РАН;
19) Сутормин Иван Александрович - магистрант 1-го курса ММФ НГУ, м.н.с. Института математики им.С.Л.Соболева СО РАН;
20) Токарева Наталья Николаевна, доцент кафедры компьютерных систем ФИТ, кафедры теоретической кибернетики ММФ, с.н.с. ИМ СО РАН.

Публикации

Статьи опубликованные (7):

- Kalgin K., Idrisova V. On combinatorial approaches to search for APN functions and the classification of quadratic APN functions in 7 variables // Cryptography and Communications, Accepted, 2021 (SETA special issue, 18 pages). Scopus - 0.816 (Q1), WoS - 1.291 (Q2).

- Tokareva N.N., Shaporenko A.S., Solé P.
  Connections between quaternary and Boolean bent functions, pp. 561-578.
  DOI 10.33048/semi.2021.18.041
  http://semr.math.nsc.ru/v18/n1/p561-578.pdf

- Gorodilova, N. Tokareva, S. Agievich, C. Carlet, V. Idrisova, K. Kalgin, D. Kolegov, A. Kutsenko, N. Mouha, M. Pudovkina, A. Udovenko. The Seventh International Olympiad in Cryptography: problems and solutions. https://arxiv.org/abs/2106.01053

- Kondyrev, D. O. Overview of privacy preserving technologies for distributed ledgers. // Eurasian Journal of Mathematical and Computer Applications. Volume 9, Issue 1, 2021, Pages 55-68.
  DOI: 10.32523/2306-6172-2021-9-1-55-68.

- Mouha N., Kolomeec N., Akhtyamov D., Sutormin I., Panferov M., Titova K., Bonich T., Ischukova E., Tokareva N., Zhantulikov B. Maximums of the Additive Differential Probability of Exclusive-Or // IACR Transactions on Symmetric Cryptology, Volume 2021, Issue 2, 2021. Pages 292-313.
  DOI: https://doi.org/10.46586/tosc.v2021.i2.292-313.

- A. Gorodilova, N. N. Tokareva, S. V. Agievich, C. Carlet, E. V. Gorkunov, V. A. Idrisova, N. A. Kolomeec, A. V. Kutsenko, R. K. Lebedev, S. Nikova, A. K. Oblaukhov, I. A. Pankratova, M. A. Pudovkina, V. Rijmen, A. N. Udovenko. On the Sixth International Olympiad in Cryptography NSUCRYPTO // Journal of Applied and Industrial Mathematics volume 14, 623–647(2020). DOI: https://doi.org/10.1134/S1990478920040031

- Kolomeec N. Some general properties of modified bent functions through addition of indicator functions // Cryptography and Communications, 2021. Available online, 18 pages.DOI:https://doi.org/10.1007/s12095-021-00528-5WoS - 1.291 (Q2); Scopus - 0.816 (Q1)

Статьи, сданные в печать (4)

- Bonich T., Panferov M., Tokareva N. On the number of unsuitable Boolean functions in constructions of filter and combining models of stream ciphers // IEEE Trans. on Inform. Theory. Submitted, 2020 (Npages). Scopus - 1.879 (Q1), WoS - 3.036 (Q2).

- Калгин К.В, Доронин А.Е. Тесты для SAT-решателей, основанные на криптографических задачах, сдано в печать, 2020 // Прикладная дискретная математика (18 pages)

- Kutsenko A. On constructions and properties of self-dual generalized bent functions // Cryptography and Communications, Submitted, 2020 (22 pages), Scopus - 0.816 (Q1), WoS - 1.291 (Q2).

- Сутормин И. О нелинейности булевых функций, построенных обобщенной конструкцией Доббертина // Дискретный анализ и исследование операций, принято к публикации (16 страниц).

Авторефераты диссертаций (2)

- Куценко А. Самодуальные бент-функции и их метрические свойства // Автореферат диссертации на соискание степени кандидата физ.-мат. наук по специальности 01.01.09. 2021. 18 страниц. Защита состоялась 24 марта 2021 года.

- Облаухов А. Метрически регулярные множества в булевом кубе: конструкции и свойства// Автореферат диссертации на соискание степени кандидата физ.-мат. наук по специальности 01.01.09. 2021. 16 страниц. Защита состоялась 24 марта 2021 года.

Труды и тезисы конференций (18)

- Kutsenko A. The duality mapping and unitary operators acting on the set of all generalized Boolean functions // Simposium "Current Trends in Cryptography" (June 2021, Moscow) ctcrypt.ru

- Shaporenko A. On derivatives of Boolean bent functions // Simposium "Current Trends in Cryptography" (June 2021, Moscow) ctcrypt.ru

- Kutsenko A., Atutova N., Zyubina D., Maro E., Filippov S. Algebraic cryptanalysis of round-reduced lightweight ciphers Simon and Speck // Simposium "Current Trends in Cryptography" (June 2021, Moscow) ctcrypt.ru

- А.Куценко, Д.Зюбина, Н.Атутова Анализ стойкости стандартов легковесной криптографии для систем связи по радиоинтерфейсу к алгебраическим атакам // III Всероссийская научно-техническая конференция «Состояние и перспективы развития современной науки по направлению «Информационная безопасность» (апрель 2021, Анапа) https://www.era-tehnopolis.ru/events/iii-vserossiyskaya-nauchno-tekhnicheskaya-konferentsiya-sostoyanie-i-perspektivy-razvitiya/

- Атутова Н. (Новосибирск). Гибридный подход к поиску булевых функций с высокой алгебраической иммунностью на основе эвристических методов// Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT'2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Кондырев Д. Метод обеспечения конфиденциальности данных на основе zk-SNARK // Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT'2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Бахарев А. Разработка и анализ оракула для гибридной атаки на криптографическую систему NTRU с использованием алгоритма квантового поиска // Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT'2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Шапоренко А. Аффинные производные бент-функций // Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT'2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Зюбина Д., Токарева Н. S-блоки с максимальной компонентной алгебраической иммунностью от малого числа переменных // Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT'2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Куценко А., Атутова Н., Зюбина Д., Маро Е., Филиппов С. Алгебраический криптоанализ легковесных шифров Simon и Speck // Сибирская научная школа-семинар с международным участием

"Компьютерная безопасность и криптография" SIBECRYPT’2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Куценко А. О некоторых свойствах самодуальных обобщённых бент-функций // Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" SIBECRYPT’2021 (сентябрь 2021, Новосибирск) http://sibecrypt.ru/

- Атутова Н. Применение эвристических методов для поиска булевых функций с высокой алгебраической иммунностью// 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Зюбина Д. S-блоки с высокой компонентной алгебраической иммунностью // 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Атутова Н., Зюбина Д., Филиппов С. Разработка автоматизированного анализа шифров на алгебраическуюкриптоустойчивость // 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Панферов М. Построение функций обратной связи в нелинейном регистре сдвига// 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Бонич Т. Свойства функции в регистре сдвига с нелинейной обратной связью// 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Бахарев А. Реализация и анализ гибридной атаки на криптографическую систему NTRU при малых значениях параметров с использованием алгоритма квантового поиска // 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

- Сутормин И. Рекуррентные формулы для разностной характеристики XOR относительно сложения по модулю 2^n// 59-ая Международная научная студенческая конференция МНСК-2021 (апрель 2021, Новосибирск) http://issc.nsu.ru/

On combinatorial approaches to search for quadratic APN functions

Konstantin Kalgin*
Sobolev Institute of Mathematics
Novosibirsk State University
Novosibirsk, Russia
kalginkv@gmail.com

Valeriya Idrisova
Sobolev Institute of Mathematics
Novosibirsk, Russia
vvitkup@yandex.ru

Abstract

Almost perfect nonlinear functions possess the optimal resistance to the differential cryptanalysis and are widely studied. Most known APN functions are obtained as functions over finite fields $\mathbb{F}_{2^n}$ and very little is known about combinatorial constructions in $\mathbb{F}_2^n$. In this work we proposed two approaches for obtaining quadratic APN functions in $\mathbb{F}_2^n$. The first approach exploits a secondary construction idea, it considers how to obtain quadratic APN function in $n+1$ variables from a given quadratic APN function in n variables using special restrictions on new terms. The second approach is searching quadratic APN functions that have matrix form partially filled with standard basis vectors in a cyclic manner. This approach allowed us to find a new APN function in 7 variables. Also, we conjectured that a quadratic part of an arbitrary APN function has a low differential uniformity. This conjecture allowed us to introduce a new subclass of APN functions, so-called stacked APN functions. We found cubic examples of such functions for dimensions up to 6.

1 Introduction

Let us recall some definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where n and m are integers, is called a *vectorial Boolean function*. If $m = 1$ such a function is called *Boolean*. Every vectorial Boolean function F can be represented as an ordered set of m *coordinate functions* $F = (f_1, \ldots, f_m)$, where f_i is a Boolean function in n variables. Any vectorial function F can be represented uniquely in its *algebraic normal form (ANF)*:

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \Big(\prod_{i \in I} x_i \Big),$$

*The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394 and 20-31-70043) and Laboratory of Cryptography JetBrains Research.

where $\mathcal{P}(N)$ is a power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2^m$. The *algebraic degree* of a given function F is the degree of its ANF: deg (F) =max$\{|I| : a_I \neq 0, I \in \mathcal{P}(N)\}$. If algebraic degree of a function F is not more than 1 then F is called *affine*. If for an affine function F it holds $F(\mathbf{0}) = \mathbf{0}$ then F is called *linear*. If algebraic degree of a function F is equal to 2 then F is called *quadratic*.

We can put the finite field $\mathbb{F}_{2^n}$ in one-to-one correspondence to the vector space $\mathbb{F}_2^n$ and consider vectorial Boolean functions as functions over $\mathbb{F}_{2^n}$. Then any vectorial function F has the unique *univariate polynomial representation* over $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} \lambda_i x^i, \ \lambda_j \in \mathbb{F}_{2^n}.$$

Two vectorial functions F and G are *extended affinely equivalent (EA-equivalent)* if $F = A_1 \circ G \circ A_2 + A$ where A_1, A_2 are affine permutations on $\mathbb{F}_2^n$ and A is an affine function. Two functions F and G are called *Carlet-Charpin-Zinoviev [7] equivalent (CCZ-equivalent)* if their graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ are affinely equivalent, that is, if there exists an affine automorphism $A = (A_1, A_2)$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = F(x) \Leftrightarrow A_2(x, y) = G(A_1(x, y))$.

Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For vectors $a, b \in \mathbb{F}_2^n$, where $a \neq 0$, consider the value

$$\delta(a, b) = \big|\{ \ x \in \mathbb{F}_2^n \mid F(x + a) + F(x) = b\}\big|.$$

Denote by Δ_F the following value:

$$\Delta_F = \max_{a \neq \mathbf{0}, \ b \in \mathbb{F}_2^n} \delta(a, b).$$

Then F is called *differentially Δ_F-uniform* function. The smaller the parameter Δ_F is the better the resistance of a cipher containing F as an S-box to differential cryptanalysis. For the vectorial functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ the minimal possible value of Δ_F is equal to 2. In this case the function F is called *almost perfect nonlinear (APN)*. This notion was introduced by K. Nyberg in [9].

APN functions are widely studied by many researchers, but there is still a significant list [6] of important open questions, such as lower and upper bounds on the number of APN functions, an upper bound on algebraic degree of an APN function [4], the existence of bijective APN functions in even dimensions, etc. We are especially interested in two open problems that are devoted to constructing APN functions. The first one is to find secondary constructions of APN functions, in particular, it was stated as Problem 3.8 in [6]. The second problem is to find new constructions of APN functions in vectorspace $\mathbb{F}_2^n$, since almost all the known constructions of this class are found only as polynomials over the finite fields, and to the best of our knowledge, the only approach to such combinatorial constructions was proposed in [8].

In this work we propose two approaches for generating quadratic APN functions in $\mathbb{F}_2^n$. The first approach considers the algebraic normal form of a given quadratic APN function G in n variables and extends it into an ANF of a quadratic function F in $n + 1$

variables, using special restrictions on coefficients of new terms. In the second method we consider special matrices that are partially filled with vectors of standard basis and search for corresponding APN functions using the same idea of restrictions. Using this approach we found previously unknown (in the sense of CCZ-equivalence) quadratic APN function for $n = 7$. Generally, quadratic APN functions are not suitable as secure S-boxes due to the low algebraic degree, but obtaining new quadratic representatives can lead us to another useful functions. This is very important for even $n \geqslant 8$, since new APN permutations CCZ-equivalent to quadratic functions can be found for these dimensions [3].

In the last part of the work we conjectured that a quadratic part of an arbitrary APN function has a low differential uniformity. We introduced the new notion of stacked APN function and for dimensions up to 6 found such functions using quadratic APN functions obtained with approaches mentioned above.

2 On secondary approach to search for quadratic APN functions

Since EA-equivalence preserves APNness, it is always possible to omit linear and constant terms in the algebraic normal form of a given APN function. We shall then consider quadratic vectorial Boolean functions that have only quadratic terms in their ANF. The following known result gives a necessary condition on the ANF of a given APN function.

Theorem 1. *[1] Let $F = (f_1, \ldots, f_n)$ be an APN function in n variables. Then every quadratic term $x_i x_j$, where $i \neq j$, appears at least in one coordinate function of F.*

This property motivated us to suggest the following construction of quadratic APN functions. Let $G = (g_1, \ldots, g_n)$ be a quadratic APN-function in n variables. Consider vectorial function $F = (f_1, \ldots, f_n, f_{n+1})$ in $n + 1$ variables such that:

$$\begin{aligned} f_1 &= g_1 + \sum_{i=1}^{n} \alpha_{1,i} x_i x_{n+1}; \\ &\ldots \\ f_n &= g_n + \sum_{i=1}^{n} \alpha_{n,i} x_i x_{n+1}; \\ f_{n+1} &= g_{n+1} + \sum_{i=1}^{n} \alpha_{n+1,i} x_i x_{n+1}, \end{aligned} \tag{1}$$

where $\alpha_{1,i} \ldots, \alpha_{n+1,i} \in \mathbb{F}_2$ for $i = 1, \ldots, n$ and $g_{n+1} = \sum_{1 \leqslant j < k \leqslant n} \beta_{j,k} x_j x_k$ for some fixed $\beta_{j,k} \in \mathbb{F}_2$. Note that if $\alpha_{1,i}, \ldots, \alpha_{n,i}$ are such that each term $x_i x_{n+1}$ appears at least in one of the coordinate functions $f_1, \ldots, f_n$, then the necessary condition of Theorem 1 is held for the constructed function F. Since the exhaustive search for the given APN function becomes complicated starting from $n = 6$, there is a need to find necessary and sufficient conditions on new coefficients of F.

Let us denote the lexicographically ordered elements of $\mathbb{F}_2^n$ as $x^0, \ldots, x^{2^n-1}$. Since all the values $G(x^0), \ldots, G(x^{2^n-1})$ of the function G are known, we can represent values of

the constructed function F only through unknown coefficients $\alpha_{i,k}$ and some constant terms. Since F is an APN function, for a nonzero a all sums $F(x) + F(x + a)$ and $F(y) + F(y + a)$, where $x \neq y$ and $x \neq y + a$, should be pairwise different. This fact applies special restrictions on coefficients $\alpha_{i,k}$. For the convenient representation of these restrictions further we consider the following matrix approach that was proposed by Beth and Ding in [1].

Each quadratic vectorial function G in n variables can be considered as a symmetric matrix $\mathcal{G} = (g_{ij})$, where each element $g_{ij} \in \mathbb{F}_2^n$ is a vector of coefficients corresponding to term $x_i x_j$ in the algebraic normal form of G and all diagonal elements g_{ii} are null.

t is necessary to mention that these matrices also were used in [11] and [10] to construct and classify a lot of new quadratic APN functions over finite fields.

Example 2. For $n = 3$ let us consider function $G = (g_1, g_2, g_3) = (x_1x_2, x_2x_3, x_1x_3)$ $= \begin{bmatrix}1\\0\\0\end{bmatrix} \cdot x_1x_2 + \begin{bmatrix}0\\0\\1\end{bmatrix} \cdot x_1x_3 + \begin{bmatrix}0\\1\\0\end{bmatrix} \cdot x_2x_3.$

Then the corresponding matrix $\mathcal{G}$ is the following:

$$\mathcal{G} = \begin{bmatrix}(000) & (100) & (001)\\(100) & (000) & (010)\\(001) & (010) & (000)\end{bmatrix}$$

It is necessary to mention that these matrices also were used in [11] and [10] to construct and classify a lot of new quadratic APN functions over finite fields. Using these matrices the APN property can be formulated in the following way:

Proposition 3. *Let $\mathcal{G}$ be the matrix that corresponds to quadratic vectorial function G. Then function G is APN if and only if $x \cdot (\mathcal{G} \cdot a) \neq 0$ for all $x \neq a$, where $a, x \in \mathbb{F}_2^n$ and $a \neq 0$.*

In terms of matrices method (1) can be considered as an extension of a given $\mathcal{G}$ with an extra bit that represents g_{n+1} in every element and an extra pair of row and column that represents a set of new terms $x_i x_{n+1}$.

Example 4. For the considered APN function $G = (g_1, g_2, g_3) = (x_1x_2, x_2x_3, x_1x_3)$ we choose null g_{n+1} and construct APN function $F = (f_1, f_2, f_3, f_4)$ in 4 variables, where:

$f_1 = g_1$;

$f_2 = g_2 + x_3x_4$;

$f_3 = g_3 + x_2x_4 + x_3x_4$;

$f_4 = x_1x_4 + x_3x_4$.

Then the corresponding matrix $\mathcal{F}$ is the following:

$$\mathcal{F} = \begin{bmatrix} (0000) & (1000) & (0010) & (0001) \\ (1000) & (0000) & (0100) & (0010) \\ (0010) & (0100) & (0000) & (0111) \\ (0001) & (0010) & (0111) & (0000) \end{bmatrix}$$

Consider a quadratic APN function G and the corresponding $n \times n$ matrix $\mathcal{G}$. Denote the vector of nonzero coefficients for new variables as $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$. Let us fix g_{n+1} and construct $(n+1) \times (n+1)$ matrix $\mathcal{F}$ by adding $(\alpha_1, \ldots, \alpha_n, 0)$ to $\mathcal{G}$ as the last column and the last row and adding new bit to every element of $\mathcal{G}$ according to the choice of g_{n+1}. Let us denote as $\mathcal{G}'$ the submatrix (f_{ij}) of $\mathcal{F}$, such that $i, j < n+1$. Let $\langle X \rangle$ denote the linear span of an arbitrary set $X \subseteq \mathbb{F}_2^n$ and F be the quadratic vectorial function corresponding to the constructed matrix $\mathcal{F}$. Then the following proposition is true.

Proposition 5. *F is APN if and only if $\alpha \cdot a'$ does not belong to $\langle \mathcal{G}' \cdot a' \rangle$ for all $a' \in \mathbb{F}_2^n$, $a' \neq \boldsymbol{0}$.*

Let us note that Proposition 5 shows how to obtain restrictions on new coefficients in the convenient form.

For the given $k \in \mathbb{N}$ let us consider the following sets:

$S_{i,k} = \{\alpha_i + v \mid v \in \langle \mathcal{G}' \cdot (e_i + e_k) \rangle\}$;

$S_{i,j,k} = \{\alpha_i + \alpha_j + v \mid v \in \langle \mathcal{G}' \cdot (e_i + e_j + e_k) \rangle\}$;

$\ldots$

$S_{1,2,\ldots,k-1,k} = \{\alpha_1 + \alpha_2 + \ldots + \alpha_{k-1} + v \mid v \in \langle \mathcal{G}' \cdot (e_1 + e_2 + \ldots + e_{k-1} + e_k) \rangle\}$,

where $e_1, \ldots, e_n$ is the standard basis in $\mathbb{F}_2^n$. Let us call a vector $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$, *admissible* for matrix $\mathcal{G}'$ if it satisfies the condition in Proposition 5. We call a sequence $(\alpha_1^*, \ldots, \alpha_k^*)$, where $\alpha_i^* \in \mathbb{F}_2^{n+1}$, to be *$k$-admissible* for some $k \leqslant n$, if vector $\alpha^* = (\alpha_1^*, \ldots, \alpha_k^*, \mathbf{0}, \ldots, \mathbf{0})$ of length n is admissible for all nonzero $a' = (a'_1, \ldots, a'_n) \in \mathbb{F}_2^n$ such that $a'_{k+1} = 0, \ldots, a'_n = 0$. An n-admissible sequence can be considered as an admissible vector of length n. Consider an APN function G in n variables and a fixed g_{n+1}.

Proposition 6. *The number of quadratic APN functions that can be obtained from function G using the construction from (1) is equal to the number of admissible vectors $\alpha = (\alpha_1, \ldots, \alpha_n)$ for matrix $\mathcal{G}'$.*

It can be seen that there are $2^{n+1} - \mid \langle \mathcal{G}' \cdot (e_1) \rangle \mid$ vectors α_1 such that (α_1) is 1-admissible. The following proposition shows how to obtain the number of admissible vectors:

Proposition 7. *Let $(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$ be the $(k-1)$-admissible sequence for some $k < n+1$. Then there exist*

$$2^{n+1} - \mid \langle \mathcal{G}' \cdot (e_k) \rangle \cup \{\bigcup_{i=1}^{k-1} S_{i,k}\} \cup \{\bigcup_{1 \leqslant i < j < k,} S_{i,j,k}\} \cup \ldots \cup S_{1,2,\ldots,k-1,k} \mid$$

vectors α_k such that sequence $(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k)$ is k-admissible.

Also, our method can be extended to the case when G is not an APN function, but the ANF of G and g_{n+1} together contain all possible quadratic terms. The following proposition describes the necessary condition on the choice of such functions.

Proposition 8. *Let G be a quadratic vectorial function in n variables and F be an APN function in $n+1$ variables that it is obtained from G using construction (1). Then $\Delta_G \leqslant 4$.*

For example, for differentially 4-uniform function $G = (g_1, g_2, g_3, g_4, g_5)$, where:
$g_1 = x_1x_2 + x_3x_5 + x_4x_5$;
$g_2 = x_1x_3 + x_4x_5$;
$g_3 = x_2x_3 + x_1x_4 + x_3x_5 + x_4x_5$;
$g_4 = x_2x_4 + x_1x_5 + x_4x_5$;
$g_5 = x_3x_4 + x_2x_5 + x_4x_5$.
and g_6 contains all the terms x_ix_j, where $i < j \leqslant n$, we obtained 13 CCZ classes of APN functions among constructed functions. Let us recall that there exist only 13 CCZ classes of quadratic APN functions in dimension 6.

It can be seen that every quadratic APN function can be obtained using construction from(1). It is worth mentioning that when $n = 3, 4$ and 5 for APN functions that are CCZ classes representatives we obtained all the possible classes of quadratic APN functions for $4, 5$ and 6 variables from the classification [2] and large variety of classes for constructing from 6 to 7 variables.

Note that for the given APN function G in n variables we have $2^{\frac{(n^2-n)}{2}}$ possibilities to choose g_{n+1}. It is interesting that the choice of g_{n+1} affects the capability to obtain APN function F in $n+1$ variables, the number of such constructed functions and the variety of different CCZ-classes among constructed classes. For example, when $n = 5$ and g_{n+1} is null both quadratic CCZ-representatives give us the only one CCZ-class for 6 variables (class 11 in the list from [2]). At the same time, when g_{n+1} contains all quadratic terms x_ix_j, these functions give 13 CCZ-classes of quadratic APN functions in 6 variables. Unfortunately, for $n \geqslant 7$ it becomes computationally harder to choose the proper initial function and g_{n+1} and to obtain a large amount of generated functions. It seems that method (1) is not so efficient on large dimensions.

3 On cyclic approach to search for quadratic APN functions

Let us introduce another approach for constructing quadratic APN functions using matrix representation from previous section. Let $e_1, \ldots, e_n$ be the standard basis in $\mathbb{F}_2^n$. For the given n consider the following matrix with elements from $\mathbb{F}_2^n$:

$$\mathcal{T} = \begin{bmatrix} 0 & e_1 & e_2 & e_3 & \ldots & e_{n-2} & e_{n-1} \\ e_1 & 0 & e_3 & e_4 & \ldots & e_{n-1} & e_n \\ e_2 & e_3 & 0 & e_5 & \ldots & e_n & t_{3,n} \\ e_3 & e_4 & e_5 & 0 & \ldots & t_{4,n-1} & t_{4,n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ e_{n-2} & e_{n-1} & e_n & t_{n-1,4} & \ldots & 0 & t_{n-1,n} \\ e_{n-1} & e_n & t_{n,3} & t_{n,4} & \ldots & t_{n,n-1} & 0 \end{bmatrix},$$

where $t_{i,j} = t_{j,i}$ and $t_{i,j}$ denote some unknown elements in $\mathbb{F}_2^n$.

Our aim is to find values of missed matrix elements such that matrix $\mathcal{T}$ represents APN function. We can apply the approach with restrictions from the previous section. Without loss of generality let us consider the first unknown element of matrix $\mathcal{T}$ that is $t_{3,n}$. According to Proposition 5 the last column of $\mathcal{T}$ should satisfy $(e_{n-1}, e_n, t_{3,n}, \ldots, 0) \cdot a' \notin \langle \mathcal{T}' \cdot a' \rangle$, where $a' \in \mathbb{F}_2^{n-1}$, $a' \neq 0$ and $\mathcal{T}' = \mathcal{T} \setminus (e_{n-1}, e_n, t_{3,n}, \ldots, 0)$. If we consider all $a' = a'_1, \ldots, a'_{n-1}$ such that $a'_3 = 1$ and $a'_i = 0$, if $i > 3$, we obtain restrictions on the value of $t_{3,n}$ that are independent from any other unknown element of $\mathcal{T}$. Repeating this procedure step by step for every new element after fixing values of previous variables $t_{i,j}$ allows us to obtain all possible fillings for the given matrix $\mathcal{T}$.

For $n = 3, 4$ and 5 this construction covered all quadratic CCZ classes of APN functions. For $n = 6$ it covered 11 out of 13 classes. Unfortunately, for larger dimensions the number of generated functions dropped dramatically and the construction covers only 7 classes for $n = 7$ and only one class for $n = 8$. As a consequence, we consider the following generalization of this construction.

Let $\mathcal{T}$ be the same matrix that contains k unknown elements. Consider the diagonal that contains all elements e_n in $\mathcal{T}$. It is easy to see that we can remove any element e_n from this diagonal and apply the above procedure to the new matrix with $k+1$ unknown elements. Moreover, we can remove any number of elements from $\mathcal{T}$ and the more elements are deleted the more APN functions can be constructed using this matrix.

For $n = 6$ when we removed one element e_n from the diagonal in $\mathcal{T}$ the new matrix had already covered all 13 CCZ classes of quadratic APN functions. For $n = 7$ and the matrix that has no elements e_n on the diagonal we generated 2341888 quadratic APN functions. We have found a new CCZ class for $n = 7$ among obtained functions. Here we provide a representative of this class in the univariate form:

$F(x) = a^{100}x + a^{88}x^2 + a^{89}x^3 + a^{107}x^4 + a^{57}x^5 + a^{98}x^6 + a^{56}x^8 + a^9x^9 + a^{58}x^{10} + a^{60}x^{12} + a^{109}x^{16} + a^{47}x^{17} + a^{44}x^{18} + a^{27}x^{20} + a^{91}x^{24} + a^{71}x^{32} + a^{96}x^{33} + a^{101}x^{34} + a^7x^{36} + a^{12}x^{40} + a^{34}x^{48} + a^{66}x^{64} + a^4x^{65} + a^4x^{66} + a^{73}x^{68} + a^{73}x^{72} + a^{56}x^{80} + a^{20}x^{96}$,

where a is the primitive element whose minimal polynomial over $\mathbb{F}_{2^7}$ is $x^7 + x + 1$.

4 The differential uniformity of quadratic parts of APN functions and the class of stacked APN functions

Let F be a vectorial Boolean function of algebraic degree d. Then it can be represented as sum $F = F^{(c)} + F^{(1)} + F^{(2)} + \ldots + F^{(d)}$, where each function $F^{(j)}$ contains only monomials of algebraic degree j and $F^{(c)}$ is a constant term. We observed that if F is an APN function then its quadratic part $F^{(2)}$ has a low differential uniformity.

Conjecture 9. Let F be an APN function in n variables, where $4 \leqslant n \leqslant 7$. Then $\Delta_{F^{(2)}} \leqslant 4$.

The conjecture is true for $n = 4$. When $n = 8, 9$ there were found APN functions F (e.g. Kasami power functions for $n = 8$ and Inverse function for $n = 9$) such that

$\Delta_{F^{(2)}} = 8$. Nevertheless, for these large dimensions the differential uniformity of quadratic parts is still quite low. Further we consider only functions without affine terms.

Proposition 10. *Let F be an APN function in n variables, where $F = F^{(2)} + F^{(3)} + \ldots + F^{(d)}$. If $H = F + F^{(2)} = (0, \ldots, 0, h_j, 0, \ldots, 0)$ for some $1 \leqslant j \leqslant n$, then $\Delta_{F^{(2)}} \leqslant 4$.*

For $n = 4, 6$ there exist cubic APN functions such that $H = F + F^{(2)} = (0, \ldots, 0, h_j, 0, \ldots, 0)$ for some $1 \leqslant j \leqslant n$. Examples of such F and $F^{(2)}$ for $n = 4$ can be found in Table 1. An example of F for $n = 6$ is the following:

$f_1 = x_1x_2 + x_4x_6 + x_5x_6 + x_2x_3x_5;$
$f_2 = x_1x_3 + x_3x_5 + x_4x_5 + x_2x_6 + x_5x_6;$
$f_3 = x_2x_3 + x_1x_4 + x_4x_5 + x_5x_6;$
$f_4 = x_2x_4 + x_1x_5 + x_3x_5 + x_2x_6 + x_3x_6 + x_4x_6 + x_5x_6;$
$f_5 = x_3x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1x_6 + x_2x_6 + x_3x_6 + x_5x_6;$
$f_6 = x_3x_5 + x_2x_6 + x_5x_6.$

Let us note that these simple results allow us to use quadratic APN or differentially 4-uniform functions to construct functions of higher degrees, particularly, cubic APN functions. The observation on low differential uniformity of quadratic parts of APN functions motivated us to introduce a new subclass of APN functions.

Definition 11. Let $F = F^{(2)} + \ldots + F^{(d)}$ be an APN function of algebraic degree d. If all functions $F - F^{(d)}$, $F - F^{(d)} - F^{(d-1)}, \ldots, F - F^{(d)} - F^{(d-1)} - \ldots - F^3$ are APN functions then F is called a *stacked APN function.*

Let us describe possible approaches to constructing stacked APN functions of degree 3. Let H be a cubic vectorial function in n variables with no affine or quadratic terms. Then $H = \sum_{i,j,k} a_{ijk}x_ix_jx_k$, where $1 \leqslant i < j < k \leqslant n$ and $a_{ijk} \in \mathbb{F}_2^n$. Let $a_{i_1j_1k_1}$ be an arbitrary nonzero coefficient in the ANF of H. Let us call H a *cubic shift* if for all $1 \leqslant i < j < k \leqslant n$ vector a_{ijk} is null or equal to $a_{i_1j_1k_1}$.

For $n = 4, 5$ we implemented the search of cubic APN functions $F = F^{(2)} + F^{(3)}$ such that $F^{(3)}$ is some cubic part and $F^{(2)}$ is an APN quadratic function, that is constructed using the cyclic matrix $\mathcal{T}$ from the previous section. For $n = 6$ we implemented the similar search, but $F^{(3)}$ was a cubic shift since it is computationally hard to search through all the possible cubic parts. We have found a large amount of cubic stacked APN functions for $n = 4, 5, 6$. Some examples are listed in Table 1.

It is worth mentioning that for quadratic APN functions from differenet different CCZ classes for $n = 6$ we have found more than 70 000 cubic stacked APN functions and all these functions belong to the same CCZ-class that is the only known class that does not contain quadratic functions (class number 13 in the list from [2]), despite that all 14 CCZ classes contains (see [5]) cubic representatives.

Table 1: Examples of stacked cubic APN functions (both F and $F^{(2)}$ are APN).§

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	0	0	0	1	0	2	4	7	0	4	6	3	8	14	11	12
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	6	3	8	14	10	13
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	0	0	0	1	0	2	4	7	0	4	10	15	19	21	28	27
	0	8	16	25	11	1	29	22	15	3	17	28	31	17	6	9
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	10	15	19	21	29	26
	0	8	16	25	11	1	31	20	15	3	21	24	23	25	9	6
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$F(x)$	0	0	0	1	0	2	4	13	0	4	8	7	16	22	28	27
	0	8	16	19	9	3	29	22	45	33	53	56	52	58	40	45
	0	16	60	45	26	8	34	59	55	35	3	28	61	43	13	26
	5	29	41	58	22	12	62	37	31	3	59	38	28	2	60	41
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	8	13	16	22	28	27
	0	8	16	25	9	3	29	22	45	33	53	56	52	58	40	39
	0	16	60	45	26	8	34	49	55	35	3	22	61	43	13	26
	5	29	41	48	22	12	62	37	31	3	59	38	28	2	60	35

Acknowledgements

We would like to cordially thank Natalia Tokareva for her valuable remarks. The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (projects no. 18-07-01394 and 20-31-70043) and Laboratory of Cryptography JetBrains Research.

References

[1] T. Beth, C. Ding. On almost perfect nonlinear permutations. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, pp. 65-76, 1993.

[2] M. Brinkmann, G. Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, vol. 49, Issue 1–3, pp. 273-288, 2008.

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe. An APN Permutation in Dimension Six. *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS*, vol. 518, pp. 33-42, 2010.

[4] L. Budaghyan, C. Carlet, T. Helleseth, N. Li and B. Sun. On Upper Bounds for Algebraic Degrees of APN Functions. *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4399-4411, 2018.

[5] M. Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptogr. Commun.* vol. 12, pp.821-840, 2020.

[6] C. Carlet. Open Questions on Nonlinearity and on APN Functions. *Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science*, vol. 9061, pp 83-107 (2015).

[7] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, vol. 15, pp. 125-156, 1998.

[8] A. A. Gorodilova. Characterization of almost perfect nonlinear functions in terms of subfunctions, *Diskr. Mat.*, vol. 27(3), pp. 3-16 (2015); *Discrete Math. Appl.*, vol. 26(4), pp. 193-202, 2016.

[9] K. Nyberg. Differentially uniform mappings for cryptography. *Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, pp. 55-64, 1994.

[10] Y. Yu, N. S. Kaleyski, L. Budaghyan, Y. Li. Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9. *IACR Cryptol. ePrint Arch.*: 1491, 2019.

[11] Y. Yu, M. Wang, Y. Li. A matrix approach for constructing quadratic APN functions. *Des. Codes Cryptogr.* 73, 587-600, 2014

S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 18, №1, стр. 561–578 (2021) УДК 519.7
DOI 10.33048/semi.2021.18.041 MSC 06E30, 11T71, 14G50

CONNECTIONS BETWEEN QUATERNARY AND BOOLEAN BENT FUNCTIONS

N.N. TOKAREVA, A.S. SHAPORENKO, P. SOLÉ

Abstract. Boolean bent functions were introduced by Rothaus (1976) as combinatorial objects related to difference sets, and have since enjoyed a great popularity in symmetric cryptography and low correlation sequence design. In this paper connections between classical Boolean bent functions, generalized Boolean bent functions and quaternary bent functions are studied. We also study Gray images of bent functions and notions of generalized nonlinearity for functions that are relevant to generalized linear cryptanalysis.

Keywords: Boolean functions, generalized Boolean functions, quaternary functions, bent functions, semi bent functions, nonlinearity, linear cryptanalysis, Gray map, $\mathbb{Z}_4$-linear codes.

1. Introduction

Boolean bent functions were introduced by Rothaus [23] as combinatorial objects related to difference sets, and have since enjoyed a great popularity in symmetric cryptography and sequence design. They are, in particular, maps from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ with some special spectral properties. Their importance in symmetric cryptography stems from linear cryptanalysis of stream ciphers [15, 16, 17]. In that context bent functions are the ones which are the worst approximated by affine functions, or, equivalently have the best possible nonlinearity. More information concerning bent functions can be found in the monographs [19, 32]. Several researchers [3, 6, 20, 21]

Tokareva, N.N., Shaporenko, A.S., Solé, P., Connections between quaternary and Boolean bent functions.

The work of the first and the second authors was supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

Received October, 5, 2020, published May, 26, 2021.

have explored extensions of linear cryptanalysis to groups other than the usual elementary abelian 2-groups. In this paper we study a notion of nonlinearity that seems consistent with their notions. We discuss the connection between two notions of $\mathbb{Z}_4$-bentness introduced from a sequence design viewpoint (for applications in CDMA systems) and the classical notion of bent function.

The first approach is to consider functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, q is any integer, see the paper [10] of Kumar, Scholtz and Welch. We call them **q-ary functions**. Another, more recent approach, which is more natural from the viewpoint of cyclic codes over rings is to consider functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$. This is the approach of Schmidt in [24]. We call these latter functions **generalized Boolean functions**. In this paper we focus on the quaternary case ($q = 4$), and explore the interplay between the three types of definitions for bentness.

Let us note that there exist other ways to generalize the concept of bent function. See surveys of distinct generalizations in [31] and [32].

The material is organized as follows. Necessary definitions are given in section 2. In section 3 we prove that a generalized Boolean function $f(x, y) = a(x, y)+2b(x, y)$ is bent if and only if Boolean functions b and $a\oplus b$ are both bent. Section 4 shows that there is no direct link between notions of Boolean and quaternary bent functions but we obtain several facts related to bent Boolean and quaternary functions. There is no direct connection between notions of quaternary and generalized bent functions either, which is shown in section 5. Then in section 6 we show that quaternary generalized Boolean bent functions in n variables yield Boolean bent functions by Gray map, or semi bent functions, depending on the parity of n. Section 7 characterizes bent functions by their nonlinearity. Section 8.1 illustrates our results by a survey of the known constructions of generalized bent functions and their Gray images. In section 8.2 we introduce two simple constructions for quaternary bent functions.

Note that the first variant of this paper appeared at ePrint archive [27], see also [28]. After that several related results were obtained by different authors. Thus, Stănică et al. [29] extended the results of [27] related to generalized Boolean bent functions by considering functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_8$. Later the results were extended for functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{16}$ by Martinsen et al. [13]. Finally, Hodžić et al. [8] gave a complete characterization of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{2^k}$ for $k > 1$ in terms of both the necessary and sufficient conditions their component Boolean functions need to satisfy. Two open problems that were mentioned in the original paper [27] were solved. More specifically, in [29] the quaternary analogue of Dillon's construction was presented. Then Li et al. [11] characterized the functions in n variables of the form $f(x) = Tr(ax + 2bx^{1+2^k})$ for odd $n/\gcd(n, k)$. The results obtained in the original paper [27] were instrumental in the following works [4, 5, 11, 18, 22]. The original paper [27] was also mentioned in [14, 26, 30].

2. Definitions and Notation

In what follows by $\oplus$ we mean addition over $\mathbb{Z}_2$ (modulo 2). We will use $+$ for two types of addition: over $\mathbb{Z}_4$ and natural one. It always depends on the context. We will also use the following two types of inner product:

$$\langle x, y\rangle = x_1y_1 \oplus ... \oplus x_ny_n,$$

$$x.y = x_1y_1 + ... + x_ny_n.$$

Let n, q be integers, $q \geqslant 2$.

We consider the following mappings:

1) $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — **Boolean function** in n variables. Its *sign function* is $F := (-1)^f$. The *Walsh–Hadamard transform* (WHT) of f is

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_2^n} (-1)^{f(y) \oplus \langle x,y \rangle} = \sum_{y \in \mathbb{Z}_2^n} F(y)(-1)^{\langle x,y \rangle}. \tag{1}$$

A Boolean function f is said to be *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. It is *semi bent* iff $\widehat{F}(x) \in \{0, \pm 2^{(n+1)/2}\}$ (sometimes such functions are called *near bent*). This is a special case of *plateaued functions* [33]. Note that Boolean bent (resp. semi bent) functions exist only if the number of variables, n, is even (resp. odd).

2) $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ — **generalized Boolean function** in n variables. Its *sign function* is $F := \omega^f$, with ω a primitive complex root of unity of order q, i. e. $\omega = e^{2\pi i/q}$. When $q = 4$, we write $\omega = i$. Its WHT is given as

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_2^n} \omega^{f(y)} (-1)^{\langle x,y \rangle} = \sum_{y \in \mathbb{Z}_2^n} F(y)(-1)^{\langle x,y \rangle}. \tag{2}$$

As above, a generalized Boolean function f is *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. In comparison to the previous case it does not follow that n should be even if f is bent. Such functions for $q = 4$ were studied by K.-U. Schmidt (2006) in [24]. Here we consider only this partial case $q = 4$.

3) $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ — **q-ary function** in n variables. Its *sign function* is given by $F := \omega^f$ as in the previous case. Its WHT is defined by

$$\widehat{F}(x) := \sum_{y \in \mathbb{Z}_q^n} \omega^{f(y)+x.y} = \sum_{y \in \mathbb{Z}_q^n} F(y)\omega^{x.y}. \tag{3}$$

Here $+$ and $x.y$ are addition and inner product over $\mathbb{Z}_q$. Note that the matrix of this transform is no longer a Sylvester type Hadamard matrix as in the previous case, but a generalized (complex) Hadamard matrix. A q-ary function f is called *bent*, iff $|\widehat{F}(x)| = q^{n/2}$ for all $x \in \mathbb{Z}_q^n$. Notice that again it does not follow from the definition that q-ary bent functions do not exist if n is odd. P. V. Kumar, R. A. Scholtz and L. R. Welch [10] studied q-ary bent functions in 1985. They proved that such functions exist for any even n and $q \neq 2 (\mathrm{mod}\, 4)$. Later S. V. Agievich [1] proposed an approach to describe regular q-ary bent functions in terms of bent rectangles. If $q = 4$ we call f a **quaternary function**. Here we study such functions only. Note that in 1994 A. S. Ambrosimov [2] studied another type of q-ary bent functions defined over the finite field.

A bent function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called **regular** if each of its Walsh–Hadamard coefficients can be expressed as $\widehat{F}(z) = q^{n/2}\omega^{h(z)}$ for every $z \in \mathbb{Z}_q^n$ and some q-ary function h. From [10] it is known that for quaternary ($q = 4$) case all bent functions are regular.

3. Connections between Boolean and generalized Boolean bent functions

Let $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_4$ be a generalized Boolean function. Represent it as $f(x, y) = a(x, y) + 2b(x, y)$, for any $x, y \in \mathbb{Z}_2^n$ where $a, b : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ are Boolean functions.

In this section we study connection between properties of bentness of generalized Boolean and Boolean functions.

Here and further by $\widehat{A \cdot B}$ we mean WHT of $a \oplus b$. It is natural, since $A \cdot B = (-1)^{a \oplus b}$. In this section and in what follows, by $x.y$ we mean the inner product over $\mathbb{Z}_4$: $x.y = x_1 y_1 + ... + x_n y_n \bmod 4$.

Lemma 1. *Between Walsh–Hadamard transforms of f, $a \oplus b$, b, there is the relation*

$$|\widehat{F}(x,y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y)\right).$$

Proof. Let us study the Walsh–Hadamard transform of f. According to (2) we have

$$\widehat{F}(x,y) = \sum_{x',y'} (-1)^{\langle x,x'\rangle \oplus \langle y,y'\rangle \oplus b(x',y')}\, i^{\,a(x',y')}.$$

Applying the formula $i^s = \frac{1+(-1)^s}{2} + \frac{1-(-1)^s}{2} i$ for $s = a(x',y')$ we get

$$\widehat{F}(x,y) = \frac{1}{2}\left(\widehat{B}(x,y) + \widehat{A \cdot B}(x,y)\right) + \frac{i}{2}\left(\widehat{B}(x,y) - \widehat{A \cdot B}(x,y)\right).$$

From this we directly get what we need. □

Note that Lemma 1 holds for any (not only even) number of variables of the function f.

Theorem 1. *The following statements are equivalent*:
(i) *the generalized Boolean function f is bent in $2n$ variables*;
(ii) *the Boolean functions in $2n$ variables b and $a \oplus b$ are both bent.*

Proof. By Lemma 1 we have $|\widehat{F}(x,y)|^2 = \frac{1}{2}\left(\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y)\right)$. If $a \oplus b$ and b are bent functions then $|\widehat{F}(x,y)|^2 = \frac{1}{2}(2^{2n} + 2^{2n}) = 2^{2n}$ and f is a bent function. Conversely, if f is bent, then it holds $\widehat{B}^2(x,y) + \widehat{A \cdot B}^2(x,y) = 2^{2n+1}$. Since WHT coefficients of a Boolean function are integer, this equality has the unique solution $\widehat{B}^2(x,y) = \widehat{A \cdot B}^2(x,y) = 2^{2n}$ (see [9] for details). So, functions $a \oplus b$ and b are bent. □

Note that there are some intersections between Lemma 1, the part (i)→(ii) of Theorem 1 and results of the last version of [24].

4. Connections between Boolean and quaternary bent functions

Define a quaternary function $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ as $g(x + 2y) = a(x,y) + 2b(x,y)$, for any $x, y \in \mathbb{Z}_2^n$ where $a, b : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ are Boolean functions. In this section we study connection between properties of bentness of quaternary and Boolean functions.

4.1. Preliminaries and necessary statements.

In this section we present several facts that will be instrumental in what follows.

Lemma 2. *Let $x, y \in \mathbb{Z}_2^n$. If $x.y \neq \langle x,y\rangle$ then $x.y = \langle x,y\rangle + 2$.*

Proof. There are four possible values for $x.y$: $0, 1, 2$ and 3. For $x.y = 0$ or 1, it is obvious that $x.y = \langle x, y\rangle$. For two remaning cases, we have

$$x.y = 2 \to \langle x, y\rangle = 0 \to x.y = \langle x, y\rangle + 2,$$

$$x.y = 3 \to \langle x, y\rangle = 1 \to x.y = \langle x, y\rangle + 2.$$

□

The following fact is well known for Boolean functions.

Lemma 3. *Let f be a linear Boolean function in n variables. Then there are two possible values of WHT coefficients of f: 0 and 2^n.*

Proof. Any linear Boolean function f in n variables can be represented for some $a \in \mathbb{Z}_2^n$ as $f(x) = \langle a, x\rangle$. Therefore, by (1)

$$\widehat{F}(x) = \sum_{y\in\mathbb{Z}_2^n} (-1)^{\langle a,y\rangle \oplus \langle x,y\rangle} = \sum_{y\in\mathbb{Z}_2^n} (-1)^{\langle a\oplus x,y\rangle}.$$

Using the well-known fact that

$$\sum_{b\in\mathbb{Z}_2^n} (-1)^{\langle b,c\rangle} = \begin{cases} 2^n, & if\ c = 0, \\ 0, & otherwise. \end{cases}$$

the result follows. □

Proposition 1. *(see, for instance, [32]) All quadratic Boolean functions in two variables, i.e. $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ such that $f(x, y) = xy \oplus c$, where $x, y, c \in \mathbb{Z}_2$, are bent.*

Proposition 2. *(Rothaus, [23]) The degree of Boolean bent function f in $n \geq 4$ variables is not more than $n/2$.*

Proposition 3. *(Rothaus, [23]) Let $x \in \mathbb{Z}_2^r$ and $y \in \mathbb{Z}_2^k$, where $r, k \geqslant 2$ and even. A Boolean function $f(x, y) = f_1(x) \oplus f_2(y)$ is a bent function in $r + k$ variables if and only if the functions f_1 and f_2 are bent functions in r and k variables respectively.*

Proposition 4. *(Singh et al., [25]) Let $x \in \mathbb{Z}_4^r$ and $y \in \mathbb{Z}_4^k$ for $r, k \geqslant 1$. A quaternary function $g(x, y) = g_1(x) \oplus g_2(y)$ is a bent function in $r + k$ variables if and only if functions g_1 and g_2 are quaternary bent functions in r and k variables respectively.*

Note that results of Propositions 3 and 4 can be easily extended to sums with more than two functions.

4.2. **Quaternary bent functions in small number of variables.** Here we present results on connections between notions of quaternary bent functions in one and two variables and Boolean bent functions. Using computer search we obtain the following facts.

Statement 1. *For every quaternary function $g(x + 2y) = a(x, y) + 2b(x, y)$ in one variable with $x, y \in \mathbb{Z}_2$, it is true that g is a quaternary bent function if and only if b is bent and a does not depend on y, i.e. $a(x, y)$ is equal to 0, 1, x or $x \oplus 1$. Moreover, if g is bent then b and $a \oplus b$ are bent functions too.*

		Number of quaternary bent functions	
Cases for b and $a \oplus b$	Types of a in the case	For each type of a	Total in the case
b and $a \oplus b$ are nonlinear (not bent)	a is bent	49152	147456
	a is linear (not constant)	3072	
	a is nonliear (not bent)	95232	
b and $a \oplus b$ are bent	a is bent	16384	53248
	a is linear (not constant)	2304	
	a is constant	768	
	a is nonlinear (not bent)	33792	

Table 1. Classification of functions b and $a \oplus b$ for quaternary bent functions in 2 variables.

Computer search shows that the number of quaternary bent functions in one variable is equal to 32.

There are 200704 quaternary bent functions in 2 variables. Among them there are 98304 fuctions such that none of Boolean functions a, b and $a \oplus b$ is bent but for 3072 of them a is a linear Boolean function. There are 36864 quaternary bent functions such that b and $a \oplus b$ are bent functions, while for 33792 of them a is a nonlinear function, and for 2304 and 768 functions a is a linear function or constant respectively. The number of quaternary bent functions in 2 variables with each of a, b and $a \oplus b$ being bent is equal to 16384. For the remaining 49152 quaternary functions, a is bent and b and $a \oplus b$ are nonlinear Boolean functions. We summarize the data described above in Table 1.

For functions in three and more variables an exhaustive search is unfeasible (there are 2^{128} quaternary functions in three variables).

4.3. **Possibilities for bentness.** From Statement 1, we know that for $n = 1$ if g is quaternary bent then b and $a \oplus b$ are bent functions too. In the previous section we showed that it does not hold for quaternary functions in 2 variables. Let us prove that it does not hold for arbitrary $n \geqslant 2$.

Proposition 5. *For every $n \geqslant 2$ there exists a quaternary bent function $g(x+2y) = a(x,y) + 2b(x,y)$ in n variables, with b and $a \oplus b$ being not bent in $2n$ variables.*

Proof. In what follows, '+' denotes the addition over $\mathbb{Z}_4$ excepting summation of indices. Any quaternary function g in n variables can be uniquely represented as follows: $g(x_1+2x_{n+1}, ..., x_n+2x_{2n}) = a(x_1, ..., x_{2n})+2b(x_1, ..., x_{2n})$. Let $b(x_1, .., x_{2n}) = \bigoplus_{i=3}^{n} x_i x_{i+n} \oplus x_1 x_{n+2} \oplus x_2 x_{n+1} \oplus x_1 x_2 x_{n+1}$,$a(x_1, .., x_{2n}) = x_1 x_{n+1}$. One can see that b can be divided into sum of $n-2$ Boolean functions in two variables and one Boolean function in four variables like this:

$$b(x_1, ..., x_{2n}) = b_1(x_1, x_2, x_{n+1}, x_{n+2}) \oplus b_2(x_3, x_{n+3}) \oplus ... \oplus b_{n-1}(x_n, x_{2n}),$$

$$b_1(x_1, x_2, x_{n+1}, x_{n+2}) = x_1 x_{n+2} \oplus x_2 x_{n+1} \oplus x_1 x_2 x_{n+1},$$

$$b_i(x_{i+1}, x_{n+i+1}) = x_{i+1} x_{n+i+1}, \quad i = 2, ..., n-1.$$

From Proposition 3, we know that b is bent if and only if all b_i are bent. According to Proposition 2, we get that function b_1 in four variables is not bent since its degree is equal to three. Therefore, b is not bent.

It is easy to check that

$$2b(x_1, .., x_{2n}) = (2x_3 x_{n+3} + ... + 2x_n x_{2n}) + 2x_1 x_{n+2} + 2x_2 x_{n+1} + 2x_1 x_2 x_{n+1}.$$

Moreover, g can be divided into sum of $n-2$ quaternary functions in one variable and one quaternary function in two variables

$$g(x_1+2x_{n+1},...,x_n+2x_{2n}) = g_1(x_1+2x_{n+1},x_2+2x_{n+2})+$$
$$+g_2(x_3+2x_{n+3})+...+g_{n-1}(x_n+2x_{2n}),$$

where

$$g_1(x_1+2x_{n+1},x_2+2x_{n+2}) = x_1x_{n+1}+2x_1x_{n+2}+2x_2x_{n+1}+2x_1x_2x_{n+1},$$
$$g_i(x_{i+1}+2x_{n+i+1}) = 2x_{i+1}x_{n+i+1},\ \ i=2,...,n-1.$$

From Proposition 1, we know that all $x_{i+1}x_{n+i+1}$ are bent, $i=2,...,n$. Therefore, according to Statement 1 functions g_i are quaternary bent functions, $i=2,...,n-1$. It was checked that the quaternary function g_1 is also bent according to the definition: its WHT coefficients are the following:

$x\in\mathbb{Z}_4^2$	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
$\widehat{G_1(x)}$	4	$4i$	4	4	4	$4i$	-4	4	4	$-4i$	4	-4	4	$-4i$	-4	-4

From Proposition 4, g is a quaternary bent function if and only if all g_i are quaternary bent functions, $i=1,...,n-1$. This completes the proof. □

The next result shows that bentness of a quaternary function does not follow from bentness of Boolean functions in general.

Proposition 6. *For every $n\geqslant 1$, there exists a quaternary function $g(x+2y)=a(x,y)+2b(x,y)$ in n variables that is not bent, while b and $a\oplus b$ are Boolean bent functions in $2n$ variables.*

Proof. Any quaternary function g in n variables can be uniquely represented as $g(x_1+2x_{n+1},...,x_n+2x_{2n}) = a(x_1,...,x_{2n})+2b(x_1,...,x_{2n})$.

Let $b(x_1,..,x_{2n}) = \bigoplus_{i=1}^{n} x_ix_{i+n}$,$a(x_1,..,x_{2n}) = x_{n+1}$. It is easy to check that $2b(x_1,..,x_{2n}) = 2x_1x_{n+1}+...+2x_nx_{2n}$. Note that g can be divided into sum of n quaternary functions in one variable:

$$g(x_1+2x_{n+1},...,x_n+2x_{2n}) = g_1(x_1+2x_{n+1})+...+g_n(x_n+2x_{2n}),$$

where

$$g_i(x_i+2x_{n+i}) = a_i(x_i,x_{n+i})+2b_i(x_i,x_{n+i}),\ i=1,..,n,$$
$$b_i(x_i,x_{n+i}) = x_ix_{n+i},\ i=1,..,n,$$
$$a_1(x_1,x_{n+1}) = x_{n+1},$$
$$a_i(x_i,x_{n+i}) = 0,\ i=2,..,n.$$

From Proposition 4, we know that g is a quaternary bent function if and only if all g_i are quaternary bent functions, $i=1,...,n$. From Statement 1 and by the choice of a and b, we get that g_1 is not quaternary bent. This completes the proof. □

From Propositions 5 and 6, we conclude that there is no direct link between notions of Boolean and quaternary bent functions. Additionally, Proposition 5 shows that if b and $a\oplus b$ are not bent, it does not imply that g is not bent. According to Proposition 6, it is also true that if g is not bent, it does not imply that b and $a\oplus b$ are not bent.

From the previous section, we can see that for quaternary bent functions in one and two variables, a Boolean function b is bent if and only if $a \oplus b$ is also bent. Whether this statement is true for arbitrary n remains an open problem.

4.4. **Nonlinearity of component Boolean functions.** Let $g(x+2y) = a(x,y) + 2b(x,y)$ be a quaternary function in n variabes, where $x, y \in \mathbb{Z}_2^n$ and a, b are Boolean functions in $2n$ variables.

Let us represent WHT coefficients of quaternary functions in terms of the coefficients of Boolean functions b and $a \oplus b$ as we did for generalized functions in section 4. Here by $\widehat{A \cdot B}$ we mean the WHT of $a \oplus b$.

Lemma 4. *Between the WHT coefficients of g, $a \oplus b$, b there is the relation*

$$\widehat{G}(x+2y) = \frac{1}{2}\left(\widehat{B}(x \oplus y, x) + \widehat{A \cdot B}(y,x) - 2c_{\,b}(x \oplus y, x) - 2c_{\,a\oplus b}(y,x)\right) +$$
$$+\frac{i}{2}\left(\widehat{B}(y,x) - \widehat{A \cdot B}(x \oplus y, x) - 2c_{\,b}(y,x) + 2c_{\,a\oplus b}(x \oplus y, x)\right),$$

with

$$c_{\,f}(u,x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables, $V_x = \{\, x' \in \mathbb{Z}_2^n \,|\, \langle x, x' \rangle \neq x.x' \,\}$, and $u \in \mathbb{Z}_2^n$.

Proof. Let us study the Walsh–Hadamard transform of g. By (3) we know that

$$\widehat{G}(x+2y) = \sum_{x',y'} i^{\,(x+2y).(x'+2y') + a(x',y') + 2b(x',y')}.$$

From the fact that for any $x'', x''' \in \mathbb{Z}_2^n$ it holds $2\langle x'', x''' \rangle \bmod 4 = 2x''.x'''$ and Lemma 2, we have

$$(x+2y).(x'+2y') = \begin{cases} \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle, & if \quad x.x' = \langle x,x' \rangle, \\ \langle x,x' \rangle + 2\langle x,y' \rangle + 2\langle y,x' \rangle + 2, & if \quad x.x' \neq \langle x,x' \rangle. \end{cases}$$

Let $U_x = \{\, x' \in \mathbb{Z}_2^n \,|\, x.x' = \langle x,x' \rangle \,\}$ and $V_x = \{\, x' \in \mathbb{Z}_2^n \,|\, x.x' \neq \langle x,x' \rangle \,\}$. Therefore, we get $U_x \cap V_x = \varnothing$ and $U_x \cup V_x = \mathbb{Z}_2^n$. Note that $|U_x| \neq |V_x|$ in general. Then

$$\widehat{G}(x+2y) = \sum_{x \in U_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\,\langle x,x' \rangle + a(x',y')} -$$
$$- \sum_{x' \in V_x, y'} (-1)^{\langle x,y' \rangle \oplus \langle y,x' \rangle \oplus b(x',y')} i^{\,\langle x,x' \rangle + a(x',y')}.$$

Here we use the standard maps $\beta, \gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ defined as

$$\beta : 0,1 \to 0 \text{ and } \beta : 2,3 \to 1;$$
$$\gamma : 0,2 \to 0 \text{ and } \gamma : 1,3 \to 1.$$

For any $t \in \mathbb{Z}_4$ it holds

$$i^t = (-1)^{\beta(t)} \left(\frac{1 + (-1)^{\gamma(t)}}{2} + \frac{1 - (-1)^{\gamma(t)}}{2} i \right).$$

Using this formula for $t = x.x' + a(x',y')$ and the fact that $\gamma(\langle x,x' \rangle + a(x',y')) = \langle x,x' \rangle \oplus a(x',y')$ we get

$$\widehat{G}(x+2y) = \frac{1}{2}\left(S_1 + S_2 - S_3 - S_4\right) + \frac{i}{2}\left(S_1 - S_2 - S_3 + S_4\right),$$

where

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_2 &= \sum_{x'\in U_x,y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_3 &= \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))},\\
S_4 &= \sum_{x'\in V_x,y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus\beta(\langle x,x'\rangle+a(x',y'))}.
\end{aligned}$$

Let $M_{\delta,x} = \{\ x' \in \mathbb{Z}_2^n \mid \langle x,x'\rangle = \delta\ \}$ for $\delta \in \mathbb{Z}_2$. Note that $M_{0,x} \cup M_{1,x} = \mathbb{Z}_2^n$ and $|M_{0,x}| = |M_{1,x}| = 2^{n-1}$. Let us divide every sum S_1, S_2, S_3 and S_4 into two sums $\sum_{x'\in M_{0,x},y'}$ and $\sum_{x'\in M_{1,x},y'}$. Note that $\beta(a(x',y')+\langle x,x'\rangle)$ is equal to 0 or $a(x',y')$ for $x' \in M_{0,x}$ and $x' \in M_{1,x}$ respectively. Thus, we have

$$\begin{aligned}
S_1 &= \sum_{x'\in U_x\cap M_{0,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} +\\
&+ \sum_{x'\in U_x\cap M_{1,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_2 &= \sum_{x'\in U_x\cap M_{0,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in U_x\cap M_{1,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle\oplus a(x',y')},\\
S_3 &= \sum_{x'\in V_x\cap M_{0,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} +\\
&+ \sum_{x'\in V_x\cap M_{1,x},y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus a(x',y')},\\
S_4 &= \sum_{x'\in V_x\cap M_{0,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in V_x\cap M_{1,x},y'} (-1)^{a(x',y')\oplus b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle a(x',y')}.
\end{aligned}$$

After grouping terms we obtain

$$\begin{aligned}
&S_1 + S_2 - S_3 - S_4 =\\
&= \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} +\\
&+ \sum_{x'\in U_x,y'} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle} -\\
&- \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle} -\\
&- \sum_{x'\in V_x,y'} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle}.
\end{aligned}$$

Then

$$\begin{aligned} S_1 - S_2 - S_3 + S_4 = \\ = \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} - \\ - \sum_{x' \in U_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle} - \\ - \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle} + \\ + \sum_{x' \in V_x, y'} (-1)^{b(x',y') \oplus a(x',y') \oplus \langle x,y' \rangle \oplus \langle y,x' \rangle \oplus \langle x,x' \rangle}. \end{aligned}$$

Since

$$c_f(u,x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables and $u \in \mathbb{Z}_2^n$, then one can see that

$$S_1 + S_2 - S_3 - S_4 =$$

$$= (\widehat{B}(x \oplus y, x) - c_b(x \oplus y, x)) + (\widehat{A \cdot B}(y,x) - c_{a \oplus b}(y,x)) - c_b(x \oplus y, x) - c_{a \oplus b}(y,x)$$

and

$$S_1 - S_2 - S_3 + S_4 =$$

$$= (\widehat{B}(y,x) - c_b(y,x)) - (\widehat{A \cdot B}(x \oplus y, x) - c_{a \oplus b}(x \oplus y, x)) - c_b(y,x) + c_{a \oplus b}(x \oplus y, x).$$

After rearranging, the result follows. □

We can see that WHT coefficients of a quaternary function g do not directly depend on WHT coefficients of Boolean functions b and $a \oplus b$. This result will be used in proof of the next theorem and also in section 8.2.

Theorem 2. *Let $g(x + 2y) = a(x,y) + 2b(x,y)$ be a quaternary bent function with $x, y \in \mathbb{Z}_2^n$ and a, b be Boolean functions in $2n$ variables. Then b and $a \oplus b$ are nonaffine functions for any $n \geqslant 1$.*

Proof. According to Lemma 3 there are two possible values of WHT coefficients of a linear Boolean function in $2n$ variables: 0 and 2^{2n}.

From Lemma 4, we get

$$\widehat{G}(2y) = \frac{1}{2}(\widehat{B}(y,0) + \widehat{A \cdot B}(y,0)) + \frac{i}{2}(\widehat{B}(y,0) - \widehat{A \cdot B}(y,0)), \text{ where } y \in \mathbb{Z}_2^n.$$

Note that V_x is empty for $x = \mathbf{0}$, hence $c_b(x \oplus y, x), c_b(y,x), c_{a \oplus b}(x \oplus y, x)$ and $c_{a \oplus b}(y,x)$ are zero too.

As it was mentioned in section 2 all quaternary bent functions are regular. It means that there is only real or imaginary part of $\widehat{G}(2y)$. Thus, we get that there are two possible cases

$$\begin{cases} (\widehat{B}(y,0) + \widehat{A \cdot B}(y,0))^2 = 0, \\ (\widehat{B}(y,0) - \widehat{A \cdot B}(y,0))^2 = 4 \cdot 4^n. \end{cases}$$

or

$$\begin{cases} (\widehat{B}(y,0) + \widehat{A \cdot B}(y,0))^2 = 4 \cdot 4^n, \\ (\widehat{B}(y,0) - \widehat{A \cdot B}(y,0))^2 = 0. \end{cases}$$

From the first system we get

$$\begin{cases} \widehat{B}(y,0) = -\widehat{A \cdot B}(y,0), \\ (2 \cdot \widehat{B}(y,0))^2 = 4 \cdot \widehat{B}(y,0)^2 = 4 \cdot 4^n. \end{cases}$$

Hence,

$$\widehat{B}(y,0) = -\widehat{A \cdot B}(y,0) = \pm 2^n.$$

By solving the second system one can get

$$\widehat{B}(y,0) = \widehat{A \cdot B}(y,0) = \pm 2^n.$$

Therefore, b and $a \oplus b$ are nonaffine functions. □

5. Connections between quaternary and generalized Boolean bent functions

Let $g(x+2y) = f(x,y)$, where $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$, $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ and $x, y \in \mathbb{Z}_2^n$.

In this section, we show that the approach of Kumar et al. and that of Schmidt are not equivalent.

Proposition 7. *For every $n \geqslant 1$, there exists a generalized bent function $f(x,y)$ in $2n$ variables such that a quaternary function $g(x+2y)$ in n variables defined as $g(x+2y) = f(x,y)$ for all $x, y \in \mathbb{Z}_2^n$ is not bent.*

Proof. From Proposition 6, there exists a quaternary function $g(x+2y) = a(x,y) + 2b(x,y)$ which is not bent, while b and $a \oplus b$ are both bent. Now from Theorem 1 we know that if b and $a \oplus b$ are both bent then $f(x,y)$ is a generalized bent function. □

Proposition 8. *For every $n \geqslant 2$, there exists a quaternary bent function $g(x+2y)$ in n variables such that a generalized function $f(x,y)$ in $2n$ variables defined as $f(x,y) = g(x+2y)$ for all $x, y \in \mathbb{Z}_2^n$ is not bent.*

Proof. From Proposition 5 there exists a quaternary bent function $g(x+2y) = a(x,y) + 2b(x,y)$ in $n \geqslant 1$ variables such that both b and $a \oplus b$ are not bent. From Theorem 1 we know that a generalized function $f(x,y)$ is bent iff b and $a \oplus b$ are both bent. Hence, $f(x,y)$ is not bent. □

6. Gray images of bent functions

Let f be a generalized Boolean function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$. Write $f = a + 2b$ with a, b Boolean functions in n variables. Its *Gray map* $\phi(f)$ is the Boolean function in variables (x,z) with $x \in \mathbb{Z}_2^n$ and $z \in \mathbb{Z}_2$ defined as $a(x)z + b(x)$. The proof of the next result is implicit in the proof of [24, Th. 3.5] and is omitted.

Proposition 9. *For the WHTs of functions f and $\phi(f)$ it holds*

$$\widehat{\Phi(f)}(u,v) = 2\Re(i^{-v}\widehat{F}(u)) = \widehat{B}(u) + (-1)^v \widehat{A \cdot B}(u), \text{ where } u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2. \quad (4)$$

Here $\Re$ denotes real part of a complex number. As far as the left side of equation (4) is a WHT coefficient of a Boolean function, we easily get

Corollary 1. *For any generalized Boolean function f in n variables it holds*

$$\max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\Re(i^{-v}\widehat{F}(u))| \geqslant 2^{(n-1)/2}.$$

Corollary 2. *If f is generalized bent in n variables then $\phi(f)$ is either bent (n odd) or semi bent (n even).*

Proof. Write $\widehat{F}(u) = X + iY$ with X, Y integers. We know that $2^n = X^2 + Y^2$. We know that the solution to that diophantine equation in $X > 0$ and $X \geqslant Y \geqslant 0$ is unique, see e.g. [9]. The obvious solutions for n odd are $\{|X| = |Y| = 2^{(n-1)/2}\}$, $\{Y = 0,\ X = \pm 2^{n/2}\}$ and $\{Y = \pm 2^{n/2},\ X = 0\}$ for n even.

Thus, if n is odd it holds $\widehat{\Phi(f)}(u, v) = \pm 2^{(n+1)/2}$ for all u, v, and hence $\phi(f)$ is bent in $n + 1$ variables. If n is even we see that $\widehat{\Phi(f)}(u, v)$ equals 0 or $\pm 2^{(n+2)/2}$, so $\phi(f)$ is semi bent in $n + 1$ variables. □

There is a partial converse to Corollary 2. The proof is immediate.

Proposition 10. *Let n be odd. If $\phi(f)$ is a Boolean bent function in $n+1$ variables then f is a generalized Boolean bent function in n variables.*

Proof. Let $\widehat{F}(u) = X + iY$ with X, Y integers. We know that for all u, v it holds $\widehat{\Phi(f)}(u, v) = \pm 2^{(n+1)/2}$. Therefore, from Proposition 9

$$\widehat{\Phi(f)}(u, 0) = 2\Re(\widehat{F}(u)) = 2X = \pm 2^{(n+1)/2},$$

and

$$\widehat{\Phi(f)}(u, 1) = 2\Re(i^{-1}\widehat{F}(u)) = 2Y = \pm 2^{(n+1)/2}.$$

Hence, $|\widehat{F}(u)|^2 = X^2 + Y^2 = 2^n$. □

This fact has also been obtained in the last variant of [24].

7. Notions of nonlinearity

It is well-known that Boolean bent functions are characterized by their maximal distance to the first order Reed–Muller code. This fact is generalized in this section to their quaternary analogues.

7.1. **Generalized Boolean functions.** Let $RM(r, k)$ be the Reed–Muller code of length 2^k and of order r, see [12]. Define, for $0 \leqslant r \leqslant m$ the quaternary code $ZRM(r, m) = \phi^{-1}(RM(r, m + 1))$. This code is spanned by vectors of values for functions of degree at most $r - 1$ together with twice functions of degree at most r, see [7] for details. We introduce the **nonlinearity** $N(f)$ of a generalized bent Boolean function f in n variables as

$$N(f) := 2^n - \frac{1}{2} \max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\widehat{\Phi(f)}(u, v)|. \tag{5}$$

The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$, respectively, and the Lee weight $wt_L(a)$ of $a \in \mathbb{Z}_4^N$ is the rational sum of the Lee weights of its components. This weight function defines a distance $d_L(f, g) = wt(f - g)$ between two generalized functions on $\mathbb{Z}_4^N$ called the Lee distance. Analogously, let $d_H(\cdot, \cdot)$ be the Hamming distance on $\mathbb{Z}_2^{2N}$. According to Corollary 1 we have

Proposition 11. *For any generalized Boolean function f in n variables, it is true $N(f) \leqslant 2^n - 2^{(n-1)/2}$.*

Proposition 12. *With the above notation, for any generalized Boolean function in n variables f we have*

$$N(f) = d_L(f, ZRM(1, n)) = d_H(\Phi(f), RM(1, n + 1)).$$

Proof. Let x, y be arbitrary vectors of $\mathbb{Z}_4^N$. Denote by i^x the vector $(i^{x_1}, \ldots, i^{x_N})$. Recall first the well-known identities

$$d_E^2(i^x, i^y) = 2d_L(x, y) = 2(N - \Re(\sum_{j=1}^{N} i^{x_j - y_j})),$$

where d_E stands for the Euclidean distance. Observe that $ZRM(1, n)$ is spanned by the all-one vector, along with twice the binary linear functions, and that $\widehat{F}(u) = \sum_{y \in \mathbb{Z}_2^n} i^{f(y)+2u.y}$. The second equality holds by the isometry property of the Gray map [7]. □

Hence, using Propositions 11 and 12 we can reformulate one partial case from Corollary 2 and Proposition 10 as follows.

Corollary 3. *Let n be odd. A generalized function f is bent if and only if $N(f)$ attains the maximal possible value $2^n - 2^{(n-1)/2}$.*

The case of even n is more complicated. We have

Corollary 4. *Let n be even. If a function f is bent then $N(f) = 2^n - 2^{n/2}$.*

Proof. By Corollary 2 the Boolean function $\phi(f)$ is semi bent in $n+1$ variables. Hence the maximum value of $|\widehat{\Phi(f)}(u, v)|$ is equal to $2^{(n+2)/2}$. Then by Proposition 9 and definition (5) we get $N(f) = 2^n - 2^{n/2}$. □

The converse statement is not right in general as far as from the equality

$$\max_{u \in \mathbb{Z}_2^n, v \in \mathbb{Z}_2} |\widehat{\Phi(f)}(u, v)| = 2^{(n+2)/2}$$

it does not follow that $|\widehat{F}(u)| = 2^{n/2}$ for any $u \in \mathbb{Z}_2^n$. Actually, it is not clear what is the maximum possible value of $N(f)$ if n is even. To know it one should find the value of covering radius of the code $RM(1, n+1)$ when $n+1$ is odd. But it is a hard old problem without analogy to the easy case of even $n+1$.

7.2. **Quaternary functions.** Let g be a quaternary function in n variables. In this case, an immediate reduction to the preceding subsection (namely, passing from g to f in the notations of section 5) yields the definition

$$N(g) := 2^{2n} - \frac{1}{2} \max_{u, v \in \mathbb{Z}_2^n, w \in \mathbb{Z}_2} |\widehat{\Phi(g)}(u, v, w)|.$$

The following analogue of Proposition 12 is immediate.

Proposition 13. *For any quaternary function g in n variables we have*

$$N(g) = d_L(g, ZRM(1, 2n)) = d_H(\phi(g), RM(1, 2n+1)).$$

In particular if g is bent then $N(g) = 2^{2n} - 2^n$. As it was mentioned above the maximal possible value of $N(g)$ is not known yet.

8. Examples of Constructions

Define algebraic normal form (ANF) of generalized Boolean function f in n variables as follows:

$$f(x_1, ..., x_n) = \sum_{k=1}^{n} \sum_{i_1,...,i_k} a_{i_1,...,i_k} x_{i_1} \cdots x_{i_k} + a_0,$$

where for each k indices $i_1, ..., i_k$ are pairwise distinct and sets $\{i_1, ..., i_k\}$ are exactly all different nonempty subsets of the set $\{1, ..., n\}$; coefficients $a_{i_1,...,i_k}, a_0$ take values from $\mathbb{Z}_4$. The number of variables in the longest item of its ANF is called the degree of a generalized function and is denoted by $\deg(f)$. For computing degrees we require the following lemma.

Lemma 5. *For a generalized Boolean function f the degree of $\phi(f)$ is at most the degree of f.*

Proof. Follows by definition of the $ZRM(r, m)$ code by its generators [7]. □

8.1. **Generalized Boolean bent functions.** In [24, Th. 4.3] figures a natural generalization of the classical Maiorana–McFarland construction.

Proposition 14. *(Schmidt,* [24]*) The generalized Boolean function f in $2n$ variables defined for x, y in $\mathbb{Z}_2^n$ by $f(x, y) = 2x.\pi(y) + \tau(y)$, with τ an arbitrary generalized Boolean function in n variables and π an arbitrary permutation of $\mathbb{Z}_2^n$ is bent.*

By Corollary 2 the Gray map of this function is a binary Boolean semi bent function in $2n + 1$ variables. By Lemma 5 its degree is $\max(2, \deg(\tau))$.

It is well-known that the binary Kerdock code contains bent functions. We assume the reader has some familiarity with Galois rings as can be gained in, e.g. [7].

For completeness, the next result from [24] we present with the proof.

Proposition 15. *(Schmidt,* [24]*) Let $n \geqslant 3$ denote an integer. Let R_n denote the Galois ring of characteristic 4 and size 4^n. Let R_n^x denote $R_n \setminus 2R_n$. Let T_n denote the Teichmuller set of R_n, and Tr the trace function of R_n. The generalized Boolean function in n variables defined for $x \in T_n$ by*

$$f(x) = \epsilon + Tr(sx)$$

for constants ϵ, s ranging in $\mathbb{Z}_4, R_n^x$ is bent. Its Gray image is either bent (n odd) or semi bent (n even).

Proof. The first assertion follows by [24, Construction 5.2] upon observing that $ZRM(1, n)$ is described by functions $f(x) = \epsilon + 2Tr(sx)$. The second assertion follows by Corollary 2. □

A monomial construction of a bent generalized Boolean function is presented in [24, Th. 5.3]. Intuitively it detects the generalized bent functions in the dual of the Goethals code.

Proposition 16. *(Schmidt,* [24]*) Keep the notation of Proposition 15. Let μ denote the "reduction mod 2"map from R_n to $\mathbb{F}_{2^n}$. The generalized Boolean function in n variables defined for $x \in T_n$ by $f(x) = \epsilon + Tr(sx + 2tx^3)$ for constants ϵ, s, t ranging*

in $\mathbb{Z}_4, R_n, T_n \setminus \{0\}$ *is bent if* $\mu(s) = 0$ *and the equation* $\mu(t)z^3 + 1 = 0$ *has no solutions in* $\mathbb{F}_{2^n}$, *or if* $\mu(s) \neq 0$ *and the equation*

$$z^3 + z + \frac{\mu(t)^2}{\mu(t)^6} = 0$$

has no solutions in $\mathbb{F}_{2^n}$.

By Corollary 2 the Gray map of this function is a binary Boolean function in $n+1$ variables which is semi bent if n is even or bent if n is odd. It is quadratic by Lemma 5.

In the original paper [27] it was mentioned that it would be interesting, for instance, to replace the exponent 3 in Proposition 16 by a Gold exponent $2^k + 1$. Then Li et al. [11] characterized the functions in n variables of the form $f(x) = Tr(ax + 2bx^{1+2^k})$ for odd $n/gcd(n/k)$.

8.2. **Quaternary bent functions.**

Proposition 17. *For every* n *a quaternary function*

$$g(x_1 + 2x_{n+1}, ..., x_n + 2x_{2n}) = c_1x_1 + ... + c_nx_n + 2(x_1x_{n+1} + ... + x_nx_{2n})$$

is a quaternary bent function with $c_i \in \mathbb{Z}_2$ *and* '$+$' *is addition over* $\mathbb{Z}_4$.

Proof. One can see that g can be divided into sum of n quaternary functions in one variable $g(x_1 + 2x_{n+1}, ..., x_n + 2x_{2n}) = g_1(x_1 + 2x_{1+n}) + ... + g_n(x_n + 2x_{2n})$,

$$g_i(x_i + 2x_{i+n}) = c_ix_i + 2x_ix_{i+n}.$$

From Proposition 1, we know that all x_ix_{i+n} are bent, $i = 1, ..., n$. From Statement 1 each of g_i is a quaternary bent function in one variable, therefore, from Proposition 4 g is also a quaternary bent function. □

Proposition 18. *Let* $g(x + 2y) = a(x, y) + 2b(x, y)$ *and* $g'(x + 2y) = a(x, y) + 2(a(x, y) \oplus b(x, y))$ *be quaternary functions with* $x, y \in \mathbb{Z}_2^n$ *and* a, b *be Boolean functions in* $2n$ *variables. Then* g *is bent if and only if* g' *is bent.*

Proof. Study the Walsh–Hadamard transform of g and g'. From Lemma 4, we have

$$\widehat{G}(x + 2y) = \frac{1}{2}\left(\widehat{B}(x \oplus y, x) + \widehat{A \cdot B}(y, x) - 2c_b(x \oplus y, x) - 2c_{a\oplus b}(y, x)\right) +$$

$$+\frac{i}{2}\left(\widehat{B}(y, x) - \widehat{A \cdot B}(x \oplus y, x) - 2c_b(y, x) + 2c_{a\oplus b}(x \oplus y, x)\right)$$

and

$$\widehat{G'}(x + 2(x \oplus y)) = \frac{1}{2}\left(\widehat{A \cdot B}(y, x) + \widehat{B}(x \oplus y, x) - 2c_{a\oplus b}(y, x) - 2c_b(x \oplus y, x)\right) +$$

$$+\frac{i}{2}\left(\widehat{A \cdot B}(x \oplus y, x) - \widehat{B}(y, x) + 2c_b(y, x) - 2c_{a\oplus b}(x \oplus y, x)\right),$$

with

$$c_f(u, x) = \sum_{x' \in V_x, y'} (-1)^{f(x',y') \oplus \langle (u,x),(x',y') \rangle},$$

where f is a Boolean function in $2n$ variables, $V_x = \{\, x' \mid \langle x, x' \rangle \neq x.x' \,\}$, and $u \in \mathbb{Z}_2^n$.

Let $\Re$ and $\Im$ be real and imaginary parts of a complex number respectively. Then $\Re(\widehat{G}(x + 2y)) = \Re(\widehat{G'}(x + 2(x \oplus y)))$, $\Im(\widehat{G}(x + 2y)) = -\Im(\widehat{G'}(x + 2(x \oplus y)))$.

As it was mentioned in section 2 all quaternary bent functions are regular. Therefore, each of Walsh–Hadamard coefficients of a quaternary bent function has only real or imaginary part. Hence, if g is bent then $|\widehat{G'}(x+2(x\oplus y))| = |\widehat{G}(x+2y)| = 4^{n/2}$. By the same way we can prove that if g' is bent then $|\widehat{G}(x+2y)| = |\widehat{G'}(x+2(x\oplus y))| = 4^{n/2}$. This completes the proof. □

9. Conclusion and open problems

In the present work we have shown how generalizations of the notion of bent functions involving the ring $\mathbb{Z}_4$ could produce, by Gray map or by base 2 expansion, bent Boolean functions in the classical sense. We have proved that the approach of Kumar et al. and that of Schmidt are not equivalent at least in quaternary case. Schmidt's definition fits better $\mathbb{Z}_4$-cyclic codes constructions. Conversely classical binary bent functions (but perhaps not semi bent functions) can yield generalized bent functions by inverse Gray map. These results motivate to explore further algebraic constructions of generalized bent functions. Although the results show that there is no direct connection between quaternary and Boolean bent functions it is still might be possible to connect these notions if we will ask for additional conditions. For instance, it would be interesting to solve the problem that we mentioned at the end of section 4.3. It is also possible that notions of q-ary and Boolean bent functions are more connected for $q > 4$.

Acknowledgment

Authors wish to thank Sihem Mesnager and Alexander Kutsenko for helpful discussions. The work of the first and the second authors was supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

References

[1] S.V. Agievich, *Bent rectangles*, in Preneel, Bart (ed.) et al., *Boolean functions in cryptology and information security. Selected papers based on the presentations at the NATO-Russia Advanced Study Institute on Boolean functions in cryptology and information security, Zvenigorod, Russia, September 8–18, 2007*, 2008, 3–22. Zbl 1167.94004

[2] A.S. Ambrosimov, *Properties of bent functions of q-valued logic over finite fields*, Discrete Math. Appl., **4**:4 (1994), 341–350. Zbl 0816.03010

[3] T. Baignères, P. Junod, S. Vaudenay, *How far can we go beyond linear cryptanalysis?,* in Lee, Pil Joong, *Advances in Cryptology — ASIACRYPT 2004*, Lecture Notes in Computer Science, **3329**, 432-450, 2004, Zbl 1094.94025

[4] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory, **59**:5 (2013), 3233–3236. Zbl 1364.94799

[5] S. Gangopadhyay, C. Riera, P. Stănică, *Gowers U2 norm of Boolean functions and their generalizations*, Workshop on Cryptography and Coding, Rennes, France 2019.

[6] L. Granboulan, É. Levieil, G. Piret, *Pseudorandom permutation families over abelian groups*, in Robshaw, Matthew (ed.), *Fast Software Encryption — FSE 2006*, Graz, Austria. March 15–17, 2006, Lecture Notes in Computer Science, **4047**, 2006, 57–77. Zbl 1234.94043

[7] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inf. Theory, **40**:2 (1994), 301–319. Zbl 0811.94039

[8] S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image*, IEEE Trans. Inf. Theory, **64**:7 (2018), 5432–5440. Zbl 1401.94263

[9] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, GTM, **84**, Springer, New York etc., 1990. Zbl 0712.11001

[10] P.V. Kumar, R.A. Scholtz, L.R. Welch, *Generalized bent functions and their properties*, J. Comb. Theory, Ser. A, **40**:1 (1985), 90–107. Zbl 0585.94016

[11] N. Li, X. Tang, T. Helleseth, *New constructions of quadratic bent functions in polynomial form*, IEEE Trans. Inf. Theory, **60**:9 (2014), 5760–5767. Zbl 1360.94479

[12] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes. Parts I, II*, North-Holland, Amsterdam etc., 1977. Zbl 0369.94008

[13] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, in Duquesne, Sylvain (ed.) et al., *Arithmetic of finite fields, WAIFI 2016*, Lect. Notes Comput. Sci., **10064**, 160–173, 2016. Zbl 1409.11135

[14] T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inf. Theory, **63**:12 (2017), 7804–7812. Zbl 1390.94951

[15] M. Matsui, A. Yamagishi, *A new method for known plaintext attack of FEAL cipher*, in Rueppel, Rainer A. (ed.), *Advances in cryptology — EUROCRYPT'92, Balatonfured, Hungary. May 24–28, 1992, Proc.*, Lect. Notes Comput. Sci. **658**, 81–91, Springer, Berlin, 1993. Zbl 0787.94019

[16] M. Matsui, *Linear cryptanalysis method for DES cipher*, in Helleseth, Tor (ed.), *Advances in Cryptology — EUROCRYPT'93 (Lofthus, Norway. May 23–27, 1993), Proc.*, Lect. Notes Comput. Sci., **765**, 386–397, Springer, Berlin, 1994. Zbl 0951.94519

[17] M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard.* in Desmedt, Yvo G. (ed.), *Advances in Cryptology — CRYPTO'94 (Santa Barbara, California, USA, August 21–25, 1994), Proc.*, Lect. Notes Comput. Sci., **839**, 1–11, Springer, Berlin, 1994. Zbl 0939.94551

[18] W. Meidl, *A secondary construction of bent functions, octal gbent functions and their duals*, Math. Comput. Simul., **143** (2018), 57–64. Zbl 07316125

[19] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.

[20] M.G. Parker, H. Raddum, *Z_4-linear cryptanalysis.* NESSIE Internal Report, 27/06/2002: NES/DOC/UIB/WP5/018/1.

[21] M.G. Parker, *Generalised S-Box Nonlinearity.* NESSIE Public Document, 11.02.03: NES/DOC/UIB/WP5/020/A.

[22] C. Riera, P. Stănică, S. Gangopadhyay, *Generalized bent Boolean functions and strongly regular Cayley graphs*, Discrete Appl. Math., **283** (2020), 367–374. Zbl 1442.05250

[23] O. Rothaus, *On bent functions*, J. Comb. Theory, Ser. A., **20**:3 (1976), 300–305. Zbl 0336.12012

[24] K-U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA.* IEEE Trans. Inf. Theory, **55**:4 (2009), 1824–1832. Zbl 1367.94344

[25] D. Singh, M. Bhaintwal, B.K. Singh, *Some results on q-ary bent functions*, Int. J. Comput. Math., **90**:9 (2013), 1761–1773. Zbl 1314.94094

[26] L. Sok, M. Shi, P. Solé, *Classification and construction of quaternary self-dual bent functions*, Cryptogr. Commun., **10**:2 (2018), 277–289. Zbl 1412.94257

[27] P. Solé, N. Tokareva, *Connections between quaternary and binary bent functions*, Cryptology ePrint Archive, Report, **2009/544**, (2009). available at `http://eprint.iacr.org/`.

[28] P. Solé, N. Tokareva, *On quaternary and binary bent functions*, Prikl. Diskr. Mat., Suppl., **1** 2009, 16–18. Zbl 07300366

[29] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptography, **69**:1 (2013), 77–94. Zbl 1322.94094

[30] C. Tang, C. Xiang, Y. Qi, K. Feng, *Complete characterization of generalized bent and 2^k-bent Boolean functions*, IEEE Trans. Inf. Theory, **63**:7 (2017), 4668–4674. Zbl 1370.94614

[31] N.N. Tokareva, *Generalizations of bent functions. A survey*, Discretn. Anal. Isslid. Oper., **17**:1 (2010), 34–64. Zbl 1249.94057

[32] N. Tokareva, *Bent functions: results and applications to cryptography*, Acad. Press. Elsevier, Burlington, 2015.

[33] Y. Zheng, X.-M. Zhang, *On plateaued functions*, IEEE Trans. Inf. Theory, **47**:3 (2001), 1215–1223. Zbl 0999.94026

Natalia Nikolaevna Tokareva
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: tokareva@math.nsc.ru

Alexander Sergeyevich Shaporenko
Novosibirsk State University,
2, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: alexandr.shaporenko@gmail.com

Patrick Solé
I2M, CNRS, Aix-Marseille University, Centrale Marseille,
Marseilles, France
Email address: patrick.sole@telecom-paristech.fr

S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 18, №2, стр. A. 4–A. 29 (2021) УДК 519.7
DOI 10.33048/semi.2021.18.061 MSC 06E30, 11T71, 14G50

THE SEVENTH INTERNATIONAL OLYMPIAD IN CRYPTOGRAPHY: PROBLEMS AND SOLUTIONS

A.A. GORODILOVA, N.N. TOKAREVA, S.V. AGIEVICH, C. CARLET, V.A. IDRISOVA, K.V. KALGIN, D.N. KOLEGOV, A.V. KUTSENKO, N. MOUHA, M.A. PUDOVKINA, A.N. UDOVENKO

Abstract. The International Olympiad in Cryptography NSUCRYPTO is the unique olympiad containing scientific mathematical problems for professionals, school and university students from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography. In 2020, it was held for the seventh time. Prizes and diplomas were awarded to 84 participants in the first round and 49 teams in the second round from 32 countries. In this paper, problems and their solutions of NSUCRYPTO'2020 are presented. We consider problems related to attacks on ciphers and hash functions, protocols, permutations, primality tests, etc. We discuss several open problems on JPEG encoding, Miller — Rabin primality test, special bases in the vector space, AES-GCM. The problem of a modified Miller — Rabin primality test was solved during the Olympiad. The problem for finding special bases was partially solved.

Gorodilova, A.A., Tokareva, N.N., Agievich, S.V., Carlet, C., Idrisova, V.A., Kalgin, K.V., Kolegov, D.N., Kutsenko, A.V., Mouha, N., Pudovkina, M.A., Udovenko, A.N., The Seventh International Olympiad in Cryptography: problems and solutions.

The work of the second and sixth authors was supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. The work of the first, fifth and eighth authors was supported by Russian Foundation for Basic Research (project no. 20-31-70043).

Received May, 31, 2021, published July, 21, 2021.

Keywords: cryptography, hash functions, CPA game, orthomorphisms, bases, primality tests, AES, steganography, Olympiad, NSUCRYPTO.

1. Introduction

NSUCRYPTO (Non-Stop University Crypto) is the International Olympiad in Cryptography that was held for the seventh time in 2020. The Olympiad program committee includes specialists from Belgium, France, the Netherlands, the USA, Norway, India, Luxembourg, Belarus', Kazakhstan, and Russia. Interest in the Olympiad around the world becomes more significant. In 2020, there were 775 participants from more than 50 countries; and 14 countries took part for the first time. Summing the results, 84 participants in the first round and 49 teams in the second round from 32 countries were awarded with prizes and honorable diplomas. The list of the winners can be found at the official website of the Olympiad [9]. Fig. 1 illustrates the Olympiad logo and winners.

Let us shortly formulate the format of the Olympiad. When registering to the Olympiad, each participant chooses his/her category: "school students" (for junior researchers: pupils and high school students), "university students" (for participants who are currently studying at universities) and "professionals" (for participants who have already completed education or just want to be in the restriction-free category). The Olympiad consists of two independent the Internet rounds. The first round is individual (duration 4 hours 30 minutes, two sections: A is for "school students", B is for "university students" and "professionals"). The second round is a team one (duration 1 week, common to all participants).

A distinctive feature of the Olympiad is that some unsolved problems at the intersection of mathematics and cryptography are offered to the participants as well as problems with known solutions. During the Olympiad, one of such open problems, "Miller — Rabin revisited" (see section 3.5), was solved completely. For another one problem, "Bases" (see section 3.13), a partial solution was proposed. All the open problems stated during the Olympiad history can be found here [10]. What is more important for us that some researchers were trying to find solutions after the Olympiad was over. In the recent paper [7], a complete solution was found for the problem "Orthogonal arrays" (2018). A partial solution for the problem "A secret sharing" (2014) was proposed in [3]. We invite everybody who has ideas on how to solve the problems to send your solutions to us!

We start with problem structure of the Olympiad in section 2. Then we present formulations of all the problems stated during the Olympiad and give their detailed solutions in section 3. Mathematical problems and their solutions of the previous International Olympiads in cryptography NSUCRYPTO from 2014 to 2019 can be found in [2], [1], [8], [4], [5], and [6] respectively.

2. Problem structure of the Olympiad

There were 14 problems stated during the Olympiad, some of them were included in both rounds (Tables 1, 2). Section A of the first round consisted of six problems, whereas the section B contained seven problems. The second round was composed of ten problems. Four problems included unsolved questions (awarded special prizes from the Program Committee).

Fig. 1. NSUCRYPTO logo and winners

Таблица 1. **Problems of the first round**

N	Problem title	Max score
1	2020	4
2	POLY	4
3	A secret house	4
4	RGB	4
5	Miller — Rabin revisited (Q1)	4
6	Mysterious event	4

Section A

N	Problem title	Max score
1	2020	4
2	A secret house	4
3	Miller — Rabin revisited	4 + add.
4	RGB	4
5	Mysterious event	4
6	CPA game	6
7	Collisions (Q1)	4

Section B

Таблица 2. **Problems of the second round**

N	Problem title	Maximum score
1	POLY	4
2	Stairs-Box	7
3	Hidden RSA	6
4	Orthomorphisms	12
5	JPEG Encoding	Unlimited (open problem)
6	Miller — Rabin revisited	4 + add. sc. for open pr.
7	CPA game	6
8	Collisions	8
9	Bases	Unlimited (open problem)
10	AES-GCM	10 + add. sc. for open pr.

3. Problems and their solutions

In this section, we formulate all the problems of NSUCRYPTO'2020 and present their detailed solutions paying attention to solutions proposed by the participants.

3.1. **Problem "2020".**

3.1.1. *Formulation.* A cipher machine `WINSTON` can transform a binary sequence in the following way. A sequence S is given, a cipher machine can add to S or remove from S any subsequence of the form 11, 101, 1001, $10\ldots01$. Also, it can add to S or remove from S any number of zeros.

When special agent Smith entered the room there were two identical `WINSTON` machines. He was curious to encrypt number 2020 and he tried to encrypt the number in it's binary form. The first cipher machine returned the binary form of number 1984, the second one returned the binary form of number 2021. Smith understood that one of the machines is broken. How did he know that?

3.1.2. *Solution.* By removing subsequences of the form 10...01 and 0...0, the parity of ones in the binary representation cannot be changed. The given numbers have the following binary representations:

$$2020 \to 11111100100 \to 7 \text{ ones},$$
$$2021 \to 11111100101 \to 8 \text{ ones},$$
$$1984 \to 11111000000 \to 5 \text{ ones}.$$

Hence, it is impossible to obtain 2021 from the input 2020. Hence, the second machine must be broken.

3.2. Problem "POLY".

3.2.1. *Formulation.* During a job interview, Bob was proposed to think up a small cryptosystem that operates with integers. Bob invented and implemented a complex algorithm `POLY` that can be represented mathematically as a polynomial. Namely, if x is a plaintext, then ciphertext y is equal to $p(x)$, where p is a polynomial with integer coefficients.

Bob's employer decided to test it. At first, he encrypted the number 20 and obtained the number 7. Secondly, he encrypted the number 15 and obtained the number 5. After that he said to Bob that there was a mistake in the implementation of the algorithm and did not hire him. What was wrong?

3.2.2. *Solution.* Let $p(x) = c_0 + c_1 x + \ldots + c_n x^n$. Then $p(a) - p(b) = c_1(a-b) + \ldots + c_n(a^n - b^n)$, where a, b are some integers. Since $(a^k - b^k)$ is divided by $(a-b)$, we have that $p(a) - p(b)$ is divided by $(a-b)$. By condition, we have $p(20) = 7$ and $p(15) = 5$, but 5 does not divide 2. Hence, there is a mistake in the implementation. Almost all the participants solved the problem.

3.3. Problem "A secret house".

3.3.1. *Formulation.* You can see a secret house in Fig. 2(a). Looking on it, could you understand what should be shown inside the frame left blank in Fig. 2(b)?

(a) (b)

FIG. 2. A secret house

3.3.2. *Solution.* Looking on the house, one can see that the number in a window is equal to "5 minus the number of shadows" inside the window. Hence, we can guess that the task is to calculate $3^{40231} \pmod 5$. Since $3^4 = 1 \pmod 5$, then $3^{40231} \pmod 5 = 3^{4 \cdot 10057 + 3} \pmod 5 = 3^3 \mod 5 = 4$. Hence, there should be one shadow inside the frame.

3.4. Problem "RGB".

3.4.1. *Formulation.* Victor is studying the Moctod search server. Inside its software, he found two integer variables a and b that change their values when special search queries "`RED`", "`GREEN`" and "`BLUE`" are processed. More precisely, the pair (a, b) is changed to $(a+18b, 18a-b)$ when processing the query "`RED`", to $(17a+6b, -6a+17b)$ when processing "`GREEN`", and to $(-10a-15b, 15a-10b)$ when processing "`BLUE`". When any of a or b reaches a multiple of 324, it resets to 0. Whenever $(a, b) = (0, 0)$, the server crashes.

On the server startup, the variables (a, b) are set to $(20, 20)$. Prove that the server will never crash with these initial values, regardless of the search queries processed.

3.4.2. *Solution.* The number 325 is the first natural number that can be written as sums of squares in three different ways (up to permutation of terms):

$$325 = 1^2 + 18^2 = 6^2 + 17^2 = 10^2 + 15^2.$$

Keeping this in mind, if (A, B) is the result of changing (a, b) with some query, then

$$A^2 + B^2 = 325(a^2 + b^2) \equiv a^2 + b^2 \pmod{324}.$$

Thus, the number $(a^2 + b^2) \bmod 324$ does not change for any chain of queries (in order words, it is an invariant). Since initially $(20^2 + 20^2) \bmod 324 = 152 \neq 0$, the server will never crash.

3.5. **Problem "Miller — Rabin revisited".**

3.5.1. *Formulation.* Bob decided to improve the famous Miller — Rabin primality test and invented his test given in Algorithm 1. The odd number n being tested is represented in the form $n - 1 = 2^k 3^\ell m$, where m is not divisible by 2 or 3.

Algorithm 1 Bob's primality test

1. Take a random $a \in \{2, \ldots, n-2\}$.
2. Put $a \leftarrow a^m \bmod n$. If $a = 1$, return "`PROBABLY PRIME`".
3. For $i = 0, 1, \ldots, \ell - 1$ do the following steps:
   (a) $b \leftarrow a^2 \bmod n$;
   (b) if $a + b + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (c) $a \leftarrow ab \bmod n$.
4. For $i = 0, 1, \ldots, k - 1$ repeat:
   (a) if $a + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (b) $a \leftarrow a^2 \bmod n$.
5. Return "`COMPOSITE`".

Q1 Prove that Algorithm 1 does not fail, that is, not return "`COMPOSITE`", for a prime n.

Q2 **Bonus problem (extra scores, a special prize!)**

A composite integer n may be classified as "`PROBABLY PRIME`" by a mistake. It is known that for the usual Miller — Rabin test the error probability is less than 1/4. Can this estimation be improved when we are switching to Algorithm 1?

Remark. The expression $a \leftarrow a^m \bmod n$ means that a takes a new value that is equal to the remainder of dividing a^m by n.

3.5.2. *Solution.* Let us prove that Algorithm 1 does not fail (**Q1**).

If n is prime, then by Fermat's Little Theorem n divides

$$a^{n-1}-1 = a^{2^k 3^l m}-1 = (a^{2^{k-1}3^l m}-1)(a^{2^{k-1}3^l m}+1) = \ldots =$$
$$= (a^{3^l m}-1)\prod_{i=0}^{k-1}\left(a^{2^i 3^l m}+1\right) = ((a^{3^{l-1}m})^3-1)\prod_{i=0}^{k-1}\left(a^{2^i 3^l m}+1\right) =$$
$$= (a^{3^{l-1}m}-1)((a^{3^{l-1}m})^2+a^{3^{l-1}m}+1)\prod_{i=0}^{k-1}\left(a^{2^i 3^l m}+1\right) = \ldots =$$
$$= (a^m-1)\prod_{j=0}^{l-1}\left((a^{3^j m})^2+a^{3^j m}+1\right)\prod_{i=0}^{k-1}\left(a^{2^i 3^l m}+1\right).$$

A prime number n must divide one of the parentheses in the last expression. The required statement follows from this.

The answer for the question **Q2** is "the estimation is not improved". Let us prove this. In the original Miller — Rabin test, instead of steps 2 and 3, the following step is performed:

23. $a \leftarrow a^{3^l m} \bmod n$. If $a = 1$, return "`PROBABLY PRIME`".

In other words, the following congruence relation is checked:

$$a^{3^l m} \equiv 1 \pmod{n}. \tag{1}$$

If (1) is satisfied, then $A = a^{3^{l-1}m}$ is the cube root of 1 modulo n:

$$A^3-1 \equiv 0 \pmod{n} \quad \Leftrightarrow \quad (A-1)(A^2+A+1) \equiv 0 \pmod{n}.$$

In this case, either $A \equiv 1 \pmod{n}$, i.e.

$$a^{3^{l-1}m} \equiv 1 \pmod{n}, \tag{2}$$

or $A^2 + A \equiv -1 \pmod{n}$. Both cases are analyzed in Bob's test. In the first case, the congruence relation (2) is analyzed in the same way as (1).

Thus, the answer "`PROBABLY PRIME`" in Miller — Rabin test is returned if and only if the same answer is returned in Bob's test. Bob's test has an advantage over Miller — Rabin test. It is more efficient since the correctness of (1) can be obtained earlier.

The question **Q2** was correctly solved by 10 participants and teams. They are Artur Puzio (Poland), Leo Boitel (France), Geng Wang (China), Gabor P. Nagy (Hungary), the team of Albert Smith, Ethan Tan, Guowen Zhang (Australia), the team of Mircea-Costin Preoteasa, Gabriel Tulba-Lecu, Ioan Dragomir (Romania), the team of Sergey Bystrevskii, Maksim Starodubov, Evgeny Mikhalchuk (Russia), the team of Mohammad Akbarizadeh, Reza Kaboli, Sajjad Bagheri (Iran), the team of Jeremy Jean, Hugues Randriam (France), Irina Slonkina (Russia).

3.6. **Problem "Mysterious event".**

3.6.1. *Formulation.* Mr. Bob is the editor in-chief of a well known magazine. He has many interests and activities in addition to work: meetings with bright people of politics and art, dancing, fishing, and even stenography and linguistics.

Every week, the magazine publishes a hard Sudoku on the last page. Mr. Bob likes this game too! So, it is a pleasure for him to personally analyze all solutions

from the readers. He sits down in his office with a cup of coffee and looks through all the PNG-files with photos of solutions.

But suddenly Mr. Bob disappeared. The last solution he could see on his monitor was that in Fig. 3 (here is a **link** to it, if you are interested in).

FIG. 3. Sudoku

But what happened? Where is Mr. Bob?

3.6.2. *Solution.* As Mr. Bob likes stenography and the format of the given file is png, one can try to find message hidden in Fig. 3 using steganography tools, for example [14]. It reveals the message "They know that you are a spy! Get back to the center right now." So, Mr.Bob is in the center.

3.7. **Problem "CPA game".**

3.7.1. *Formulation.* Suppose we have a system for the encryption of binary messages. The system has the following characteristics:

- Every message is divided into blocks of length n that are called plaintexts (it is supposed that the length of messages is divisible by n).
- The system employs a block cipher with the encryption function E in cipher block chaining (CBC) mode (see the picture below). A block, an initialization vector IV and a key lengths are equal to n. The result of encryption of the message is a concatenation of IV and the ciphertexts of all plaintexts it consists of.
- The IV for the first message is chosen randomly by using a secure pseudo-random number generator. The last ciphertext block of the i-th message is used as the IV for the $(i+1)$-st message.

Let Alice be an honest user of the system. Victor, an adversary, convinced her to play **chosen–plaintext attack game** (CPA game) with him.

The game is the following:

1. Alice selects a key $k \in \{0,1\}^n$ and chooses a bit $b \in \{0,1\}$.
2. Victor submits a sequence of q queries to Alice. For $i = 1, 2, \ldots, q$ repeat
   (a) Victor chooses a pair of messages, $m_{i,0}, m_{i,1}$ of the same length.
   (b) Alice encrypts $m_{i,b}$ with the key k and gets c_i (that is the sequence of corresponding IV and ciphertexts). She sends c_i to Victor.
3. Victor outputs a bit $b^* \in \{0,1\}$.

Let W be the event that Victor guesses the bit, that is $b^* = b$. We define Victors's advantage with respect to E as $\mathrm{CPAadv} := |\Pr[\mathrm{W}] - 1/2|$. Victor wins the game if he can build an efficient algorithm such that CPAadv is not negligible.

Task. Construct an efficient probabilistic polynomial-time (PPT) algorithm that wins the CPA game against this implementation with an advantage close to 1/2.

3.7.2. *Solution.* We describe two deterministic algorithms that win the given CPA game with two queries in Algorithms 2, 3. Let $\mathbf{0}$ and $\mathbf{1}$ denote all zeros and all ones vectors from the space $\mathbb{F}_2^n$.

Algorithm 2 The first deterministic algorithm

q1: (a) Victor chooses a pair of messages $m_{1,0} = m_{1,1} = \mathbf{0}$ and sends them to Alice;
(b) Alice sends $c_1 = (IV, E_k(IV))$ to Victor;
q2: (a) Victor chooses a pair of messages $m_{2,0} = IV \oplus E_k(IV)$, $m_{2,1} = IV \oplus E_k(IV) \oplus \mathbf{1}$ and sends them to Alice;
(b) Alice sends $c_2 = (E_k(IV), C)$ to Victor. Depending on the value of b, the ciphertext C is equal to $E_k(IV)$ if $b = 0$, and it holds $C = E_k(IV \oplus \mathbf{1})$ if $b = 1$.

Finally, Victor outputs $b^* = 0$ if $C = E_k(IV)$ and $b^* = 1$ otherwise.

Algorithm 3 The second deterministic algorithm

q1: (a) Victor chooses a pair of messages $m_{1,0} = \mathbf{0}$, $m_{1,1} = \mathbf{1}$ and sends them to Alice;
(b) Alice sends $c_1 = (IV, C)$ to Victor, where the ciphertext C is equal to $E_k(IV)$ if $b = 0$, and it holds $C = E_k(IV \oplus \mathbf{1})$ if $b = 1$;
q2: (a) Victor chooses a pair of messages $m_{2,0} = m_{2,1} = IV \oplus C$ and sends them to Alice;
(b) Alice sends $c_2 = (E_k(IV), E_k(IV))$ to Victor.

Finally, Victor outputs $b^* = 0$ if $C = E_k(IV)$ and $b^* = 1$ otherwise.

There were several solutions from the participants that proposed the approaches described above, as well as many 3-queries deterministic and probabilistic algorithms.

3.8. **Problem "Stairs-Box".**

3.8.1. *Formulation.* Nicole was climbing stairs and has found a box containing a curious permutation on the set of elements $\{0, 1, \ldots, 63\}$:

$$S = [\ 13,18,20,55,23,24,34,\ 1,62,49,11,40,36,59,61,30,\\ 33,46,56,27,41,52,14,45,\ 0,29,39,\ 4,\ 8,\ 7,17,50,\\ 2,54,12,47,35,44,58,25,10,\ 5,19,48,43,31,37,\ 6,\\ 21,26,32,\ 3,15,16,22,53,38,57,63,28,60,51,\ 9,42\ ]$$

So, the element 0 it maps to 13, the element 1 to 18, etc.

Nicole understands that it is possible to consider such a permutation as a vectorial Boolean function $S : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ if every number between 0 and 63 one replaces with a binary vector of length 6. For instance, $S(000010) = (010100)$, since S maps 2 to 20. She knows that S can be given in terms of coordinate functions as $S(x) = (s_1(x), \ldots, s_6(x))$, and each Boolean function s_i can be represented in the algebraic normal form using binary operations XOR and AND in the following way:

$s_i(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I \big(\prod_{i \in I} x_i \big)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \dots, 6\}$ and $a_I \in \mathbb{F}_2$.

A label on the box said that the function S can be represented as a composition of three maps in the following way:

$$S = A \circ X \circ B,$$

where $A, B : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ are **linear maps** and X is a function with a **short arithmetic expression modulo** 64. Nicole knows that a linear map over $\mathbb{F}_2^6$ can be defined by multiplication with a 6×6 matrix over $\mathbb{F}_2$. But she wonders what is supposed by "a short arithmetic expression modulo 64"? Probably, Nicole also should consider maps as classical modular operations such as addition, substraction, multiplication modulo 64?..

Help Nicole to find the secret function X and the respective maps A, B!

3.8.2. *Solution.* Arithmetic operations modulo 2^6 can be reduced modulo smaller powers of 2. Most importantly, the output modulo 2 depends only on the input modulo 2 (1 bit), the output modulo 2^i depends only on the input modulo 2^i (i input bits, $1 \leqslant i \leqslant 6$).

It follows that there must exist linear combinations of outputs of S with algebraic degrees less or equal to each of 1, 2, 3, 4, 5, 5 ("staircase"). And indeed, such combinations do exist for the given S-box S. While there is some freedom left in choosing such combinations, the number of possibilities is reasonably small. Any such choice identifies a candidate for the linear map A. The same idea can be applied to S^{-1} to obtain candidates for B. Using the fact that i least significant bits of the output of X must depend only on i least significant bits of the input of X, correct candidates for A, B can be recovered in a sequential bit-by-bit manner.

There exist 8 solutions, any of which was accepted as a correct answer:

$$X : \mathbb{Z}_{64} \to \mathbb{Z}_{64},\ X(x) \in \{x+1,\ x+17,\ x+33,\ x+49,\\ 33x+1,\ 33x+17,\ 33x+33,\ 33x+49\}.$$

In total, 15 teams managed to solve this problem completely and 12 teams got only partial progress. Many teams guessed the linear shape of the polynomial of X and used creative ways to verify their guess. Teams of Gongyu Shi, Xinzhou Wang, Yu-hang Jii (China) and Weidan Ji, Wenwen Xia, Zhang Hongyi (China) used the Walsh spectrum exploiting its invariance under composition of the function with linear maps and further recovered A, B efficiently by matching the rows/columns of the Linear Approximation Tables (LAT) of S and X. The team of Gyumin Roh, Hyunsik Jeong, Mincheol Son (South Korea) developed similar method but using Difference Distribution Table (DDT) instead of the LAT. Hieu Nguyen Duy (Vietnam) used more direct approach to reconstructing A, B row-by-row/column-by-column with the constraint of the partial solution X modulo 2^i having the form linear polynomial $x \mapsto ax + b$.

3.9. **Problem "Hidden RSA".**

3.9.1. *Formulation.* Bob has learned about the public-key cryptography and now anyone can send a secret message to him. The message is encoded by a nonnegative integer x which has at most 70 digits in the decimal representation. To send a

message for Bob, one has to enter it on his webpage [11]. After the message is entered, it is immediately encrypted using RSA. The encryption result is

$$\texttt{Encr}(x) = x^e \bmod n,$$

where n is a modulus (product of two distinct odd primes p and q) and e is a public exponent (coprime with $p-1$ and $q-1$). Bob is afraid of hackers and does not disclose either n or e (even though this contradicts the usual usage of the RSA cryptosystem).

Victor has intercepted the encrypted message

$$y = 715118966813248334583613928851843449333331598308638786001892120737775821781 73,$$

which Alice has sent to Bob.

Help Victor to decrypt y. You can enter any allowed message x on the Bob's website [11] and receive in response the corresponding ciphertext $\texttt{Encr}(x)$.

3.9.2. *Solution.* Victor takes advantage of the fact that RSA typically uses a small open exponent e. Victor views small candidate exponents $\hat{e} = 3, 5, \ldots$, searching for the correct one among them and at the same time determining n.

Viktor processes $\hat{e}$ as follows. First, he checks the condition $2^{\hat{e}} \geqslant \texttt{Encr}(2)$. If the condition is not satisfied, then $\hat{e}$ is rejected. Second, Victor defines $\hat{n} = 2^e - \texttt{Encr}(2)$. This is an estimate of the modulus n in the sense that if $\hat{e} = e$, then $\hat{n}$ is a multiple of n. Third, for several random x Victor refines the estimate:

$$\hat{n} \leftarrow \gcd(\hat{n}, (x^{\hat{e}} \bmod \hat{n}) - \texttt{Encr}(x)).$$

If $\hat{e} = e$, then the estimate $\hat{n}$ quickly converges to n. If $\hat{e} \neq e$, then $\hat{n}$ quickly converges to 1.

Using the method described above, Victor finds $e = 65537$ and

$$n = 76200708443433250012501342992033571586971760218934756930058661627867825188509.$$

The module n (256-bit) can be quickly factorized using programs like `msieve` or `cado-nfs`.

As a result, prime divisors can be found

$$p = 232086664036792751646261018215123451301,$$
$$q = 328328681700354546732404725320581286809.$$

Then the secret exponent is determined

$$d = e^{-1} \bmod (p-1)(q-1) =$$
$$= 58041460011714671214337771652949080061981291861469879231637604933853779098273$$

and the desired message

$$y^d \bmod n = 202010181600.$$

This is the NSUCRYPTO'2020 start time code (October 18, 2020, 16:00).

3.10. **Problem "Orthomorphisms".**

3.10.1. *Formulation.* A young cryptographer Bob wants to build a new block cipher based on the Lai-Massey scheme. The Lai-Massey scheme depends on a finite group G with the neutral element e and an orthomorphism of G. Bob decides to use a nonabelian group and chooses a dihedral group D_{2^m}, $m \geqslant 4$, generated by a, u with presentation

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u.$$

Let θ be a permutation of a finite group G. Then θ is called an **orthomorphism of** G if the mapping $\pi : \alpha \mapsto \alpha^{-1}\theta(\alpha)$ is a permutation of G.

Bob needs to construct an orthomorphism of D_{2^m}. He considers the set DM_m consisting of all mappings $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$ on D_{2^m} given by

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)} : a^i \mapsto \begin{cases} a^{r_1 i + c_1} & \text{if } i \in \{0,\dots,2^{m-2}-1\}, \\ a^{r_2 i + c_2}u & \text{if } i \in \{2^{m-2},\dots,2^{m-1}-1\}, \end{cases}$$

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)} : a^i u \mapsto \begin{cases} a^{q_1 i + b_1}u, & \text{if } i \in \{0,\dots,2^{m-2}-1\}, \\ a^{q_2 i + b_2}, & \text{if } i \in \{2^{m-2},\dots,2^{m-1}-1\}, \end{cases}$$

and depending on $b_i, c_i, r_i, q_i \in \{0,\dots,2^{m-1}-1\}$ for $i \in \{1,2\}$, where the operations addition and multiplication are over the residue ring $\mathbb{Z}_{2^{m-1}}$.

Q1 Let $m = 4$. Help Bob to describe all orthomorphisms of DM_m and find their number.

Q2 For each $m \geqslant 4$, help Bob to describe all orthomorphisms of DM_m, i. e. give necessary and sufficient conditions on b_i, c_i, r_i, q_i for $i \in \{1,2\}$ such that $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$ is an orthomorphism of D_{2^m}.

3.10.2. *Solution.* Let $Z_n = \{0, ..., n-1\}$ for a positive integer $n \geqslant 1$.

Theorem. Let $m \geqslant 4$. A mapping $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)} \in \mathrm{DM}_m$ is an orthomorphism if and only if $b_i, c_i, r_i, q_i \in Z_{2^{m-1}}$ for $i \in \{1,2\}$ satisfy one of the following conditions:

(1) If $r_1 \equiv r_2 \equiv 3 \pmod 4$, then $r_1 = q_2, r_2 = q_1$,
$c_1 = b_2, c_2 = b_1,\ c_1 + c_2 \equiv 1 \pmod 2$.

(2) If $r_1 \equiv r_2 \equiv 2 \pmod 4$, then $r_1 = q_1,\ r_2 = q_2$,
$q_1 - 1 \equiv b_1 + c_1 \pmod{2^{m-1}},\ q_2 - 1 \equiv b_2 + c_2 \pmod{2^{m-1}}$,
$b_1 + c_2 \equiv 1 \pmod 2,\ b_2 + c_1 \equiv 1 \pmod 2$.

Proof of Theorem. Let $\theta = \theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$. It is clear that θ is a permutation if and only if

$$\bigcup_{j=0}^{2^{m-2}-1} \{r_1 j + c_1\} \cap \bigcup_{j=2^{m-2}}^{2^{m-1}-1} \{q_2 j + b_2\} = \emptyset,$$
$$\bigcup_{j=2^{m-2}}^{2^{m-1}-1} \{r_2 j + c_2\} \cap \bigcup_{j=0}^{2^{m-2}-1} \{q_1 j + b_1\} = \emptyset,$$
$$\bigcup_{j=0}^{2^{m-2}-1} \{r_1 j + c_1\} \cup \bigcup_{j=2^{m-2}}^{2^{m-1}-1} \{q_2 j + b_2\} = Z_{2^{m-1}},$$
$$\bigcup_{j=2^{m-2}}^{2^{m-1}-1} \{r_2 j + c_2\} \cup \bigcup_{j=0}^{2^{m-2}-1} \{q_1 j + b_1\} = Z_{2^{m-1}},$$

where the operations addition and multiplication are over the residue ring $\mathbb{Z}_{2^{m-1}}$. They are equivalent to conditions

$$r_1 j_1 - q_2 j_2 \not\equiv q_2 2^{m-2} + b_2 - c_1 \pmod{2^{m-1}}, \tag{3a}$$
$$r_2 j_1 - q_1 j_2 \not\equiv q_1 2^{m-2} + b_1 - c_2 \pmod{2^{m-1}}, \tag{3b}$$
$$r_1 (j'_1 - j'_2) \not\equiv 0 \pmod{2^{m-1}}, \tag{3c}$$
$$r_2 (j'_1 - j'_2) \not\equiv 0 \pmod{2^{m-1}}, \tag{3d}$$
$$q_1 (j'_1 - j'_2) \not\equiv 0 \pmod{2^{m-1}}, \tag{3e}$$
$$q_2 (j'_1 - j'_2) \not\equiv 0 \pmod{2^{m-1}}, \tag{3f}$$

which hold for all $j_1, j_2 \in Z_{2^{m-2}}$ and all $j'_1, j'_2 \in Z_{2^{m-2}}$ with $j'_1 \neq j'_2$.

From conditions (3c) – (3f), it follows that

$$r_1 \not\equiv 0 \pmod 4,\ r_2 \not\equiv 0 \pmod 4,\ q_1 \not\equiv 0 \pmod 4,\ q_2 \not\equiv 0 \pmod 4. \tag{4}$$

Note that $\pi : \alpha \mapsto \alpha^{-1}\theta(\alpha)$ is given by

$$\pi : a^i \mapsto \begin{cases} a^{(r_1-1)i+c_1} & \text{if } i \in Z_{2^{m-2}}, \\ a^{(r_2-1)i+c_2}u & \text{if } i \in \{2^{m-2}, ..., 2^{m-1}-1\}, \end{cases}$$
$$\pi : a^i u \mapsto \begin{cases} a^{-(q_1-1)i-b_1} & \text{if } i \in Z_{2^{m-2}}, \\ a^{-(q_2-1)i-b_2}u & \text{if } i \in \{2^{m-2}, ..., 2^{m-1}-1\}, \end{cases}$$

where the operations addition, multiplication and subtraction are over $\mathbb{Z}_{2^{m-1}}$.

For each $i \in \{1, 2\}$, we suppose $\tilde{r}_i = r_i - 1 \bmod 2^{m-1}$, $\tilde{q}_i = 1 - q_i \bmod 2^{m-1}$, $\tilde{b}_i = 2^{m-1} - b_i$.

It is clear that π is a permutation if and only if

$$\bigcup_{j=0}^{2^{m-2}-1}\{\tilde{r}_1 j+c_1\}\cap\bigcup_{j=0}^{2^{m-2}-1}\left\{\tilde{q}_1 j+\tilde{b}_1\right\}=\emptyset,$$
$$\bigcup_{j=0}^{2^{m-2}-1}\{\tilde{r}_1 j+c_1\}\cup\bigcup_{j=0}^{2^{m-2}-1}\left\{\tilde{q}_1 j+\tilde{b}_1\right\}=Z_{2^{m-1}},$$
$$\bigcup_{j=2^{m-2}}^{2^{m-1}-1}\{\tilde{r}_2 j+c_2\}\cap\bigcup_{j=2^{m-2}}^{2^{m-1}-1}\left\{\tilde{q}_2 j+\tilde{b}_2\right\}=\emptyset,$$
$$\bigcup_{j=2^{m-2}}^{2^{m-1}-1}\{\tilde{r}_2 j+c_2\}\cup\bigcup_{j=2^{m-2}}^{2^{m-1}-1}\left\{\tilde{q}_2 j+\tilde{b}_2\right\}=Z_{2^{m-1}},$$

where the operations addition and multiplication are over the residue ring $\mathbb{Z}_{2^{m-1}}$.

They are equivalent to conditions

$$(r_1-1)j_1-(1-q_1)j_2\not\equiv -b_1-c_1 \pmod{2^{m-1}}, \tag{5a}$$
$$(r_2-1)j_1-(1-q_2)j_2\not\equiv -b_2-c_2 \pmod{2^{m-1}}, \tag{5b}$$
$$(r_1-1)(j_1'-j_2')\not\equiv 0 \pmod{2^{m-1}}, \tag{5c}$$
$$(r_2-1)(j_1'-j_2')\not\equiv 0 \pmod{2^{m-1}}, \tag{5d}$$
$$(q_1-1)(j_1'-j_2')\not\equiv 0 \pmod{2^{m-1}}, \tag{5e}$$
$$(q_2-1)(j_1'-j_2')\not\equiv 0 \pmod{2^{m-1}}, \tag{5f}$$

which hold for all $j_1,j_2\in Z_{2^{m-2}}$ and all $j_1',j_2'\in Z_{2^{m-2}}$ with $j_1'\neq j_2'$.

From conditions (5c) – (5f), it follows that

$$r_1\not\equiv 1 \pmod 4,\ r_2\not\equiv 1 \pmod 4,\ q_1\not\equiv 1 \pmod 4,\ q_2\not\equiv 1 \pmod 4. \tag{6}$$

Then we will use the following Lemma.

Lemma. Let $d\geqslant 4$, $R^{(d)}=\{r\in Z_{2^{d-1}}|r\equiv t \pmod 4,\ t\in\{1,2,3\}\}$, and $\bar{A}^{(d)}(h_1,h_2)=\left\{h_1j_1-h_2j_2 \mod 2^d\,|j_1,j_2\in Z_{2^{d-1}}\right\}$, $h_1,h_2\in R^{(d)}$.

Then

$$\bar{A}^{(d)}(h_1,h_2)=\begin{cases} Z_{2^d}\backslash\{2^{d-1}\} & \text{if } h_1=h_2,\ h_1\equiv h_2\equiv 1 \pmod 2,\\ Z_{2^d}\backslash\{h_2\} & \text{if } h_2=2^d-h_1,\ h_1\equiv h_2\equiv 1 \pmod 2,\\ Z_{2^d} & \text{if } h_2\notin\{h_1,2^d-h_1\},\ h_1\equiv h_2\equiv 1 \pmod 2,\\ \{2j|j\in Z_{2^{d-1}}\} & \text{if } h_1\equiv h_2\equiv 2 \pmod 4.\end{cases}$$

Proof of Lemma. For all $s,v_1,v_2\in Z_{2^{d-1}}$, we denote

$$s\bar{A}^{(d)}(v_1,v_2)=\left\{sb \bmod 2^d|b\in\bar{A}^{(d)}(v_1,v_2)\right\}.$$

Let t be an element from $\bar{A}^{(d)}(h_1,h_2)$. Therefore, $t=h_1i_1-h_2i_2 \bmod 2^d$ for some $i_1,i_2\in Z_{2^{d-1}}$.

Let $h_i\equiv 1 \pmod 2$ for some $i\in\{1,2\}$. Without loss of generality, we suppose $h_1\equiv 1 \pmod 2$. Then $h_1^{-1}t=i_1-h_1^{-1}h_2i_2 \mod 2^d$. So, $t'=i_1-h\cdot i_2 \mod 2^d$, where $t'=h_1^{-1}t$, $h=h_1^{-1}h_2$.

Obviously, $\bar{A}^{(d)}(h_1,h_2)=\bar{A}^{(d)}(h_1,h_1h)=h_1\bar{A}^{(d)}(1,h)$.

Now, we consider two cases.

Case 1. Let h be odd. For all $i_1, i_2 \in Z_{2^{d-1}}$, we have

$$i_1 - i_2 h \not\equiv \begin{cases} 2^{d-1} \pmod{2^d} & \text{if } h = 1, \\ 2^d - 1 \pmod{2^d} & \text{if } h = 2^d - 1. \end{cases}$$

If $h \in \{3, 5, 7, ..., 2^d - 3\}$, then

$$\begin{aligned} \bar{A}^{(d)}(1,h) = \bigcup_{j_2=0}^{2^{d-1}-1} \{j_1 - h \cdot j_2 \,|j_1 \in Z_{2^{d-1}}\} = \\ = Z_{2^{d-1}} \cup \left\{2^d - h, 2^d - h + 1, \ldots, 2^{d-1} - h - 1\right\} \cup \ldots \\ \cup \left\{2^d - 2h, 2^d - 2h + 1, ..., 2^{d-1} - 2h - 1\right\} \cup \\ \cup \left\{2h + 2^{d-1}, 2h + 1 + 2^{d-1}, ..., 2h - 1\right\} \cup \ldots \\ \cup \left\{h + 2^{d-1}, h + 1 + 2^{d-1}, ..., h - 1\right\} = Z_{2^d}, \end{aligned}$$

where the operations addition and subtraction are over $\mathbb{Z}_{2^d}$.

Hence,

$$\bar{A}^{(d)}(1,h) = \begin{cases} Z_{2^d} \backslash \{2^{d-1}\} & \text{if } h = 1, \\ Z_{2^d} \backslash \{2^d - 1\} & \text{if } h = 2^d - 1, \\ Z_{2^d} & \text{if } h \in \{3, 5, ..., 2^d - 3\}. \end{cases}$$

Case 2. Let h be even. From condition (4), it follows that $h_2 \equiv 2 \pmod 4$. Thus, $h \equiv 2 \pmod 4$. Hence,

$$\begin{aligned} \bar{A}^{(d)}(1,h) = \bigcup_{j_2=0}^{2^{d-1}-1} \{j_1 - h \cdot j_2 | j_1 \in Z_{2^{d-1}}\} = \\ = Z_{2^{d-1}} \cup \left\{2^d - h, 2^d - h + 1, ..., 2^{d-1} - h - 1 \right\} \cup \ldots \\ \cup \left\{2h, 2h + 1, ..., 2h + 2^{d-1} - 1\right\} \cup \\ \cup \left\{h + 2^{d-1}, h + 1 + 2^{d-1}, ..., 2^d - 2, 2^d - 1, 0, 1, ..., h - 1\right\} = Z_{2^d} \end{aligned}$$

where the operations addition and subtraction are over $\mathbb{Z}_{2^d}$.

So, if $h_i \equiv 1 \pmod 2$ for some $i \in \{1, 2\}$, then

$$\bar{A}^{(d)}(h_1,h_2) = \begin{cases} Z_{2^d} \backslash \{2^{d-1}\}, & \text{if } h_1 = h_2, \\ Z_{2^d} \backslash \{2^d - h_1\}, & \text{if } h_2 = 2^d - h_1, \\ Z_{2^d}, & \text{if } h_2 \notin \{h_1, 2^d - h_1\}. \end{cases}$$

Suppose $h_1 \equiv h_2 \equiv 2 \pmod 4$. Thus, $t = 2\tilde{t} \mod 2^d$, where $\tilde{t} = \tilde{h}_1 i_1 - \tilde{h}_2 i_2 \mod 2^{d-1}$, $\tilde{h}_1 = h_1/2$, $\tilde{h}_2 = h_2/2$. Note that $\tilde{h}_1 \equiv \tilde{h}_2 \equiv 1 \pmod 2$. From

$$Z_{2^{d-1}} = \left\{\tilde{h}_1 j_1 - \tilde{h}_2 j_2 \mod 2^{d-1} | j_1, j_2 \in Z_{2^{d-1}}\right\},$$

we get

$$\bar{A}^{(d)}(h_1,h_2) = \{2j | j \in Z_{2^{d-1}}\}.$$

End of Lemma proof.

From Lemma and conditions (3a), (3b), it follows that we must consider four cases:

- $r_1 \equiv r_2 \equiv 1 \pmod 2$,
- $r_1 \equiv 1 \pmod 2$, $r_2 \equiv 2 \pmod 4$,

- $r_1 \equiv 2 \pmod 4$, $r_2 \equiv 1 \pmod 2$,
- $r_1 \equiv r_2 \equiv 2 \pmod 4$.

If $r_1 \equiv r_2 \equiv 1 \pmod 2$, then

$$r_1 \in \{q_2, 2^{m-1} - q_2\},\ r_2 \in \{q_1, 2^{m-1} - q_1\}. \tag{7}$$

From condition (6), we get $r_1 \equiv r_2 \equiv 3 \pmod 4$.

For each $i, j \in \{1, 2\}$, $i \neq j$, if $r_j = 2^{m-1} - q_i$, then $q_i \equiv 1 \pmod 4$ that contradicts (6). Consequently, $r_j \neq 2^{m-1} - q_i$ for $q_i \equiv 1 \pmod 4$. From Lemma and conditions (5a), (5b), we get

$$b_1 + c_1 \equiv 1 \,(\mathrm{mod}\, 2),\ b_2 + c_2 \equiv 1 \,(\mathrm{mod}\, 2). \tag{8}$$

If $r_1 = q_2$, $r_2 = q_1$, then relations (3a), (3b) hold if and only if c_1, c_2, b_1, b_2 satisfy conditions

$$2^{m-2} \equiv q_2 2^{m-2} + b_2 - c_1 \pmod{2^{m-1}}, \quad 2^{m-2} \equiv q_1 2^{m-2} + b_1 - c_2 \pmod{2^{m-1}},$$

i.e.

$$c_1 = b_2, c_2 = b_1. \tag{9}$$

From (8) and (9), we get $c_1 + c_2 \equiv 1 \,(\mathrm{mod}\, 2)$.

Let $i, j \in \{1, 2\}$, $i \neq j$. If $r_j \equiv 1 \pmod 2$, $r_i \equiv 2 \pmod 4$, then

$$r_j \in \{q_i, 2^{m-1} - q_i\}, \quad r_i \equiv q_j \equiv 2 \pmod 4. \tag{10}$$

From (10), it follows that $r_j - 1 \not\equiv 1 - q_j \,(\mathrm{mod}\ 2)$. Therefore, from relations (5a), (5b) and Lemma, we get that condition (10) is impossible.

If $r_1 \equiv r_2 \equiv 2 \,(\mathrm{mod}\ 4)$, then $q_2 2^{m-2} + b_2 - c_1 \equiv 1 \,(\mathrm{mod}\ 2)$, $q_1 2^{m-2} + b_1 - c_2 \equiv 1 \pmod 2$. Thus,

$$b_1 + c_2 \equiv 1 \pmod 2,\ b_2 + c_1 \equiv 1 \pmod 2. \tag{11}$$

From Lemma and relations (5a), (5b), we have $r_i - 1 \in \{1 - q_i, 2^{m-1} - 1 + q_i\}$ for each $i \in \{1, 2\}$, where

$$-b_i - c_i = \begin{cases} 2^{m-2} & \text{if } r_i - 1 = 1 - q_i, \\ 1 - q_i & \text{if } r_i - 1 = 2^{m-1} - 1 + q_i, \end{cases}$$

where the operations addition and subtraction are over $\mathbb{Z}_{2^{m-1}}$.

If $r_i - 1 = 1 - q_i$ for some $j \in \{1, 2\}$, then $r_j = 2 - q_j$. Hence, $q_j \equiv 0 \pmod 4$ that contradicts (4). So, there is only one relation $r_i - 1 = 2^{m-1} - 1 + q_i \pmod{2^{m-1}}$ for each $i \in \{1, 2\}$. Thus,

$$r_i = q_i \text{ for each } i \in \{1, 2\}. \tag{12}$$

If $r_1 \equiv r_2 \equiv 2 \pmod 4$, then π is a permutation if and only if conditions (11), (12) hold and $q_i - 1 = b_i + c_i \bmod 2^{m-1}$ for each $i \in \{1, 2\}$.

End of Theorem proof.

Let OMD_m be the subset of MD_m consisting of all orthomorphisms. From Theorem, it follows that $|\mathrm{OMD}_4| = 2^8$.

Full and complete solutions for this problem were proposed by four team. The best one was given by the team of Jeremy Jean and Hugues Randriam (France).

3.11. **Problem "JPEG Encoding".**

3.11.1. *Formulation.* In order to decrease the readability of the exchanged messages, Alice and Bob decided to encode their messages using JPEG image compression. They write (or draw) their message in a graphics software, save it as a JPEG file and then encrypt the resulting file using some encryption algorithm.

Let us describe the details of the JPEG encoding. The matrix of pixels is first divided into 8×8 matrices, and then the matrices of the type presented below are obtained from them using discrete cosine transform (DCT) and quantization. An interesting characteristic of these matrices is that most of the non-zero data is concentrated in the upper left corner of the matrix, and most of the data in the lower right corner is 0. After that, the matrix is encoded using 0's and 1's.

One example of the matrix encoding is the following algorithm:

1. First, the zigzag rule is used to convert the 8×8 matrix into a one-dimensional vector;
2. Then the Exp-Golomb code is used to encode each number in the vector. Each number (aside from 0, which is encoded as just one bit 0) is encoded by three parts:
   - *length*: a sequence of 1's corresponding to the length of the binary representation of the number, followed by 0 to mark the end of the length sequence;
   - *sign*: a bit representing the sign of the number: 0 for negative, 1 for positive number;
   - *residual*: the binary representation of the number, with the leading 1 omitted.

   For example, the number 47 is encoded as the sequence $\underbrace{1111110}_{length}\ \underbrace{1}_{sign}\ \underbrace{01111}_{residual}$;
3. All encoded sequences are then concatenated and a 6-bit sequence is added to the front. These 6 bits represent the number of non-zero elements in the encoded sequence.

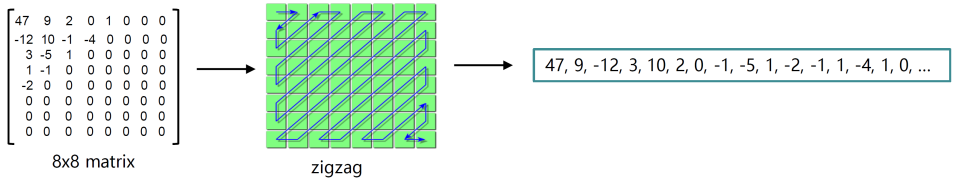


FIG. 4. Zig-zag transformation of the matrix

An example. Let us consider how the algorithm works. We can see that after Exp-Golomb coding (see Fig. 4), the 8×8 DCT quantized matrix above can be binarized using 91 bits (see below). Note that using the inverse process of the encoding method, we can get the original 8×8 matrix from these 91 bits.

001110	1111110101111	111101001	111100100	11011	1111010101	11010	0	100	1110001	101	11000	100	101	1110000	101
# of non-zero elements	47	9	−12	3	10	2	0	−1	−5	1	−2	−1	1	−4	1

Problem for a special prize! Your task is to design an encoding algorithm providing as short as possible output strings for the given 100 000 matrices (here is a file with matrices, and non-zero elements of each matrix are concentrated in

the upper left corner). The less the sum of the lengths of the strings, the more scores you get for this problem. The encoding process must be reversible, that is, the original matrix can be obtained from the bit string using inverse coding.

3.11.2. *Solution.* By the authors opinion there were no great algorithms suggested. So, the problem remains open.

Let us discuss some criterions that were used for checking. An adequate algorithm for data processing should take into account the internal structure of the data involved. Therefore, the algorithms like: 1) get bits from the text file with matrices neglecting the matrix numeric data itself and compress them just as a stream of bits, scored low; 2) mechanical replacement of the suggested Exp-Golomb code with Huffman code or arithmetic code scored low; 3) the absence of the decoding procedure scored low; 4) not working code scored low. The higher score got solutions which: 1) provided working encoder and decoder; 2) provided data analysis and were able to utilize the results of the data analysis in the algorithm; 3) provided good compression.

The initial authors' algorithm that used the Exp-Golomb code provides the compression size equal to 6 694 303 bits. The lowest compression size 5 878 894 bits was achieved by team of Nhat Linh LE Tan and Viet Sang Nguyen (France). Unfortunately, this algorithm just used the Huffman code instead of Exp-Golomb code. Also, the team of Mikhail Kudinov, Alexey Zelenetskiy, and Denis Nabokov (Russia) suggested an interesting solution. They made some reasonable observations about the data and proposed changes into Exp-Golomb encoding depending on the position in the matrix which allows to improve compression. Their result was 5 684 601 bits. Unfortunately, there were some problems with executing the codes provided during the Olympiad.

3.12. **Problem "Collisions".**

3.12.1. *Formulation.* Consider a hash function H that takes as its input a message m consisting of $k \cdot n$ bits and returns an n-bit hash value $H(m)$. The message m is at least one block long ($k \geqslant 1$), and can be split into k blocks of n bits each: m_1, m_2, ..., m_k. Let f be a function which takes an n-bit input and returns an n-bit output. We will use $\oplus$ to denote the bitwise exclusive-or operator.

The hash function H is defined iteratively as follows:

$$h_i := m_i \oplus f(h_{i-1} \oplus m_i),$$

where all n bits of h_0 are zero, and $H(m) := h_k$. An illustration of function H is given in Fig. 5.

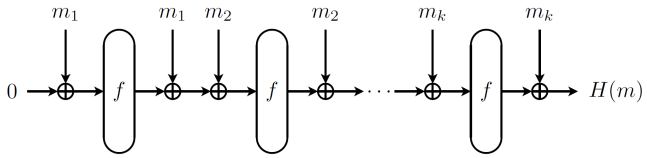


FIG. 5. The hash function H.

A *collision* for H is defined as a pair of distinct messages (m, m') so that $H(m) = H(m')$. Given a message m and its corresponding hash value $H(m)$, a *second preimage* for H is defined as a message $m' \neq m$ so that $H(m) = H(m')$.

Suppose that f is a secret random function and that you have obtained $10 \cdot n$ random different pairs $(x, f(x))$ of argument and value of the function f. Under these restrictions, solve the following problems. Algorithms in Q1 and Q2 must give a solution with a high probability ($> 1/2$).

Q1 Propose an algorithm which finds a collision for H.

Q2 Propose an algorithm which, given a message m and its corresponding hash value $H(m)$, finds a second preimage m' for H.

Q3 Suppose that $n = 256$ bits and the message m is "`A random matrix is likely decent`". Find a second preimage m' for this message.

Remark 1. The text message is converted into a bit sequence as follows: first, each character is converted into a 8-bit integer according to the UTF-8 encoding, and then these integers are concatenated together using the big-endian ordering. For example, the string "`Hello`" is converted into the sequence of integers $(72, 101, 108, 108, 111)$ which then gives the following binary string: 0100100001100101011011000110110001101111. You can give your answer to this task in the form of a binary sequence or a hexadecimal sequence.

Remark 2. You can evaluate the hash function H on any input message here [12]. The message being hashed should be presented as either a binary sequence or a hexadecimal sequence, starting with a symbol `b` or `h` which specifies the representation. Here [13] you can find a list of values of f on 512 different inputs (binary sequences are presented as integers).

3.12.2. *Solution.* Let $||$ denote the concatenation of bit strings. Below we give solutions for all subproblems.

Q1. It is easy to notice that $H(x||f(x)) = 0$ for any n-bit string. Therefore, for any two vectors x, y with known values $f(x), f(y)$, messages $x||f(x)$ and $y||f(y)$ produce the same hash value 0.

Q2. By **Q1**, we can see that for any message m and any n-bit string x it holds

$$H(x||f(x)||m) = H(m).$$

So, we can easily construct $10 \cdot n$ preimages for any given message m. Alternatively, one can append messages to the end: $H\big(m||H(m) \oplus x||H(m) \oplus f(x)\big) = H(m)$.

Q3. This subproblem essentially asks one to apply their solution for Q2 to a specific example. The easiest solution is to append the string $0||f(0)$ to the message. The hexadecimal representation of the given message "`A random matrix is likely decent`" is

$m =$ `412072616e646f6d206d617472697820697320c696b656c7920646563656e74`.

Taking the value of $f(0)$ from the given list, one can construct the following collision:

$m' = 0||f(0)||m =$

`000000000000000000000000000000000000000000000000000000000000000000`
`ff1282609f458d732888e2736fd1b98cc36f809b1c116e77015b8d7d4d8996ae`
`412072616e646f6d206d617472697820697320c696b656c7920646563656e74`.

Let us describe also an **alternative solution for Q2** that was found by Andy Yu (Taiwan). Let us denote $g_i = h_{i-1} \oplus m_i$ for $i = 1, 2, \ldots, k$. We then claim that

$$h_j = \bigoplus_{i=1}^{j} g_i \oplus f(g_i)$$

for any $j = 1, 2, \ldots, k$. The proof is by induction. Since $g_1 = h_0 \oplus m_1 = m_1$, we have $h_1 = m_1 \oplus f(m_1) = g_1 \oplus f(g_1)$. Let $j > 1$ and assume that $h_{j-1} = \bigoplus_{i=1}^{j-1}(g_i \oplus f(g_i))$. Then

$$h_j = m_j \oplus f(m_j \oplus h_{j-1}) = g_j \oplus h_{j-1} \oplus f(g_j) = g_j \oplus f(g_j) \oplus \bigoplus_{i=1}^{j-1} g_i \oplus f(g_i) = \bigoplus_{i=1}^{j} g_i \oplus f(g_i),$$

which proves the claim. Note now that $H(m) = h_k = \bigoplus_{i=1}^{k} g_i \oplus f(g_i)$. If we find a set of values $g'_1, g'_2, \ldots, g'_s$ such that $H(m) = \bigoplus_{i=1}^{s} g'_i \oplus f(g'_i)$, we can easily construct a second preimage m' by flipping the definition of g_i's:

$$m'_j = g'_j \oplus h_{j-1} = g'_j \oplus \bigoplus_{i=1}^{j-1} g'_i \oplus f(g'_i),\ j = 1, 2, \ldots s. \tag{13}$$

So, the task becomes the following: given the set of $10 \cdot n$ pairs $\{(x_i, f(x_i))\}_{i=1}^{10 \cdot n}$, find a subset of indices $i_1, \ldots, i_s$ such that $H(m) = x_{i_1} \oplus f(x_{i_1}) \oplus \ldots \oplus x_{i_s} \oplus f(x_{i_s})$. Let us denote $y_i = x_i \oplus f(x_i),\ i = 1, \ldots, 10 \cdot n$. Then our goal is to express $H(m)$ as a linear combination of vectors y_i. Representing y_i's as binary vectors of length n, we can easily solve this task by writing out and solving a system of binary linear equations with n equations and $10 \cdot n$ variables. But this works only if the value $H(m)$ is in the linear span of the vectors y_i. The probability of this event can be estimated as follows:

$$\begin{aligned}
&\Pr[H(m) \text{ is in the span of } y_i\text{'s}] \geqslant \Pr[y_i\text{'s span the whole space } \mathbb{F}_2^n] = \\
&= \Pr[\text{Random binary } n \times 10 \cdot n \text{ matrix has full rank } n] = \\
&= \frac{(2^{10n} - 1)(2^{10n} - 2)(2^{10n} - 4) \ldots (2^{10n} - 2^{n-1})}{2^{10n^2}} = \prod_{i=0}^{n-1} (1 - 2^{-10n+i}) \geqslant \\
&\geqslant 1 - \sum_{i=0}^{n-1} 2^{-10n+i} = 1 - 2^{-10n}(2^n - 1) \geqslant 1 - 2^{-9n}.
\end{aligned}$$

Here the 4th line is obtained from the 3rd by repeatedly applying $(1 - a)(1 - b) \geqslant 1 - a - b$.

So, the algorithm is then the following:

1. Calculate $y_i = x_i \oplus f(x_i)$ for $i = 1, 2 \ldots 10 \cdot n$.
2. Construct an $n \times 10 \cdot n$ matrix A using y_i's as its columns.
3. Solve the linear system $A \cdot z = H(m)$. The probability of success of this step is at least $1 - 2^{-9n}$.
4. Taking vectors y_i for which $z_i = 1$, reconstruct the second preimage m' using (13). If $m' = m$, shuffle the order of y_i's.

As well as the solution described above, notable solutions with extensive research was given by the team of Nhat Linh LE Tan and Viet Sang Nguyen (France), the team of Mircea-Costin Preoteasa, Gabriel Tulba-Lecu, and Ioan Dragomir (Romania).

3.13. Problem "Bases".

3.13.1. *Formulation.* **Problem for a special prize!** Let us consider the vector space $\mathbb{F}_2^r$ consisting of all binary vectors of length r. For any d vectors $x^i = (x_1^i, \ldots, x_r^i)$, $i = 1, \ldots, d$, $d > 0$, it is defined the componentwise product of these vectors equal to $(x_1^1 \ldots x_1^d, \ldots, x_r^1 \ldots x_r^d)$. The empty product (when no element is involved in it) equals the all-ones vector.

Let $s \geqslant d > 1$ be positive integers and let r be defined by the formula $r = \sum_{i=0}^{d} \binom{s}{i}$, where $\binom{s}{i}$ denotes the binomial coefficient. Let $\mathcal{B}$ be a basis of the vector space $\mathbb{F}_2^r$, and let $\mathcal{F} \subseteq \mathbb{F}_2^r$ be a family of s binary vectors such that all possible componentwise products of up to d vectors from the family $\mathcal{F}$ (including the empty product) form the basis $\mathcal{B}$.

Given s, d, r defined above, describe all (or at least some) bases $\mathcal{B}$ for which such family $\mathcal{F}$ exists or prove that such bases do not exist.

Suggest practical applications of such bases.

Example. Let $s = 2$, $d = 2$ and $r = 4$. Consider the following family of 2 vectors $\mathcal{F} = \{(1100), (0110)\}$. Then all componentwise products of 0, 1 and 2 vectors from the family $\mathcal{F}$ form the basis $\mathcal{B} = \{(1111), (1100), (0110), (0100)\}$ of $\mathbb{F}_2^4$.

3.13.2. *Solution.* The problem "determine what are the bases" was not solved. This problem remains open. The sub-problem "determine some bases" was solved constructively by the team of Mikhail Kudinov, Alexey Zelenetskiy, and Denis Nabokov (Russia). Let us describe the main ideas of this solution.

We will prove that such bases exist for all $s \geqslant d > 1$ and give a construction of such bases.

Let $\mathbf{1}$ be all-one vector and $r = \sum_{i=0}^{d} \binom{s}{i}$. Suppose that there exists $\mathcal{F} \subseteq \mathbb{F}_2^r$ such that $\mathcal{F} = \{v_1, v_2, \ldots, v_s\}$ and $\mathcal{B} = \{v_{i_1} \ldots v_{i_k} \mid 1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant s \text{ and } 0 \leqslant k \leqslant d\}$ is a basis of $\mathbb{F}_2^r$. Let A be $(r \times r)$-matrix over $\mathbb{F}_2^n$ whose rows are exactly the vectors from $\mathcal{B}$. The rank of A is equal to r since $\mathcal{B}$ is a basis. Let $A^{(i)}$ denote the i-th column of A. We number the rows of A and, accordingly, the coordinates of $A^{(i)}$ as follows. The row corresponding to the vector $v_{i_1} v_{i_2} \ldots v_{i_k}$ we number as $i_1 i_2, \ldots, i_k$, the first row of A we number as 0. For each $A^{(i)}$, the coordinate number 0 is nonzero and the coordinates $1, 2, \ldots, s$ determine the rest coordinates. Namely, the coordinate $i_1 i_2 \ldots i_k$ is equal to the product of coordinates numbered $i_1, i_2, \ldots, i_k$.

Case $s = d$**.** In this case $r = \sum_{i-0}^{d} \binom{d}{i} = 2^d$. Let $x = (x_0, x_1, \ldots, x_{r-1}) \in \mathbb{F}_2^r$ with $x_0 = 1$ and $x_1, \ldots, x_d$ determine $x_{d+1}, \ldots, x_{r-1}$. The number of such vectors is equal to $2^d = r$. Only these vectors can be the columns of the matrix A. Since A has r columns and its rank is r, then A (and as a consequence, a basis in $\mathbb{F}_2^r$) is uniquely defined by these vectors up to permutation of columns. Thus, if there are bases in $\mathbb{F}_2^r$, then the number of them is $r! = (2^d)!$.

Let us prove that these bases exist for an arbitrary d. Let us consider $\mathbb{F}_2^r$, $r = 2^d$, as a set of values vectors of all Boolean functions in d variables. Since each Boolean function has the unique algebraic normal form (ANF), then the values vectors of all 2^d elementary monomial functions

$$\{1,\ x_1,\ x_2,\ \ldots,\ x_d,\ x_1x_2,\ \ldots,\ x_{d-1}x_d,\ \ldots,\ x_1 \ldots x_d\}$$

form a basis in $\mathbb{F}_2^r$.

Case $s > d$. Let us construct an invertible matrix A (and as a consequence, a basis in $\mathbb{F}_2^r$) for an arbitrary $s > d$. Let the first column of A be the vector $(1, 0, 0, \ldots, 0)$. The next s columns are

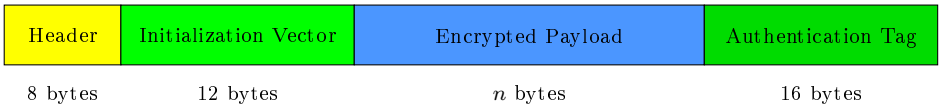
$$(1, 1, 0, \ldots, 0), (1, 0, 1, \ldots, 0), \ldots, (1, 0, \ldots 0, 1, 0, \ldots, 0)$$

. We denote them as A_1. The next $\binom{s}{2}$ vectors we denote as A_2. Each vector in A_2 has only four nonzero coordinate numbered $0, i, j, ij$, $1 \leqslant i < j \leqslant s$. Analogically, the set A_j consists of $\binom{s}{j}$ vectors and each vector has 2^j nonzero coordinates numbered $0, i_1, i_2, \ldots, i_j, i_1i_2, i_1i_3, \ldots, i_1i_2 \ldots i_j$, $1 \leqslant i_1 < i_2 < \ldots, i_j \leqslant s$.

The matrix A constructed above is a triangular matrix and each element on the main diagonal is equal to 1. Therefore, the matrix A is invertible. Any permutation of the columns gives us a new matrix, whose rows give us a basis. Thus, we have $\geqslant r!$ bases in $\mathbb{F}_2^r$.

3.14. Problem "AES-GCM".

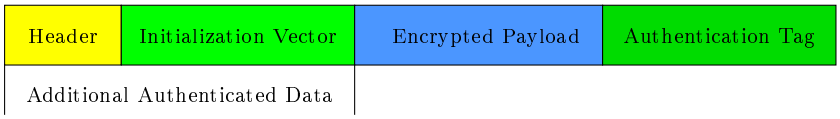
3.14.1. *Formulation.* Alice is a student majoring in cryptography. She wants to use AES-GCM-256 to encrypt the communication messages between her and Bob (for more details of GCM, we refer to [15]). The message format is as follows:



However, Alice made some mistakes in the encryption process since she is new to AES-GCM. Your task is to attack the communications.

Q1 You intercepted some messages sent by Alice. You can find them in the directory "Task_1". Also, you know that the plaintext (unencrypted payload) of the first message (0.message) is "`Hello, Bob! How's everything?`" (without quotes, encoded in UTF-8). Try to decrypt any message in the directory "Task_1".

Q2 In this task, you further know that the AAD (additional authenticated data) used by Alice in each message is Header || Initialization Vector:



You want to tamper some messages in the directory "Task_2". You pass this task if you can modify at least one bit in some message so that Bob can still decrypt the message successfully.

Q3 Alice has noticed that the messages sent by her have been tampered with. So she decides to enhance the security of her encryption process. Instead of using Header || Initialization Vector as the additional authenticated data (AAD), Alice further generates 8 bytes data X by some deterministic function f and the AES secret key K, where

$$X = f(K).$$

In each message, she uses Header || Initialization Vector || X as the AAD.

You also intercepted some messages sent by Alice, see these messages in the directory "Task_3". Try to tamper any message!

Q4 Bonus problem (extra scores, a special prize!)

You have successfully tampered with the messages in Q2. However, the attacks will be easy to detect if the tampered message cannot be decrypted to some meaningful plaintext.

In this task, try to tamper the messages in Q2 so that the tampered message can still be decrypted to some plaintext that people can understand.
Remark: Tampering with the Header or Initialization Vector of a message will not be accepted as a solution, you need to tamper with the encrypted payload to produce some other ciphertext which did not appear in any message included.

3.14.2. *Solution.* Let us give solutions or ideas for all subproblems.

Q1. Note that blocks of the ciphertext C_i are obtained by XORing blocks of the plaintext P_i with the values $E_k(CB_i)$. The values $E_k(CB_i)$ depend on the IV and some other parameters which are common for all messages within one subproblem. Going through the messages, we can see that the messages number 0, 5 and 6 all use the same initialization vector. Since we know the plaintext for the message number 0, we can compute the first 29 bytes of the values $E_k(\cdot)$ for this IV and use them to decipher the entirety of the 20-byte message number 5 and 29 symbols of the 46-byte message number 6:

$$m_5 = \texttt{Lincoln Park, 10:15.}$$
$$m_6 = \texttt{Nostalgia is a eternal motif}$$

Q2. In this subproblem, the messages number 1 and 6 also have the same initialization vector. We can apply the **Forbidden Attack** [16] to reconstruct the secret value H, which will allow us to forge messages by changing the ciphertext and recalculating the Authentication Tag. In this solution, we will briefly describe the attack.

Let $A = A_1||A_2||\dots||A_m$ be the AAD of a message, and let $C = C_1||C_2||\dots||C_n$ be the encrypted payload. Then the Authentication Tag can be presented as follows:

$$\text{AuthTag} = E_k(CB_0) \oplus \sum_{i=1}^{m+n+1} T_i H^{m+n+2-i}, \tag{14}$$

where $T = A_1||A_2||\dots||A_m||C_1||C_2||\dots||C_n||(len(A)||len(C))$ and all operations are performed in the Galois field $\mathbb{F}_{2^{128}}$.

Let us consider (14) as an equation which we want to solve for H. Since we know the AuthTag, the AAD and the ciphertext for every message, each coefficient in this equation is known except for $E_k(CB_0)$. However, since the messages number 1 and 6 have the same IV, they also have the same value $E_k(CB_0)$. Subtracting equations of the form (14) constructed for the messages number 1 and 6 one from another, we obtain the following equation:

$$\text{AuthTag}_1 - \text{AuthTag}_6 = g(H),$$

where $g(H)$ is a polynomial in the variable H with all coefficients known. We can find the root of it in the field $\mathbb{F}_{2^{128}}$:

$$\begin{aligned}H = {} & a^{126} + a^{125} + a^{122} + a^{120} + a^{119} + a^{116} + a^{114} + a^{111} + a^{110} + a^{107} + a^{99} \\ & + a^{96} + a^{95} + a^{94} + a^{93} + a^{92} + a^{90} + a^{89} + a^{87} + a^{85} + a^{84} + a^{83} + a^{82} + a^{81} \\ & + a^{80} + a^{78} + a^{76} + a^{73} + a^{67} + a^{66} + a^{62} + a^{61} + a^{60} + a^{59} + a^{56} + a^{53} + a^{52} \\ & + a^{49} + a^{47} + a^{45} + a^{40} + a^{39} + a^{38} + a^{37} + a^{36} + a^{35} + a^{34} + a^{33} + a^{29} + a^{28} \\ & + a^{24} + a^{22} + a^{21} + a^{19} + a^{18} + a^{17} + a^{16} + a^{14} + a^{11} + a^{10} + a^{9} + a^{6} + a^{4} + a^{2},\end{aligned}$$

where a is the generator of the field. Knowing H, we can easily find $E_k(CB_0)$ and calculate the Authentication Tag for any ciphertext which was obtained using the same IV as in the messages number 1 and number 6.

Q3. Observing messages from the subproblem, we can notice that the messages number 1, 3 and 7 have the same Header h, the same IV and the same length of the ciphertext $len(C^j)$, $j = 1, 3, 7$. Let us split the Initialization Vector $IV = IV_0||IV_1$ so that the AAD for each of the three messages can be written as $A = A_1||A_2$, where $A_1 = h||IV_0$ and $A_2 = IV_1||X||0^{32}$. Then for $j = 1, 3, 7$, we have:

$$\begin{aligned}\text{AuthTag}_j = E_k(CB_0) \oplus A_1H^{23} \oplus A_2H^{22} \oplus C_1^jH^{21} \oplus C_2^jH^{20} \oplus \dots \\ \dots \oplus C_{20}^jH^2 \oplus (len(A)||len(C)H.\end{aligned}$$

Here, we do not know $E_k(CB_0)$ and we also do not know A_2 since it contains the secret value $X = f(K)$. However, since the degrees of all three equations are the same, when we subtract one from another, the term with A_2 vanishes along with $E_k(CB_0)$. So, we can still apply the method used in $Q2$ to solve these equations for H. After trying all possible combinations, we find the only value of H which satisfies all equations at once:

$$\begin{aligned}H = {} & a^{123} + a^{122} + a^{112} + a^{110} + a^{107} + a^{102} + a^{100} + a^{99} + a^{97} + a^{96} + a^{95} + a^{92} \\ & + a^{90} + a^{87} + a^{85} + a^{83} + a^{82} + a^{81} + a^{78} + a^{77} + a^{74} + a^{73} + a^{71} + a^{70} + a^{65} \\ & + a^{63} + a^{62} + a^{60} + a^{59} + a^{58} + a^{57} + a^{54} + a^{53} + a^{50} + a^{49} + a^{47} + a^{45} + a^{43} \\ & + a^{42} + a^{41} + a^{37} + a^{36} + a^{32} + a^{30} + a^{28} + a^{23} + a^{13} + a^{12} + a^{10} + a^{7} + a^{5} \\ & + a^{3} + 1.\end{aligned}$$

Knowing H, we can once again modify any of the ciphertexts of the messages number 1, 3 or 7 and recalculate the Authentication Tag.

Q4. This subproblem remains open in general since there were no complete theoretical solutions given. However, many different approaches were presented to modify these particular messages utilizing the properties of the natural language.

Some participants suggested that we can flip the least significant bits in parts of the ciphertext in order to obtain a text with a "typo". Alternatively, we can try shuffling parts of ciphertexts encrypted with the same IV, which may produce a readable text, although likely not semantically connected.

Other participants used the properties of the natural English language to decipher the messages number 1 and 6 by hand. Note that, since the messages use the same IV, if we XOR the shorter ciphertext C^6 with the part of the longer ciphertext C^1, we will get

$$C^6 \oplus C^1 = P^6 \oplus P^1.$$

Trying to find pairs of texts P^1, P^6 that are readable and sum to $C^6 \oplus C^1$ by hand, it is possible to discover the following two texts:

$P^6 =$ `"Do not you want to know who has taken it?"`
`cried his wife impatiently.`

$P^1 =$ `However little known the feelings or views`
`of such a man may be on his`

Note that we cannot be completely sure that these texts were the original messages, and we also cannot guarantee which text is P^1 and which is P^6. However, it is highly likely we correctly decrypted the message number 6. We can now replace it with an arbitrary new message $\tilde{P}^6$ of the same length, and its corresponding ciphertext can be calculated as follows: $\tilde{C}^6 = \tilde{P}^6 \oplus C^6 \oplus P^6$. We are also able to calculate an Authentication Tag for this new message as we have solved Q2 and know H.

The most complete solutions to this problem were given by the team of Himanshu Sheoran, Sahil Jain, and Tirthankar Adhikari (India), the team of Mikhail Kudinov, Alexey Zelenetskiy, and Denis Nabokov (Russia), the team of Pham Cong Bach, Phu Nghia Nguyen, and Ngan Nguyen (Vietnam), the team of Roman Sychev, Diana Bespechnaya, and Nikolay Prudkovskiy (Russia), the team of Roman Lebedev, Vladimir Sitnov, Ilia Koriakin (Russia).

Acknowledgments. We thank Alexey Oblaukhov for valuable comments and fruitful discussions.

References

[1] S. Agievich A. Gorodilova, V. Idrisova, N. Kolomeec, G. Shushuev, N. Tokareva, *Mathematical problems of the second international student's olympiad in cryptography*, Cryptologia, **41**:6 (2017), 534–565.

[2] S Agievich, A. Gorodilova, N. Kolomeec, S. Nikova, B. Preneel, V. Rijmen, G. Shushuev, N. Tokareva, V. Vitkup, *Problems, solutions and experience of the first international student's olympiad in cryptography*, Prikl. Diskretn. Mat., **2015**:3(29) (2015), 41–62. Zbl 07310308

[3] K. Geut, K. Kirienko, P. Sadkov, R. Taskin, S. Titov, *On explicit constructions for solving the problem "A secret sharing"*, Prikl. Diskr. Mat. Suppl., **2017**:10, (2017) 68–70.

[4] A. Gorodilova, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, S. Nikova, A. Oblaukhov, S. Picek, B. Preneel, V. Rijmen, N. Tokareva, *Problems and solutions from the fourth international students' olympiad in cryptography (NSUCRYPTO)*, Cryptologia, **43**:2 (2019), 138–174.

[5] A. Gorodilova, S. Agievich, C. Carlet, X. Hou, V. Idrisova, N. Kolomeec, A. Kutsenko, L. Mariot, A. Oblaukhov, S. Picek, B. Preneel, R. Rosie, N. Tokareva, *The fifth international students' olympiad in cryptography — NSUCRYPTO: problems and their solutions*, Cryptologia, **44**:3 (2020), 223–256.

[6] A. Gorodilova, N. Tokareva, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, R. Lebedev, S. Nikova, A. Oblaukhov, I. Pankratova, M. Pudovkina, V. Rijmen, A. Udovenko, *On the sixth international olympiad in cryptography NSUCRYPTO*, J. Appl. Ind. Math., **14**:4 (2020), 623–647.

[7] Kiss R., Nagy G. P. *On the nonexistence of certain orthogonal arrays of strength four*, 2020. ArXiv:2011.09935. https://arxiv.org/abs/2011.09935

[8] N. Tokareva, A. Gorodilova, S. Agievich, V. Idrisova, N. Kolomeec, A. Kutsenko, A. Oblaukhov, G. Shushuev, *Mathematical methods in solutions of the problems presented at the third international students' olympiad in cryptography.* Prikl. Diskretn. Mat., **40** (2018), 34–58. Zbl 07311617

[9] https://nsucrypto.nsu.ru/

[10] https://nsucrypto.nsu.ru/unsolved-problems/
[11] https://nsucrypto.nsu.ru/archive/2020/round/2/task/3/
[12] https://nsucrypto.nsu.ru/archive/2020/round/2/task/8
[13] https://nsucrypto.nsu.ru/media/MediaFile/Collisions-Values_of_F.txt
[14] https://stylesuxx.github.io/steganography/
[15] M. Dworkin, *Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC*, NIST Special Publication 800-38D, 2007. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
[16] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, Ph. Jovanovic, *Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS*, Cryptology ePrint Archive: Report 2016/475. https://eprint.iacr.org/2016/475.pdf

Anastasiya Aleksandrovna Gorodilova
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: gorodilova@math.nsc.ru

Natalia Nikolaevna Tokareva
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Laboratory of Cryptography JetBrains Research,
1, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: tokareva@math.nsc.ru

Sergey Valer'evich Agievich
Belarusian State University,
4, Nezavisimosti ave.,
Minsk, 220030, Belarus
Email address: agievich@gmail.com

Claude Carlet
University of Paris 8,
2 rue de la Liberté,
Saint-Denis, 93526, France
Email address: Claude.Carlet@univ-paris8.fr

Valeriya Aleksandrovna Idrisova
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: vvitkup@yandex.ru

Konstantin Viktorovich Kalgin
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Novosivirsk State University,
1, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: kalginkv@gmail.com

Denis Nikolaevich Kolegov
Tomsk State University,
36, Lenin ave.,
Tomsk, 634050, Russia
Email address: d.n.kolegov@gmail.com

Aleksandr Vladimirovich Kutsenko
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Novosivirsk State University,
1, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: alexandrkutsenko@bk.ru

Nicky Mouha
National Institute of Standards and Technology,
100, Bureau Drive,
Gaithersburg, 20899, USA
Email address: nicky@mouha.be

Marina Aleksandrovna Pudovkina
Bauman Moscow State Technical University,
5/1, Baumanskaya 2-ya str.,
Moscow, 105005, Russia
Email address: maricap@rambler.ru

Aleksei Nikolaevich Udovenko
CryptoExperts,
41, Boulevard des Capucines,
Paris, 75002, France
Email address: aleksei.udovenko1@gmail.com

EURASIAN JOURNAL OF MATHEMATICAL AND COMPUTER APPLICATIONS
ISSN 2306–6172
Volume , Number (20) –

OVERVIEW OF PRIVACY PRESERVING TECHNOLOGIES FOR DISTRIBUTED LEDGERS

Kondyrev D. O.

Abstract The paper analyzes the privacy preserving problem for distributed ledgers. It provides an overview of technologies such as mixers, zero-knowledge proof algorithms, homomorphic encryption, secure multi-party computation, anonymous signatures, and hardware solutions. Advantages and disadvantages of each technology are identified, as well as usage samples in the existing distributed ledgers. As a result, unsolved problems and prospects for further research are formulated.

Key words: distributed ledgers, blockchain, privacy, zero-knowledge proof, homomorphic encryption, secure multi-party computation, anonymous signatures.

AMS Mathematics Subject Classification: 68-02, 68M14.

1 Introduction

Distributed ledgers are widely used in various fields such as financial technology, e-voting, logistics, etc. Distributed ledger technology allows to create a decentralized system with no need for an intermediary, which solves the trust problem. The data in such systems is distributed on the network nodes, the transaction history cannot be changed or deleted.

Among the technical issues that hinder the distributed ledger technology implementation, scalability and privacy are particularly significant. Active research is currently underway to find a solution to the privacy problem.

The privacy problem is especially acute in open distributed ledgers (such as blockchain systems). In such ledgers, all data is stored in open form and is available to all participants, which is not always acceptable when creating production software systems. In addition, users are identified by their account address, so it is possible to track the user's actions by analyzing transactions involving a specific address and comparing the account and user addresses.

This work purpose is to analyze existing technologies for hiding private data in distributed ledgers, identify the main directions of development and unresolved research problems.

The paper provides an overview of the technologies that have the greatest application in existing distributed ledgers, as well as promising developments that can become the basis for new platforms: mixers, zero-knowledge proof algorithms, homomorphic encryption, secure multi-party computation, anonymous signatures and hardware solutions. The existing algorithms advantages and disadvantages, as well as the area of their applicability in distributed ledgers, are regarded.

2 Mixers

The idea of mixers was first proposed by David Chaum in 1981. The article [1] presents an algorithm based on a public key cryptosystem, which gives the e-mail system the possibility to hide who the participant communicates with, as well as the message content when using an unsecured underlying telecommunication system.

With the advent of open distributed ledgers, the problem of hiding the transactions recipients arose in this area as well. The first solution applied in practice was algorithms that implement a similar mixing idea.

Protocols based on this approach take different forms, but all of them implement the same idea. A basic mixing network, also known as a mixnet, is a routing protocol in which a specific node (or group of nodes) receives messages from multiple senders as input, shuffles them, and sends randomly to recipients. The purpose of such a network is to eliminate the ability to trace the correspondence between the senders and recipients of transactions.

Over the past few years, many different mixing mechanisms have been developed for blockchain systems to hide the transaction history and reduce the risk of deanonymization. Research was conducted in two directions:

- centralized mixers;
- decentralized mixers.

2.1 Centralized mixers

Centralized mixers are services that provide users with the functionality of anonymously mixing transactions. In this case, the user sends a transaction to some server or network node, where transactions from different users are mixed and then sent to addressees. This approach raises the problem that a possible attacker could be a service provider who would steal user assets without transferring them to the analyzed recipients.

The first solution to this problem was proposed in 2013. Gregory Maxwell introduced a third party mixing protocol for the Bitcoin blockchain called CoinSwap. According to the protocol, senders deliver transactions to recipients using a mixer acting as an intermediary. All transactions between the sender and the mixer, as well as between the mixer and the receiver, are escrow transactions that are protected by a hash lock. This mechanism ensures that no one can steal the user's assets.

Another attempt to solve the problem of trust in the mixer was Mixcoin, proposed by Bonneau et al. in 2014 [2]. Mixcoin adds a mechanism that unequivocally proves to users that the mixer performed incorrect actions.

One of the first attempts to provide anonymity in digital currency was the Dash project, launched in 2014. In this project, the PrivateSend coin mixing service was created, which removes all unique user information from the blockchain. The mixing network is made up of the specific nodes (called master nodes) set, rather than a single server, which limits the mixing process to only accepting certain denominations. In addition, each master node must pay 1000 Dash (the cryptocurrency in the Dash network) as a deposit, which acts as a guarantee of the master nodes honesty. However,

the mixing process in the system is limited by the number of participants who are currently connected to the network [3].

However, in all centralized mixer protocols, transactions are sent as plain text, which means that the mixer can track all pairs of senders and receivers and all information about transactions between them.

2.2 Decentralized mixers

Decentralized protocols have evolved to solve the problems of centralized mixers. The purpose of these protocols was to exclude the intermediary that has all the information.

In 2013, Gregory Maxwell proposed CoinJoin, a special type of transaction on the Bitcoin network. Any two independent transactions can be combined into one CoinJoin transaction, while the inputs and outputs of the transactions remain unchanged. The resulting joint transaction hides the connection between inputs and outputs, so that other network participants have no way to determine the exact direction of the data flow [3].

This approach formed the basis for the more complex CoinShuffle algorithm [4]. CoinShuffle is a completely decentralized protocol that allows users to mix their coins with those of other interested users. To ensure anonymity and resistance against active attacks, CoinShuffle uses the Dissent protocol of anonymous group communication. The key idea is similar to decryption mixnets and requires only standard primitives such as signatures and public key cryptosystems.

A fundamentally different approach to solving the problem was proposed in XIM, a two-party mixing protocol. It is the first decentralized protocol designed to counter Sybil attack, DoS attacks, and timing attacks at the same time. XIM includes a decentralized system for anonymous searching for mixing partners based on ads posted on the blockchain. No outside party can confirm the fact of interaction between the protocol participants [5]. However, the high degree of protocol anonymity requires a significant waiting time for mixing, this operation can take up to several hours [3].

Despite the fact that transaction mixers are widely used, all these algorithms have the following disadvantages:

- The approach can be considered only a partial solution to the anonymity problem, since it does not completely hide information about transactions.
- Mixing is only applicable for the anonymization task (hides the sender and the recipient), there is no way to extend the algorithm for the more general problem of hiding arbitrary data in transactions.

3 Zero-knowledge proofs

Zero-knowledge proof is a cryptographic protocol that involves two parties, the prover and the verifier.

The purpose of the protocol is for the verifier to be sure that the prover has knowledge of the secret parameter. At the same time, the secret parameter itself should not be disclosed to the verifier or anyone else [6].

By definition, a zero-knowledge proof must satisfy the following three properties:

- **Completeness:** if the statement is true and both parties follow the same protocol, then the verifier can check the truth of the statement.
- **Soundness:** if a statement is false, the verifier will not be convinced of its truth with high probability.
- **Zero-knowledge:** the verifier does not receive any additional information.

The concept of interactive zero-knowledge proof systems was first introduced by Goldwasser, Micali and Rakof in [7]. Over the years of zero-knowledge proof research, systems based on this method have gradually improved with an emphasis on optimizing their effectiveness for specific applications. It led to the algorithms that significantly reduced the number of interaction rounds between protocol participants.

The distributed ledger technology imposes several restrictions on the used cryptographic protocols, in particular on zero-knowledge proofs. Since the system is distributed, users may not be online at the same time. But the proof must be available to all participants. After the proof has been provided, any user should be able to verify its correctness at any time. It makes interactive zero-knowledge proof protocols difficult to implement.

In [8], a non-interactive zero-knowledge proof protocol was first proposed. The non-interactive system contains only one message (proof), which the prover sends to the verifier, i.e. interaction between the protocol parties is reduced to one round.

Further research in the field of non-interactive protocols has focused on optimizing computational efficiency and reducing proof size.

As a significant breakthrough in this field the zk-SNARK can be considered [9], which in 2013 made it possible to effectively use non-interactive zero-knowledge proof protocols in distributed ledgers.

3.1 zk-SNARK protocol

zk-SNARK (zero-knowledge Succinct Non-Interactive Argument of Knowledge) is a non-interactive zero-knowledge proof cryptographic protocol [10]. It proves some private data satisfies the constraint system expressed in the form of an arithmetic circuit without revealing this data.

The advantage of zk-SNARK over other zero-knowledge proof protocols lies in the efficiency guarantees: the proof length depends only on the security parameter, and the verification time does not depend on the circuit or witness size.

Thus, zk-SNARK can be considered as a non-interactive protocol with short proof and fast verification time, which makes it most suitable for use in distributed ledgers [11].

In 2014, Zerocash was introduced, the first blockchain system based on the zk-SNARK protocol [10]. Zerocash provides a high protection level for the anonymity and privacy of blockchain transactions, but its computational cost to generate proofs is high.

The ideas behind Zerocash were further developed in the Hawk system introduced in 2016 [12]. Hawk is the first system that simultaneously ensures the transaction confidentiality and the ability to create smart contracts for financial transactions. Users have the ability to send information to a smart contract in encrypted form, and also generate a zk-SNARK proof, due to which the correct contract execution and the funds transfer are guaranteed. While a smart contract result can be verified by any participant, the entire sequence of transactions carried out in the contract is confidential to the parties not involved in the transaction [3].

In 2017, in the Metropolis update, zk-SNARK was integrated into the Ethereum blockchain platform.

In zk-SNARK, the proof verification procedure consists of operations on elliptic curves. In particular, the verifier requires elliptic curve scalar multiplication and addition, as well as bilinear pairing, a computationally more complicated operation.

Ethereum provides the implementation of these operations in the form of precompiled contracts. With their help, it is possible to implement schemes based on zero-knowledge proof in the smart contract code [13, 14].

This was the first attempt to implement zk-SNARK in a distributed ledger as a tool that can be applied to a wide range of tasks. The ability to create arbitrary smart contracts in Ethereum and the added cryptographic primitives permit to go beyond just solving the problem of financial transactions.

Despite the fact that zk-SNARK has found the most widespread use in distributed ledgers of all zero-knowledge proof algorithms, it has several disadvantages that limit its use.

Firstly, the algorithm needs a setup phase, during which a key pair for generating and verifying the proofs is generated. This phase is critical in terms of system security. Anyone who possesses the security parameter on the basis of which the keys are generated will be able to generate false evidence that will be accepted by the verification algorithm as correct.

Typically, multi-party protocols are used to generate parameters securely without relying on the honesty of a single participant. The parameter initialization process involves a number of parties using a multi-party protocol to generate proof and verification keys. To ensure the reliability of the created cryptographic scheme, it is enough that at least one of the parties is honest. The distributed parameter generation protocol for zk-SNARK is given in [11].

Secondly, the computational complexity of the operations used in zk-SNARK makes their implementation in smart contracts inefficient. For example, the implementation of an arbitrary zk-SNARK cryptographic scheme in the Ethereum smart contract code is impossible due to restrictions on the size of the contract code and on the complexity of operations that can be performed within a single transaction.

3.2 zk-STARK protocol

In 2018, Eli Ben-Sasson, one of the creators of Zerocash, along with a group of other researchers developed a new non-interactive zero-knowledge proof algorithm called zk-STARK.

zk-STARK (zero-knowledge Scalable Transparent Argument of Knowledge) is the first transparent zero-knowledge system in which the verification time grows exponentially slower than the database size [15]. The advantages of zk-STARK are universality (it can be used for any NP-complete problems), scalability (in terms of generation and proof verification time) and the use of post-quantum cryptography. However, the greatest achievement of zk-STARK is its transparency, the protocol does not require trusted parameter setup, which was a significant problem of zk-SNARK. At the same time, the size of the zk-STARK proof is significantly larger than in zk-SNARK.

Today zk-STARK is practically not used in distributed ledgers, all integrations are experimental in nature. However, active research is underway in this field. The significant advantages of this protocol allow us to consider its application in distributed ledgers quite promising.

4 Homomorphic encryption

The term homomorphic encryption was first coined by Rivest, Adleman and Dertouzos in 1978 [16].

A homomorphic cryptosystem is an encryption methodology that satisfies the homomorphism property with respect to arithmetic operations performed on ciphertexts. It allows any party to perform various operations on ciphertexts, while maintaining the confidentiality of the original data.

One of the striking examples of a homomorphic system is the RSA algorithm. Let (e, n) be the public key and (d) be the private key (i.e. integers that satisfy the equalities $n = p * q$, where p and q are prime, and $d * e = 1 \ mod \ \phi(n)$). The encryption of the message x is defined as $E(x) = x^e \ mod \ n$. Then it can be shown that RSA satisfies the homomorphism property with respect to the multiplication operation: $E(x)E(y) = x^e y^e = (xy)^e \ mod \ n = E(xy)$ [17].

A homomorphic cryptosystem performs the function of a black box: for given ciphertexts and operations it produces an encrypted result of performing the same operations on the corresponding source data. That is, the encryption function must have some properties that allow it to work with ciphertext and get the same encrypted result as if the same operations were performed on plaintext and then encrypted using the same function.

This feature makes homomorphic cryptography well suited for hiding and updating various numeric transaction data. Typical homomorphic cryptographic schemes that can be used to protect privacy in distributed ledgers are the Pedersen commitment scheme and the Paillier cryptosystem [3].

The Pedersen commitment scheme [18], developed in 1991, is one of the implementations of homomorphic commitment schemes. It supports homomorphic operations (addition and multiplication) on commitments and can provide perfect hiding of the real message.

The Pedersen Commitment Scheme is one of the cryptographic algorithms that Zerocoin has used to ensure the anonymity of cryptocurrency transfers.

In 2018, Bulletproof was developed, a zero-knowledge proof protocol focused on blockchain systems that was based on the Pedersen scheme [19]. An elliptic curve

version of this scheme has been integrated into Monero.

Another system based on the Pedersen scheme was zkLedger [20].

The Paillier cryptosystem was created in 1999 [21]. It is an efficient additive homomorphic encryption system based on the composite residuosity class problem. Using only encrypted messages m_1 and m_2 together with the same public key, the ciphertext for $m_1 + m_2$ can be calculated. This method works very well for maintaining the confidentiality of financial transactions, where transactions are mainly related to balance changes — adding or subtracting a certain amount.

Resolving the transfer privacy issue Wang et al. developed a framework for the Bitcoin blockchain [22]. The framework is based on the Paillier homomorphic encryption system that is used to encrypt the amount of transactions. The correctness of the encrypted amounts is verified by zero-knowledge proofs. This verification ensures the encrypted transaction amounts are positive and that the inputs sum and the outputs sum are equal. The proposed framework provides anonymity and prevents active and passive attacks, which effectively increases the transactions confidentiality.

5 Secure multi-party computation

Secure multi-party computation (SMPC) is a multi-party cryptographic protocol that allows participants to jointly perform certain computations on their private data. At the same time, the data remains private. The parties can learn only the overall result and their own inputs.

Andrew Yao in 1982 developed the first secure two-party computation protocol to solve the millionaire problem [23], and in 1986 generalized it to solve other problems [24]. In 1987 [25] Goldreich et al. proposed a generalization to multi-party computation based on secret sharing (for inputs) and zero-knowledge proof. This generalization has served as the basis for many subsequent and increasingly efficient MPC protocols [26].

Previous works in the field of SMPC formed the basis for new protocols developed specifically to solve the problem of data privacy in distributed ledgers.

Andrychowicz et al. developed protocols based on secure multi-party computation for the Bitcoin blockchain in 2014 [27]. They proposed a protocol that secures multi-party lotteries without relying on a trusted third party. The protocol is based on the concept of "time commitment", a commitment scheme where the committer must reveal the secret within a specified period of time or pay a fine. It ensures security guarantees, excludes the possibility for dishonest participants to deceive the system. If one of the parties interrupts the protocol, then its money is transferred to the honest participants.

In 2015, Zyskind and colleagues developed the Enigma platform, a peer-to-peer network that allows different parties to share data and perform calculations on it, while maintaining complete confidentiality [28]. Enigma itself is not a distributed ledger, instead it uses a third-party blockchain as an immutable storage and peer-to-peer regulator for identity management and access control. Enigma's computational model is based on a highly optimized version of multi-party computation. The Enigma network can execute code without passing raw data to any of the nodes, while ensuring correct execution. Data requests are made in a distributed manner, without a trusted

third party. The data is shared between different nodes, and they compute functions together, without passing information to other nodes.

[29] proposed SMPC protocols use samples to ensure data privacy in the Hyperledger Fabric distributed ledger. Secure multi-party computation in the developed system is performed as part of the smart contracts execution. The protocol participants store their private data in the ledger in encrypted form. When private data is required to execute a smart contract, the participant holding the corresponding private key decrypts it and uses it as his input to the SMPC protocol. This approach allows smart contracts to use any necessary private and public data stored in the ledger.

6 Anonymous signatures

Anonymous signatures are a group of cryptographic digital signature schemes that have the property of hiding the signer identity. Among the large number of anonymous signatures, two classes of algorithms (group signatures and ring signatures) have been the most efficient in distributed ledger systems.

6.1 Group signatures

A group signature is a cryptographic scheme first proposed in 1991 [30]. Each group member can sign messages on behalf of the group. The message recipient can verify that it is a valid group signature, but cannot determine which group member made it. Thus, group signatures are a "generalization" of membership authentication schemes in which a member proves the belonging to a particular group.

The group has a special manager role who adds new members to the group, resolves arising disputes, including identifying the participant who signed a particular message. A distributed ledger also needs an object that has the authority to create and delete a group, as well as dynamically add new members to the group and revoke the membership.

The article [31] proposes a special linkable group signature algorithm for signing cryptocurrency transactions, which can be used to trace the payer identity in anonymous cryptocurrencies based on the consortium blockchain in case of illegal payers actions. At the same time, the algorithm guarantees complete anonymity for honest participants, which makes it possible to reach a tradeoff between anonymity and transactions traceability.

6.2 Ring signatures

The ring signature was originally developed by Rivest, Shamir and Tauman in 2001 as a digital signature that can be used to create a correct but anonymous signature on behalf of a possible signers group, without disclosing information about which group member actually produced the signature [32].

This idea was further developed in the work of Fujisaki and Suzuki in 2007. They proposed a modified version, a traceable ring signature [33, 34]. It can determine whether two signatures were produced by the same user.

Ring signatures cover the limitations of group signatures, and, in particular, they provide greater anonymity guarantees and they need neither complicated setup procedures nor group manager. Users must be a part of the existing public key infrastructure [32]. Due to these properties, ring signatures have found wider application in distributed ledgers.

The CryptoNote protocol, developed by Nicholas van Saberhagen in 2013, can be considered as the first successful application of the ring signature mechanism in distributed ledgers. CryptoNote is a completely anonymous transaction scheme that satisfies both untraceability and unlinkability conditions. By using a one-time ring signature, CryptoNote hides the relationship between sender transaction addresses. An important CryptoNote feature is its autonomy: the sender does not need to cooperate with other users or a trusted third party to complete the transactions.

In 2016, RingCT (Ring Confidential Transaction) was developed, a new protocol that improved CryptoNote. RingCT simultaneously ensures the sender anonymity and the transaction confidentiality. The most successful algorithm implementation is the Monero project.

Ethereum added a ring signature in 2015, which gave users the same anonymity guarantees that CryptoNote provides.

7 Hardware solutions

Hardware solutions based on the trusted execution environment concept are a separate line of information privacy in distributed systems. All the previously described methods relied, to varying degrees, on cryptographic protocols, but here the hardware acts as a guarantee of confidentiality.

An environment is called the Trusted Execution Environment (TEE), it provides a completely isolated environment for running applications. TEE prevents other software applications and operating systems from interfering with execution and deprives the ability to read the running application state. Intel Software Guard eXtensions (SGX) is a typical technology for TEE implementation.

The Ekiden blockchain platform was developed on the basis of Intel SGX [35]. Smart contracts at Ekiden have strong guarantees of confidentiality, integrity and availability. These properties are achieved due to a hybrid architecture that combines TEE and blockchain. Computations in the system are separated from the consensus mechanism; for this purpose there are two separate types of nodes — compute nodes and consensus nodes. Ekiden uses compute nodes to perform off-chain smart contract computations on private data in TEE, and then uses a remote attestation protocol to validate those computations on-chain.

Enigma has integrated Intel SGX to allow users to create privacy-preserving smart contracts. TEE enables the Enigma protocol to prove data confidentiality and correctness with minimal overhead.

In 2018, the Private Data Objects (PDO) technology was introduced, it provides data exchange and coordination between parties that do not trust each other. Interaction is carried out through a smart contract that defines the data access rights and the rules for updating them. The correct execution of smart contract rules is guaranteed by

working in the Intel SGX trusted execution environment. It ensures the data privacy in the distributed ledger is maintained. Smart contracts implemented with PDO ensure the contract state is completely hidden from all participants, including validators. At the moment, this technology is implemented on the basis of the Hyperledger Sawtooth distributed ledger [36].

To solve similar problems for the Hyperledger Fabric distributed ledger, the Hyperledger Fabric Private Chaincode framework was developed. This project uses Intel SGX to protect the data privacy and computation from potentially untrusted hosts. Smart contract code is executed in a trusted environment. The framework enables the development of applications where the stored data is encrypted and can be accessed only by authorized participants [37].

8 Open problems

Despite significant efforts to develop and integrate new cryptographic methods for protecting the information privacy, modern protocols are still far from a complete solution to the problem.

Based on the analysis, we can identify the following promising lines for the development of cryptographic privacy protection protocols in distributed ledgers:

- **The development of more computationally efficient cryptographic protocols.** The existing algorithms used in distributed ledgers are often highly suboptimal. For example, the anonymous signature size is proportional to the number of participants. The zero-knowledge proof algorithms, although they guarantee a fast proof verification time, require several minutes to generate it [10]. It severely limits their applicability for solving privacy problems and does not allow scaling such solutions to a large number of users. Therefore, one of the possible ways is to optimize existing cryptographic protocols (both in terms of execution time and data size) or to develop new ones.

- **Providing greater guarantees of confidentiality with fewer assumptions**. Many algorithms used in distributed ledgers, while solving the problem of privacy, are forced to rely on a trusted third party to perform certain actions. For example, zk-SNARK, which is most widely used in distributed ledgers among all zero-knowledge proof algorithms, requires trusted parameter setup [9]. One potential research area is to completely eliminate or minimize trust assumptions.

- **New post-quantum cryptographic algorithms.** Recent quantum computing advances become a serious threat to the classical cryptographic algorithms which are the existing distributed ledgers basis. Therefore, to implement the post-quantum algorithms meeting the requirements of distributed systems is a currently important task [38].

- **Interaction between the various ledgers while maintaining privacy.** To this date, many distributed ledgers have been developed with different transaction formats and incompatible protocols. However, the need for interaction

between them will increase as they are implemented. The interaction mechanisms start appearing, and the algorithms maintaining confidentiality have not been developed at all [39].

- **Solving the audit problem.** Some tasks solved by distributed ledger technology require opposite requirements. On the one hand, the user data confidentiality must be ensured. On the other hand, certain verification of particular user categories should be conducted. The first attempts to create a cryptographic system meeting both requirements were undertaken in [20]. However, the problem in general form has not yet been solved.

9 Conclusion

In this paper, the analysis of technologies for hiding private data in distributed ledgers was carried out.

All considered protocols rely on a cryptographic base that was laid back in the 70s of the 20th century. Thus, the development and improvement of methods for hiding private data in distributed ledgers has been around for about 50 years. But despite a long history and significant efforts to develop and integrate new cryptographic methods for protecting the information privacy, modern protocols are still far from a holistic solution to confidentiality problems in distributed ledgers.

All currently proposed algorithms are suitable for solving only a certain class of problems. The problem of hiding arbitrary information about transactions has not been completely resolved at the moment.

We can conclude that this area is promising. The development of algorithms for hiding transaction information will expand the scope of distributed ledger technology in production software systems. Such algorithms will raise the distributed computing systems techlogies to a qualitatively new level for solving various applied problems that require information confidentiality.

Acknowledgement

The work is supported by Mathematical Center in Akademgorodok, the agreement with Ministry of Science and High Education of the Russian Federation number 075-15-2019-1613 and Laboratory of Cryptography JetBrains Research.

References

[1] Chaum D. L., *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM. 1981. V. 24, N. 2. P. 84–90. DOI: 10.1145/358549.358563.

[2] Bonneau J., Narayanan A., Miller A., Clark J., Kroll J. A., Felten E. W., *Mixcoin: Anonymity for Bitcoin with Accountable Mixes*, Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2014. V. 8437. P. 486–504. DOI: 10.1007/978-3-662-45472-5_31.

[3] Feng Q., He D. Zeadally S., Khan M. K., Kumar N., *A survey on privacy protection in blockchain system*, Journal of Network and Computer Applications. 2019. V. 126. P. 45–58. DOI: 10.1016/j.jnca.2018.10.020.

[4] Ruffing T., Moreno-Sanchez P., Kate A., *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin*, Computer Security — ESORICS 2014. Lecture Notes in Computer Science. Springer, Cham, 2014. V. 8713. P. 345–364. DOI: 10.1007/978-3-319-11212-1_20.

[5] Bissias G., Ozisik A. P., Levine B. N., Liberatore M., *Sybil-Resistant Mixing for Bitcoin* Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES '14). Association for Computing Machinery, New York, NY, USA, 2014. P. 149–158. DOI: 10.1145/2665943.2665955.

[6] Schneier, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley & Sons, Inc., New York, NY, USA, 2015.

[7] Goldwasser S., Micali S., Rackof C., *The Knowledge Complexity of Interactive Proof Systems*, Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85). Association for Computing Machinery, New York, NY, USA, 1985. P. 291–304. DOI: 10.1145/22145.22178.

[8] Blum M., Feldman P., Micali S., *Non-interactive zero-knowledge proof systems and applications*, Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC '88). Association for Computing Machinery, New York, NY, USA, 1988. P. 103–112. DOI: 10.1145/62212.62222.

[9] Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M., *SNARKs for C: Verifying program executions succinctly and in zero knowledge*, Advances in Cryptology — CRYPTO 2013. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2013. V. 8043. P. 90–108. DOI: 10.1007/978-3-642-40084-1_6.

[10] Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E., Virza M., *Zerocash: Decentralized Anonymous Payments from Bitcoin*, Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP '14). IEEE Computer Society, USA, 2014. P. 459–474. DOI: 10.1109/SP.2014.36.

[11] Virza M., *On deploying succinct zero-knowledge proofs*, Thesis: Ph. D., Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, 2017.

[12] Kosba A., Miller A., Shi E., Wen Z., Papamanthou C., *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, 2016 IEEE Symposium on Security and Privacy (SP). San Jose, CA, 2016. P. 839–858. DOI: 10.1109/SP.2016.55.

[13] Galal H. S., Youssef A. M., *Verifable Sealed-Bid Auction on the Ethereum Blockchain*, Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2019. V. 10958. P. 265–278. DOI: 10.1007/978-3-662-58820-8_18.

[14] Eberhardt J., Tai S., *Eberhardt, J. ZoKrates — Scalable Privacy-Preserving Off-Chain Computations*, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, NS, Canada, 2018. P. 1084–1091. DOI: 10.1109/Cybermatics_2018.2018.00199.

[15] Ben-Sasson E., Bentov I., Horesh Y., Riabzev M., *Scalable, transparent, and post-quantum secure computational integrity*, IACR Cryptology ePrint Archive. 2018.

[16] Rivest R. L., Adleman L., Dertouzos M. L., *On data banks and privacy homomorphisms*, Foundations of Secure Computation. Academia Press, 1978. P. 169–179.

[17] Bernabe J. B., Canovas J. L., Hernandez-Ramos J. L., Moreno R. T., Skarmeta A., *Privacy-Preserving Solutions for Blockchain: Review and Challenges*, IEEE Access. 2019, V. 7. P. 164908–164940. DOI: 10.1109/ACCESS.2019.2950872.

[18] Pedersen T. P., *Non-interactive and information-theoretic secure verifiable secret sharing*, Advances in Cryptology — CRYPTO '91. CRYPTO 1991. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 1992. V. 576. P. 129–140. DOI: 10.1007/3-540-46766-1_9.

[19] Bunz B., Bootle J., Boneh D., Poelstra A., Wuille P., Maxwell G., *Bulletproofs: Short Proofs for Confidential Transactions and More*, 2018 IEEE Symposium on Security and Privacy. San Francisco, CA, 2018. P. 315–334. DOI: 10.1109/SP.2018.00020.

[20] Narula N.,Vasquez W., Virza M., *zkLedger: Privacy-Preserving Auditing for Distributed Ledgers*, Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation (NSDI'18). USENIX Association, Renton, WA, USA, 2018. P. 65–80.

[21] Paillier P., *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, Advances in Cryptology — EUROCRYPT '99. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 1999. V. 1592. P. 223–238. DOI: 10.1007/3-540-48910-X_16.

[22] Wang Q., Qin B., Hu J., Xiao F., *Preserving transaction privacy in bitcoin*, Future Generation Computer Systems. 2020. V. 107. P. 793–804. DOI: 10.1016/j.future.2017.08.026.

[23] Yao A. C., *Protocols for secure computations*, 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982). Chicago, IL, USA, 1982. P. 160–164. DOI: 10.1109/SFCS.1982.38.

[24] Yao A. C., *How to generate and exchange secrets*, 27th Annual Symposium on Foundations of Computer Science (sfcs 1986). Toronto, ON, Canada, 1986. P. 162–167. DOI: 10.1109/SFCS.1986.25.

[25] Goldreich O., Micali S., Wigderson A., *How to play any mental game or A completeness theorem for protocols with honest majority*, Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC '87). Association for Computing Machinery, New York, NY, USA, 1987. P. 218–229. DOI: 10.1145/28395.28420.

[26] Zhang R., Xue R., Liu L., *Security and Privacy on Blockchain*, ACM Computing Surveys. 2019. V. 52. N. 3. DOI: 10.1145/3316481.

[27] Andrychowicz M., Dziembowski S., Malinowski D., Mazurek L., *Secure multiparty computations on bitcoin*, 2014 IEEE Symposium on Security and Privacy. San Jose, CA, 2014. P. 443–458. DOI: 10.1109/SP.2014.35.

[28] Shrobe H., Shrier D. L., Pentland A., *New Solutions for Cybersecurity*, MIT Press, 2018. P. 425–454.

[29] Benhamouda F., Halevi S., Halevi T., *Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation*, 2018 IEEE International Conference on Cloud Engineering (IC2E). Orlando, FL, 2018. P. 357–363. DOI: 10.1109/IC2E.2018.00069.

[30] Chaum D., van Heyst E., *Group Signatures*, Advances in Cryptology — EUROCRYPT '91. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 1991. V. 547. P. 257–265. DOI: 10.1007/3-540-46416-6_22.

[31] Zhang L., Li H., Li Y., Yu Y, Au M. H., Wang B., *An efficient linkable group signature for payer tracing in anonymous cryptocurrencies*, Future Generation Computer Systems. 2019. V. 101. P. 29–38. DOI: 10.1016/j.future.2019.05.081.

[32] Rivest R. L., Shamir A., Tauman Y., *How to Leak a Secret*, Advances in Cryptology — ASIACRYPT 2001. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2001. V. 2248. P. 552–565. DOI: 10.1007/3-540-45682-1_32.

[33] Fujisaki E., Suzuki K., *Traceable Ring Signature*, Public Key Cryptography — PKC 2007. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2007. V. 4450. P. 181–200. DOI: 10.1007/978-3-540-71677-8_13.

[34] Fujisaki E., *Sub-linear Size Traceable Ring Signatures without Random Oracles*, Topics in Cryptology — CT-RSA 2011. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2011. V. 6558. P. 393–415. DOI: 10.1007/978-3-642-19074-2_25.

[35] Cheng R., Zhang F., Kos J., He W., Hynes N., Johnson N., Juels A., Miller A., Song D., *Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts*, 2019 IEEE European Symposium on Security and Privacy (EuroS&P). Stockholm, Sweden, 2019. P. 185–200. DOI: 10.1109/EuroSP.2019.00023.

[36] Bowman M., Miele A., Steiner M., Vavala B., *Private Data Objects: an Overview*, ArXiv e-prints. 2018. https://arxiv.org/abs/1807.05686.

[37] Brandenburger M., Cachin C., Kapitza R., Sorniotti A., *Blockchain and Trusted Computing: Problems, Pitfalls, and a Solution for Hyperledger Fabric*, ArXiv e-prints. 2018. https://arxiv.org/abs/1805.08541.

[38] Fernandez-Carames T. M., Fraga-Lamas P., *Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks*, IEEE Access. 2020. V. 8. P. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.

[39] Raikwar M., Gligoroski D. Kralevska K., *SoK of Used Cryptography in Blockchain*, IEEE Access. 2019. V. 7. P. 148550–148575. DOI: 10.1109/ACCESS.2019.2946983.

Kondyrev Dmitriy Olegovich,
Sobolev Institute of Mathematics, Novosibirsk State University, Laboratory of Cryptography JetBrains Research.
Novosibirsk, Pirogova st., 1.
Email: dkondyrev@gmail.com.

IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 2, pp. 292–313. DOI:10.46586/tosc.v2021.i2.292-313

Maximums of the Additive Differential Probability of Exclusive-Or

Nicky Mouha[1], Nikolay Kolomeec[2], Danil Akhtiamov[3], Ivan Sutormin[2], Matvey Panferov[4], Kseniya Titova[4], Tatiana Bonich[4], Evgeniya Ishchukova[5], Natalia Tokareva[2] and Bulat Zhantulikov[4]

[1] Strativia, Largo, MD, USA, nicky@mouha.be
[2] Sobolev Institute of Mathematics, Novosibirsk, Russia, {kolomeec,tokareva}@math.nsc.ru
[3] The Hebrew University of Jerusalem, Jerusalem, Israel, akhtyamoff1997@gmail.com
[4] Novosibirsk State University, Novosibirsk, Russia, ivan.sutormin@gmail.com,sitnich@gmail.com,{m.panferov,t.bonich,b.zhantulikov}@g.nsu.ru
[5] Southern Federal University, Taganrog, Russia, uaishukova@sfedu.ru

Abstract. At FSE 2004, Lipmaa et al. studied the additive differential probability $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ of exclusive-or where differences $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ are expressed using addition modulo 2^n. This probability is used in the analysis of symmetric-key primitives that combine XOR and modular addition, such as the increasingly popular Addition-Rotation-XOR (ARX) constructions. The focus of this paper is on maximal differentials, which are helpful when constructing differential trails. We provide the missing proof for Theorem 3 of the FSE 2004 paper, which states that $\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ for all γ. Furthermore, we prove that there always exist either two or eight distinct pairs α, β such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and we obtain recurrence formulas for calculating $\mathrm{adp}^{\oplus}$. To gain insight into the range of possible differential probabilities, we also study other properties such as the minimum value of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and we find all γ that satisfy this minimum value.

Keywords: Differential cryptanalysis · ARX · XOR · modular addition

1 Introduction

Differential cryptanalysis [BS91] is a well-known statistical method for the analysis of symmetric-key primitives. The main idea is to see how a difference ΔX between two inputs (e. g., plaintexts) propagates to a difference ΔY between the corresponding outputs (e. g., ciphertexts). The ordered pair $(\Delta X, \Delta Y)$ is referred to as a differential. A differential trail is defined as a sequence $(\Delta X, \Delta X_2, \ldots, \Delta X_{p-1}, \Delta Y)$ where $\Delta X_2, \ldots, \Delta X_{p-1}$ are some intermediate values that appear in the primitive.

A common technique to construct a differential trail is to use a "greedy" strategy to pick the intermediate differences that have the highest differential probability. Under some assumptions, the probabilities of a differential trail can be multiplied together to obtain a good estimate of the probability of a differential.

However, this presupposes that the maximal differential probabilities of elementary operations can be efficiently calculated. For ciphers based on S-boxes, this is rather straightforward: their size is usually small enough so that all input and output differences can be enumerated in a Difference Distribution Table (DDT).

However, this is often not the case for Addition-Rotation-XOR (ARX) constructions, where the addition modulo 2^n can have $n = 32$ or $n = 64$, thereby making it infeasible to

Received: 2020-11-23 Revised: 2021-03-01 Accepted: 2021-05-01 Published: 2021-06-11

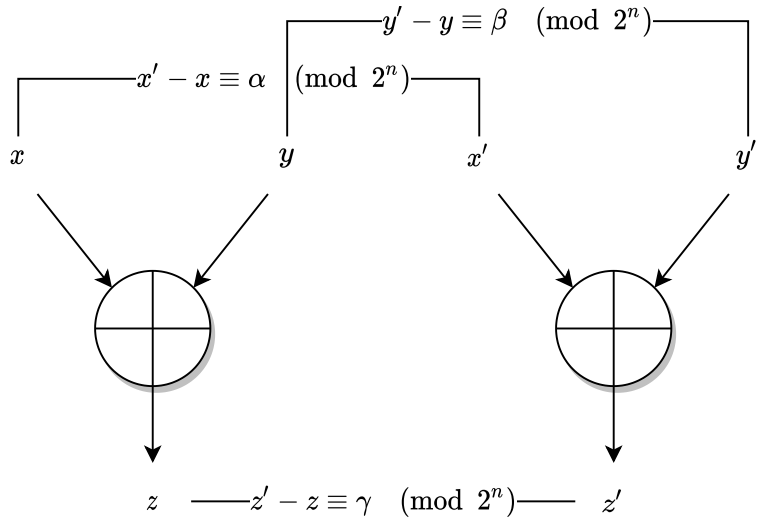


Figure 1: The differential probability $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ of exclusive-or when differences are represented using differences α, β, γ are expressed using addition modulo 2^n. The probability is obtained by averaging over all values of x and y.

construct a DDT. Two of the five finalists of the NIST SHA-3 hash function competition are ARX constructions: BLAKE [AMPH14] which uses either 32-bit or 64-bit additions (depending on the length of the hash value), and Skein [FLS+09] which uses 64-bit additions.

The differential probability $\mathrm{adp}^{\oplus}$ of exclusive-or (XOR) when differences are expressed using addition modulo 2^n was studied at FSE 2004 by Lipmaa et al. [LWD04]. It is defined as $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \Pr_{x,y \in \mathbb{F}_2^n}[(x + \alpha) \oplus (y + \beta) = \gamma + (x \oplus y)]$, and illustrated in Fig. 1.

Lipmaa et al. showed that $\mathrm{adp}^{\oplus}$ can be expressed as a rational series. That is, if we define $\omega_i = 4\alpha_i + 2\beta_i + \gamma_i$, then (as we will recall in Sect. 3) there are eight 8-dimensional square matrices A_j, a column vector C, and a row vector L, such that

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = L \cdot A_{\omega_{n-1}} \cdot \ldots \cdot A_{\omega_0} \cdot C,$$

here ω_i, i. e., which matrix is used as the i-th term of the product, depends on $\alpha_i, \beta_i, \gamma_i$. This formula allows us to easily calculate the probability given a differential $(\alpha, \beta \to \gamma)$.

Lipmaa et al. point out in their FSE 2004 paper [LWD04] that "many of the enumerative aspects of $\mathrm{adp}^{\oplus}$ seem infeasible," but nevertheless provide a theorem related to the maximal differential probability when the output difference γ is fixed. More specifically, Theorem 3 of their paper states that for all output differences γ,

$$\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Unfortunately, this theorem is not proven in the FSE 2004 paper, and communication with one of the authors revealed that the proof has been lost. Therefore, it is interesting to know whether the theorem is correct (or if there exists a counterexample), and the proof techniques may allow us to better understand $\mathrm{adp}^{\oplus}$ and help to prove other properties.

Outline. This paper is organized as follows. We give an overview of related work in Sect. 2. Sect. 3 provides some basic definitions. In Sect. 4, we give some useful argument symmetries for $\mathrm{adp}^{\oplus}$: the order of the arguments does not matter for $\mathrm{adp}^{\oplus}$, and the probability is unchanged under certain transformations of the arguments. In Sect. 5, we finally provide a proof of Theorem 3 of the FSE 2004 paper [LWD04]. Sect. 6 shows that

there are either eight (if $\gamma \notin \{0, 2^{n-1}\}$) or two (otherwise) distinct pairs (α, β) such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. Recurrence formulas for an arbitrary $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ are obtained in Sect. 7. Sect. 8 focuses on properties of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$: a simplified matrix form by 2×2 matrices is proven; we find the minimum value of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and obtain all γ that satisfy this minimum value. Lastly, we calculate the sum of all $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, and conclude the paper in Sect. 9 along with some suggestions for future work.

2 Related Work

At the Dagstuhl "Symmetric Cryptography" seminar in January 2009, Weinmann introduced the term AXR for symmetric-key primitives based on additions modulo 2^n, XORs and rotations. Later at the FSE 2009 rump session, he renamed the term to ARX. The design strategy, however, is much older: perhaps the earliest example of an ARX primitive is the block cipher FEAL [SM88] (Fast Data Encipherment Algorithm), introduced at EUROCRYPT 1987.

More recent examples of ARX ciphers include the eSTREAM finalist Salsa20 [Ber05], the ChaCha [Ber08] stream cipher included in the Transport Layer Security (TLS) protocol version 1.3, the block cipher Speck [BSS+13] (standardized as ISO/IEC 29167-22), the CHAM block cipher [KRK+17] (which has been revised to increase the number of rounds [RKJ+19]), and several submissions to the NIST lightweight cryptography project including COMET [GJN19] (which relies on SPECK and CHAM), SNEIK [Saa19], and Sparkle [BBCdS+20b].

To apply differential cryptanalysis to an ARX primitive, one approach is to use XOR differences: these differences pass through rotation and XOR operations with probability one, and formulas for the differential probability xdp^{+} of the modular addition were provided at FSE 2001 by Lipmaa et al. [LM01].

In this paper, however, we are interested in differences that are expressed using addition modulo 2^n. These differences go through the modular addition with probability one. The additive differential probability of rotation was studied by Berson [Ber92], and Lipmaa et al. [LWD04] provided a formula for $\mathrm{adp}^{\oplus}$, the additive differential probability of XOR.

Using Lipmaa et al.'s expression for $\mathrm{adp}^{\oplus}$, Velichkov et al. [VMDCP12, App. C] provided a search algorithm to list the output differences γ that maximize $\mathrm{adp}^{\oplus}$ for a given (α, β). Although this search algorithm can be very helpful, it cannot be used to provide general statements that hold for any value of n. At FSE 2011, Velichkov et al. [VMDCP11] explained how to calculate the additive differential probability of one ARX operation. Sun et al. [SHW+16] showed how to model $\mathrm{adp}^{\oplus}$ using the Mixed-Integer Linear Programming (MILP) approach for differential cryptanalysis [MWGP11].

Compared to additive differences, XOR differences not only propagate through two operations with probability one (XOR and rotation) instead of only one operation (addition). Another advantage of using XOR differences over additive differences is that the differential probabilities have simpler expressions (see Lipmaa et al. [LWD04, Table 3]). Lipmaa et al. [LWD04] pointed out that the number of possible differentials is larger for $\mathrm{adp}^{\oplus}$ than for xdp^{+}, but the average possible differential has a smaller probability.

Despite the advantages of using XOR differences, there are ciphers for which additive differences may be more appropriate. For example, when Biryukov and Velichkov [BV14] provided a differential cryptanalysis using additive differences for TEA [WN94] and Raiden [PHCER08]; they argued that additive differences are more appropriate given that round keys and round constants are added (instead of XORed), and that there is a higher number of add operations compared to XOR operations in one round. In similar spirit, when SPARX and LAX were proposed by Dinu et al. [DPU+16], and when Beierle et al. [BBCdS+20a] introduced the ARX-based S-box called Alzette (used in CRAX,

TRAX and Sparkle) [BBCdS+20a], they provided some rationale of why their designs resist differential attacks using additive differences.

Lastly, we would like to point out that care should be taken when multiplying probabilities of differentials. For example, in the differential cryptanalysis of XTEA [NW97] by Hong et al. [HHK+03] using XOR differences, the authors constructed a three-round iterative trail $(\alpha, 0) \to (\alpha, 0)$, where $\alpha = \texttt{0x80402010}$. The trail contains two consecutive addition operations, which separately have probabilities $\mathrm{xdp}^+(\alpha, 0 \to \alpha) = 2^{-3}$ and $\mathrm{xdp}^+(\alpha, \alpha \to 0) = 2^{-3}$. Hong et al. found that the joint probability $\mathrm{xdp}^+(\alpha, 0, \alpha \to 0)$ is higher than the product of the two probabilities $2^{-3} \cdot 2^{-3} = 2^{-6}$, and estimated the probability to be $2^{-4.755}$. Mouha et al. [MVDCP11, Sect. 3.6] revisited this problem by correctly calculating the XOR-differential probability of the three-input addition as 2^{-3}, which can be trivially confirmed using the commutative property of addition: $\mathrm{xdp}^+(\alpha, \alpha \to 0) \cdot \mathrm{xdp}^+(0, 0 \to 0) = 2^{-3} \cdot 1 = 2^{-3}$.

Mutatis mutandis, a similar observation also holds when analyzing, for example, the two consecutive XOR operations in one round of TEA using additive differences: calculating the differential probabilities of each XOR operation separately using the formulas in this paper and multiplying them, may not lead to a correct estimate. Therefore, some caution is needed when applying the results in this paper to differential trails of an ARX primitive. We consider these issues to be outside the scope of this paper, but we mention the analysis of larger components as a suggestion for future work in Sect. 9.

3 Definitions

Let G, H be abelian groups and $f : G \to H$ be a function. *A differential* of f is a pair $(\alpha, \beta) \in G \times H$ denoted by $\alpha \to \beta$, where f maps some $x, x + \alpha \in G$ to $f(x), f(x) + \beta \in H$ respectively. *The differential probability* is defined as

$$\mathrm{dp}^f(\alpha \to \beta) = \Pr_{x \in G}[f(x + \alpha) = f(x) + \beta].$$

In this work, we consider the additive differential probability $\mathrm{adp}^{\oplus}$ of exclusive-or, i. e., $G = H = \mathbb{Z}_{2^n}$ and the function $f(x, y) = x \oplus y$ in two arguments. In other words,

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \Pr_{x,y \in \mathbb{F}_2^n}[(x + \alpha) \oplus (y + \beta) = \gamma + (x \oplus y)].$$

For convenience, we denote that $x, y, \alpha, \beta, \gamma \in \mathbb{F}_2^n$, i. e., they are elements of the n-dimensional vector space over the two-element field. In this context, $x + y$, $x - y$ and $-x$ mean $x' + y' \mod 2^n$, $x' - y' \mod 2^n$ and $-x' \mod 2^n$ respectively, where $x' = x_0 + x_1 2^1 + ... + x_{n-1} 2^{n-1}$ (the same for y'), i. e., x is a binary representation of the integer $x' \in \{0, \ldots, 2^n - 1\}$. Note that the coordinates of $x \in \mathbb{F}_2^n$ start with 0: $x = (x_0, x_1, \ldots, x_{n-1})$.

Working with $\mathbb{F}_2^n$, we denote the XOR operation by $x \oplus y$. Also, we define

$$\overline{x} = (x_0 \oplus 1, x_1 \oplus 1, \ldots, x_{n-1} \oplus 1).$$

By 0^n and 1^n we denote $(0, \ldots, 0)$ and $(1, \ldots, 1) \in \mathbb{F}_2^n$ respectively. We will often use integers, e. g., 0 and 2^{n-1}, instead of elements of $\mathbb{F}_2^n$ if n is clear from the context.

There is a matrix (or rational series) approach for calculating $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma), \alpha, \beta, \gamma \in \mathbb{F}_2^n$. Let $e_0, \ldots, e_7$ be standard basis vectors of $\mathbb{Q}^8$ (they are vector-columns).

Theorem 1 (Lipmaa et al. [LWD04]). *Let* $L = (1, 1, 1, 1, 1, 1, 1, 1)$, $A_0, \ldots, A_7$ *be* 8×8

matrices, where

$$A_0 = \frac{1}{4}\begin{pmatrix} 4 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $A_k = ((A_k)_{i,j}) = ((A_0)_{i\oplus k, j\oplus k})$*, here* $i, j, k \in \mathbb{F}_2^3$*. Then*

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\omega) = LA_{\omega_{n-1}} A_{\omega_{n-2}} \dots A_{\omega_0} e_0,$$

where the differential $(\alpha, \beta \to \gamma)$ *is written as the octal word* $\omega = \omega_{n-1} \dots \omega_0$ *with* $\omega_i = \omega_i(\alpha, \beta, \gamma) = 4\alpha_i + 2\beta_i + \gamma_i$*. For convenience, the matrices* $A_0, ..., A_7$ *are given below.*

$$A_0 = \frac{1}{4}\begin{pmatrix} 4&0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&0&0 \\ 0&0&0&1&0&0&1&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0 \end{pmatrix} \quad A_1 = \frac{1}{4}\begin{pmatrix} 0&0&1&0&1&0&0&0 \\ 0&4&1&0&1&0&0&1 \\ 0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1 \end{pmatrix} \quad A_2 = \frac{1}{4}\begin{pmatrix} 0&1&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&1&4&0&1&0&0&1 \\ 0&1&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&1 \end{pmatrix} \quad A_3 = \frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&1&0 \\ 1&0&0&4&0&1&1&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&1&0 \end{pmatrix}$$

$$A_4 = \frac{1}{4}\begin{pmatrix} 0&1&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&1&1&0&4&0&0&1 \\ 0&1&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&1 \\ 0&0&0&0&0&0&0&1 \end{pmatrix} \quad A_5 = \frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&0&1&0 \\ 1&0&0&1&0&4&1&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&1&0 \end{pmatrix} \quad A_6 = \frac{1}{4}\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0 \\ 1&0&0&1&0&1&4&0 \\ 0&0&0&1&0&1&0&0 \end{pmatrix} \quad A_7 = \frac{1}{4}\begin{pmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&1&0&0&1&0&0&0 \\ 0&0&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0&4 \end{pmatrix}$$

Note that we consider coordinates $\{0, \dots, 7\}$ in terms of $\mathbb{Z}_{2^3}$ and $\mathbb{F}_2^3$ by their binary representations too. By the matrix approach it is easy to check (see [LWD04]) that

Lemma 1. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > 0$ *if and only if the first (i. e., least significant) nonzero coordinate of* $\omega(\alpha, \beta, \gamma)$ *is equal to* $3, 5$ *or* 6*.*

Lemma 2. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ *equal to either* 0 *or* 1 *for* $\alpha, \beta, \gamma \in \mathbb{F}_2$ *and equal to either* 0 *or* $\frac{1}{2}$ *or* 1 *for* $\alpha, \beta, \gamma \in \mathbb{F}_2^2$*.*

Lemma 3. *We have* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$ *if and only if* $\omega(\alpha, \beta, \gamma) = v0^*$*, where* $v \in \{0, 3, 5, 6\}$*.*

4 Argument Symmetries of $\mathrm{adp}^{\oplus}$

First, we list several argument symmetries of $\mathrm{adp}^{\oplus}$.

Proposition 1. *The function* $\mathrm{adp}^{\oplus}$ *is symmetric, i. e., for any* $\alpha, \beta, \gamma \in \mathbb{F}_2^n$*, it holds that*

$$\begin{aligned} &\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \gamma \to \alpha) \\ = \ &\mathrm{adp}^{\oplus}(\gamma, \beta \to \alpha) = \mathrm{adp}^{\oplus}(\gamma, \alpha \to \beta) = \mathrm{adp}^{\oplus}(\alpha, \gamma \to \beta). \end{aligned}$$

Proof. We have $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma)$ by definition. Furthermore,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y \in \mathbb{F}_2^n}[((x+\alpha) \oplus (y+\beta)) - (x \oplus y) = \gamma] \\
&= \Pr_{x,y \in \mathbb{F}_2^n}[((x+\alpha) \oplus (y+\beta)) = (x \oplus y) + \gamma] \\
&= \Pr_{x,y \in \mathbb{F}_2^n}[((x+\alpha) \oplus (y+\beta)) \oplus ((x \oplus y) + \gamma) = 0] \\
&= \Pr_{z=x \oplus y, y \in \mathbb{F}_2^n}[((z \oplus y) + \alpha) \oplus (y+\beta) \oplus (z+\gamma) = 0] \\
&= \Pr_{z,y \in \mathbb{F}_2^n}[(z+\gamma) \oplus (y+\beta) = (z \oplus y) + \alpha] \\
&= \Pr_{z,y \in \mathbb{F}_2^n}[(z+\gamma) \oplus (y+\beta) - (z \oplus y) = \alpha] \\
&= \mathrm{adp}^{\oplus}(\gamma, \beta \to \alpha).
\end{aligned}$$

Note that all other argument permutations are combinations of these two. □

Proposition 2. *For any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ it holds that*

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha + 2^{n-1}, \beta + 2^{n-1} \to \gamma) = \mathrm{adp}^{\oplus}(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1} \to \gamma),$$

in light of Proposition 1, we can add 2^{n-1} to any two arguments.

Proof. It is easy to see that $\alpha + 2^{n-1} = \alpha \oplus 2^{n-1}$, therefore, $\alpha + x + 2^{n-1} = (\alpha + x) \oplus 2^{n-1}$, where $x \in \mathbb{F}_2^n$. Thus,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y \in \mathbb{F}_2^n}[((x+\alpha) \oplus (y+\beta)) - (x \oplus y) = \gamma] \\
&= \Pr_{x,y \in \mathbb{F}_2^n}[\big((x+\alpha) \oplus 2^{n-1} \oplus (y+\beta) \oplus 2^{n-1}\big) - (x \oplus y) = \gamma] \\
&= \Pr_{x,y \in \mathbb{F}_2^n}[\big((x+\alpha+2^{n-1}) \oplus (y+\beta+2^{n-1})\big) - (x \oplus y) = \gamma] \\
&= \mathrm{adp}^{\oplus}(\alpha + 2^{n-1}, \beta + 2^{n-1} \to \gamma).
\end{aligned}$$

□

Proposition 3. *For any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ it holds that* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to -\gamma)$. *In light of Proposition 1, we can replace by "$-$" any argument without changing the value of* $\mathrm{adp}^{\oplus}$.

Proof. First, we prove that

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) &= \Pr_{x,y \in \mathbb{F}_2^n}[((x+\alpha) \oplus (y+\beta)) - (x \oplus y) = \gamma] \\
&= \Pr_{x,y \in \mathbb{F}_2^n}[(x \oplus y) - ((x+\alpha) \oplus (y+\beta)) = -\gamma] \\
&= \Pr_{x'=x+\alpha, y'=y+\beta \in \mathbb{F}_2^n}[((x'-\alpha) \oplus (y'-\beta)) - (x' \oplus y') = -\gamma] \\
&= \mathrm{adp}^{\oplus}(-\alpha, -\beta \to -\gamma). \qquad (1)
\end{aligned}$$

For further calculations we will use that $\overline{x+y} = \overline{x} - y$. To confirm this, we have

$$-x = 2^n - x = ((2^n - 1) - x) + 1 = \overline{x} + 1. \qquad (2)$$

Therefore, $\overline{x} = -x - 1$ and

$$\overline{x+y} = -(x+y) - 1 = (-x-1) - y = \overline{x} - y.$$

Next, we prove that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma)$:

$$\begin{aligned}
\mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma) &= \Pr_{x,y \in \mathbb{F}_2^n}[((x-\alpha) \oplus (y-\beta)) - (x \oplus y) = \gamma] \\
&= \Pr_{x'=\overline{x}, y'=\overline{y} \in \mathbb{F}_2^n}[\big((\overline{x'}-\alpha) \oplus (\overline{y'}-\beta)\big) - (\overline{x'} \oplus \overline{y'}) = \gamma] \\
&= \Pr_{x',y' \in \mathbb{F}_2^n}[\big(\overline{x'+\alpha} \oplus \overline{y'+\beta}\big) - (\overline{x'} \oplus \overline{y'}) = \gamma] \\
&\overset{u \oplus v = \overline{u} \oplus \overline{v}}{=} \Pr_{x',y' \in \mathbb{F}_2^n}[((x'+\alpha) \oplus (y'+\beta)) - (x' \oplus y') = \gamma] \\
&= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma). \qquad (3)
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha, \beta \to -\gamma) &\overset{(1)}{=} \mathrm{adp}^{\oplus}(-\alpha, -\beta \to -(-\gamma)) \\
&= \mathrm{adp}^{\oplus}(-\alpha, -\beta \to \gamma) \\
&\overset{(3)}{=} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma). \qquad \square
\end{aligned}$$

5 Maximum of $\mathrm{adp}^{\oplus}(x, y \to \gamma)$ for Fixed γ

In this section we give the missing proof of Theorem 3 from [LWD04]: we will prove that

$$\max_{\alpha,\beta \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Let us define

$$A'_t = \begin{cases} A_0, & \text{if } t \text{ is even} \\ A_3, & \text{if } t \text{ is odd} \end{cases} \quad \text{and} \quad \overline{A'_t} = \begin{cases} A_3, & \text{if } t \text{ is even} \\ A_0, & \text{if } t \text{ is odd} \end{cases}.$$

Then

$$\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = LA'_{\omega_{n-1}} \dots A'_{\omega_0} e_0 \text{ for any } \omega = \omega(\alpha, \beta, \gamma).$$

Lemma 4. *For any octal word $\omega_n \dots \omega_0$, where $n \geq 0$, and $0 \leq k \leq 7$ the following holds:*

$$LA_{\omega_n} \dots A_{\omega_0} e_k = LA_{\omega_n \oplus k} \dots A_{\omega_0 \oplus k} e_0.$$

Proof. Let us denote by T_k the 8×8 involution matrix that swaps the i and $i \oplus k$ coordinates, $i = 0, \dots, 7$. Then

$$\begin{aligned}
LA_{\omega_n} \dots A_{\omega_0} e_k &= (LT_k) A_{\omega_n} \dots A_{\omega_0} (T_k e_0) \\
&= L(T_k A_{\omega_n} T_k)(T_k A_{\omega_{n-1}} T_k) \dots (T_k A_{\omega_0} T_k) e_0 \\
&= LA_{\omega_n \oplus k} \dots A_{\omega_0 \oplus k} e_0,
\end{aligned}$$

since $(T_k A_m T_k)_{ij} = (A_m)_{i \oplus k, j \oplus k} = (A_0)_{i \oplus m \oplus k, j \oplus m \oplus k} = (A_{m \oplus k})_{ij}$ and T_k^2 is the identity matrix. $\square$

Note that $A'_{\omega_i \oplus k} = A'_{\omega_i}$ for even k (as an integer number, i. e., for $k = 0, 2, 4, 6$) and $A'_{\omega_i \oplus k} = \overline{A'_{\omega_i}}$ for odd k.

Theorem 2. *For any $\gamma \in \mathbb{F}_2^n$, we have*

$$\max_{\alpha,\beta \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

Proof. Let us use induction by n. The base case of the induction, $n = 1$, follows from Lemma 2: it holds that $\mathrm{adp}^{\oplus}(0, 0 \to 0) = \mathrm{adp}^{\oplus}(0, 1 \to 1) = 1$.

Suppose that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ for any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$. This means that

$$LA_{v_{n-1}} \dots A_{v_0} e_0 \leq LA'_{v_{n-1}} \dots A'_{v_0} e_0$$

for any octal word v of length n. Let us prove that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, where $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$, i. e.,

$$LA_{\omega_n} \dots A_{\omega_0} e_0 \leq LA'_{\omega_n} \dots A'_{\omega_0} e_0$$

for any octal word ω of length $n+1$. We consider four cases for A_{ω_0}, the first two of them are very easy.

Case $A_{\omega_0} \in \{A_1, A_2, A_4, A_7\}$:

$$LA_{\omega_n} \dots A_{\omega_0} e_0 \overset{\text{Lemma 1}}{=} 0 < LA'_{\omega_n} \dots A'_{\omega_0} e_0.$$

Case $A_{\omega_0} = A_0$, i. e., $A'_{\omega_0} = A_0$:

$$\begin{aligned} LA_{\omega_n} \dots A_{\omega_0} e_0 &= LA_{\omega_n} \dots A_{\omega_1} e_0 \\ &\overset{\text{induction}}{\leq} LA'_{\omega_n} \dots A'_{\omega_1} e_0 \\ &= LA'_{\omega_n} \dots A'_{\omega_0} e_0. \end{aligned}$$

Case $A_{\omega_0} = A_6$, i. e., $A'_{\omega_0} = A_0$. It is easy to see that

$$A_6 e_0 = \frac{1}{4} e_0 + \frac{1}{4} e_2 + \frac{1}{4} e_4 + \frac{1}{4} e_6.$$

Also, if $\omega_1 \in \{0, 3, 5, 6\}$, $LA_{\omega_n} \dots A_{\omega_1}(e_2 + e_4) = 0$; otherwise $LA_{\omega_n} \dots A_{\omega_1}(e_0 + e_6) = 0$. Indeed, $A_{\omega_1} e_2 = A_{\omega_1} e_4 = 0$ if $\omega_1 \in \{0, 3, 5, 6\}$ and $A_{\omega_1} e_0 = A_{\omega_1} e_6 = 0$ if $\omega_1 \in \{1, 2, 4, 7\}$. Thus, we can deduce that

$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_{p_1} + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_{p_2},$$

where p_1 and p_2 are even. According to Lemma 4,

$$\begin{aligned} LA_{\omega_n} \dots A_{\omega_0} e_0 &= \frac{1}{4} LA_{\omega_n \oplus p_1} \dots A_{\omega_1 \oplus p_1} e_0 + \frac{1}{4} LA_{\omega_n \oplus p_2} \dots A_{\omega_1 \oplus p_2} e_0 \\ &\overset{\text{induction}}{\leq} \frac{1}{4} LA'_{\omega_n \oplus p_1} \dots A'_{\omega_1 \oplus p_1} e_0 + \frac{1}{4} LA'_{\omega_n \oplus p_2} \dots A'_{\omega_1 \oplus p_2} e_0. \end{aligned}$$

Taking into account that both $\omega_i \oplus p_1$ and $\omega_i \oplus p_2$ are even if and only if ω_i is even (as an integer number), we have $A'_{\omega_i \oplus p_j} = A'_{\omega_i}$ (here $i \in \{1, \dots, n\}$, $j \in \{1, 2\}$). Therefore,

$$\begin{aligned} LA_{\omega_n} \dots A_{\omega_0} e_0 &\leq \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 \\ &= \frac{1}{2} LA'_{\omega_n} \dots A'_{\omega_1} e_0. \end{aligned}$$

Finally, let us calculate $LA'_{\omega_n} \dots A'_{\omega_0} e_0$. Recall that $A'_{\omega_0} = A_0$ for the case that we are considering here, and that $A_0 e_0 = e_0$, so that:

$$\begin{aligned} LA'_{\omega_n} \dots A'_{\omega_0} e_0 &= LA'_{\omega_n} \dots A'_{\omega_1} e_0 \\ &> \frac{1}{2} LA'_{\omega_n} \dots A'_{\omega_1} e_0 \\ &\geq LA_{\omega_n} \dots A_{\omega_0} e_0. \end{aligned} \tag{4}$$

Case $A_{\omega_0} \in \{A_3, A_5\}$, i. e., $A'_{\omega_0} = A_3$. It is easy to see that

$$A_3 e_0 = \frac{1}{4}e_0 + \frac{1}{4}e_1 + \frac{1}{4}e_2 + \frac{1}{4}e_3,$$
$$A_5 e_0 = \frac{1}{4}e_0 + \frac{1}{4}e_1 + \frac{1}{4}e_4 + \frac{1}{4}e_5.$$

Note that $LA_{\omega_n} \dots A_{\omega_1} e_j = 0$ for

- $\omega_1 \in \{0, 3, 5, 6\}$ and $j \notin \{0, 3, 5, 6\}$,
- $\omega_1 \notin \{0, 3, 5, 6\}$ and $j \in \{0, 3, 5, 6\}$,

since in these cases $A_{\omega_1} e_j = 0$. The latter was already noted by Lipmaa et al. [LWD04] when they showed by direct computation that the kernels are $\ker A_0 = \ker A_3 = \ker A_5 = \ker A_6 = \langle e_1, e_2, e_4, e_7 \rangle$ and $\ker A_1 = \ker A_2 = \ker A_4 = \ker A_7 = \langle e_0, e_3, e_5, e_6 \rangle$.

Thus, we can deduce that

$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_p + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_q,$$

where p is even and q is odd. Moreover, either $p, q \in \{0, 3, 5, 6\}$ or $p, q \in \{1, 2, 4, 7\}$. Indeed,

- if $\omega_1 \in \{0, 3, 5, 6\}$ and $A_{\omega_0} = A_3$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_0 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_3, \text{ i. e., } p = 0 \text{ and } q = 3;$$
- if $\omega_1 \in \{0, 3, 5, 6\}$ and $A_{\omega_0} = A_5$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_0 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_5, \text{ i. e., } p = 0 \text{ and } q = 5;$$
- if $\omega_1 \notin \{0, 3, 5, 6\}$ and $A_{\omega_0} = A_3$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_1 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_2, \text{ i. e., } p = 2 \text{ and } q = 1;$$
- if $\omega_1 \notin \{0, 3, 5, 6\}$ and $A_{\omega_0} = A_5$,
$$LA_{\omega_n} \dots A_{\omega_0} e_0 = \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_1 + \frac{1}{4} LA_{\omega_n} \dots A_{\omega_1} e_4, \text{ i. e., } p = 4 \text{ and } q = 1.$$

According to Lemma 4,

$$\begin{aligned} LA_{\omega_n} \dots A_{\omega_0} e_0 &= \frac{1}{4} LA_{\omega_n \oplus p} \dots A_{\omega_1 \oplus p} e_0 + \frac{1}{4} LA_{\omega_n \oplus q} \dots A_{\omega_1 \oplus q} e_0 \\ &\overset{\text{induction}}{\leq} \frac{1}{4} LA'_{\omega_n \oplus p} \dots A'_{\omega_1 \oplus p} e_0 + \frac{1}{4} LA'_{\omega_n \oplus q} \dots A'_{\omega_1 \oplus q} e_0. \end{aligned} \tag{5}$$

Taking into account that $\omega_i \oplus p$ is even if and only if ω_i is even and $\omega_i \oplus q$ is even if and only if ω_i is odd, it is easy to see that $A'_{\omega_i \oplus p} = A'_{\omega_i}$ and $A'_{\omega_i \oplus q} = \overline{A'_{\omega_i}}$. Therefore,

$$LA_{\omega_n} \dots A_{\omega_0} e_0 \leq \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} L\overline{A'_{\omega_n}} \dots \overline{A'_{\omega_1}} e_0.$$

To complete the case, let us calculate $LA'_{\omega_n} \dots A'_{\omega_0} e_0$:

$$\begin{aligned} LA'_{\omega_n} \dots A'_{\omega_0} e_0 &= LA'_{\omega_n} \dots A'_{\omega_1} (\frac{1}{4}e_0 + \frac{1}{4}e_3) \\ &\overset{\text{Lemma 4}}{=} \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} LA'_{\omega_n \oplus 3} \dots A'_{\omega_1 \oplus 3} e_0 \\ &= \frac{1}{4} LA'_{\omega_n} \dots A'_{\omega_1} e_0 + \frac{1}{4} L\overline{A'_{\omega_n}} \dots \overline{A'_{\omega_1}} e_0 \\ &\geq LA_{\omega_n} \dots A_{\omega_0} e_0. \end{aligned}$$

This completes the proof of the theorem. □

In light of Proposition 1, it does not matter which argument we fix: $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(\alpha, \alpha \to 0)$ and $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leq \mathrm{adp}^{\oplus}(\beta, \beta \to 0)$ hold too.

6 Number of Maximums of $\mathrm{adp}^{\oplus}$ for Fixed γ

Let us define

$$\mathrm{adpmax}(\gamma) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \mathrm{adp}^{\oplus}(x, y \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)\}, \ \gamma \in \mathbb{F}_2^n.$$

Proposition 4. *Let $\gamma \in \mathbb{F}_2^n$, $\gamma \in \{0, 2^{n-1}\}$. Then $\#\mathrm{adpmax}(\gamma) = 2$. More precisely,*

$$\mathrm{adpmax}(0) = \{(0,0), (2^{n-1}, 2^{n-1})\},$$
$$\mathrm{adpmax}(2^{n-1}) = \{(0, 2^{n-1}), (2^{n-1}, 0)\}.$$

Proof. According to Lemma 3, $\mathrm{adp}^{\oplus}(0, 0 \to 0) = \mathrm{adp}^{\oplus}(0, 2^{n-1} \to 2^{n-1}) = 1$. The lemma also provides the conditions for α, β, γ such that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$:

$$4\alpha_i + 2\beta_i + \gamma_i = 0 \text{ for } 0 \leq i < n-1 \text{ and } 4\alpha_{n-1} + 2\beta_{n-1} + \gamma_{n-1} \in \{0, 3, 5, 6\},$$

i. e., $\alpha_i = \beta_i = \gamma_i = 0$ for $0 \leq i < n-1$ and $(\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1})$ is either $(0,0,0)$ or $(1,1,0)$ or $(1,0,1)$ or $(0,1,1)$. □

Proposition 5. *Let $\gamma \in \mathbb{F}_2^n$, $\gamma \notin \{0, 2^{n-1}\}$. Then the following eight pairs are distinct and belong to* $\mathrm{adpmax}(\gamma)$*:*

$$\begin{array}{llll} (0,\gamma), & (0,-\gamma), & (2^{n-1}, \gamma \oplus 2^{n-1}), & (2^{n-1}, -\gamma \oplus 2^{n-1}), \\ (\gamma,0), & (-\gamma,0), & (\gamma \oplus 2^{n-1}, 2^{n-1}), & (-\gamma \oplus 2^{n-1}, 2^{n-1}). \end{array}$$

Proof. Theorem 2 gives us that $(0, \gamma) \in \mathrm{adpmax}(\gamma)$. The other pairs are provided by Propositions 1, 2 and 3, since $\mathrm{adp}^{\oplus}$ has the same value for these pairs with fixed γ.

Next, we know that $\gamma \notin \{0, 2^{n-1}\}$. Let us divide these pairs into two sets: $P = \{(0,\gamma), (0,-\gamma), (\gamma,0), (-\gamma,0)\}$ and P' contains the other pairs.

Any two pairs from P are distinct, since $\gamma \neq -\gamma$ and $\gamma, -\gamma \neq 0$. The same is true for P': indeed, any pair $(a, b) \in P'$ is equal to $(a' \oplus 2^{n-1}, b' \oplus 2^{n-1})$, where $(a', b') \in P$. This is why any two pairs from P' coincide if and only if the corresponding pairs from P coincide.

At the same time, a pair from P cannot be equal to a pair from P', since at least one coordinate of any pair from P' is equal to 2^{n-1}, but $0, \gamma, -\gamma \neq 2^{n-1}$. □

To prove auxiliary lemmas, we introduce the following notation: for $A \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$, let us define $\mathrm{swap}(A) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : (y, x) \in A\}$. It is clear that $\#\mathrm{swap}(A) = \#A$. Also,

$$\mathrm{perfmax}(\gamma) = \{(x, y) \in \mathrm{adpmax}(\gamma) : (x, \overline{y}) \in \mathrm{adpmax}(\overline{\gamma})\}. \tag{6}$$

Note that $\mathrm{swap}(\mathrm{adpmax}(\gamma)) = \mathrm{adpmax}(\gamma)$, since $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\beta, \alpha \to \gamma)$ by Proposition 1. Therefore,

$$\mathrm{swap}(\mathrm{perfmax}(\gamma)) = \{(x, y) \in \mathrm{adpmax}(\gamma) : (\overline{x}, y) \in \mathrm{adpmax}(\overline{\gamma})\}. \tag{7}$$

Let us list some of their straightforward properties.

Lemma 5. *The following statements hold:*

- $\#\mathrm{perfmax}(\gamma) \leq \min\{\#\mathrm{adpmax}(\gamma), \#\mathrm{adpmax}(\overline{\gamma})\}$*;*
- $(\alpha, \beta) \in \mathrm{perfmax}(\gamma)$ *if and only if* $(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}) \in \mathrm{perfmax}(\gamma)$*.*

Proof. The first point directly follows from the definition. Next, Proposition 2 provides that

$$(\alpha, \beta) \in \mathrm{adpmax}(\gamma) \iff (\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}) \in \mathrm{adpmax}(\gamma),$$
$$(\alpha, \overline{\beta}) \in \mathrm{adpmax}(\overline{\gamma}) \iff (\alpha \oplus 2^{n-1}, \overline{\beta} \oplus 2^{n-1}) \in \mathrm{adpmax}(\overline{\gamma}).$$

The equality $\overline{\beta \oplus 2^{n-1}} = \overline{\beta} \oplus 2^{n-1}$ completes the proof. □

Lemma 6. *Let* $\gamma \in \mathbb{F}_2^n$, $\#\mathrm{adpmax}(\gamma) \leq 8$ *and* $\#\mathrm{adpmax}(\overline{\gamma}) \leq 8$. *Then* $\#\mathrm{perfmax}(\gamma) \leq 2$.

Proof. Let $\gamma \in \{0, 2^{n-1}\}$. Lemma 5 provides that $\#\mathrm{perfmax}(\gamma) \leq \#\mathrm{adpmax}(\gamma)$. At the same time, $\#\mathrm{adpmax}(\gamma) = 2$ by Proposition 4. The case of $\overline{\gamma} \in \{0, 2^{n-1}\}$ is completely identical. Hence, the lemma is proven for these cases.

Let $\gamma, \overline{\gamma} \notin \{0, 2^{n-1}\}$. Note that this excludes the case of $n = 1$. Under the lemma assumption, Proposition 5 describes all 8 distinct pairs from $\mathrm{adpmax}(\gamma)$ (the same for $\mathrm{adpmax}(\overline{\gamma})$). In light of Lemma 5, it is sufficient to prove that at most one pair from $P = \{(0, \gamma), (0, -\gamma), (\gamma, 0), (-\gamma, 0)\} \subseteq \mathrm{adpmax}(\gamma)$ belongs to $\mathrm{perfmax}(\gamma)$, since any of the other four pairs from $\mathrm{adpmax}(\gamma)$ are equal to $(\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1})$, where $(\alpha, \beta) \in P$.

First, we consider $(\gamma, 0)$ and $(-\gamma, 0)$. Since $\gamma \notin \{0, 2^{n-1}\}$ and $n > 1$, we have $\gamma, -\gamma, \overline{0} \notin \{0, 2^{n-1}\}$. But one coordinate of any pair from $\mathrm{adpmax}(\overline{\gamma})$ is always equal to 0 or 2^{n-1}, i. e., both $(\gamma, \overline{0})$ and $(-\gamma, \overline{0})$ do not belong to $\mathrm{adpmax}(\overline{\gamma})$ and, as a consequence, they are not elements of $\mathrm{perfmax}(\gamma)$.

Next, we consider $(\alpha, \beta) = (0, -\gamma)$. Using (2), we obtain

$$\begin{aligned}(\alpha, \overline{\beta}) &= (0, \overline{-\gamma}) \\ &\overset{\overline{x} = -x-1}{=} (0, -(-\gamma) - 1) \\ &\overset{-x = \overline{x}+1}{=} (0, -(\overline{\gamma} + 1) - 1) \\ &= (0, -\overline{\gamma} - 2).\end{aligned}$$

Since $\alpha = 0$, let us consider the first elements of the pairs from $\mathrm{adpmax}(\overline{\gamma})$ described by Proposition 5: none of $\overline{\gamma}$, $-\overline{\gamma}$, $\overline{\gamma} \oplus 2^{n-1}$, $-\overline{\gamma} \oplus 2^{n-1}$, 2^{n-1} is equal to 0 due to $\overline{\gamma} \notin \{0, 2^{n-1}\}$. It means that $(\alpha, \overline{\beta})$ may only be equal to $(0, \overline{\gamma})$ or $(0, -\overline{\gamma})$ from $\mathrm{adpmax}(\overline{\gamma})$.

This implies that γ satisfies one of the two following equalities:

- $-\overline{\gamma} - 2 = -\overline{\gamma}$, which is inconsistent for $n > 1$;
- $-\overline{\gamma} - 2 = \overline{\gamma}$, i. e., $2\overline{\gamma} + k2^n = -2$, where $k \in \mathbb{Z}$ or, equivalently,

  $$\overline{\gamma} = -1 - k2^{n-1}, \text{ where } k = \{0, 1\}, \text{ since } k2^{n-1} \bmod 2^n \in \{0, 2^{n-1}\}.$$

  By again using (2), we have that $\overline{\gamma} = -1 - k2^{n-1} = \overline{k2^{n-1}}$. But $\overline{\gamma} = \overline{k2^{n-1}}$ (where $k = \{0, 1\}$) if and only if $\gamma \in \{0, 2^{n-1}\}$, which is a contradiction.

Thus, only $(0, \gamma)$ and $(2^{n-1}, \gamma \oplus 2^{n-1})$ belong to $\mathrm{perfmax}(\gamma)$. Thereby, the lemma is proven. □

Corollary 1. *Let* $\gamma \in \mathbb{F}_2^n$. *Then* $\#\mathrm{adpmax}(\gamma) \leq 8$.

Proof. Let us use induction by n. The base case of the induction, $n = 1$, is straightforward: the only possible values of γ are 0 and $2^{n-1} = 1$, for which Proposition 4 holds.

We suppose that $\#\mathrm{adpmax}(c) \leq 8$ for any $c \in \mathbb{F}_2^n$. Let us prove that $\#\mathrm{adpmax}(\gamma) \leq 8$ for $\gamma \in \mathbb{F}_2^{n+1}$. We denote $(x_0, \ldots, x_{n-1})$ by x' for $x \in \mathbb{F}_2^{n+1}$.

Case $\gamma_0 = 0$. Let us consider $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. It is easy to see that $\omega_0(\alpha, \beta, \gamma) \notin \{2, 4\}$ (this follows from Case $A_{\omega_0} \in \{A_1, A_2, A_4, A_7\}$ of Theorem 2), and that $\omega_0(\alpha, \beta, \gamma) \neq 6$

(by (4) from the proof of Theorem 2). This means that $\alpha_0 = \beta_0 = 0$. Thus, $\#\mathrm{adpmax}(\gamma) = \#\mathrm{adpmax}(\gamma') \leq 8$ by induction.

Case $\gamma_0 = 1$. We rely on the case $A_{\omega_0} \in \{A_3, A_5\}$ of Theorem 2. Let us consider $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. Like in the previous case, $\omega_0(\alpha, \beta, \gamma) \notin \{1, 7\}$, i. e., we have two variants: 3 or 5. Also, we have two distinct choices for $\omega_1(\alpha, \beta, \gamma)$: it can belong to either $\{0, 3, 5, 6\}$ or $\{1, 2, 4, 7\}$. Recall that p and q depend on this choice. Thus, we have $2 \cdot 2 = 4$ different "branches" for α, β. Let us consider any of them.

Let $p = 4p_1 + 2p_2$ (p is even), $q = 4q_1 + 2q_2 + 1$ (q is odd), where $p_1, p_2, q_1, q_2 \in \{0, 1\}$. Considering the sums $x \oplus p_i$, $x \oplus q_i$, where $x \in \mathbb{F}_2^n$, we mean $x \oplus 0^n$ for $p_i, q_i = 0$ and $x \oplus 1^n$ otherwise.

According to (5), $LA_{\omega_n} \dots A_{\omega_0} e_0 = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ is equal to $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ if and only if

- $LA_{\omega_n \oplus p} \dots A_{\omega_1 \oplus p} e_0 = \mathrm{adp}^{\oplus}(\alpha' \oplus p_1, \beta' \oplus p_2 \to \gamma')$ is equal to $\mathrm{adp}^{\oplus}(0, \gamma' \to \gamma')$ and
- $LA_{\omega_n \oplus q} \dots A_{\omega_1 \oplus q} e_0 = \mathrm{adp}^{\oplus}(\alpha' \oplus q_1, \beta' \oplus q_2 \to \gamma' \oplus 1^n)$ is equal to $\mathrm{adp}^{\oplus}(0, \overline{\gamma'} \to \overline{\gamma'})$.

It means that $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$ if and only if $(\alpha' \oplus p_1, \beta' \oplus p_2) \in \mathrm{adpmax}(\gamma')$ and $(\alpha' \oplus q_1, \beta' \oplus q_2) \in \mathrm{adpmax}(\gamma' \oplus 1) = \mathrm{adpmax}(\overline{\gamma'})$.

Since $p, q \in \{0, 3, 5, 6\}$ or $p, q \in \{1, 2, 4, 7\}$, $(p_1, p_2) \oplus (q_1, q_2) \in \{(0, 1), (1, 0)\}$. Thus, taking $a = \alpha' \oplus p_1$, $b = \beta' \oplus p_2$, we have $(\alpha' \oplus q_1, \beta' \oplus q_2) \in \{(a, \overline{b}), (\overline{a}, b)\}$. In other words, by (6) and (7),

$$\text{either } (a, b) \in \mathrm{perfmax}(\gamma') \text{ or } (a, b) \in \mathrm{swap}(\mathrm{perfmax}(\gamma')).$$

In light of the induction hypothesis, Lemma 6 provides that for the both cases

$$\#\mathrm{perfmax}(\gamma') = \#\mathrm{swap}(\mathrm{perfmax}(\gamma')) \leq 2,$$

i. e., there are at most two distinct pairs (a, b) satisfying the conditions. For any "branch" (a, b) uniquely determines (α, β). Therefore, we have at most $4 \cdot 2$ distinct choices for $(\alpha, \beta) \in \mathrm{adpmax}(\gamma)$. The statement is proven. □

7 Recurrence Formulas for $\mathrm{adp}^{\oplus}$

A matrix approach to calculate $\mathrm{adp}^{\oplus}$ and Lemma 4 allow us to obtain recurrence formulas for $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$. It is possible to rewrite the proof of Theorem 2 in terms of these formulas. First, let us denote the vector $(0, x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_2^{n+1}$ by $x0$, i. e., in terms of integers, $x0 = 2x$. We define $x1$: $x1 = 2x + 1$ in exactly the same way.

Let us prove an auxiliary lemma.

Lemma 7. *Let* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > 0$. *Then* $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$.

Proof. By Lemma 1, $\omega_0 = 4\alpha_0 \oplus 2\beta_0 \oplus \gamma_0 \in \{0, 3, 5, 6\}$, which implies $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$. □

Now we can give the recurrence formulas for $\mathrm{adp}^{\oplus}$.

Theorem 3. *For all $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ the following equalities hold.*

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) &= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 0) &= \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \overline{\beta} \to \gamma)\\
&\quad + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 1) &= \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \overline{\gamma})\\
&\quad + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}) + \frac{1}{4}\mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma),\\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) &= \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma})\\
&\quad + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}),\\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 1) &= \mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 0)\\
&= \mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 1) = 0.
\end{aligned}$$

Note 1. Any of $\overline{\alpha}$, $\overline{\beta}$ and $\overline{\gamma}$ can be replaced by $\alpha + 1$, $\beta + 1$ and $\gamma + 1$, respectively. Indeed, $\overline{\alpha} \overset{(2)}{=} -\alpha - 1 = -(\alpha + 1)$, that we can transform to $\alpha + 1$ by Proposition 3, the same is true for $\overline{\beta}$ and $\overline{\gamma}$.

Proof. First, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ easily follows from the matrix representation. Next, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 1) = \mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 1) = 0$ since the sum of the least significant bits is odd, see Lemma 7.

In light of Proposition 1, it is sufficient to prove that

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma})\\
+ \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}).
\end{aligned}$$

By the matrix approach, $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = LA_{w_n} \dots A_{w_0} e_0$, where $w_{i+1} = 4\alpha_i + 2\beta_i + \gamma_i$ and $w_0 = 4 \cdot 0 + 2 \cdot 1 + 1 \cdot 1 = 3$, next,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) &= LA_{w_n} \dots A_{w_0} e_0\\
&= \frac{1}{4}LA_{w_n} \dots A_{w_1} e_0 + \frac{1}{4}LA_{w_n} \dots A_{w_1} e_1\\
&\quad + \frac{1}{4}LA_{w_n} \dots A_{w_1} e_2 + \frac{1}{4}LA_{w_n} \dots A_{w_1} e_3\\
&\overset{\text{Lemma 4}}{=} \frac{1}{4}LA_{w_n} \dots A_{w_1} e_0 + \frac{1}{4}LA_{w_n \oplus 1} \dots A_{w_1 \oplus 1} e_0\\
&\quad + \frac{1}{4}LA_{w_n \oplus 2} \dots A_{w_1 \oplus 2} e_0 + \frac{1}{4}LA_{w_n \oplus 3} \dots A_{w_1 \oplus 3} e_0,
\end{aligned}$$

At the same time,

$$\begin{aligned}
LA_{w_n} \dots A_{w_1} e_0 &= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma),\\
LA_{w_n \oplus 1} \dots A_{w_1 \oplus 1} e_0 &= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma \oplus 1^n) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}),\\
LA_{w_n \oplus 2} \dots A_{w_1 \oplus 2} e_0 &= \mathrm{adp}^{\oplus}(\alpha, \beta \oplus 1^n \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma),\\
LA_{w_n \oplus 3} \dots A_{w_1 \oplus 3} e_0 &= \mathrm{adp}^{\oplus}(\alpha, \beta \oplus 1^n \to \gamma \oplus 1^n) = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}),
\end{aligned}$$

which completes the proof. □

Corollary 2. *For any $\gamma \in \mathbb{F}_2^n$, we have*

$$\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

Proof. Since $0 \oplus \overline{\gamma}_0 \oplus \gamma_0 = 1$, Lemma 7 provides that

$$\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \overline{\gamma}) = 0.$$

Therefore, $\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$ by Theorem 3. □

Corollary 3. *For any of* $\mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 0)$, $\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 1)$, *and* $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1)$, *at least two terms of the corresponding sum in Theorem 3 are zero.*

Proof. In light of Proposition 1, it is sufficient to prove the statement for $\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1)$.

Since $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = \alpha_0 \oplus \overline{\beta}_0 \oplus \overline{\gamma}_0$ and $\alpha_0 \oplus \overline{\beta}_0 \oplus \gamma_0 = \alpha_0 \oplus \beta_0 \oplus \overline{\gamma}_0 = \alpha_0 \oplus \beta_0 \oplus \gamma_0 \oplus 1$, Lemma 7 provides that either

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}) = 0 \text{ or}$$
$$\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}) = 0.$$ □

The recurrence formulas help to determine the minimum nonzero value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$:

Corollary 4. *Let $n > 1$. Then the minimum nonzero* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, $\alpha, \beta, \gamma \in \mathbb{F}_2^n$, *is equal to* $8 \cdot 4^{-n}$.

Note 2. The formula for $n = 1$ differs: Lemma 2 shows us that either $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 0$ or $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = 1$ for $\alpha, \beta, \gamma \in \mathbb{F}_2$.

Proof. Let us denote this minimum nonzero value by m_n. Applying to a nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$, a recurrence formula from Theorem 3, it is easy to see that $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \geq \frac{1}{4}m_n$, which implies $m_{n+1} \geq \frac{1}{4}m_n$.

Let us consider $\gamma_{10}^n = (1, 0, 1, 0, \ldots) \in \mathbb{F}_2^n$ (i. e., the least significant bit is 1 and each next bit is the negation of the previous bit), e. g., $\gamma_{10}^3 = (1, 0, 1)$. Also, $\alpha 1 = (1, \alpha_0, \alpha_1, ..., \alpha_{n-1})$ by definition, where α_0 is the least significant bit of α. Then, by the recurrence formulas,

$$\begin{aligned}
\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) &= \mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \overline{\gamma_{10}^n} 1) \\
&= \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \gamma_{10}^n) \\
&\quad + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \\
&\overset{\text{Lemma 7}}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n). \qquad (8)
\end{aligned}$$

Moreover, the first (i. e., least significant) and the second bits of $\overline{\gamma_{10}}$ are 0 and 1 respectively, which implies that $\mathrm{adp}^{\oplus}(0^n, 0^n \to \overline{\gamma_{10}^n}) = 0$ for $n > 1$. Indeed, it holds by Lemma 1 since $\omega_0 = 4 \cdot 0 + 2 \cdot 0 + 0 = 0$ and $\omega_1 = 4 \cdot 0 + 2 \cdot 0 + 1 = 1 \notin \{0, 3, 5, 6\}$. Therefore, (8) provides that

$$\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) = \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \text{ for } n > 1. \qquad (9)$$

Let us prove by induction that

$$m_n = \mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n).$$

The base case of the induction is $n = 2$. According to (8) and Note 2, the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^2$ is $\mathrm{adp}^{\oplus}(0^2, 1^2 \to \gamma_{10}^2) = \frac{1}{2}$. Note that this is consistent with Lemma 2.

Now, we prove that if the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ is m_n, then the minimum nonzero $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$ is m_{n+1}.

$$\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) \overset{(9)}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0^n, 1^n \to \gamma_{10}^n) \overset{\text{induction}}{=} \frac{1}{4}m_n.$$

Note that $\mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1})$ is nonzero. Moreover, it is also the minimum nonzero value. This can be seen as follows. Clearly, there must exist some $\alpha, \beta, \gamma \in \mathbb{F}_2^{n+1}$ that corresponds to the minimum nonzero value, and therefore one of the eight recurrence formulas of Theorem 3 applies. As the value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ is nonzero, at least one term in the recurrence formulas must be nonzero, and therefore $m_{n+1} \geq \frac{1}{4}m_n$. We found this smallest nonzero value: $m_{n+1} = \mathrm{adp}^{\oplus}(0^{n+1}, 1^{n+1} \to \gamma_{10}^{n+1}) = \frac{1}{4}m_n$, thereby proving the induction step.

Finally, we can now express m_n in terms of n: $m_n = \frac{1}{2} \cdot (\frac{1}{4})^{n-2} = 8 \cdot 4^{-n}$ for $n > 1$ by (9). □

8 Properties of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

8.1 Simplified Matrix Form for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

When calculating $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ using Theorem 1, we only need A_0 (for bit positions where $\gamma_i = 0$) and A_3 (for bit positions where $\gamma_i = 1$). These matrices can be minimized to size 3×3 using the S-function toolkit of Mouha et al. [MVDCP11]: applying the software toolkit to remove non-accessible states and to merge indistinguishable states leads to:

$$A_0'' = \frac{1}{4}\begin{pmatrix} 4 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_3'' = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 0 & 4 \end{pmatrix},$$

where A_0'' and A_3'' can be obtained from A_0 and A_3 by removing the last four columns (the non-accessible states) and rows, and by merging the middle two remaining rows and columns (which correspond to indistinguishable states).

Note that $(1, 1, 1)A_0'' = (1, 1, 1)A_3'' = (1, 0, 1)$, which will help us to minimize the size of the matrices to 2×2 if we "cheat" by excluding the most significant bit from the matrix product. More formally, we can obtain matrices B_0 and B_1 by removing all rows and columns from A_0 and A_3 except 0 and 3, and calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ as follows:

Proposition 6. *Let $\gamma \in \mathbb{F}_2^n$. Then*

$$\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = (1, 1)B_{\gamma_{n-2}}B_{\gamma_{n-3}} \dots B_{\gamma_0}(1, 0)^T,$$

where

$$B_0 = \frac{1}{4}\begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}, \quad B_1 = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix}.$$

Proof. According to Theorem 1, we can calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ by matrices A_0 and A_3. First, A_0x^T and A_3x^T depend only on x_0, x_3, x_5, x_6, where $x \in \mathbb{Q}^8$. Secondly, they have a block structure

$$\begin{pmatrix} P_i & Q_i \\ 0 & Q_i \end{pmatrix},$$

where P_i and Q_i are matrices of size 4×4. In addition, coordinates $\{4, 5, 6, 7\}$ of e_0 are zero. This means that coordinates 5 and 6 of the vector $A_{\omega_i}A_{\omega_{i-1}} \dots A_{\omega_0}e_0$, where $\omega_i = 3\gamma_i$,

$i = 0, \ldots, n-1$, are zero. Thus, we can consider only coordinates 0 and 3. It is easy to see that

$$(A_0 x^T)_0 = x_0 + \frac{1}{4}x_3, \quad (A_0 x^T)_3 = \frac{1}{4}x_3, \tag{10}$$

and

$$(A_3 x^T)_0 = \frac{1}{4}x_0, \quad (A_3 x^T)_3 = \frac{1}{4}x_0 + x_3. \tag{11}$$

Thus,

$$LA_0 x^T = LA_3 x^T = x_0 + x_3 + x_5 + x_6 = x_0 + x_3$$

for $x^T = A_{\omega_i} A_{\omega_{i-1}} \ldots A_{\omega_0} e_0$ due to the block structure.

Finally, let us associate the first coordinate of a $v \in \mathbb{Q}^2$ with x_0 and the second coordinate with x_3. Then,

$$B_0 v^T = \begin{pmatrix} v_0 + \frac{1}{4}v_1 \\ \frac{1}{4}v_1 \end{pmatrix}, \text{ which completely corresponds (10), and}$$
$$B_1 v^T = \begin{pmatrix} \frac{1}{4}v_0 \\ \frac{1}{4}v_0 + v_1 \end{pmatrix}, \text{ which completely corresponds (11).}$$

Also, e_0 and $LA_0 x^T = LA_3 x^T = x_0 + x_3$ correspond $(1,0)^T$ and $(1,1)v^T = v_0 + v_1$ respectively, i. e.,

$$\begin{aligned} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) &= (LA_{\omega_{n-1}})(A_{\omega_{n-2}} \ldots A_{\omega_0} e_0) \\ &= (1,1) B_{\gamma_{n-2}} B_{\gamma_{n-3}} \ldots B_{\gamma_0} (1,0)^T. \end{aligned}$$ □

8.2 Minimum of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

Let us calculate the minimum value among $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. We will start with the following lemma.

Lemma 8. *Let* $\gamma \in \mathbb{F}_2^n$. *Then* $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$.

Proof. By induction: for $n = 1$ the statement holds. Suppose that for any $\gamma \in \mathbb{F}_2^n$, it holds that $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$. Let us prove that the statement holds for $\gamma' \in \mathbb{F}_2^{n+1}$. We have two cases:

1. $\gamma' = \gamma 0$, $\gamma \in \mathbb{F}_2^n$. Then, using the recurrence formula for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, we obtain

   $$\mathrm{adp}^{\oplus}(0, \gamma 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{3}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma).$$

   At the same time,

   $$3\mathrm{adp}^{\oplus}(0, \overline{\gamma 0} \to \overline{\gamma 0}) = 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} 1 \to \overline{\gamma} 1) = \frac{3}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{3}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

   It completes the case, since $\frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) < \frac{3}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma})$ by the induction hypothesis.

2. $\gamma' = \gamma 1$, $\gamma \in \mathbb{F}_2^n$. Like for the previous point,

   $$\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

   The induction hypothesis completes the proof, since

   $$3\mathrm{adp}^{\oplus}(0, \overline{\gamma 1} \to \overline{\gamma 1}) = 3\mathrm{adp}^{\oplus}(0, \overline{\gamma} 0 \to \overline{\gamma} 0) = \frac{11}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}).$$

□

Corollary 5. *Let* $\gamma \in \mathbb{F}_2^n$. *Then* $\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) < \mathrm{adp}^{\oplus}(0, \gamma 0 \to \gamma 0)$.

Proof. Indeed, $\mathrm{adp}^{\oplus}(0, \gamma 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma} \to \overline{\gamma}) < \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) + \frac{3}{4}\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \mathrm{adp}^{\oplus}(0, \gamma 0 \to \gamma 0)$. □

Theorem 4. *Let* $m_n^d = \min\limits_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. *Then for any* n, *we have*

$$m_{n+2}^d = \frac{1}{4} m_{n+1}^d + \frac{1}{4} m_n^d.$$

Moreover, $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = m_n^d$, *where* $\gamma \in \mathbb{F}_2^n$, *if and only if* $\gamma_0 = 1$ *(only if* $n > 1$*) and* $\gamma_{i+1} = \overline{\gamma_i}$ *for any* $i = 1, \ldots, n-3$. *This means that* γ_{n-1} *and* γ_1 *can be arbitrary, and* $\gamma_2, \ldots, \gamma_{n-2}$ *depend on* γ_1.

Note 3. Note that we have no restrictions for $\gamma \in \mathbb{F}_2$. Also, if $n = 2, 3$, we have only one restriction: $\gamma_0 = 1$, i. e., the value of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ is the same for any $\gamma \in \mathbb{F}_2^2, \mathbb{F}_2^3$ where $\gamma_0 = 1$.

Proof. Let us use induction by n. The statement of the theorem holds for $n = 1$ and $n = 2$ by Lemmas 2 and 3.

Let us suppose that the theorem holds for n. Now we will prove that it is true for $n+1$. Let $\gamma \in \mathbb{F}_2^{n+1}$. We consider first two bits γ_0 and γ_1 of γ: first of all, Corollary 5 provides that $\gamma_0 = 1$ for the minimum of $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$. Next, let

$$c = \begin{cases} (\gamma_2, \ldots, \gamma_n) & \text{if } \gamma_1 = 0, \\ (\overline{\gamma}_2, \ldots, \overline{\gamma}_n) & \text{if } \gamma_1 = 1, \end{cases}$$

where $c \in \mathbb{F}_2^{n-1}$. Then

$$\{\gamma', \overline{\gamma'}\} = \{c0, \overline{c0}\} \text{ for } \gamma' = (\gamma_1, \gamma_2, \ldots, \gamma_n). \tag{12}$$

Indeed, $\gamma' = c0$ if $\gamma_1 = 0$, otherwise $\gamma' = (1, \overline{\overline{\gamma_2}}, \ldots, \overline{\overline{\gamma_n}}) = (\overline{0}, \overline{c_0}, \ldots, \overline{c_{n-1}}) = \overline{c0}$.

Since $\gamma_0 = 1$, Corollary 2 give us

$$\begin{aligned} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) &= \frac{1}{4}\mathrm{adp}^{\oplus}(0, \gamma' \to \gamma') + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{\gamma'} \to \overline{\gamma'}) \\ &\overset{(12)}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0, c0 \to c0) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{c0} \to \overline{c0}) \\ &\overset{\text{Theorem 3}}{=} \frac{1}{4}\mathrm{adp}^{\oplus}(0, c \to c) + \frac{1}{4}\mathrm{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1). \end{aligned}$$

Since $\mathrm{adp}^{\oplus}(0, c \to c) \geq m_{n-1}^d$ and $\mathrm{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1) \geq m_n^d$, we have

$$m_{n+1}^d \geq \frac{1}{4} m_n^d + \frac{1}{4} m_{n-1}^d.$$

Moreover, $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d$ if and only if $\mathrm{adp}^{\oplus}(0, \overline{c}1 \to \overline{c}1) = m_n^d$, which gives us by the induction hypothesis the restriction

$$\begin{aligned} &c_{i+1} = \overline{c_i} \text{ for any } i = 0, \ldots, n-4, \text{ or, equivalently,} \\ &\gamma_{i+1} = \overline{\gamma_i} \text{ for any } i = 2, \ldots, n-2, \end{aligned} \tag{13}$$

and $\mathrm{adp}^{\oplus}(0, c \to c) = m_{n-1}^d$, which has for $n - 1 > 1$ one additional restriction: $c_0 = 1$. Since $c_0 = \gamma_1 \oplus \gamma_2$ by the definition of c, we have $\gamma_2 = \overline{\gamma_1}$ and extend (13) to $i = 1$.

Note that for the case $n-1=1$ (which excludes $c_0=1$) the theorem gives no $\gamma_{i+1}=\overline{\gamma_i}$. Indeed, $n+1=3$ and i should satisfy $1 \le i \le (n+1)-3$, but $1 > (n+1)-3 = 0$.

These restrictions for γ with $\gamma_0 = 1$ always guarantee that such a γ exists and, therefore, it holds that

$$\frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d = \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) \ge m_{n+1}^d \ge \frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d.$$

It implies that $\mathrm{adp}^{\oplus}(0,\gamma\to\gamma) = m_{n+1}^d = \frac{1}{4}m_n^d + \frac{1}{4}m_{n-1}^d$ and makes the induction step proven. □

The numbers m_n^d, $n = 1, 2, \ldots$, form a Horadam sequence $H(1, \frac{1}{2}, \frac{1}{4}, -\frac{1}{4})$ — a generalization of the Fibonacci numbers. A sequence $H_1, H_2, H_3, \ldots$ is a Horadam sequence $H(a, b, p, q)$ if $H_1 = a$, $H_2 = b$ and $H_{n+2} = pH_{n+1} - qH_n$. Horadam [Hor65a, Hor65b] provides information on Horadam sequences and properties of sequence members, which help to obtain the following result.

Corollary 6. *The following formula holds:*

$$m_n^d = \frac{1}{34 \cdot 8^n}\Big((17+7\sqrt{17})(1+\sqrt{17})^n + (17-7\sqrt{17})(1-\sqrt{17})^n\Big).$$

Proof. According to [Hor65a, p. 161],[1]

$$H_n = A\alpha^{n-1} + B\beta^{n-1},$$

where α and β are roots of the polynomial $x^2 - px + q = 0$, $\beta \le \alpha$ for real roots, and

$$A = \frac{b - a\beta}{\alpha - \beta},\ B = \frac{a\alpha - b}{\alpha - \beta}.$$

Since $p = \frac{1}{4}, q = -\frac{1}{4}$,

$$\alpha = \frac{1}{8}(1+\sqrt{17}),\ \beta = \frac{1}{8}(1-\sqrt{17}),\ \alpha - \beta = \frac{\sqrt{17}}{4}.$$

Taking $a = 1$, $b = \frac{1}{2}$, we have

$$A = \frac{17+3\sqrt{17}}{34},\ B = \frac{17-3\sqrt{17}}{34}.$$

Finally, it is not difficult to check that

$$A = \frac{(17+7\sqrt{17})(1+\sqrt{17})}{34\cdot 8},\ B = \frac{(17-7\sqrt{17})(1-\sqrt{17})}{34\cdot 8}.$$

□

8.3 Results about $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$

It is easy to see that Propositions 2 and 3 provide

Proposition 7. *Let* $a, u, v \in \mathbb{F}_2^n$. *Then* $\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, v \to v)$ *if* $u + v = 0 \pmod{2^{n-1}}$.

[1] Note that we use $n-1$ instead of n as the sequence starts with $n = 1$.

Proof. Let $u, v \in \mathbb{F}_2^n$. Since $2^{n-1}|2^n$, we can correctly consider modulo 2^{n-1} operations.

Without loss of generality, we can assume that both $u, v < 2^{n-1}$. Otherwise, we can consider $u' = u \oplus 2^{n-1}$ instead of u, here $u' < 2^{n-1}$ and $u' = u \pmod{2^{n-1}}$, since Proposition 2 guarantees that $\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, u' \to u')$ (and the same for v).

Thus, $v = 2^{n-1} - u$. Finally, by Propositions 2 and 3 we have

$$\mathrm{adp}^{\oplus}(a, u \to u) = \mathrm{adp}^{\oplus}(a, -u \to -u) = \mathrm{adp}^{\oplus}(a, 2^{n-1} - u \to 2^{n-1} - u) = \mathrm{adp}^{\oplus}(a, v \to v).$$

□

Computational experiments performed for n up to 32 show that there exist at most $32 = 2^5$ distinct γ with the same value $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$, which implies that

$$\#\{\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) : \gamma \in \mathbb{F}_2^n\} \geq 2^{n-5}, \text{ where } n \leq 32.$$

Taking into account Theorem 4 (and Corollary 6), it looks like that the simplest way to calculate $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$ is to use the recurrence formula (Corollary 2) and the minimized matrix representation (Proposition 6).

It is not difficult to compute the sum of all $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma)$:

Proposition 8. *For all n, we have*

$$\sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 2\left(\frac{3}{2}\right)^{n-1}.$$

Proof. For $n = 1$, the equality holds: $\mathrm{adp}^{\oplus}(0, 0 \to 0) + \mathrm{adp}^{\oplus}(0, 1 \to 1) = 1 + 1 = 2$. For all $n > 1$, the sum can be expressed using the sum for smaller n:

$$\begin{aligned}
\sum_{\gamma \in \mathbb{F}_2^{n+1}} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma \to \gamma) &= \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma 0 \to \gamma 0) + \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^{n+1}, \gamma 1 \to \gamma 1) \\
&= \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma) \\
&\qquad + \frac{1}{4} \sum_{\gamma \in \mathbb{F}_2^n} \left(\mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma)) + \mathrm{adp}^{\oplus}(0^n, \overline{\gamma} \to \overline{\gamma})\right) \\
&= \frac{3}{2} \sum_{\gamma \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0^n, \gamma \to \gamma).
\end{aligned}$$

□

9 Conclusion and Future Work

In this work we investigated some properties of $\mathrm{adp}^{\oplus}$ that are interesting for the differential cryptanalysis of ARX ciphers. We provide the missing proof of the theorem about $\max_{\alpha,\beta} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ from [LWD04], and established that there are either two (for $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = 1$) or eight (for any other cases) distinct pairs α, β on which $\mathrm{adp}^{\oplus}$ attains this maximum value. We obtained recurrence formulas for an arbitrary $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ which help to find minimum nonzero value of $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, find all $\gamma \in \mathbb{F}_2^n$ for which $\mathrm{adp}^{\oplus}(0, \gamma \to \gamma) = \min_{c \in \mathbb{F}_2^n} \mathrm{adp}^{\oplus}(0, c \to c)$, and calculate this minimum value. As with any paper that analyzes the components of a primitive (e. g., additions, rotations, and XORs, but also S-boxes or matrix multiplications), some caution is necessary when extending the results to the analysis of a full primitive. We mention the analysis of larger components and the application to a full primitive as suggestions for future work.

Acknowledgments

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. The authors are very grateful to organizers of The First Workshop at the Mathematical Center in Akademgorodok.

References

[AMPH14] Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, and Luca Henzen. *The Hash Function BLAKE*. Information Security and Cryptography. Springer, 2014.

[BBCdS+20a] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Alzette: A 64-bit ARX-box - (feat. CRAX and TRAX). In *CRYPTO 2020*, volume 12172 of *LNCS*, pages 419–448. Springer, 2020.

[BBCdS+20b] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Lightweight AEAD and hashing using the Sparkle permutation family. *IACR Trans. Symmetric Cryptol.*, 2020(S1):208–261, 2020.

[Ber92] Thomas A. Berson. Differential cryptanalysis mod 2^32 with applications to MD5. In *EUROCRYPT 1992*, volume 658 of *LNCS*, pages 71–80. Springer, 1992.

[Ber05] D.J. Bernstein. Salsa20 specification. https://cr.yp.to/snuffle/spec.pdf, April 2005.

[Ber08] D.J. Bernstein. ChaCha, a variant of Salsa20. https://cr.yp.to/chacha/chacha-20080128.pdf, January 2008.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, January 1991.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. https://eprint.iacr.org/2013/404.

[BV14] Alex Biryukov and Vesselin Velichkov. Automatic search for differential trails in ARX ciphers. In *CT-RSA 2014*, volume 8366 of *LNCS*, pages 227–250. Springer, 2014.

[DPU+16] Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In *ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 484–513. Springer, 2016.

[FLS+09] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein hash function family, 2009. http://www.skein-hash.info.

[GJN19] Shay Gueron, Ashwin Jha, and Mridul Nandi. COMET: COunter Mode Encryption with authentication Tag. Submission to the NIST Lightweight Cryptography Project (Round 2), September 2019.

[HHK+03] Seokhie Hong, Deukjo Hong, Youngdai Ko, Donghoon Chang, Wonil Lee, and Sangjin Lee. Differential cryptanalysis of TEA and XTEA. In *ICISC 2003*, volume 2971 of *LNCS*, pages 402–417. Springer, 2003.

[Hor65a] Alwyn Francis Horadam. Basic properties of a certain generalised sequence of numbers. *The Fibonacci Quarterly*, 3(3):161–176, 1965.

[Hor65b] Alwyn Francis Horadam. Generating functions for powers of a certain generalised sequence of numbers. *Duke Mathematical Journal*, 32(3):437 – 446, 1965.

[KRK+17] Bonwook Koo, Dongyoung Roh, Hyeonjin Kim, Younghoon Jung, Donggeon Lee, and Daesung Kwon. CHAM: A family of lightweight block ciphers for resource-constrained devices. In *ICISC 2017*, volume 10779 of *LNCS*, pages 3–25. Springer, 2017.

[LM01] Helger Lipmaa and Shiho Moriai. Efficient algorithms for computing differential properties of addition. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 336–350. Springer, 2001.

[LWD04] Helger Lipmaa, Johan Wallén, and Philippe Dumas. On the additive differential probability of exclusive-or. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 317–331. Springer, 2004.

[MVDCP11] Nicky Mouha, Vesselin Velichkov, Christophe De Cannière, and Bart Preneel. The differential analysis of S-functions. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *SAC 2010*, volume 6544 of *LNCS*, pages 36–56. Springer, 2011.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Inscrypt 2011*, volume 7537 of *LNCS*, pages 57–76. Springer, 2011.

[NW97] Roger M. Needham and David J. Wheeler. Tea extensions. Technical report, Computer Laboratory, University of Cambridge, October 1997. http://www.cix.co.uk/~klockstone/xtea.pdf.

[PHCER08] Javier Polimón, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. Automated design of a lightweight block cipher with genetic programming. *Int. J. Knowl. Based Intell. Eng. Syst.*, 12(1):3–14, 2008.

[RKJ+19] Dongyoung Roh, Bonwook Koo, Younghoon Jung, Ilwoong Jeong, Donggeon Lee, Daesung Kwon, and Woo-Hwan Kim. Revised version of block cipher CHAM. In *ICISC 2019*, volume 11975 of *LNCS*, pages 1–19. Springer, 2019.

[Saa19] Markku-Juhani O. Saarinen. SNEIKEN and SNEIKHA v1.1: Authenticated encryption and cryptographic hashing. Technical report, PQShield Ltd., May 2019. https://github.com/pqshield/sneik.

[SHW+16] Siwei Sun, Lei Hu, Peng Wang, Meiqin Wang, Danping Shi, Xiaoshuang Ma, Qianqian Yang, and Kai Fu. Mixed integer programming models for finite automaton and its application to additive differential patterns of exclusive-or. Cryptology ePrint Archive, Report 2016/338, 2016. https://eprint.iacr.org/2016/338.

[SM88] Akihiro Shimizu and Shoji Miyaguchi. Fast data encipherment algorithm FEAL. In David Chaum and Wyn L. Price, editors, *EUROCRYPT 1987*, volume 304 of *LNCS*, pages 267–278. Springer, 1988.

[VMDCP11] Vesselin Velichkov, Nicky Mouha, Christophe De Cannière, and Bart Preneel. The additive differential probability of ARX. In *FSE 2011*, volume 6733 of *LNCS*, pages 342–358. Springer, 2011.

[VMDCP12] Vesselin Velichkov, Nicky Mouha, Christophe De Cannière, and Bart Preneel. UNAF: A special set of additive differences with application to the differential analysis of ARX. In *FSE 2012*, volume 7549 of *LNCS*, pages 287–305. Springer, 2012.

[WN94] David J. Wheeler and Roger M. Needham. TEA, a tiny encryption algorithm. In *FSE 1994*, volume 1008 of *LNCS*, pages 363–366. Springer, 1994.

ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2020, Vol. 14, No. 4, pp. 623–647. © Pleiades Publishing, Ltd., 2020.
Russian Text © The Authors, 2020, published in Diskretnyi Analiz i Issledovanie Operatsii, 2020, Vol. 27, No. 4, pp. 21–57.

On the Sixth International Olympiad in Cryptography NSUCRYPTO

A. A. Gorodilova[1*], N. N. Tokareva[1,2*], S. V. Agievich[3*], C. Carlet[4*], E. V. Gorkunov[1,5*], V. A. Idrisova[1*], N. A. Kolomeec[1*], A. V. Kutsenko[1,5*], R. K. Lebedev[5*], S. Nikova[6*], A. K. Oblaukhov[1*], I. A. Pankratova[7*], M. A. Pudovkina[8*], V. Rijmen[6*], and A. N. Udovenko[9*]

[1] *Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia*
[2] *Laboratory of Cryptography JetBrains Research, ul. Pirogova 1, Novosibirsk, 630090 Russia*
[3] *Belarusian State University, pr. Nezavisimosti 4, Minsk, 220030 Belarus*
[4] *University of Paris 8, 2 Rue de la Liberté, 93200 Saint-Denis, France*
[5] *Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090 Russia*
[6] *ESAT-COSIC, KU Leuven, Kasteelpark Arenberg, 10, B-3001 Leuven, Belgium*
[7] *Tomsk State University, pr. Lenina 36, Tomsk, 634050 Russia*
[8] *Bauman Moscow State Technical University, ul. Vtoraya Baumanskaya 5/2, Moscow, 105005 Russia*
[9] *SnT, University of Luxembourg, 2 Avenue de l'Universite, L-4365 Esch-sur-Alzette, Luxembourg*

Received May 20, 2020; in final form, August 18, 2020; accepted August 21, 2020

Abstract—NSUCRYPTO is the unique cryptographic Olympiad containing scientific mathematical problems for professionals, school and university students from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography. From the very beginning, the concept of the Olympiad was not to focus on solving olympic tasks but on including unsolved research problems at the intersection of mathematics and cryptography. The Olympiad history starts in 2014. In 2019, it was held for the sixth time. We present the problems and their solutions of the Sixth International Olympiad in cryptography NSUCRYPTO'2019. Under consideration are the problems related to attacks on ciphers and hash functions, protocols, Boolean functions, Dickson polynomials, prime numbers, rotor machines, etc. We discuss several open problems on mathematical countermeasures to side-channel attacks, APN involutions, S-boxes, etc. The problem of finding a collision for the hash function `Curl27` was partially solved during the Olympiad.

DOI: 10.1134/S1990478920040031

Keywords: *cryptography, cipher, hash function, Hamming code, slide attack, threshold implementation, Dickson polynomial, APN function, Olympiad, NSUCRYPTO*

INTRODUCTION

NSUCRYPTO (Non-Stop University Crypto) is the International Olympiad in cryptography that was held for the sixth time in 2019.

Interest in the Olympiad around the world is significant. This year, there were hundreds of participants from 26 countries; 42 participants in the first round and 21 teams in the second round from 16 countries were awarded with prizes and honorable diplomas. The Olympiad Program Committee includes specialists from Belgium, France, the Netherlands, the USA, Norway, India, Luxembourg, Belarus', Kazakhstan, and Russia.

Let us shortly formulate the format of the Olympiad. One of the Olympiad main ideas is that everyone can participate! Each participant chooses his/her category when registering on the Olympiad website [1]. There are three categories: "*school students*" (for junior researchers: pupils and high

* E-mail: nsucrypto@nsu.ru

school students), "*university students*" (for participants who are currently studying at universities) and "*professionals*" (for participants who have already completed education or just want to be in the restriction-free category). Awarding of the winners is held in each category separately.

The Olympiad consists of the two independent Internet rounds: the first one is individual (duration 4 hours 30 minutes) while the second round is a team one (duration 1 week). The first round is divided into two sections: A—for "school students," B—for "university students" and "professionals." The second round is common to all participants. Participants read the Olympiad problems and submit their solutions through the Olympiad website. The language of the Olympiad is English.

The Olympiad participants are always interested in solving various problems of any complexity at the intersection of mathematics and cryptography. The participants show their knowledge, creativity, and professionalism. That is why the Olympiad not only includes interesting tasks with known solutions but also offers unsolved problems. This year, one of such open problems, "`Curl27`" (see Section 2.14), was partially solved during the second round! All open problems stated during the Olympiad history can be found in [2].

On the website we also mark the current status of each problem. For example, in addition to "`Curl27`", the problem "Sylvester matrices" was solved by three teams in 2018, and the problem "Algebraic immunity" was completely solved during the Olympiad in 2016. And what is important for us, some participants were trying to find solutions after the Olympiad was over. For example, a partial solution for the problem "A secret sharing" (2014) was proposed in [3]. We invite everybody who has ideas on solving the problems to send solutions to us!

The paper is organized as follows: We start with the problem structure of the Olympiad in Section 1. Then we present formulations of all problems stated during the Olympiad and give their detailed solutions in Section 2. Finally, we publish the lists of NSUCRYPTO'2019 winners in Section 3.

Mathematical problems and their solutions of the previous International Olympiads in cryptography NSUCRYPTO from 2014 to 2018 can be found in [4], [5], [6], [7], and [8] respectively.

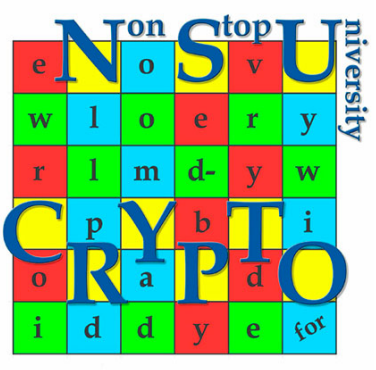


Fig. 1. NSUCRYPTO logo.

1. PROBLEM STRUCTURE OF THE OLYMPIAD

There were 16 problems stated during the Olympiad; some of them were included in both rounds (Tables 1 and 2). Section A of the first round consisted of six problems, whereas the section B contained seven problems. Three problems were common for both sections. The second round was composed of eleven problems. Five problems of the second round included unsolved questions (with special awards of the Program Committee).

2. PROBLEMS AND THEIR SOLUTIONS

In this section, we formulate all problems of NSUCRYPTO'2019 and present their detailed solutions paying attention to the solutions by the participants.

2.1. Problem "A 1024-Bit Key"

2.1.1. Formulation. Alice has a 1024-bit key for a symmetric cipher (the key consists of 0s and 1s). Alice is afraid of malefactors, so she changes her key everyday in the following way:

1. Alice chooses a subsequence of key bits such that the first bit and the last bit are equal to 0. She also can choose a subsequence of length 1 that contains only 0.

2. Alice inverts all bits in this subsequence (0 turns into 1 and vice versa); bits outside of this subsequence remain as they are.

Prove that the process will stop. Find the key that will be obtained by Alice in the end of the process.

Example of an operation. 11001 01101110 011... turns to 11001 10010001 011...

2.1.2. Solution. Let us encode the binary vector of the key as the corresponding decimal number. It is obvious that this number will increase on the next day since all bits on the left from the sequence are not changing, but the first bit of the sequence turns from 0 to 1. Let us note that this number can not increase infinitely since the size of the key is restricted by 1024 bits, so, in the very end the key will be maximal possible and, thus, will consist of all 1s.

Almost all participants successfully solved the problem.

2.2. Problem "The Magnetic Storm"

2.2.1. Formulation. A hardware random number generator is a device that generates random sequences consisting of 0s and 1s. Unfortunately, a disturbance caused by a magnetic storm affected this random

Table 1. Problems of the first round

N	Problem title	Maximum score
1	A 1024-bit key	4
2	The magnetic storm	4
3	Autumn leaves	4
4	A rotor machine	4
5	Broken `Calculator`	4
6	A promise	6

Section A

N	Problem title	Maximum score
1	Autumn leaves	4
2	The magnetic storm	4
3	A rotor machine	4
4	16QAM	8
5	A promise and money	6
6	`Calculator`	6
7	APN + Involutions	7

Section B

Table 2. Problems of the second round

N	Problem title	Maximum score
1	A 1024-bit key	4
2	Sharing	6 + additional scores for open questions
3	Factoring in 2019	8
4	`TwinPeaks-3`	8
5	`Curl27`	10 + additional scores for open questions
6	8-bit S-box	Unlimited (open problem)
7	A rotor machine	4
8	16QAM	8
9	`Calculator`	6
10	APN + Involutions (extended)	12 + additional scores for open questions
11	Conjecture	Unlimited (open problem)

Fig. 2. Autumn Leaves.

number generator. As a result, the device had generated a sequence of 0s of length k (where k is a positive integer), and then started to generate an infinite sequence of 1s.

Prove that at some point the generator will produce the number $1\ldots10\ldots0$ that is divisible by 2019.

2.2.2. Solution. Let us prove that a number of form $1\ldots11\ldots1$ is divisible by 2019. Consider all numbers that consists only of 1s. Since there are infinitely many of these numbers, there can be found a pair of numbers A and B such that they have the same remainder when divided by 2019. Therefore, $C = A - B = 1\ldots10\ldots0$ consisting of m 1s for some natural m is divisible by 2019, and, since 2019 is not divisible by 2 and 5,

$$C^* = C \times 10\ldots0 = 1\ldots10\ldots0$$

is divisible by 2019 for any number of 0s.

There were many correct solutions by the participants.

2.3. Problem "Autumn Leaves"

2.3.1. Formulation. Read a hidden message (see Fig. 2)!

2.3.2. Solution. We see different leaves and spaces between them. It looks like a simple substitution cipher was used there and distinct leaves corresponded to distinct English letters. By English grammar, we can suppose that the second and the third words are "`is a`." Then the first word starts with "`a`" and by its structure can be "`autumn`" (which is very likely as the autumn landscape is depicted). Also, the leaf  is the most common letter in the text and we can guess that it is "`e`." Then we see "`*ea*`" in the third line that seems to be "`leaf`". As a result the last word becomes "`fl**e*`" that is "`flower`." Finally, we get "`Autumn is a second spring when every leaf is a flower`" that is a famous quote by Albert Camus. Almost all participants read the message.

2.4. Problem "A Rotor Machine"

2.4.1. Formulation. In a country rotor machines were very useful for encryption of information (see examples in Fig. 3).

Eve knows that for some secret communication a simple rotor machine was used. It works with letters `O, P, R, S, T, Y` only and has an input circle with lamps (start), one rotor, and a reflector. See Fig. 4.

Fig. 3. Examples of rotor machines.

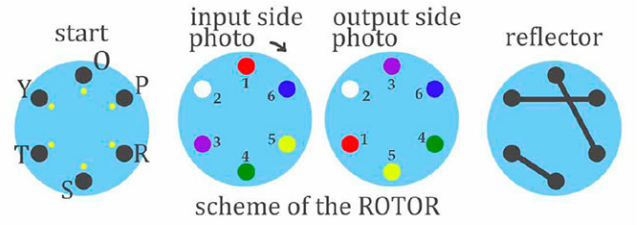


Fig. 4. Scheme of the rotor.

The input circle and the reflector are fixed in their positions, while the rotor can be in one of the six possible positions. After pressing a button on a keyboard, an electrical signal corresponding to the letter goes through the machine, comes back to the input circle, and the appropriate lamp shows the result of encryption. After each letter is encrypted, the rotor turns right (i.e. clockwise) on 60 degrees. Points of different colors (enumerated) on the rotor sides indicate different noncrossing signal lines within the rotor.

For instance, if the rotor is fixed as shown on the picture above then if you press the button `O`, it will be encrypted as `T` (the signal enters the rotor via red (color 1) point, is reflected, and then comes back via purple (color 5) line). If you press `O` again, it will be encrypted as `R`. If you press `T` then, you will get `S`, and so on.

Eve intercepted the secret message

TRRYSSPRYRYROYTOPTOPTSPSPRS.

Help her to decrypt it keeping in mind that Eve does not know the initial position of the rotor.

2.4.2. Solution. To solve the problem and decrypt the message, we need to correctly understand the scheme of work. A key for the cipher is the initial position of the rotor. We denote it by a color of the circle (enumerated) on the input side of the rotor that corresponds to the letter `O`. Table 3 represents the encryption tables depending on the key.

Table 3. Encryption tables

	O	P	R	S	T	Y
red (color 1)	T	Y	S	R	O	P
white (color 2)	R	S	O	P	Y	T
purple (color 3)	Y	R	P	T	S	O

	O	P	R	S	T	Y
green (color 4)	S	R	P	O	Y	T
yellow (color 5)	S	T	Y	O	P	R
blue (color 6)	R	T	O	Y	P	S

Trying all six possible keys, we find the only one meaningful message `POST TO TOP OOPS SORRY STOP ROTOR` that corresponds to the "yellow" (color 5) key.

Almost all participants solved the problem. The most interesting solutions were obtained by creating real models for this rotor machine, for example, by a school student Varvara Lebedinskaya (The Specialized Educational Scientific Center of Novosibirsk State University), by the team of Kristina Geut, Sergey Titov, and Dmitry Ananichev (Ural State University of Railway Transport).

2.5. Problem "Broken `Calculator`*"*

2.5.1. Formulation. Alice and Bob are practicing in developing toy cryptographic applications for smartphones. This year they have invented `Calculator` that allows one to perform the following operations modulo 2019 (that is to get the result as the reminder of division by 2019):

- to insert at most 4-digit positive integers (digits from 0 to 9);
- to perform addition, subtraction, and multiplication of two numbers;
- to store temporary results and read them from the memory.

Suppose that Alice wants to send Bob a ciphertext y (given by a 4-digit integer). She sends y from her smartphone to Bob's `Calculator` memory. To decrypt y, Bob needs to get the plaintext x (using his `Calculator`) by the rule: x is equal to the remainder of dividing $f(y) = y^5 + 1909y^3 + 401y$ by 2019.

At the most inopportune moment, Bob dropped his smartphone and broke its screen (see Fig. 5). Now, the button "+" as well as all digits except "1" and "5" are not working.

Help Bob to invent an efficient algorithm of how to decrypt any ciphertext y using `Calculator` in his situation. More precisely, suggest a short list of commands such that each command has one of the following types ($1 \leqslant j, k < i$):

$$S_i = y, \qquad S_i = a, \qquad S_i = S_j - S_k, \qquad S_i = S_j * S_k,$$

where a is an at most 4-digit integer consisting of digits 1 and 5 only; for example, $a = 1$, $a = 15$, $a = 551$, $a = 5115$, etc.

The first command has to be $S_1 = y$. In the last command, the resulting plaintext x has to be calculated. We remind that all calculations are modulo 2019. In particular, the integer 2500 becomes 481 and -1000 becomes 1019 immediately after entering or calculations. The shorter the list of commands you suggest, the more scores you get for this problem.

Example. The following list of commands calculates $x = y^2 - 55$:

Command	Result
$S_1 = y$	y
$S_2 = S_1 * S_1$	y^2
$S_3 = 11$	11
$S_4 = 5$	5
$S_5 = S_3 * S_4$	55
$S_6 = S_2 - S_5$	$y^2 - 55$

Fig. 5. Broken `Calculator`.

2.5.2. Solution. Let us present the original solution in 14 steps by the Program Committee.

Let $a \equiv_m b$ mean that integers a and b are congruent modulo m. The following relations hold:

$$\begin{aligned} f(y) &\equiv_{2019} y^5 + 1909y^3 + 401y \equiv_{2019} y(y^4 - 110y^2 + 401) \\ &\equiv_{2019} y(y^4 - 2 * 55y^2 + 55^2 - 55^2 + 401) \equiv_{2019} y((y^2 - 55)^2 - 55^2 + 5 * 22^2) \\ &\equiv_{2019} y((y^2 - 55)^2 - 11^2 * (5^2 - 5 * 2^2)) \equiv_{2019} y((y^2 - 55)^2 - 11^2 * 5) \\ &\equiv_{2019} y((y^2 - 55)^2 - 11 * 55). \end{aligned}$$

Thus, the reminder of division of $f(y)$ by 2019 can be calculated for any y by the list of commands in Table 4. A similar solution was found by Borislav Kirilov (Bulgaria, The First Private Mathematical Gymnasium).

Note. The polynomial $f(y) = y^5 + 1909y^3 + 401y$ is the Dickson polynomial $D_5(y, a) = y^5 - 5y^3a + 5ya^2$ for $a = 22$ with coefficients taken modulo 2019.

Table 4. List of commands for the Program Committee solution

Command	Result	Command	Result	Command	Result
$S_1 = y$	y	$S_4 = S_2 - S_3$	$y^2 - 55$	$S_7 = S_3 * S_6$	$11 * 55$
$S_2 = S_1 * S_1$	y^2	$S_5 = S_4 * S_4$	$(y^2 - 55)^2$	$S_8 = S_5 - S_7$	$(y^2 - 55)^2 - 11 * 55$
$S_3 = 55$	55	$S_6 = 11$	11	$S_9 = S_1 * S_8$	$y((y^2 - 55)^2 - 11 * 55)$

2.6. Problem "`Calculator`*"*

2.6.1. Formulation. Alice and Bob are practicing in developing toy cryptographic applications for smartphones. This year they have invented `Calculator` that allows one to perform the following operations modulo 2019:

- to insert at most 4-digit positive integers (digits from 0 to 9);
- to perform addition, subtraction, and multiplication of two numbers;
- to store temporary results and read them from the memory.

Suppose that Alice wants to send Bob a ciphertext y (given by a 4-digit integer). She sends y from her smartphone to Bob's `Calculator` memory. To decrypt y, Bob needs to get the plaintext x (using his `Calculator`) by the rule $x = f(y) \bmod 2019$, where f is a secret polynomial known to Alice and Bob only.

At the most inopportune moment, Bob dropped his smartphone and broke its screen (see Fig. 6). Now, the button "+" as well as all digits except "2" are not working.

Help Bob to invent an efficient algorithm of how to decrypt any ciphertext y using `Calculator` in his situation if the current secret polynomial is $f(y) = y^5 + 1909y^3 + 401y$. More precisely, suggest a short list of commands, where each command has one of the following types ($1 \leqslant j, k < i$):

$$S_i = y, \quad S_i = 2, \quad S_i = 222, \quad S_i = S_j - S_k, \quad S_i = 22, \quad S_i = 2222, \quad S_i = S_j * S_k.$$

The first command has to be $S_1 = y$. In the last command, the resulted plaintext x has to be calculated. We remind that all calculations are modulo 2019. In particular, the integer 2222 becomes 203 immediately after entering. The shorter the list of commands you suggest, the more scores you get for this problem.

Example. The following list of commands calculates $x = y^2 - 4$:

Command	Result
$S_1 = y$	y
$S_2 = S_1 * S_1$	y^2
$S_3 = 2$	2
$S_4 = S_3 * S_3$	4
$S_5 = S_2 - S_4$	$y^2 - 4$

Fig. 6. Broken `Calculator`.

2.6.2. Solution. The polynomial $f(y) = y^5 + 1909y^3 + 401y$ is the Dickson polynomial $D_5(y, a) = y^5 - 5y^3a + 5ya^2$ for $a = 22$ with coefficients taken modulo 2019. The following relations hold:

$$\begin{aligned} D_5(y, a) &= yD_4(y, a) - aD_3(y, a) = yD_2(D_2(y, a), a^2) - aD_3(y, a) \\ &= y((y^2 - 2a)^2 - 2a^2) - ay(y^2 - 2a - a). \end{aligned}$$

For $a = 22$, the value $f(y)$ can be calculated for any y by the list of commands given in Table 5.

What was surprising that the participants found two solutions that has 11 and 13 steps! These solutions were awarded by additional points. The solution with 11 steps were found by Madalina Bolboceanu (Romania, Bitdefender) during the first round (Table 6). The solution with 13 steps were given by Henning Seidler and Katja Stumpp team (Germany, TU Berlin) during the second round. Both solutions were based on the representation $f(y) = y((y^2 - 44)(y^2 - 66) - 22^2)$.

Table 5. List of commands for the Program Committee solution

Command	Result	Command	Result
$S_1 = y$	y	$S_8 = S_7 * S_7$	$(y^2 - 2a)^2$
$S_2 = 2$	2	$S_9 = S_8 - S_5$	$(y^2 - 2a)^2 - 2a^2$
$S_3 = 22$	a	$S_{10} = S_1 * S_9$	$y((y^2 - 2a)^2 - 2a^2)$
$S_4 = S_2 * S_3$	$2a$	$S_{11} = S_7 - S_2$	$y^2 - 2a - a$
$S_5 = S_3 * S_4$	$2a^2$	$S_{12} = S_1 * S_{11}$	$y(y^2 - 2a - a)$
$S_6 = S_1 * S_1$	y^2	$S_{13} = S_3 * S_{12}$	$ay(y^2 - 2a - a)$
$S_7 = S_6 - S_4$	$y^2 - 2a$	$S_{14} = S_{10} - S_{13}$	$f(y)$

Table 6. List of commands for the 11-step solution

Command	Result	Command	Result
$S_1 = y$	y	$S_7 = S_6 - S_4$	$y^2 - 44 - 22$
$S_2 = S_1 * S_1$	y^2	$S_8 = S_6 * S_7$	$(y^2 - 44) * (y^2 - 44 - 22)$
$S_3 = 2$	2	$S_9 = S_4 * S_4$	22^2
$S_4 = 22$	22	$S_{10} = S_8 - S_9$	$(y^2 - 44) * (y^2 - 44 - 22) - 22^2$
$S_5 = S_3 * S_4$	44	$S_{11} = S_1 * S_{10}$	$f(y)$
$S_6 = S_2 - S_5$	$y^2 - 44$		

2.7. Problem "A Promise"

2.7.1. Formulation. Young cryptographers, Alice, Bob and Carol, are interested in quantum computings and really want to buy a quantum computer. A millionaire gave them some certain amount of money (say, X_A for Alice, X_B for Bob, and X_C for Carol). He also made them promise that they would not tell anyone including each other, how much money everyone of them had received.

• Could you help the cryptographers to invent an algorithm of how to find out (without breaking the promise) whether the total amount of money they have, $X_A + X_B + X_C$, is enough to buy a quantum computer?

• What weaknesses does your algorithm have (if someone breaks the promise)? Does it always protect the secret of the honest participants from the dishonest ones?

2.7.2. Solution. This problem is a particular case for the problem "A promise and money" for only three participants (see Section 2.8).

2.8. Problem "A Promise and Money"

2.8.1. Formulation. A group of young cryptographers are interested in quantum computings and really want to buy a quantum computer. A millionaire gave them a certain amount of money (say, n cryptographers; X_i for each of them, $i = 1, \ldots, n$). He also made a promise from them that they would not tell anyone, including each other, how much money everyone of them had received.

• Could you help the cryptographers to invent an algorithm of how to find out (without breaking the promise) whether the total amount of money they have, $\sum_{i=1}^{n} X_i$, is enough to buy a quantum computer?

• What do you think whether there are such algorithms protecting the secrets of honest participants from dishonest ones?

• What weaknesses does your algorithm have (if someone breaks the promise)? Does it always protect the secret of honest participants from dishonest ones?

2.8.2. Solution. Here we give an idea of the solution proposed by Mikhail Kudinov (Bauman Moscow State Technical University).

First of all, it is supposed that no one can buy a quantum computer himself without other participants. Let us assume that N' is the amount of money that one needs to buy a quantum computer and

$$N = nN',$$

where n is the number of participants. The millionaire gave them X_i money for $i \in \{1, \dots, n\}$. Each participant chooses random secrets $s_{i,j}$ uniformly so that

$$\sum_{j=1}^{n} s_{i,j} \equiv X_i \pmod{N}.$$

Then each of them gives the share $s_{i,j}$ to the owner of X_j by the secure channel. After this procedure, the owner of X_i has shares $s_{k,i}$ for each $k \in \{1, \dots, n\}$. It is obvious that

$$\sum_{j=1}^{n} \sum_{i=1}^{n} s_{i,j} = \sum_{i=1}^{n} X_i \pmod{N}.$$

Under the first suggestion, all participants can together calculate the common amount of money.

The main disadvantage of the algorithm, in addition to the suggestion, is a big amount of private communication (though the number of keys can be n for asymmetric schemes).

By analogy, many participants described algorithms similar to Schneier's calculating average salary algorithm [9]. In general, all these algorithms are vulnerable if $n - 1$ participants are dishonest. Some participants tried to describe a possibility of using a cryptosystem that is homomorphic by "+" and preserves relation "<," as some general analysis.

The problem of the first school round is the same problem for $n = 3$ (score assignment was more loyal). Despite there was quite a few solutions for this problem in the student round, each solution had big or small lacks in analysis of the general case, in analysis of the algorithm advantages and disadvantages, in description of communications (the number of the private communications, what kind of cryptography is used, the number of required private keys), and so on. As a result, there was no possibility to chose the "best of the best" for 6 scores, and we decided to give 5 scores as maximum. There were nine maximal-scored solutions.

2.9. Problem "16QAM"

2.9.1. Formulation. For sending messages, Alice and Bob use a fiber-optic communication via 16QAM technology. This technology allows them to send messages whose alphabet consists of 16 letters, where each letter is usually encoded with a 4-bit Gray code. While a message is transmitted in the channel, single errors in codewords of the Gray code are possible.

Alice has read an interesting book and would like to share her enthusiasm with Bob! Alice sent a short fragment from the book to Bob. Owing to the characteristics of the communication channel used, she divided the text into two parts and sent them separately. In the first part, she placed all of the 16 consonants that occurred in this fragment; in the second part, she placed vowels ("y" is a vowel), a space, a hyphen, and punctuation marks. Then Alice also encoded the letters with a Hamming code to be able to correct single errors. She applied a 7-bit Hamming code with the parity-check matrix whose columns are written in lexicographical order.

Bob received the two parts of ciphertext given in hexadecimal notation (see Table 7).

Also, he received the following number sequence:

22, 19, 3, 3, 36, 53, 3, 33, 20, 28.

Each number indicates how many consonants are contained between the punctuation marks.

Recover the text and find the main character of the book Alice has read!

Table 7. The ciphertext that Bob received from Alice (Problem "16QAM")

Part 1	Part 2
66674C36666F43D3C199900AA1AA325992A	66CA61967319CCD2CE76998CE6433332D19
67A59D9B4A8B69330D1BC000153367A5E33	B46784C65334E999A402ADA0265A99A6633
D30E6692D0F349D3321FFFF0ED706667A7F	33319B32D3299698CCC96986619967134CC
670D999679F4AA67561BA679B4AA54F34D5	B4CE23333334CC6730CE90170CCCD2CE669
AB0F4AACCF000055CE633670D9DA54CE37F	996A61999EA63332CCA4C3332D4CD3334CC
660DE19CD995335495523CCAAA8F1E03325	D3319994730CCCD3A6669D96A66999699B3
86CF48A98CD9B387FD9D546A99E9D200033	98640CC86CE619676AD4CD3308999866D33
3201513FE5B4AA00CCCE9667554CD2CCCB3	79321C33210B4C6732199B53218019A404C
330F32A666553CD756AC3E0674E9D369E1D	D2DE65A986663398CCCCCB5319CC6665997
C6A9999780007F00961E66465519FEA8B25	B96A63398CD9CCD2CD9A399A66339866619
14CCCB332AA63332CCCE6D2A99AACCCC004	98CD9CC325A6339CCE619998C04C66CE633
	996A61998CF66967334CC66CA6199865E$(0)_2$

2.9.2. Solution. Some details in the problem statement are insignificant. Namely, we could omit the step with the Gray code and mind that Alice substitutes 7-bit codewords of the Hamming code for each symbol in each part of the plaintext.

The crucial idea to broke the cipher Alice and Bob use is analyzing the frequency distribution in each part of the ciphertext. This helps them to deduce the probable meaning of the most common symbols and form partial words. Tentative search for the combinations of consonants and vowels giving actual words in English expands the partial solution. Frequencies of the pairs of letters also give an improvement but it could seem inessential. At last, one can employ search engine on the Internet to find the fragment of the book that Alice sent to Bob.

Let us consider a possible solution. Alice uses the Hamming code with the parity check matrix H and the corresponding generator matrix G, where

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \qquad G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

First, rewrite each part of the given ciphertext in the binary form. Split them into 7-bit words and correct errors using the parity check matrix H. One can decode the Hamming code into a 4-bit Gray code but it is not a necessary step for the solution. Calculating the frequencies of the codewords separately in each part of the given ciphertext, we put them in Table 8.

Compare the frequencies obtained with those of letters in the English language. The suitable frequency distribution can be found in [10] cited, e.g., at [11]. According to Lewand, arranged from most to least common in appearance, the letters are:

e t a o i n s h r d l c u m w f g y p b v k j x q z.

We start with vowels, punctuation marks, spaces, and a hyphen, which are placed in Part 2. Make a guess that the most frequent symbol in Part 2 is the space. It is also worth to note that most of the punctuation marks are followed by a space in contrast to a hyphen, which is usually embraced by letters. Using letter frequencies, we determine the probable spaces, vowels, and hyphen and construct the following partial solution for this part of the plaintext (the sign # substitutes punctuation):

```
ee ae e oe o e ua iaia# e oo oy-oy i o ea ee# u# ea# auae o ie ea o e aoy a oe
o i a i eae# a i o o o eae a oo o i o iee ay ue aeii o aa aie# uuay# e uai uy oy
oe i a e ea i e eae# i e ee oeee o e a a ee a# e e a uy ee e i a e oe o ee a a#
```

Let us turn to Part 1 which contains 16 consonants occurring in the fragment of the book. Let us order the codewords of the Hamming code from most to least frequent in Part 1, as it is shown in Table 8, a. Denote the 7-bit codewords by hexadecimal numbers from 0 till F. Then we get the following ciphertext

Table 8. Frequencies of Hamming codewords in the text

Gray code	Hamming code	Frequency
1011	0110011	46
0010	0101010	30
1001	0011001	24
0001	1101001	24
0011	1000011	19
0000	0000000	15
0110	1100110	13
1100	0111100	8
1111	1111111	8
1101	1010101	7
0100	1001100	6
1110	0010110	5
1010	1011010	5
0101	0100101	4
1000	1110000	4
0111	0001111	2

(a) Part 1

Gray code	Hamming code	Frequency
0100	1001100	85
1011	0110011	50
1001	0011001	33
0001	1101001	26
1010	1011010	17
0011	1000011	9
0000	0000000	8
1110	0010110	7
1100	0111100	2
0010	0101010	1
1000	1110000	1
0111	0001111	0
0101	0100101	0
1101	1010101	0
0110	1100110	0
1111	1111111	0

(b) Part 2

of 220 symbols in length that is splitted into 10 pieces (according to the number sequence given in the task):

```
023402C43E0251412B0103  02C1B32407551003703  4A3  B46  33A4884CE02E804020631094106311739943
1675510A0040C1068047266101D10619FF56D4031A00048090103  355
025108B315023021A3020246102173994  E2333C72410275585D46  021281BD102021A0202631016055
```

Then we match the symbol frequencies in Part 1 of the ciphertext with those of consonants in the English alphabet. The first five pairs are like as follows: `0 - t`, `1 - n`, `2 - s/h`, `3 - s/h`, and `4 - r`.

The bigram "`th`" is the most frequent in English. This allows us to make a suggestion that "`2`" substitutes "`h`" and "`3`" substitutes "`s`." Then we obtain a partial solution for Part 1 and, combining with one for Part 2, get the following pieces of the plaintext given in Table 9. It is not difficult to recognize words "`these are the`" at the beginning in (1). Also, we can see "`the`" as the first word in (2) and (8).

The best idea for the next step is to search through the English dictionary for the words that have given vowels in the prescribed order. It is possible to use one of the tools for the pattern recognition available on the Internet, e.g., [12]. Advanced participants of the Olympiad implemented some computer programs on their own.

Consider several examples. We have a word with consonants "`s55`" and vowels "`uuay`" in (7), and the last two consonants are identical. The only match is "`usually`", so we assume that "`5`" substitutes the letter "`l`." The pattern "`auae`" in combination with double "`s`" gives us two possibilities in (5): "`assuage`" and "`sausage`." In any case, it seems like "`A`" means "`g`." Then we have "`rugs`" in (3). The pattern "`uai`" and consonants "`5nt8B`" lead us to "`lunatic`" in (8), so "`8`" probably means "`c`."

At this point we revise our matching the letters and their frequencies corresponding to the Part 1 of the ciphertext. Let us look at the first eight letters with large frequencies: "`t n h s r l 6 7/c`."

Table 9. Partial plaintext

No.	Partial plaintext
(1)	thsrthCrsEth5nrnhBtnts ee ae e oe o e ua iaia#
(2)	thCnBshrt755ntts7ts e oo oy-oy i o ea ee#
(3)	rAs u#
(4)	Br6 ea#
(5)	ssAr88rCEthE8trtht6snt9rnt6snn7s99rs auae o ie ea o e aoy a oe o i a i eae#
(6)	n6755ntAttrtCnt68tr7h66ntnDnt6n9FF56DrtsnAtttr8t9tnts a i o o o eae a oo o i o iee ay ue aeii o aa aie#
(7)	s55 uuay#
(8)	th5nt8Bsn5thsthnAsththr6nthn7s99r e uai uy oy oe i a e ea i e eae#
(9)	EhsssC7hrnth75585Dr6 i e ee oeee o e a a ee a#
(10)	thnh8nBDnththnAthth6sntn6t55 e e a uy ee e i a e oe o ee a a#

We can see that the letter "d" has still been hidden. According to the Lewand distribution it is the most probable that "6" means "d." Then (4) contains "Brd" and "ea" that gives us possible words "beard" and "bread." Therefore, it seems like "B" substitutes "b."

A thorough analysis of the remaining ciphertext and search for words by patterns and number of letters eventually lead us to the plaintext (with punctuation replaced by #):

these are the mores of the lunar inhabitants# the moon boy-shorty will not eat sweets# rugs# bread# sausage or ice cream of the factory that does not print ads in newspapers# and will not go to treatment a doctor who did not invented any puzzle advertising to attract patients# usually# the lunatic buys only those things that he read in the newspaper# if he sees somewhere on the wall a clever ad# then he can buy even the thing that he does not need at all#

This is a fragment of the fairytail novel "Dunno on the Moon" by the Russian writer Nikolay Nosov. The title character of the novel is a boy-shorty Dunno. The problem was completely solved by 13 teams in the second round and by Samuel Tang (Hong Kong, Black Bauhinia) in the first round. The best solutions were proposed by the team of Irina Slonkina, Mikhail Sorokin, and Vladimir Bobrov (Bauman Moscow State Technical University) and the team of Vladimir Paprotski, Dmitry Zarembo, and Karina Kruglik (Belarusian State University).

2.10. Problem "APN + Involutions"

The first three questions **Q1**, **Q2**, and **Q3** were given as the problem "APN + Involutions" in the first round. The extended version of the task for the second round included also Question **Q4** that contains some open problems.

2.10.1. Formulation. Alice wants to construct a block cipher with heavy use of **involutions** as subcomponents; this minimizes the difference between the algorithms for encryption and decryption. She knows that APN *permutations* are the best choice of subcomponents to resist the attacks based on differential technique. She wants to construct some set of APN permutations that are involutions for every $n \geqslant 2$.

Alice knows that every involution can be expressed as the product of disjoint *transpositions*. So, she decides to study the following involution

$$g = \prod_{i=1}^{d} (\alpha_i, \alpha'_i),$$

where $\{\alpha_i, \alpha'_i\} \cap \{\alpha_j, \alpha'_j\} = \varnothing$ for all $i, j \in \{1, ..., d\}$, $i \neq j$, and $1 \leqslant d \leqslant 2^{n-1}$.

Alice needs your help to get APN permutations among such involutions g. Find answers to the following questions!

Q1: Let

$$\Lambda(g) = \{\alpha_i \oplus \alpha'_i : \ i = 1, ..., d\}, \qquad \widehat{\Lambda}(g) = [\alpha_i \oplus \alpha'_i : \ i = 1, ..., d],$$
$$\mathrm{B}(g) = \{x \oplus y : \ \{x, y\} \subseteq \mathrm{FixP}(g), \ x \neq y\}, \qquad \widehat{\mathrm{B}}(g) = [x \oplus y : \ \{x, y\} \subseteq \mathrm{FixP}(g), \ x \neq y],$$

where $\mathrm{FixP}(g)$ is the set of all *fixed points* of g; i.e. $\mathrm{FixP}(g) = \{x \in \mathbb{F}_2^n : \ g(x) = x\}$.

Suppose that g is an APN permutation. Get necessary conditions for multisets $\widehat{\Lambda}(g)$, $\widehat{\mathrm{B}}(g)$ and sets $\Lambda(g)$, $\mathrm{B}(g)$. Prove that if your conditions do not hold then g is not an APN permutation.

Q2: Let $\mathrm{d}_{a,b}(g) = |\{x \in \mathbb{F}_2^n : g(x \oplus a) \oplus g(x) = b\}|$, $a, b \in \mathbb{F}_2^n$. Let g be an involution and APN. Find $\mathrm{d}_{a,a}(g)$ for each nonzero $a \in \mathbb{F}_2^n$.

Q3: Can you get the nontrivial upper bound on $|\mathrm{FixP}(g)|$?

Q4: Let M_n be the set of all n-bit involutions that are APN permutations.

(1) Can you find the size of M_n for $n = 2, 3, 4$?

(2) Can you find the size of M_n for $n = 5$?

(3) *A Bonus Problem (extra scores, a special prize!)*

Let $n \geqslant 6$. Can you get the lower and the upper bounds for the size of M_n? Can you describe involutions from M_n? Can you suggest constructions for involutions from M_n?

Note that the mapping $x \mapsto x^{-1}$ in the Galois field $GF(2^n)$ belongs to M_n for odd $n \geqslant 3$.

Remark. Let us recall some relevant definitions:

• $\mathbb{F}_2^n$ is the vector space of dimension n over $\mathbb{F}_2 = \{0, 1\}$.

• A vector $x \in \mathbb{F}_2^n$ has the form $x = (x_1, ..., x_n)$, where $x_i \in \mathbb{F}_2$. For two vectors $x, y \in \mathbb{F}_2^n$ their sum is $x \oplus y = (x_1 \oplus y_1, ..., x_n \oplus y_n)$, where $\oplus$ stands for XOR operation.

• Let $\widehat{X} = [x_1, ..., x_d]$ be a multiset with the underlying set $\mathbb{F}_2^n$, where $x_1, ..., x_d \in \mathbb{F}_2^n$. Note that all elements in a set are distinct. Unlike a set, a multiset allows for multiple instances for each of its elements.

• A *permutation* s is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $s(x) \neq s(y)$ for all $x, y \in \mathbb{F}_2^n$, $x \neq y$.

• An *involution* s is a permutation that is its own inverse, $s^2(x) = s(s(x)) = x$ for all $x \in \mathbb{F}_2^n$.

• For every different vectors $\alpha, \beta \in \mathbb{F}_2^n$, a permutation s is called a *transposition* if $s(\alpha) = \beta$, $s(\beta) = \alpha$, and $s(x) = x$ for all $x \in \mathbb{F}_2^n \backslash \{\alpha, \beta\}$; it is denoted by $s = (\alpha, \beta)$.

• A permutation s is called APN (Almost Perfect Nonlinear) if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$, the equation $s(x \oplus a) \oplus s(x) = b$ has at most 2 solutions.

2.10.2. Solution. Consider the solutions of the problem.

Q1: Let $a \in \Lambda(g)$. Hence, $a = x \oplus y$, where $y = g(x)$ and $(x, y) = (\alpha_i, \alpha_i')$ for some i. Then

$$g(x \oplus a) = g(y) = x = y \oplus a = g(x) \oplus a.$$

Let $a \in \mathrm{B}(g)$. Hence, $a = x \oplus y$, where $x, y \in \mathrm{FixP}(g)$. Then

$$g(x \oplus a) = g(y) = y = x \oplus a = g(x) \oplus a.$$

Thus, $\mathrm{d}_{a,a}(g) \geqslant 2$ for every vector $a \in \Lambda(g) \cup \mathrm{B}(g)$.

Let g be an APN permutation. Then $\mathrm{d}_{a,a}(g) = 2$. Hence, the multiplicity of all elements from $\Lambda(g)$ and $\mathrm{B}(g)$ is 1. Thus, $\Lambda(g) = \widehat{\Lambda}(g)$ and $\mathrm{B}(g) = \widehat{\mathrm{B}}(g)$. Note that $\Lambda(g) \cap \mathrm{B}(g) = \varnothing$.

Q2: Since g is an APN permutation; therefore, $\mathrm{d}_{a,a}(g) \leqslant 2$. As we get in **Q1**, $\mathrm{d}_{a,a}(g) = 2$ for every vector $a \in \Lambda(g) \cup \mathrm{B}(g)$. Let us prove that $\mathrm{d}_{a,a}(g) = 0$ for $a \notin \Lambda(g) \cup \mathrm{B}(g)$.

Let a be a nonzero vector and x be a solution of $g(x \oplus a) \oplus g(x) = a$. Since g is a permutation, either $x \in \mathrm{FixP}(g)$ or $x = \alpha_i$ $(x = \alpha_i')$ for some i. Consider the two cases:

1. Let $x \in \mathrm{FixP}(g)$. Then, $g(x \oplus a) \oplus g(x) = a$ implies $g(x \oplus a) = x \oplus a$. Hence, $x \oplus a \in \mathrm{FixP(g)}$. As a result, $a \in B(g)$.

2. Without loss of generality, let $x = \alpha_i$ for some i and $y = x \oplus a$. If $y \in \mathrm{FixP}(g)$ then $g(x \oplus a) \oplus g(x) = a$ implies $g(x) = x$, which is a contradiction. Hence, without loss of generality, $y = \alpha_j'$ for some j (so, we have $\alpha_i \oplus \alpha_j' = a$). Then

$$g(\alpha_i \oplus a) \oplus g(\alpha_i) = a \;\;\Rightarrow\;\; g(\alpha_j') \oplus \alpha_i' = a \;\;\Rightarrow\;\; \alpha_j \oplus \alpha_i' = a.$$

Let us show that α_i' and α_j is also solutions. Indeed,

$$g(\alpha_i' \oplus a) \oplus g(\alpha_i') = g(\alpha_j) \oplus \alpha_i = \alpha_j' \oplus \alpha_i = a, \quad g(\alpha_j \oplus a) \oplus g(\alpha_j) = g(\alpha_i') \oplus \alpha_j' = \alpha_i \oplus \alpha_j' = a.$$

Thus, if $i \neq j$ then we get at least 3 solutions that is a contradiction for the APN property of g. Hence, $j = i$ and $a \in \Lambda(g)$.

Q3: Let us prove that $|\mathrm{FixP}(g)| \leqslant 1 + (2^{n-1} - 1)^{1/2}$.

The involution g is APN. From **Q1** we have

$$\mathrm{B}(g) \cap \Lambda(g) = \varnothing. \tag{1}$$

Let $q = |\mathrm{FixP}(g)|$. Since g is an involution, q is even. Owing to (1) and $\Lambda(g) \cup \mathrm{B}(g) \subseteq \mathbb{F}_2^n \backslash \{\mathbf{0}\}$, we have

$$|\Lambda(g)| + |\mathrm{BB}(g)| \leqslant 2^n - 1. \tag{2}$$

Since $|\mathrm{B}(g)| = \binom{q}{2}$, $|\Lambda(g)| = 2^{n-1} - q/2$, we have $|\Lambda(g)| + |\mathrm{BB}(g)| = q(q-1)/2 + 2^{n-1} - q/2$.

From (2), we have $q(q-1)/2 + 2^n - q \leqslant 2^n - 1$. Thus, $q(q-2)/2 \leqslant 2^{n-1} - 1$; i.e.,

$$q \leqslant 1 + (2^{n-1} - 1)^{1/2}.$$

Q4: (a) It could be computationally verified that $M_2 = \varnothing$ and $|M_3| = 224$. Then, it is known [13] that there are no APN permutations for $n = 4$. Hence, $M_4 = \varnothing$.

(b) Recall some definitions:. A function $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *affine* if $A(x \oplus y) = A(x) \oplus A(y) \oplus A(\mathbf{0})$ for all $x, y \in \mathbb{F}_2^n$. Two functions $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called *affine equivalent* if there exist affine permutations A_1 and A_2 such that $F = A_1 \circ F \circ A_2$. It is easy to see that the APN permutation property of a function is an invariant under the affine equivalence. There exist [13] only five affine equivalence classes of APN permutations. Moreover, by [13, theorem 3], only one class contains functions together with their inverses. Hence, only this class of APN permutations can contain involutions. The representative of this class is the famous inverse function over the finite field: $F(x) = x^{-1}$ for nonzero x and $F(0) = 0$ (here, functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ are considered as functions over the finite field of order 2^n). The inverse function is an involution. Thus, all APN involutions for $n = 5$ are affine equivalent to the inverse function.

(c) There were no interesting suggestions by the participants for these open problems.

The unique full correct solution in the first round was proposed by Henning Seidler (Germany, TU Berlin). In the second round, the best solution for 11 scores was proposed by the team of Kristina Geut, Sergey Titov, and Dmitry Ananichev (Russia, Ural State University of Railway Transport, Ural Federal University).

2.11. Problem "Sharing"

2.11.1. Formulation. Bob is interested in studying mathematical countermeasures to side-channel attacks on block ciphers. He found out that the techniques such as special sharings of functions can be applied. Now he is thinking about the following mathematical problem in this approach:

Let $\mathcal{F}$ denote the set of *invertible functions* (*permutations*) from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$ and let $\mathcal{F}^n$ denote the set of invertible functions from $(\mathbb{F}_2^4)^n$ to $(\mathbb{F}_2^4)^n$. Let $F \in \mathcal{F}^n$ be

$$F(x_1, x_2, \ldots, x_n) = \big(F_1(x_1, x_2, \ldots, x_n), F_2(x_1, x_2, \ldots, x_n), \ldots, F_n(x_1, x_2, \ldots, x_n)\big),$$

with component functions $F_i : (\mathbb{F}_2^4)^n \to \mathbb{F}_2^4$, $i = 1, \ldots, n$.

For every $f \in \mathcal{F}$, a function $F \in \mathcal{F}^n$ is called a *sharing* of f if

$$\sum_{i=1}^{n} F_i(x_1, x_2, \ldots, x_n) = f\left(\sum_{i=1}^{n} x_i\right) \quad \text{for all } (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_2^4)^n.$$

Moreover, F is an *noncomplete* sharing of f if F is a sharing of f with the additional property that each component function F_i is independent of x_i.

Bob needs your help to study functions for which a noncomplete sharing exists. Find answers to the following questions!

Q1: Let $\mathcal{A}$ denote the set of *affine functions* from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$. Two functions $f, g \in \mathcal{F}$ are *affine equivalent* if there exist $a, b \in \mathcal{A}$ such that $g = b \circ f \circ a$.

Let f and g be two functions in the same affine equivalence class of $\mathcal{F}$ and let F be a noncomplete sharing of f. Derive from F a noncomplete sharing for g.

All functions of the same affine equivalence class have the same degree. It is known [14] that this equivalence relation partitions $\mathcal{F}$ into 302 classes: 1 class corresponds to $\mathcal{A}$, 6 classes contain quadratic functions, and 295 classes contain cubic functions.

Also, Bob knows that when $n \geqslant 5$ then there exists a noncomplete sharing for each $f \in \mathcal{F}$ (it can be shown by construction). When $n = 2$ then a noncomplete sharing exists only for the functions in $\mathcal{A}$. When $n = 3$ then a noncomplete sharings exist for $\mathcal{A}$ and also for 5 out of the 6 equivalence classes containing quadratic functions. When $n = 4$ then noncomplete sharings exist for $\mathcal{A}$, for all 6 quadratic equivalence classes, and for 5 cubic classes.

Q2: *A Bonus problem (extra scores, a special prize!)*

Find a concise mathematical property that $f \in \mathcal{F}$ must have in order that a noncomplete sharing F exists for $n = 3$ and $n = 4$.

Q3: *A Bonus problem (extra scores, a special prize!)*

Generalize to functions over $\mathbb{F}_2^5$ and $\mathbb{F}_2^6$.

2.11.2. Solution. **Q1:** Let f and g be two functions in the same affine equivalence class of $\mathcal{F}$; i.e., $g = b \circ f \circ a$ for some $a, b \in \mathcal{A}$, and let $F \in \mathcal{F}^n$ be a noncomplete sharing of f. At first, one can notice that since f and g are invertible, the mappings a and b must be invertible as well. Let us denote

$$a(x) = Ax + a', \qquad x \in \mathbb{F}_2^4, \qquad\qquad b(x) = Bx + b', \qquad x \in \mathbb{F}_2^4,$$

where A and B are nonsingular binary matrices of order 4×4 and $a', b' \in \mathbb{F}_2^4$.

Using the components functions $\{F_i\}_{i=1}^n$ of F, we define the invertible function $G \in \mathcal{F}^n$ with components functions

$$G_j\,(x_1, x_2, ..., x_n) = \begin{cases} BF_1\,(Ax_1 + a', Ax_2, ..., Ax_n) + b', & j = 1, \\ BF_j\,(Ax_1 + a', Ax_2, ..., Ax_n)\,, & j \neq 1, \end{cases}$$

where $j = 1, 2, ..., n$.

Then for every $(x_1, x_2, ..., x_n) \in \left(\mathbb{F}_2^4\right)^n$, we have

$$\sum_{j=1}^{n} G_j(x_1, x_2, ..., x_n) = BF_1\left(Ax_1 + a', Ax_2, ..., Ax_n\right) + b'$$

$$+ \sum_{j=2}^{n} BF_j\left(Ax_1 + a', Ax_2, ..., Ax_n\right) = B\left(\sum_{j=1}^{n} F_j\left(Ax_1 + a', Ax_2, ..., Ax_n\right)\right) + b'$$

$$= Bf\left(Ax_1 + a' + Ax_2 + \ldots + Ax_n\right) + b'$$

$$= Bf\left[A\left(\sum_{i=1}^{n} x_i\right) + a'\right] + b' = b \circ f \circ a\left(\sum_{i=1}^{n} x_i\right) = g\left(\sum_{i=1}^{n} x_i\right).$$

Therefore, the function $G \in \mathcal{F}^n$ defined as

$$G(x_1, x_2, ..., x_n) = \left(G_1(x_1, x_2, ..., x_n), G_2(x_1, x_2, ..., x_n), ..., G_n(x_1, x_2, ..., x_n)\right),$$

is a sharing of g.

From noncompleteness of F it follows that G_j, which is in fact an affine transformation of F_j, does not depend on x_j. Hence, G is a noncomplete sharing of g.

Q2–Q3: These open problems were not solved completely during the Olympiad. Nevertheless, one perspective solution was proposed by the team of Victoria Vlasova, Mikhail Polyakov, and Alexey Chilikov (Bauman Moscow State Technical University). They found a sufficient condition for the existence of a noncomplete sharing for $n = 3$. Let us describe it here.

Let $\mathrm{wt}(y)$ be the Hamming weight of a binary vector y. Given $\sigma \in \mathbb{F}_2$, put

$$\delta_\sigma(y) = \begin{cases} y, & \sigma = 1, \\ \mathbf{0}, & \sigma = 0, \end{cases}$$

where $\mathbf{0}$ is the zero vector of the same dimension as y.

Let V be a vector space over the field K and assume that for the invertible function $f : V \to V$ it holds

$$\sum_{\sigma \in \mathbb{F}_2^n} (-1)^{\mathrm{wt}(\sigma)} f\left(\sum_{i=1}^{n} \delta_{\sigma_i}(x_i)\right) = 0. \tag{3}$$

Then there exists a noon-complete sharing for f. Further we consider the case $n = 3$.

Indeed, given $(x_1, x_2, x_3) \in V^3$, put

$$F_1(x_1, x_2, x_3) = f(x_2) - f(x_2 + x_3), \qquad F_2(x_1, x_2, x_3) = f(x_3) - f(x_1 + x_3),$$

$$F_3(x_1, x_2, x_3) = f(x_1) - f(x_1 + x_2).$$

It is clear that every $F_i : V^3 \to V$ does not depend on x_i, where $i = 1, 2, 3$. Consider the expression

$$\sum_{i=1}^{3} F_i(x_1, x_2, x_3) = f(x_2) - f(x_2 + x_3) + f(x_3) - f(x_3 + x_1) + f(x_1) - f(x_1 + x_2)$$

$$= \sum_{\sigma \in \mathbb{F}_2^3} (-1)^{\mathrm{wt}(\sigma)} f\left(\sum_{i=1}^{3} \delta_{\sigma_i}(x_i)\right) + f(x_1 + x_2 + x_3) - f(0) = f(x_1 + x_2 + x_3) - f(0).$$

Without loss of generality we assume that $f(0) = 0$. Otherwise, we can consider the initial problem for the function $g(x) = f(x) - f(0)$ with $g(0) = 0$ and which, by the arguments from **Q1**, has a noncomplete sharing if and only if f does.

Finally, $\sum_{i=1}^{3} F_i(x_1, x_2, x_3) = f(x_1 + x_2 + x_3)$, which completes the proof.

It was also shown by the authors that the condition (3) is necessary for the existence of a noncomplete sharing of f for all n.

Taking $V = \mathbb{F}_2^m$ with $m = 4, 5, 6$ and $K = \mathbb{F}_2$, we can obtain a solution of **Q2** and **Q3** for the case $n = 3$.

2.12. Problem "Factoring in 2019"

2.12.1. Formulation. Nicole is learning about the RSA cryptosystem. She has chosen random 500-bit prime numbers p and q, $2^{499} \leqslant p, q < 2^{500}$, and computed $n = p \cdot q$. Being a curious and creative person, she has also combined the three numbers in funny ways. Her favorite one is an integer h such that

$$h \equiv 3^{2019}p^2 + 5^{2019}q^2 \pmod{n^2 + 8 \cdot 2019}.$$

Unfortunately, she has lost the paper where she wrote the two prime numbers. Luckily, she remembers n and h. Help Nicole to recover p and q.

$$\begin{aligned} n = {} & 40763613025504836845249840044831561583564626405535158138667037\\ & 18791672670905308860844304055285019651507728831663677166092475\\ & 16155419756121537288444995708421977847213953345126368990185271\\ & 10259760189356588305406519080647582874212687596214191915933827\\ & 67252094717222418132289251314647500491996323400002019, \end{aligned}$$

$$\begin{aligned} h = {} & 78307999278336577586961528110240026923828914927526911949501196\\ & 64549497756373569985393554661132717198368717093111812566649031\\ & 17342818449633588647098544612151278035131454234786653136500887\\ & 08830470996542888912418213532073622903727205396807848603735835\\ & 72653630883685906916701587362236649126895719656663293825501223\\ & 97088799629252601249428062432254738935764304610281613264225641\\ & 74990272864680012560095992125783832230234589257650929348364268\\ & 48117494065463529201859600747521892957258104033195441014023432\\ & 36581529201392185327635674923459290749241831590661903965132514\\ & 21544515183088866585058200066678369344118 81. \end{aligned}$$

2.12.2. Solution. This problem is based on a (simplified) variation of the Coppersmith method.

Let $m = n^2 + 8 \cdot 2019$. It is a composite number with unknown factors. The idea is to find an integer a such that the numbers $a_1 = a \cdot 3^{2019} \mod m$ and $a_2 = a \cdot 5^{2019} \mod m$ are small enough and $a_1p^2 + a_2q^2$ exceeds the modulus m by a small amount and can be recovered from $a \cdot h \mod m$. This can be done using the Lagrange–Gauss algorithm (which is a special case and the building block of the LLL algorithm). Let Λ be the lattice spanned by the two vectors

$$v_1 = \big(1,\ (5^{2019} \cdot (3^{2019})^{-1} \mod m)\big), \qquad v_2 = \big(0,\ m\big).$$

Consider an arbitrary vector $v = (a_1, a_2)$ in this lattice. It is easy to verify that

$$a_1p^2 + a_2q^2 \equiv a_1 \cdot h \cdot (3^{2019})^{-1} \pmod{m}.$$

The lattice reduction guarantees to find such vector v with the norm

$$\|v\| = \sqrt{a_1^2 + a_2^2} \leq 2^{(d-1)/4}(\det \Lambda)^{1/d} = \sqrt{m}/\sqrt[4]{2},$$

where $d = 2$ is the dimension of the lattice. In particular,

$$|a_1p^2 + a_2q^2| \leq n(p^2 + q^2) < n(p + q)^2 < 10n^2,$$

where the last two inequalities follow from the balancedness of the primes (i.e., $\max(p, q) \leq 2\min(p, q)$).

It follows that there exists an integer z, $|z| < 10$, such that

$$a_1 \cdot h \cdot (3^{2019})^{-1} \mod m + zm = a_1p^2 + a_2q^2.$$

In result, we obtain an equation in p^2 and q^2. By replacing $p = n/q$, we obtain a biquadratic equation in q which is easy to solve and factor n.

The final solution is:

$$p = 2019000075878154181681129810414477022346818209175194524879208890921501144547048007953722271285690350264116081579241189587393202602664199899594021414383,$$

$$q = 2019000073973494194521339805682093959182265746083995594826393753631669289175827851666668014167119439386543289850940734885806826120718179729242641026893.$$

The best solution was proposed by Alexey Zelenetskiy, Mikhail Kudinov, and Denis Nabokov team (Russia, Bauman Moscow State Technical University).

2.13. Problem "`TwinPeaks3`*" (online)*

2.13.1. Formulation. As Bob's previous cipher `TwinPeaks2` (NSUCRYPTO-2018) was broken again, he finally decided to read some books on cryptography. His new cipher is now inspired by practical ciphers, while the number of rounds was reduced a bit for better performance.

Not only the best techniques were adopted by Bob, but also he decided to enhance his cipher by security through obscurity, so the round functions are now unknown. The only thing known about these functions is that they are the same for odd and even rounds.

New Bob's cipher works as follows: A message X is represented as a binary word of length 128. The latter is divided into four 32-bit words a, b, c, and d; then the following round transformation is applied 32 times:

$$(a, b, c, d) \leftarrow (b, c, d, a \oplus (F_i(b, c, d))),$$
$$F_i = F_1 \text{ for odd rounds and } F_i = F_2 \text{ for the rest.}$$

Here F_1 and F_2 are secret functions accepting three 32-bit words and returning one word; and $\oplus$ is the binary bitwise XOR. The concatenation of the final a, b, c, d is the resulting ciphertext Y for the message X.

Agent Cooper again wants to read the Bob's messages. He caught the ciphertext

$$Y = \texttt{e473f19a247429ab33b66268d57dd241}$$

(the ciphertext is given in hexadecimal notation, the first byte is `e4`).

He was also able to gain access to Bob's testing server with encryption and decryption routines, using the secret key (see [15]). Unfortunately, the version of software available on this server is not final. So, the decryption routine is incomplete and only uses keys in the reverse order, which is not sufficient for decryption:

$$(a, b, c, d) \leftarrow (b, c, d, a \oplus (F_i(b, c, d))),$$
$$F_i = F_2 \text{ for odd rounds and } F_i = F_1 \text{ for the rest.}$$

The server can also process multiple blocks of text at a time: they will be processed one-by-one and then concatenated, as in the regular ECB cipher mode of operation. Ciphertexts and plaintexts are given and processed by the server in hexadecimal notation.

Help Cooper to decrypt Y.

2.13.2. Solution. Let f_i be the round transformation of round i:

$$f_i : \ (a, b, c, d) \leftarrow (b, c, d, a \oplus (F_{k(i)}(b, c, d))),$$

where $k(i) = 1$ for odd i and $k(i) = 2$ otherwise.

Hence, we can represent the encryption transformation E as $E = (f_1 f_2)^{16}$.

Let I be the incomplete decryption transformation described in the problem statement. The encryption and the incomplete decryption processes only differ in the key order, so I can be written as $I = (f_2 f_1)^{16}$.

The decryption transformation E^{-1} can be represented as $E^{-1} = (f_2^{-1} f_1^{-1})^{16}$, where f_i^{-1} is the inverse of f_i and is given by the transformation

$$f_i^{-1} : (a, b, c, d) \leftarrow (d \oplus (F_{k(i)}(a, b, c)), a, b, c).$$

Thus, to apply E^{-1} to the ciphertext one should be able to compute $F_1(x, y, z)$ and $F_2(x, y, z)$ that are secret. To recover these functions a *slide attack* can be used.

The idea is to find the words $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ such that $f_i(x) = y$. If such a pair is found then F_i can be found as $F_i(x_2, x_3, x_4) = y_4 \oplus x_1$.

We use the following idea to find a desired pair: If $Ef_i(x) = E(y)$ then $f_i(x) = y$. Let us start with F_1. We need a pair of x and y such that $Ef_1(x) = E(y)$. This relation can be written as

$$(f_1 f_2)^{16} f_1(x) = (f_1 f_2)^{16}(y), \qquad f_1 (f_2 f_1)^{16}(x) = (f_1 f_2)^{16}(y), \qquad f_1 I(x) = E(y).$$

We come to a conclusion that if $f_1 I(x) = E(y)$ then $f_1(x) = y$. The condition $f_1 I(x) = Ey$ can be checked by using the definition of f_1: if

$$(I(x))_2 = (E(y))_1, \qquad (I(x))_3 = (E(y))_2, \qquad (I(x))_4 = (E(y))_3$$

then it is *likely* that $f_1 I(x) = E(y)$. The probability of false positives is approximately 2^{-96} for random F_i functions. So, it can be considered as negligible. Both $I(x)$ and $E(y)$ are available on the encryption oracle for arbitrary x and y as the incomplete decryption and the encryption routines respectively.

To find $F_i(a, b, c)$, let us brute force over x and y of the following forms: $x = (X, a, b, c)$ and $y = (a, b, c, X')$. According to the birthday paradox, a desired pair can be found in $2 * 2^{16}$ operations average (instead of 2^{32} if we lock X or X' to some constant value).

As soon as we find such a pair x and y, we can compute $F_1(a, b, c)$ and apply f_1^{-1} to the ciphertext and decrypt the last round. Then F_2 can be found in the same way by replacing I and E with each other due to the symmetry. By doing this round by round, we decrypt the whole ciphertext and get the desired message (in hexadecimal notation)

`acherrypieplease`

The reference implementation of this attack requires 2^{22} blocks of text to be encrypted and 10 minutes of time average. It is important to use the server's ability to process multiple blocks of text at a time to minimize the amount of HTTP requests.

Four teams successfully solved the problem using the same method.

2.14. Problem "`Curl27`*"*

2.14.1. Formulation. Bob is developing the 3OTA infrastructure and has designed a new hash function Curl27 for it. A distinguishing feature of the infrastructure is the ternary logic: Trits from the set $\mathbf{T} = \{0, 1, -1\}$ are used instead of bits, ternary strings and words are used instead of binary ones. The Curl27 hash function is defined below. Its implementation in Java can be found in [16].

Find a collision for Curl27; i.e., different ternary strings X and X' such that $\mathsf{Curl27}(X) = \mathsf{Curl27}(X')$. Submit colliding strings as two lines of trits separated by commas. An example of a (wrong!) solution is:

$$-1, 1, 0, 1, 1, 0 \qquad -1, -1, 1, 0, 1, 1, -1, 0$$

Description of Curl27. The Curl27 function maps a ternary string X of arbitrary length to a hash value from $\mathbf{T}^{243}$. When hashing, an auxiliary sponge function Curl27-f: $\mathbf{T}^{729} \to \mathbf{T}^{729}$ is used. The hashing algorithm is as follows:

(1) Pad X with zeros to make its length a multiple of 243. Divide the resulting string into blocks $X_1, X_2, \ldots, X_d \in \mathbf{T}^{243}$.

(2) Prepare the state $W = W_0 W_1 W_2 \in \mathbf{T}^{729}$ consisting of words $W_i \in \mathbf{T}^{243}$. Initialize the state by filling W_0 and W_2 with zeros and W_1 with the encoded initial (before padding) length of X. The length is encoded by a ternary word according to the little-endian conventions: less significant trits go first. For example, the length $25 = 1 - 3^1 + 3^3$ is presented by the word $\underbrace{1\bar{1}01000\ldots0}_{243}$. Here $\bar{1}$ stands for -1.

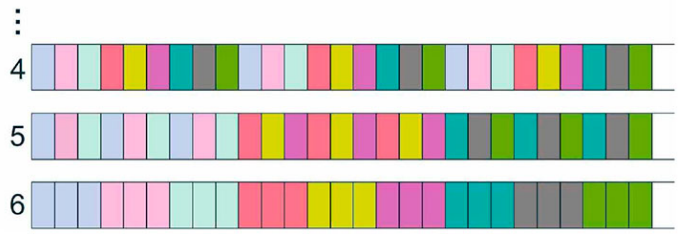


Fig. 7. Groupings (3 last steps, grouped trits are painted the same color).

(3) For $i = 1, 2, \ldots, d$, do: $W_0 \leftarrow X_i$, $W \leftarrow$ Curl27-f(W).
(4) Return W_0.

Description of Curl27-f. In Curl27-f the S-box

$$S\colon \mathbf{T}^3 \to \mathbf{T}^3, \qquad (a, b, c) \mapsto (F(a, b, c), F(b, c, a), F(c, a, b))$$

is used. Here

$$F(a, b, c) = a^2b^2c + a^2bc^2 - ab^2c^2 + a^2b^2 - a^2bc + a^2c^2 + ab^2c - a^2c + ab^2 - ac^2 + b^2c + bc^2 - a^2 - b^2 + bc - c^2 - c + 1,$$

where the calculations are carried out modulo 3 while the residue 2 is represented by the trit -1.

To transform the state W, 27 rounds are performed. A round consists of 6 steps. At each step triplets of trits of W are grouped in a certain way. Then each triplet (a, b, c) is replaced with $S(a, b, c)$.

Groupings are organized as follows (see Fig. 7): At the first step, the state is divided into 3 words of 243 trits. Trits of these words in the same positions are grouped. At the second step, the state is divided into 9 words of 81 trits. Trits of the 1st, 2nd and 3rd words in the same positions are grouped, then trits of the 4th, 5th and 6th words, and so on. After that, the state is divided into words of length 27, then length 9, then length 3, while maintaining the logic of groupings. At the last sixth step, consecutive triplets of trits are grouped.

A bonus problem (extra scores, a special prize!). Find a collision when the state is initialized in a different way: Now W_0 and W_2 are not filled with 0s; in each of them, $\underbrace{01\bar{1}01\bar{1}\ldots01\bar{1}}_{243}$ is written instead.

2.14.2. Solution. For a word u in the alphabet $\mathbf{T}$, let u^m be the word of m copies of u. Supposing $u = u_0u_1\ldots u_{n-1}$ denote $u^{[m]} = u_0^m u_1^m \ldots u_{n-1}^m$. We call a word of the form $u^{[m]}$ *m-fragmented*.

Theorem. *Let m be a power of 3, $m \le 729$. The sponge function Curl27-f preserves m-fragmentation; i.e., if W is m-fragmented then Curl27-f(W) is also m-fragmented.*

Proof. At the ith step of the Curl27-f round function, the state W is divided into words of length

$$n = 3^{6-i}, \qquad i = 1, 2, \ldots, 6.$$

For $n \le m$ the step function preserves equality of trits inside fragments. It follows from the fact that $S(a, a, a) = (b, b, b)$. For $n > m$ equality is also preserved since in each fragment trits at the different positions are processed in the same way. □

Let m be a small power of 3 (interesting cases are $m = 3$, 9, and 27). Consider a ternary string X of length

$$1 + 3 + 3^2 + \ldots + 3^{m-1} = (3^m - 1)/2.$$

The length is given by a word of m ones. Consequently, the initial state of Curl27 when processing X is m-fragmented (one fragment of 1s, the remaining fragments of 0s).

Let us choose trits of X so as to preserve m-fragmentation of the state during hashing. This is easy to do using the Theorem: Each full m-fragment of X must have the form α^m, $\alpha \in \mathbf{T}$, and, in addition, trits

of the last (incomplete) fragment must be zero to be consistent with the padding trits. Having achieved m-fragmentation of states, we automatically obtain m-fragmentation of hash values. Now a hash value is determined by $243/m$ trits each of which is repeated m times. We can find a collision for Curl27 after processing of about $\sqrt{3^{243/m}}$ strings X of the described structure, that is, in time of order

$$3^m \cdot \sqrt{3^{243/m}} = 3^{m+121.5/m}.$$

The minimum of the above function is achieved at $m = 9$. During the attack with $m = 9$ it is required to process approximately $\sqrt{3^{13.5}}$ strings of $9841 = 243 \cdot 40 + 121$ trits each.

An example of colliding messages:

$$X = 0^{243\cdot 39}(101100110101111100101100000)^{[9]}0^{121},$$
$$X' = 0^{243\cdot 39}(000011110100111111001000000)^{[9]}0^{121}.$$

This collision was found by Jeremy Jean (National Cybersecurity Agency of France), the only participant who solved the problem.

The preservation of fragmentation is an invariant of Curl27-f which allows to decrease the dimension and thereby effectively solve the basic problem. To solve the bonus problem, Jeremy Jean proposed to use another invariant for Curl27-f: If each part W_0, W_1, W_2 of the state W is 3-expanded then this fact also holds for Curl27-f(W). Here we call a word $U \in \mathbf{T}^{243}$ 3-*expanded* if it has the form $(abc)^{81}$, $abc \in \mathbf{T}^3$.

At the initial state, the parts W_0 and W_2 are indeed 3-expanded. To comply with the invariant, the part W_1 representing the length of a hashed string X must have one of the forms $(ab1)^{81}$, $(a10)^{81}$ or $(100)^{81}$ (the length is nonzero and positive). As a result, X consists of at least

$$1 + 27 + \cdots + 27^{80} > 3^{240} \text{ trits.}$$

It is easy to maintain the invariant during hashing: Full 243-fragments of X must be 3-expanded and the last incomplete fragment (if it exists) must be filled with zeros. The resulting hash values are 3-expanded, there are only 27 choices for them, and a collision will surely be found after processing only 28 strings X. Of course, the attack is impractical: The time of order 3^{240}, which is required only for recording colliding messages, is unacceptably large even compared to the time $3^{243/2}$ of the standard birthday attack.

2.15. Problem "8-Bit S-Box"

2.15.1. Formulation. Permutations S of the set $\{0,1\}^n$ or $\mathbb{F}_2^n$ are usually called *n-bit S-boxes*. We will focus on the following cryptographic properties of S-boxes:

(1) The (*minimal*) *algebraic degree* of S denoted by $\deg(S)$ is the minimum of algebraic degrees of all component functions of S.

(2) The *nonlinearity* of S denoted by $\mathrm{nl}(S)$ is the minimal Hamming distance between all component functions of S and the set of all affine functions.

(3) The *differential uniformity* of S denoted by $\mathrm{du}(S)$ is the maximal number of solutions of the equation $S(x) \oplus S(x \oplus \alpha) = \beta$ for any nonzero vector α and any vector β.

(4) The (*graph*) *algebraic immunity* of S denoted by $\mathrm{ai}(S)$ is the minimal algebraic degree of all nonzero Boolean functions f in $2n$ variables such that $f(x, y) = 0$ for all $x \in \mathbb{F}_2^n$ and $y = S(x)$.

In modern symmetric cryptography, S-boxes of dimension $n = 8$ are probably most popular. For example, such an S-box is used in the AES block cipher. The characteristics of S_{AES}:

$$(\deg, \mathrm{nl}, \mathrm{du}, \mathrm{ai})(S_{\mathrm{AES}}) = (7, 112, 4, 2).$$

The value $\mathrm{ai}(S_{\mathrm{AES}}) = 2$ means that S_{AES} (and the whole AES) can be compactly described by quadratic equations. This can be a weakness in the context of algebraic attacks.

Imposing the restrictions $(\deg, \mathrm{ai})(S) = (7, 3)$ (optimal values), we need to maximize $\mathrm{nl}(S)$ and minimize $\mathrm{du}(S)$. The current best result [17, 18] is $(\deg, \mathrm{nl}, \mathrm{du}, \mathrm{ai})(S) = (7, 108, 6, 3)$.

A problem for a special prize! You need to improve this result: Find 8-bit S with $\mathrm{nl}(S) > 108$ and/or $\mathrm{du}(S) < 6$ while preserving $\deg(S) = 7$ and $\mathrm{ai}(S) = 3$.

Remarks. Let us recall the relevant definitions:

(1) A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in the *algebraic normal form* (ANF) in the following way:

$$f(x) = \bigoplus_{I \in \mathcal{P}(N)} a_I \Big(\prod_{i \in I} x_i\Big),$$

where $\mathcal{P}(N)$ is the power set of $N = \{1, \dots, n\}$ and $a_I \in \mathbb{F}_2$.

(2) The *algebraic degree* of F is the degree of its ANF:

$$\deg(F) = \max\{|I| : \ a_I \neq 0, \ I \in \mathcal{P}(N)\}.$$

(3) Boolean functions of the algebraic degree at most 1 are called *affine*.

(4) The Hamming distance between Boolean functions f and g is the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) \neq g(x)$.

(5) A function $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be given as $S = (s_1, \dots, s_n)$, where s_i is a Boolean function; a nontrivial linear combination of $s_1, \dots, s_n$ is a *component* function of S.

2.15.2. Solution. There were no valuable ideas from the Olympiad participants. The problem remains unsolved for the considered configuration of cryptographic properties. There exist several dozen of constructions based on the well-known butterfly structure that provide current record $(7, 108, 6, 3)$, see [17, 18]. This leads to the idea that if candidates for improvement exist then they are likely outside the known structures and constructions of cryptographic permutations.

2.16. Problem "Conjecture"

2.16.1. Formulation. Let $\mathbb{F}_2$ be the finite field with two elements and let n be a positive integer at least 3. Let $f(X)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$. It is known that the set of the equivalence classes β of polynomials over $\mathbb{F}_2$ modulo $f(X)$ is a finite field of order 2^n, that we denote by $\mathbb{F}_{2^n}$. It is known that different choices of the irreducible polynomial give automorphic finite fields and such choice has then no incidence on the algebraic problems on the corresponding fields.

A problem for a special prize! Prove or disprove the following

Conjecture. *Let k be co-prime with n. For every $\beta \in \mathbb{F}_{2^n}$, let $F(\beta) = \beta^\xi$, $\xi = 4^k - 2^k + 1$. Let*

$$\Delta = \{F(\beta) + F(\beta + 1) + 1; \ \beta \in \mathbb{F}_{2^n}\}.$$

For every distinct nonzero v_1 and v_2 in $\mathbb{F}_{2^n}$, we have

$$\big|\{(x, y, z) \in \Delta^3; \ v_1 x + v_2 y + (v_1 + v_2) z = 0\}\big| = 2^{2n-3}.$$

Example for $n = 3$: We can take $f(X) = X^3 + X + 1$, then each element β of the field $\mathbb{F}_{2^3}$ can be written as a polynomial of degree at most 2: $a_0 + a_1 X + a_2 X^2$, $a_0, a_1, a_2 \in \mathbb{F}_2$. The element 0 corresponds to the null polynomial; and the unity, denoted by 1, corresponds to the constant polynomial 1. We can calculate the table of multiplication in $\mathbb{F}_{2^3}$ (the table of addition just corresponds to adding polynomials of degree at most 2); this allows us to calculate any power of any element of the field and check the property.

2.16.2. Solution. This mathematical problem is open and difficult. It was presented in [19] for the first time and discussed in [20]. The conjecture was verified for small n (odd values $n \leqslant 11$, even values $n \leqslant 8$). The Olympiad participants suggested several ideas. Unfortunately, none of them gave significant advances to prove the conjecture or search for a counterexample.

The team of Kristina Geut, Sergey Titov, and Dmitry Ananichev (Ural State University of Railway Transport) and the team of Alexey Zelenetskiy, Mikhail Kudinov, and Denis Nabokov (Bauman Moscow State Technical University) proved the conjecture for a particular case $k = 1$. Nevertheless, this case is peculiar since the function is then quadratic and the result is known for quadratic functions. The proofs cannot be generalized to the common case.

3. WINNERS OF THE OLYMPIAD

Summing up the results of the Olympiad, 42 participants in the first round and 21 teams in the second round from 16 countries were awarded by prizes and honorable diplomas. Tables 10, 11, 12, 13, and 14 illustrate the information about the prize winners of NSUCRYPTO'2019.

All information about the winners can be found on the official website [21].

Table 10. Winners of the first round in School Section A ("School Student")

Place	Name	Country, City	School	Score
1	Borislav Kirilov	Bulgaria, Sofia	The First Private Mathematical Gymnasium	16
1	Alexey Lvov	Russia, Novosibirsk	Gymnasium 6	16
2	Lenart Bucar	Slovenia, Ljubljana	Gymnasium Bezigrad	15
3	Varvara Lebedinskaya	Russia, Novosibirsk	The Specialized Educational Scientific Center of Novosibirsk State University	14
3	Gabriel Ericson	Sweden, Örebro	Tullangsskolan	14

Table 11. Winners of the first round, Section B (in the category "University Student")

Place	Name	Country, City	University	Score
1	Maxim Plushkin	Russia, Moscow	Lomonosov Moscow State University	22
1	Mikhail Kudinov	Russia, Moscow	Bauman Moscow State Technical University	21
2	Narendra Patel	India, Roorkee	Indian Institute of Technology Roorkee	19
2	Vladimir Schavelev	Russia, Saint Petersburg	Saint Petersburg State University	19
3	Thanh Nguyen Van	Vietnam, Ho Chi Minh City	Ho Chi Minh City University of Technology	16
3	Daria Grebenchuk	Russia, Yaroslavl	Yaroslavl State University	16
3	Roman Gibadulin	Russia, Yaroslavl	Yaroslavl State University	16
3	Tuong Nguyen	Vietnam, Ho Chi Minh City	Ho Chi Minh City University of Technology	15

Table 12. Winners of the first round, Section B (in the category "Professional")

Place	Name	Country, City	Organization	Score
1	Henning Seidler	Germany, Berlin	TU Berlin	26
2	Samuel Tang	Hong Kong, Hong Kong	Black Bauhinia	20
2	Madalina Bolboceanu	Romania, Bucharest	Bitdefender	20
3	Irina Slonkina	Russia, Moscow	National Research Nuclear University MEPhI	16

Table 13. Winners of the second round (in the category "University Student")

Place	Name	Country, City	University	Score
1	Alexey Zelenetskiy, Mikhail Kudinov, Denis Nabokov	Russia, Moscow	Bauman Moscow State Technical University	51
2	Ngoc Ky Nguyen, Dung Truong, Phuoc Nguyen Ho Minh	Vietnam, Ho Chi Minh City; France, Paris	Ho Chi Minh City University of Technology, Ecole Normale Superieure	43
2	Thanh Nguyen Van, Quoc Bao Nguyen, Ngan Nguyen	Vietnam, Ho Chi Minh City	Ho Chi Minh City University of Technology	40
3	Maxim Plushkin	Russia, Moscow	Lomonosov Moscow State University	34
3	Ilya Trusevich, Maxim Bibik, Alexander Shulga	Belarus, Minsk	Belarusian State University	38

Table 14. Winners of the second round (in the category "Professional")

Place	Names	Country, City	Organization	Score
1	Irina Slonkina, Mikhail Sorokin, Vladimir Bobrov	Russia, Moscow	Bauman Moscow State Technical University	48
1	Kristina Geut, Sergey Titov, Dmitry Ananichev	Russia, Yekaterinburg	Ural State University of Railway Transport, Ural Federal University	46
2	Henning Seidler, Katja Stumpp	Germany, Berlin	Berlin Technical University	42
3	Victoria Vlasova, Mikhail Polyakov, Alexey Chilikov	Russia, Moscow	Bauman Moscow State Technical University	37
3	Duc Tri Nguyen, Quan Doan, Tuong Nguyen	Vietnam, Ho Chi Minh City	Cryptographic Engineering Research Group, pwnphofun, Ho Chi Minh City University of Technology	36
3	Madalina Bolboceanu, Andrei Mogage, Radu Titiu	Romania, Bucharest	Bitdefender, Alexandru Ioan Cuza University	34
Special prize	Jeremy Jean	France, Paris	National Cybersecurity Agency of France	20

FUNDING

The work of the first two authors and the sixth author was supported by the Mathematical Center in Akademgorodok under Agreement No. 075–15–2019–1613 with the Ministry of Science and Higher Education of the Russian Federation and the Laboratory of Cryptography JetBrains Research. The work of the fifth author was supported by the State Task to the Sobolev Institute of Mathematics (project no. 0314–2019–0016). The work of the seventh, eighth, and eleventh authors was supported by the

Russian Foundation for Basic Research (projects nos. 20–31–70043, 18–07–01394, and 19–31–90093).

REFERENCES

1. https://nsucrypto.nsu.ru/.
2. https://nsucrypto.nsu.ru/unsolved-problems/.
3. K. Geut, K. Kirienko, P. Sadkov, R. Taskin, and S. Titov, "On Explicit Constructions for Solving the Problem 'A Secret Sharing'," Prikl. Diskret. Mat. Pril. No. 10, 68–70 (2017).
4. S. Agievich, A. Gorodilova, N. Kolomeec, S. Nikova, B. Preneel, V. Rijmen, G. Shushuev, N. Tokareva, and V. Vitkup, "Problems, Solutions, and Experience of the First International Student's Olympiad in Cryptography," Prikl. Diskret. Mat. (Appl. Discret. Math.) No. 3, 41–62 (2015).
5. S. Agievich, A. Gorodilova, V. Idrisova, N. Kolomeec, G. Shushuev, and N. Tokareva, "Mathematical Problems of the Second International Student's Olympiad in Cryptography," Cryptologia **41** (6), 534–565 (2017).
6. N. Tokareva, A. Gorodilova, S. Agievich, V. Idrisova, N. Kolomeec, A. Kutsenko, A. Oblaukhov, and G. Shushuev, "Mathematical Methods in Solutions of the Problems from the Third International Students' Olympiad in Cryptography," Prikl. Diskret. Mat. (Appl. Discret. Math.) No. 40, 34–58 (2018).
7. A. Gorodilova, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, S. Nikova, A. Oblaukhov, S. Picek, B. Preneel, V. Rijmen, and N. Tokareva, "Problems and Solutions of the Fourth International Students Olympiad in Cryptography (NSUCRYPTO)," Cryptologia **43** (2), 138–174 (2019).
8. A. Gorodilova, S. Agievich, C. Carlet, X. Hou, V. Idrisova, N. Kolomeec, A. Kutsenko, L. Mariot, A. Oblaukhov, S. Picek, B. Preneel, R. Rosie, and N. Tokareva, "The Fifth International Students' Olympiad in Cryptography—NSUCRYPTO: Problems and Their Solutions," Cryptologia **44** (3), 223–256 (2020).
9. B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd Ed. (Wiley, Indianapolis, 1996).
10. R. E. Lewand, *Cryptological Mathematics* (MAA, Washington, 2000).
11. "Letter Frequency," in *Wikipedia*. Available at https://en.wikipedia.org/wiki/Letter_frequency.
12. "Find Words Using Pattern Matching," in *Litscape.com*. Available at http://www.litscape.com/word_tools/pattern_match.php.
13. M. Brinkmann and G. Leander, "On the Classification of APN Functions up to Dimension Five," Designs, codes and cryptography **49**, 273–288 (2008).
14. C. De Canni‘ere, *Analysis and Design of Symmetric Encrytption Algorithms*, Ph.D. Thesis (Katholieke Universiteit Leuven, Heverlee, 2007).
15. https://nsucrypto.nsu.ru/archive/2019/round/2/task/4/.
16. https://nsucrypto.nsu.ru/media/Olympiads/2019/Round_2/Tasks/curl27.java.
17. R. A. de la Cruz Jimènez, "Generation of 8-Bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-Bit S-Boxes and Finite Field Multiplication," in *Progress in Cryptology—LATINCRYPT 2017: 5th International Conference on Cryptology and Information Security in Latin America (Havana, Cuba, September 20–22, 2017): Revised Selected Papers*, Ed. by T. Lange and O. Dunkelman (Springer, Cham, 2019), pp. 191–206 [*Lecture Notes in Computer Science*, Vol. 11368].
18. D. B. Fomin, "New Classes of 8-Bit Permutations Based on a Butterfly Structure," Mat. Vopr. Kript. **10** (2), 169–180 (2019). https://ctcrypt.ru/files/files/2018/09_Fomin.pdf.
19. C. Carlet, "Componentwise APNness, Walsh Uniformity of APN Functions, and Cyclic-Additive Difference Sets," Finite Fields and Their Applications **53**, 226–253 (2018).
20. C. Carlet, "On APN Exponents, Characterizations of Differentially Uniform Functions by the Walsh Transform, and Related Cyclic-Difference-Set-Like Structures," in *Proceedings of WCC 2017* Designs, Codes and Cryptography **87** (2), 203–224 (2018).
21. https://nsucrypto.nsu.ru/archive/2019/total_results/#data.

Cryptography and Communications
https://doi.org/10.1007/s12095-021-00528-5

Some general properties of modified bent functions through addition of indicator functions

Nikolay Kolomeec[1]

Received: 21 October 2020 / Accepted: 9 August 2021 / Published online: 27 August 2021

Abstract
Properties of a secondary bent function construction that adds the indicator of an affine subspace of arbitrary dimension to a given bent function in n variables are obtained. Some results regarding normal and weakly normal bent functions are generalized. An upper bound for the number of generated bent functions is proven. This bound is attained if and only if the given bent function is quadratic. In certain cases, the addition of the indicator of an m-dimensional subspace, for different m, will not generate bent functions. Such examples are presented for any even $n \geq 10$. It is proven that there exists an infinite family of Maiorana–McFarland bent functions such that the numbers of generated bent functions differ for the bent function and its dual function.

Keywords Boolean functions · Bent functions · Affine functions · Balanced functions · Subspaces

Mathematics Subject Classification (2010) 06E30 · 94C10 · 94A60

1 Introduction

A bent function is a Boolean function in even number of variables that is at the maximal possible Hamming distance from the set of all affine Boolean functions. In other words, it has the best nonlinearity. Bent functions were introduced by O. Rothaus [26]. Since 1960, they have been actively researched. As extreme objects, they have many applications in various fields: algebra, coding theory, combinatorics, communication theory, cryptography.

This article belongs to the Topical Collection: *Boolean Functions and Their Applications V*
Guest Editors: Lilya Budaghyan, Claude Carlet, Tor Helleseth and Kaisa Nyberg

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075–15–2019–1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

✉ Nikolay Kolomeec
kolomeec@math.nsc.ru

[1] Sobolev Institute of Mathematics, Novosibirsk, Russia

Boolean functions with high nonlinearity are especially interesting for symmetric cryptography, since they help to resist linear cryptanalysis [23]. Useful information regarding bent functions can be found in reviews, dissertations and monographs [6, 7, 9–11, 14, 21, 25, 28].

This work is dedicated to the following secondary construction of bent functions. Let f be a given bent function in n variables and L be an affine subspace of $\mathbb{F}_2^n$. We consider all bent functions of the form $f \oplus \mathrm{Ind}_L$, where Ind_L is the indicator function of L. For the first time it was mentioned by J. Dillon [11] for $n/2$-dimensional subspaces. Later, C. Carlet [4] proved a criterion of "bentness" of $f \oplus \mathrm{Ind}_L$, where L is of arbitrary dimension. The most popular and well studied case is $\dim L = n/2$. In this case, the criterion transforms to the affinity of f on L. Also, the construction generates exactly all bent functions at the Hamming distance $2^{n/2}$ from the given one, which is the minimal possible distance between two distinct bent functions (see [17]). This connects the construction properties with the metric properties of the set of all bent functions (see, for instance, [16]). Note that this case was studied in terms of (weakly) normal bent functions, which means that a function is constant (resp. affine) on some $n/2$-dimensional affine subspace (see [3, 8, 13, 20]). It should be emphasized that the affinity on an affine subspace is an interesting property for cryptography by itself. Subspaces of large dimension deserve attention too. For instance, A. Canteaut and P. Charpin considered the case of $(n-2)$-dimensional subspaces in the function decomposition context [2]. Note that it is rather difficult to find a suitable affine subspace L such that $f \oplus \mathrm{Ind}_L$ is a bent function. Also, it is hard to determine which of bent function subclasses contain $f \oplus \mathrm{Ind}_L$ and which do not. Nevertheless, some results related to these problems have been obtained [3, 4, 22, 27].

In this work, we investigate the properties of the construction $f \oplus \mathrm{Ind}_L$, where L is an affine subspace of arbitrary dimension m. On the one hand, they are similar to the case of $m = n/2$. The construction properties are closely connected with the affinity of the dual function on affine subspaces. Some known results for $m = n/2$ are generalized for the case of arbitrary dimensions, for instance, an upper bound for the number of constructed bent functions [16], the use of the simplest iterative construction $f(x) \oplus y_1 y_2$ of bent functions [3, 8]. In certain cases, the addition of the indicator of an m-dimensional subspace, for different m, will not generate bent functions. Such examples are presented for any even $n \geq 10$. On the other hand, the numbers of generated bent functions may differ for some bent function f and its dual function $\widetilde{f}$, which is opposite to the case of $m = n/2$. Examples of such bent functions for any even $n \geq 8$ and $m = n-2$ are provided. Interestingly, these examples are Maiorana–McFarland bent functions [24].

The article is organized as follows. Section 2 contains basic definitions. In Section 3, the notion of a balanced representation of a bent function f by a linear subspace L is introduced. It means that f is either constant or balanced on each coset of L. This notion is directly connected with the criterion proven in [4]. Also, properties of such representations (Theorem 2) are considered. Note that bent functions [5, 24, 29] obtained by the concatenation of affine functions always have a balanced representation by some nontrivial linear subspace. In Section 4, we assume that $f \oplus \mathrm{Ind}_L$ is a bent function for some given bent function f and an affine subspace L and consider how to find affine subspaces L' and L'', where $L' \subset L \subset L''$, such that $f \oplus \mathrm{Ind}_{L'}$ and $f \oplus \mathrm{Ind}_{L''}$ are bent functions. Note that the conditions related to the existence of L' and L'' are, in general, not trivial. There is one simple case: we can always find an $n/2$-dimensional L' by an $(n/2+1)$-dimensional L. The case of $\dim L = n/2+1$ similarly to the case of $\dim L = n/2$ guarantees that the construction is symmetric for the bent function f and its dual function $\widetilde{f}$: $\mathrm{sup}(\widetilde{f} \oplus \widetilde{(f \oplus \mathrm{Ind}_L)})$ is an affine subspace too (Theorem 3). In other words, the dual functions of f and $f \oplus \mathrm{Ind}_L$ differ

exactly on an affine subspace of dimension $\dim L$. Actually, the case of $\dim L = n/2+1$ is equivalent to applying the construction twice for some $n/2$-dimensional $L' \subset L$ and its shift $L \setminus L'$: $(f \oplus \mathrm{Ind}_{L'}) \oplus \mathrm{Ind}_{L\setminus L'} = f \oplus \mathrm{Ind}_L$, where $f \oplus \mathrm{Ind}_{L'}$ is bent. Hence, these two cases are practically similar. Let us denote by $\mathrm{BS}_m(f)$ the set of all bent functions of the form $f \oplus \mathrm{Ind}_L$, where L is m-dimensional. In Section 5, an upper bound for $\#\mathrm{BS}_m(f)$ is proven. This bound is attained for a nontrivial dimension if and only if the given bent function f is quadratic (Theorem 4). Also, it is shown how to choose a bent function f in n variables such that $\#\mathrm{BS}_m(f) = 0$, where $m = n-2, n-1, \ldots, k$. In light of A. Gorodilova's results [15], $k \le n/2+4$ for the dual function of a suitable Kasami [12, 19] bent function (Theorem 6). Thus, 0 is a tight lower bound for $\#\mathrm{BS}_m(f)$. Section 6 focuses on the simplest iterative construction $f_{+2}(x, y) = f(x) \oplus y_1 y_2$ of bent functions. It is proven (Theorem 8) that "bentness" of $f_{+2} \oplus \mathrm{Ind}_L$ for an m-dimensional affine subspace L implies "bentness" of $f \oplus \mathrm{Ind}_{L'}$ for some affine subspace L' of dimension $m-1$ or $m-2$. This fact generalizes the properties of normal bent functions [3]. It allows us to construct a bent function f such that $\#\mathrm{BS}_m(f) = 0$, where $m = n/2, n/2+1, n/2+2, n/2+3$ (the number of dimensions depends on the initial function; such example is based on the bent function found in [20]). Note that these dimensions complement the ones from Theorem 6. In addition, $\#\mathrm{BS}_n(f_{+2})$ is calculated by constant derivatives (Theorem 9) and it is shown that it is impossible to find $\#\mathrm{BS}_n(f_{+2})$ by $\#\mathrm{BS}_{n-2}(f)$. The counterexample is found in the Maiorana–McFarland class. Section 7 demonstrates an infinite family of Maiorana–McFarland bent functions f_n in n variables such that $\#\mathrm{BS}_{n-2}(f_n) \ne \#\mathrm{BS}_{n-2}(\widetilde{f_n})$, i. e. f and its dual $\widetilde{f}$ structurally differ. This can make it more difficult to determine the class containing $\widetilde{f \oplus \mathrm{Ind}_L}$ even if f is a Maiorana–McFarland bent function.

2 Preliminaries

Let us denote the finite field with two elements by $\mathbb{F}_2$. *A Boolean function* in n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\langle x, y\rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$, where $x, y \in \mathbb{F}_2^n$. Let us denote the characteristic Boolean function of a set $S \subseteq \mathbb{F}_2^n$ by Ind_S and *the derivative* of f *in the direction* α by $D_\alpha f$, $D_\alpha f(x) = f(x) \oplus f(x \oplus \alpha)$. Let $D_L f(x) = \bigoplus_{a\in L} f(x \oplus a)$, i. e. the derivative $D_L f = D_{a_1} D_{a_2} \ldots D_{a_k} f$, where $a_1, \ldots, a_k$ is a basis of L and L is a k-dimensional linear subspace of $\mathbb{F}_2^n$. We denote the cardinality of the set S by $\#S$, the set $\{x \oplus s \mid s \in S\}$ by $x \oplus S$ and the set $\{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ by $\mathrm{sup}(f)$. *The Hamming distance* between two Boolean functions in n variables is the number of arguments on which these functions differ. A function f is *balanced on a set* S if $\#(\mathrm{sup}(f) \cap S) = \frac{1}{2}\#S$.

The degree of f ($\deg f$) is the degree of its *algebraic normal form* that is a representation of f as a polynomial over $\mathbb{F}_2$:

$$f(x_1, \ldots, x_n) = \bigoplus_{a\in\mathbb{F}_2^n} c_a x_1^{a_1} \ldots x_n^{a_n},\ c_a \in \mathbb{F}_2,\ \text{where}$$

$x_i^{a_i} \equiv x_i$ for $a_i = 1$ and $x_i^{a_i} \equiv 1$ for $a_i = 0$. A function is called *affine* if its degree is at most 1 and *quadratic* if its degree equals to 2. A function f is *affine on an affine subspace* L if $f(x) \oplus \langle a, x\rangle$ is constant on L for some $a \in \mathbb{F}_2^n$.

The Walsh–Hadamard transform of f is the mapping $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ such that

$$W_f(y) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle y,x\rangle}.$$

The numbers $W_f(y)$ are called *the Walsh–Hadamard coefficients*. A Boolean function f in n variables, n is even, is *a bent function* if $|W_f(y)| = 2^{n/2}$ for all $y \in \mathbb{F}_2^n$. We denote by $\mathcal{B}_n$ the set of all bent functions in n variables. *The dual* function $\widetilde{f}$ is defined in the following way:

$$(-1)^{\widetilde{f}(y)} = 2^{-n/2} W_f(y),\ y \in \mathbb{F}_2^n.$$

The function $\widetilde{f}$ is a bent function too, and $\widetilde{\widetilde{f}} = f$ (see, for instance, [26]).

Two Boolean functions f, g in n variables are called *extended affinely equivalent* (*EA-equivalent*) if there exist an invertible n-by-n binary matrix A, a vector $b \in \mathbb{F}_2^n$ and an affine function ℓ in n variables such that

$$f(x) = g(xA \oplus b) \oplus \ell(x) \text{ for all } x \in \mathbb{F}_2^n.$$

Hereinafter, we suppose that n is even. In this work, we consider properties of a bent function construction $f \oplus \mathrm{Ind}_U$, where f is a given bent function in n variables and U is an affine subspace of arbitrary dimension. For $f \in \mathcal{B}_n$ and $0 \le m \le n$, we define

$$\mathrm{BS}_m(f) = \{f \oplus \mathrm{Ind}_U \mid U \text{ is an } m\text{-dimensional affine subspace of } \mathbb{F}_2^n\} \cap \mathcal{B}_n.$$

Note that for $f, g \in \mathcal{B}_n$ that are EA-equivalent $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(g)$ holds.

Necessary and sufficient conditions for $f \oplus \mathrm{Ind}_U$ to be a bent function were proven by C. Carlet [4].

Theorem 1 (C. Carlet, 1994) *Let $f \in \mathcal{B}_n$, $L \subseteq \mathbb{F}_2^n$ be a linear subspace and $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{a \oplus L}$ is a bent function if and only if any of the following equivalent conditions hold:*

1. *$D_\alpha f$ is balanced on $a \oplus L$ for all $\alpha \in \mathbb{F}_2^n \setminus L$;*
2. *$\widetilde{f}(x) \oplus \langle a, x \rangle$ is either constant or balanced on each coset of $L^\perp$.*

In the next section, additional details for the second condition of the criterion will be provided. They will be often used in the proofs.

Note that trivial subspace dimensions for $f \in \mathcal{B}_n$ are $n-1$ and n. In these cases we just add an affine function to the bent function, i. e. the result is always a bent function too. It is also well known that $f \oplus \mathrm{Ind}_L$ is not a bent function if $\dim L < n/2$ (see [4]). Thus, we will focus on dimensions $n/2, n/2+1, \ldots, n-2$.

3 A balanced representation

Let us introduce the following notion.

Definition 1 A Boolean function f in n variables has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$ if f is either constant or balanced on each coset of L.

Note that any function has a balanced representation by the 0-dimensional linear subspace. The same situation holds for a 1-dimensional linear subspace.

First of all, there are some additional details regarding balanced representations of bent functions. These statements mostly follow from Theorem 1 and [16].

Theorem 2 *Let $f \in \mathcal{B}_n$ and L be a linear subspace of $\mathbb{F}_2^n$, $\dim L \le n/2$. Then the following holds.*

1. *Let f be constant on each of $a_1 \oplus L, \ldots, a_m \oplus L$, where $a_1, \ldots, a_m \in \mathbb{F}_2^n$, $m \in \mathbb{N}$, and be balanced on each other $a \oplus L$, where $a \in \mathbb{F}_2^n \setminus U$, $U = (a_1 \oplus L) \cup \ldots \cup (a_m \oplus L)$. Then $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$ and $\widetilde{f} \oplus \widetilde{f \oplus \mathrm{Ind}_U} = \mathrm{Ind}_{L^\perp}$.*
2. *f has a balanced representation by L if and only if f is constant on each of $2^{n-2\dim L}$ distinct cosets of L.*
3. *f cannot be constant on more than $2^{n-2\dim L}$ distinct cosets of L.*

Proof Starting with the first point, let us consider $W_f(x)$ and $W_{f\oplus \mathrm{Ind}_U}(x)$:

$$W_{f\oplus \mathrm{Ind}_U}(x) = \sum_{y\notin U}(-1)^{f(y)\oplus\langle x,y\rangle} + \sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle\oplus 1} =$$

$$W_f(x) - 2\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle} = W_f(x) - 2\sum_{i=1}^{m}\sum_{y\in a_i\oplus L}(-1)^{f(a_i)\oplus\langle x,y\rangle}.$$

Since the function $y \mapsto \langle x, y\rangle$ (here x is a fixed parameter) is balanced on any $a_i \oplus L$ if $x \notin L^\perp$, it holds that $W_f(x) = W_{f\oplus \mathrm{Ind}_U}(x)$ for $x \notin L^\perp$.

Next, let $x \in L^\perp$. In this case, we use the following:

$$W_{f\oplus \mathrm{Ind}_U}(x) = W_f(x) - 2\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle}.$$

It can be seen that $\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle} = W_f(x)$. Indeed, $\langle x, z\rangle \equiv \mathrm{const}$ on $z \in y \oplus L$, $y \notin U$, and, therefore, $f(z) \oplus \langle x, z\rangle$ is balanced on $y \oplus L$. Thus, $\sum_{y\notin U}(-1)^{f(y)\oplus\langle x,y\rangle} = 0$ and $W_f(x) = \sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle}$, i. e. $W_{f\oplus \mathrm{Ind}_U}(x) = -W_f(x)$. At the same time, $W_f(x) = \pm 2^{n/2}$. Consequently, $f \oplus \mathrm{Ind}_U$ is a bent function. Also, $W_{f\oplus \mathrm{Ind}_U}(x) = W_f(x)$ if and only if $x \notin L^\perp$. The first point is proven.

We can see that the first point implies that $m = 2^{n-2\dim L}$, since $\#L^\perp = 2^{n-\dim L}$ and it is well known that the duality mapping preserves the Hamming distance between bent functions (see, for instance, [4]). Some results related to this mapping can be found in [18]. This proves the first half of the second point. To complete the second point and to prove the third point, we refer to [16, Lemma 8]. □

Corollary 1 *Let f, $f \oplus \mathrm{Ind}_{a\oplus L} \in \mathcal{B}_n$, where L is a linear subspace of $\mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$. Then $\mathrm{sup}(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L})) = (a_1 \oplus L^\perp) \cup \ldots \cup (a_{2^{n-2\dim L^\perp}} \oplus L^\perp)$, where $f(x) \oplus \langle a, x\rangle$ is constant on each of $a_i \oplus L^\perp$ (each two of them are distinct). Note that this does not guarantee that $\mathrm{sup}(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$ is an affine subspace.*

The case of $\dim L = n/2$ is especially interesting for bent functions. A large class of normal bent functions for this representation was introduced by H. Dobbertin [13]. Also, any bent function represented by the concatenation of affine functions in k variables [5, 24, 29] has a balanced representation by some k-dimensional linear subspace.

Note that the algorithm described in [3] can find all balanced representations of bent functions $f(x) \oplus \langle a, x\rangle$ for all $a \in \mathbb{F}_2^n$, i. e. all elements of $\mathrm{BS}_m(\widetilde{f})$. Such algorithms have many applications (see, for instance, [1]).

4 Subspaces and superspaces of U where $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$

In this section, we consider a possibility to increase and decrease the dimension of a subspace by 1 which is suitable for the construction. Let us start with balanced representations.

Proposition 1 *Suppose that $f \in \mathcal{B}_n$ has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$. Then*

1. *f has a balanced representation by $L \cup (a \oplus L)$, where $a \in \mathbb{F}_2^n \setminus L$, if and only if $a \oplus U = U$, where U is the union of all cosets of L such that f is constant on each of them.*
2. *f has a balanced representation by $L_w = \{x \in L \mid \langle w, x\rangle = 0\}$, where $w \in \mathbb{F}_2^n L^\perp$, if and only if $f(x) \oplus \langle w, x\rangle$ has a balanced representation by L.*

Proof To prove the first point, it is enough to note that f is either constant or balanced on $L \cup (a \oplus L)$ if and only if there are no cases when f is constant on $x \oplus L$ and balanced on $a \oplus x \oplus L$. It is equivalent to $a \oplus U = U$.

Let us consider the second point. Since $w \notin L^\perp$, $L = L_w \cup (s \oplus L_w)$ for some $s \in L$ such that $\langle w, s\rangle = 1$. First of all, let $b \in U$. Then f is constant on $b \oplus L_w$ and $b \oplus s \oplus L_w$, i. e. U consists of $2 \cdot 2^{n-2\dim L}$ cosets of L_w. At the same time, $f(x) \oplus \langle w, x\rangle$ is not constant on $b \oplus L$ since $\langle w, b\rangle \neq \langle w, b \oplus s\rangle$.

Let $b \notin U$. Therefore, f is balanced on $b \oplus L$. As a consequence, f is constant on $b \oplus L_w$ if and only if f is constant on $b \oplus s \oplus L_w = (b \oplus L) \setminus (b \oplus L_w)$. Note that $f(x) \oplus \langle w, x\rangle = f(x) \oplus \langle w, b\rangle$ for $x \in b \oplus L_w$ and $f(x) \oplus \langle w, x\rangle = f(x) \oplus \langle w, b\rangle \oplus 1$ for $x \in b \oplus s \oplus L_w$. It implies that $f(x) \oplus \langle w, x\rangle$ is constant on $b \oplus L$ if and only if f is constant on $b \oplus L_w$ and $b \oplus s \oplus L_w$.

Hence, f is constant on $2^{n-2\dim L_w} = 2 \cdot 2^{n-2\dim L} + 2 \cdot 2^{n-2\dim L}$ distinct cosets of L_w if and only if $f(x) \oplus \langle w, x\rangle$ is constant on $2^{n-2\dim L}$ distinct cosets of L. Theorem 2 completes the proof. □

The following property follows from the previous proposition. Theorem 1 and bent function distance properties can also provide it.

Proposition 2 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$, where L is an affine subspace of $\mathbb{F}_2^n$. Let $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{L \cup (a \oplus L)} \in \mathcal{B}_n$ if and only if $f \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_n$.*

Proof Without loss of generality, we assume that L is a linear subspace. Otherwise, we can consider $f(x \oplus b)$ instead of f, where $b \in L$. If $a \in L$, the statement is obvious. Let $a \notin L$. First of all, Theorem 1 provides that $\widetilde{f}$ has a balanced representation by $L^\perp$. Next, $(L \cup (a \oplus L))^\perp = \{x \in L^\perp \mid \langle a, x\rangle = 0\} = (L^\perp)_a$, where $(L^\perp)_a$ is defined in the second point of Proposition 1. According to this point, $\widetilde{f}$ has a balanced representation by $(L^\perp)_a$ if and only if $\widetilde{f}(x) \oplus \langle a, x\rangle$ has a balanced representation by $L^\perp$. Theorem 1 completes the proof. □

Let us rewrite the first point of Proposition 1 in terms of the construction.

Proposition 3 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$, where L is an affine subspace of $\mathbb{F}_2^n$. Let $a \in \mathbb{F}_2^n$ and $L_a = \{x \in L \mid \langle a, x\rangle = 0\}$. Then $f \oplus \mathrm{Ind}_{L_a} \in \mathcal{B}_n$ if and only if $D_a\widetilde{f} \equiv D_a(\widetilde{f \oplus \mathrm{Ind}_L})$.*

Proof It is easy to see that $D_a\widetilde{f} \equiv D_a(\widetilde{f \oplus \mathrm{Ind}_L})$ is equivalent to $a \oplus U = U$, where $U = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$. Without loss of generality, we can assume that L is a linear subspace, similarly to Proposition 2. Let $L' = \{x \in L \mid \langle a, x\rangle = 0\}$. If $L' = L$, the statement is obvious: it means that $a \in L^\perp$ and we know that U is the union of cosets of $L^\perp$. In other cases, either $L_a = L'$ or $L_a = L \setminus L'$, where $\dim L' = \dim L - 1$. According to Proposition 1, $\widetilde{f}$ has a balanced representation by $L'^\perp = L^\perp \cup (a \oplus L^\perp)$ if and only if $a \oplus U = U$. Thus, $f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n$ if and only if $a \oplus U = U$. In light of Proposition 2, it does not matter whether $L_a = L'$ or $L_a = L \setminus L'$. □

Note that Propositions 1, 2 and 3 give nontrivial conditions to increase and decrease the dimension of a subspace. It looks like it is rather hard to construct a subspace or a superspace of the given one. In other words, nonempty $\mathrm{BS}_m(f)$, in general, does not guarantee that $\mathrm{BS}_{m+1}(f)$ and $\mathrm{BS}_{m-1}(f)$ are nonempty too. It is confirmed by the computational experiments and by the results obtained in Sections 5.1 and 6.2 that are dedicated to bent functions with empty $\mathrm{BS}_m(f)$.

It is known [4] that the set $\sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$ is always an affine subspace for f, $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$ and an $n/2$-dimensional U. Next, we prove that the same is true for an $(n/2+1)$-dimensional subspace.

Theorem 3 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$ of dimension at most $n/2+1$. Then $\sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$ is an affine subspace too.*

Proof The case of $\dim U = n/2$ is obvious. Suppose that $\dim U = n/2+1$. By Theorem 1, let us move to a balanced representation by $L^\perp$ for $g(x) = \widetilde{f}(x) \oplus \langle a, x\rangle$, where $a \oplus L = U$, L is a linear subspace. According to Corollary 1, we have $2^{n-2\dim L^\perp} = 2^2 = 4$ "constant" cosets C_1, C_2, C_3, C_4 of $L^\perp$, i. e. $C_1 \cup C_2 \cup C_3 \cup C_4 = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$. Without loss of generality, we can suppose that $g|_{C_1} \equiv g|_{C_2}$. By Theorem 2, the function g has a balanced representation by the affine subspace $C_1 \cup C_2$ of dimension $n/2$. But Proposition 1 provides that there exists $a \notin L^\perp$ such that $a \oplus (C_1 \cup C_2 \cup C_3 \cup C_4) = C_1 \cup C_2 \cup C_3 \cup C_4$. Since $a \notin L^\perp$, it holds $a \oplus C_{i_1} = C_{i_2}$ and $a \oplus C_{i_3} = C_{i_4}$ for some $\{i_1, i_2, i_3, i_4\} = \{1, 2, 3, 4\}$. It means that $a \oplus (C_{i_1} \cup C_{i_3}) = C_{i_2} \cup C_{i_4}$. Since $C_{i_1} \cup C_{i_3}$ is an affine subspace, $(C_{i_1} \cup C_{i_3}) \cup (C_{i_2} \cup C_{i_4}) = C_1 \cup C_2 \cup C_3 \cup C_4$ is an affine subspace too. □

An important corollary of the theorem is the following proposition.

Proposition 4 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$, where L is an $(n/2+1)$-dimensional affine subspace of $\mathbb{F}_2^n$. Then there exists an $n/2$-dimensional affine subspace $L' \subset L$ such that $f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n$.*

Proof Due to Theorem 3, let $U = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$ be a coset of a linear subspace U'. Since $L^\perp \subset U'$, Proposition 3 gives us that $f \oplus \mathrm{Ind}_{L_a} \in \mathcal{B}_n$, where $a \in U'$ and $a \notin L^\perp$. In this case $\dim L_a = n/2$. □

Proposition 4 claims that the case of $(n/2+1)$-dimensional L is equivalent to applying the construction twice for some $n/2$-dimensional $L' \subset L$ (that always exists by the proposition) and its shift $L \setminus L'$, i. e.

$$(f \oplus \mathrm{Ind}_{L'}) \oplus \mathrm{Ind}_{L \setminus L'} = f \oplus \mathrm{Ind}_L, \text{ where } f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n.$$

5 Bounds for #BS$_m(f)$

The following theorem estimates #BS$_m(f)$. It generalizes the upper bound from [16] that works for $m = n/2$.

Theorem 4 *For $f \in \mathcal{B}_n$ and $m \geq n/2$, it holds*

$$\#\mathrm{BS}_m(f) \leq 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{2m-n+2i} - 1}{2^i - 1}.$$

Moreover, for $m \leq n-2$, the bound is attained if and only if f is quadratic.

Proof To prove the bound, we refer to [16, Theorem 2]. In the first part of that theorem, the following was shown:

$$\#D^s(g) \leq 2^n \prod_{t=0}^{s-1} \frac{2^{n-2t} - 1}{2 \cdot (2^{t+1} - 1)} = \#D^s(h),$$

where $g, h \in \mathcal{B}_n$, h is quadratic, $D^s(g)$ is the set of all s-dimensional affine subspaces such that g is affine on each of them.

Let $U \in D^s(g)$, i. e. $g(x) \oplus \langle a, x\rangle$ is constant on U for some $a \in \mathbb{F}_2^n$. Next, we define $\mathrm{nc}_g(U) = \#\{b \oplus U \mid g(x) \oplus \langle a, x\rangle \text{ is constant on } b \oplus U, b \in \mathbb{F}_2^n\}$.

Theorem 1 gives us that $\#\mathrm{BS}_{n-s}(\widetilde{g}) = \#P^s(g)$, where

$$P^s(g) = \{a \oplus L^\perp \mid a \in \mathbb{F}_2^n, L \text{ is a linear subspace of dimension } s$$
$$\text{and the function } g(x) \oplus \langle a, x\rangle \text{ has a balanced representation by } L\}.$$

Note that $a \oplus L^\perp = b \oplus L^\perp$ if and only if $\langle a, x\rangle \oplus \langle b, x\rangle$ is constant on $u \oplus L$, $a, b, u \in \mathbb{F}_2^n$. In other words, if $g(x) \oplus \langle a, x\rangle$ is constant on $u \oplus L$, then $g(x) \oplus \langle b, x\rangle$ is constant on $u \oplus L$ if and only if $a \oplus L^\perp = b \oplus L^\perp$. In light of Theorem 2, it implies that $\#P^s(g) = 2^{2s-n}\#\{U \in D^s(g) \mid \mathrm{nc}_g(U) = 2^{n-2s}\}$. Therefore, $\#\mathrm{BS}_{n-s}(\widetilde{g}) = \#P^s(g) \leq 2^{2s-n}\#D^s(g)$. According to [16, Proposition 4], $\mathrm{nc}_h(U) = 2^{n-2\dim U}$ for any $U \in D^s(h)$, i. e. $\#\mathrm{BS}_{n-s}(\widetilde{h}) = 2^{2s-n}\#D^s(h)$. As a result,

$$\#\mathrm{BS}_m(\widetilde{g}) \leq 2^{2(n-m)-n}\#D^{n-m}(g) \leq 2^{2(n-m)-n}2^n \prod_{t=0}^{n-m-1} \frac{2^{n-2t} - 1}{2 \cdot (2^{t+1} - 1)} =$$

$$2^{n-m} \prod_{i=1}^{n-m} \frac{2^{n-2i+2} - 1}{2^i - 1} = 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{n-2(n-m-i+1)+2} - 1}{2^i - 1} = \#\mathrm{BS}_m(\widetilde{h}).$$

It is more difficult to prove that the bound is attained only by quadratic functions for any $m \leq n-2$. The second part of the proof of [16, Theorem 2] gives us that $\#D^s(g) < \#D^s(h)$ if there exists $U \in D^2(g)$ such that $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$, where $s > 2$. Let us prove the existence of such U by contradiction. Note that we exclude the case of $\#D^2(g) = 0$ since it is straightforward.

Let g be not quadratic. Suppose that $\mathrm{nc}_g(U) = 2^{n-2\cdot 2}$ for any $U \in D^2(g)$. We consider any $U \in D^2(g)$, $U = u \oplus L$, where L is a linear subspace, $u \in \mathbb{F}_2^n$. Since $\mathrm{nc}_g(u \oplus L) = 2^{n-2\cdot 2}$, Theorem 2 provides that $g_a(x) = g(x) \oplus \langle a, x\rangle$ for some $a \in \mathbb{F}_2^n$ has a balanced representation by L, i. e. g_a is either constant or balanced on each coset of L. But any function balanced on 2-dimensional subspace is affine on it (see, for instance, [16, Proposition 2]). Thus, g_a is affine on each coset of L. As a consequence, $g(x) = g_a(x) \oplus \langle a, x\rangle$ is affine on each coset of L as well. Hence, g is completely affinely decomposable of order 2.

Recall that g is completely affinely decomposable of order 2 if 1) g is affine on at least one 2-dimensional affine subspace; 2) if g is affine on a 2-dimensional affine subspace, then g is affine on any its coset as well. It is known [16, Theorem 1] that only affine and quadratic functions can satisfy these conditions, which contradicts the choice of g.

Thus, there exists $U \in D^2(g)$ such that $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$. In other words, $\#D^s(g) < \#D^s(h)$ for any $s > 2$. It implies that $\#\mathrm{BS}_m(\widetilde{g}) < \#\mathrm{BS}_m(\widetilde{h})$ for any $m < n-2$. Let us consider $s = 2$. Since $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$, it can be seen that $\#\mathrm{BS}_{n-2}(\widetilde{g}) = \#P^2(g) < 2^{2\cdot 2-n}\#D^2(g) \le 2^{2\cdot 2-n}\#D^2(h) = \#\mathrm{BS}_{n-2}(\widetilde{h})$. Finally, we choose $\widetilde{f}$ as g since f is quadratic if and only if $\widetilde{f}$ is quadratic. The same is true for h. □

5.1 Bent functions with $\#\mathrm{BS}_m(f) = 0$

Let us show that $\#\mathrm{BS}_m(f) = 0$ for some $f \in \mathcal{B}_n$ and some m. First of all, the following necessary condition for derivatives holds.

Lemma 1 *Let $f \in \mathcal{B}_n$ and the function $f(x) \oplus \langle w, x\rangle$, $w \in \mathbb{F}_2^n$, have a balanced representation by a linear subspace L, $\dim L \ge 2$. Then $D_L f \equiv 0$.*

Proof First of all, $D_L\langle w, x\rangle \equiv 0$ since $\dim L \ge 2$. Next, let us recall that $D_L f(x) = \bigoplus_{a\in L} f(x\oplus a)$. Since f is either constant or balanced on a fixed $x \oplus L$, the number of ones among $f(x \oplus a)$, $a \in L$, is either 0 or $2^{\dim L-1}$ or $2^{\dim L}$, i. e. it is always even. Therefore, $D_L f(x) = 0$ for any $x \in \mathbb{F}_2^n$. □

This subsection focuses on *the Kasami* bent functions. It was proven [12, 19] that the functions of the form $f(x) = \mathrm{tr}(\alpha x^{2^{2k}-2^k+1})$ are bent, where

- $\alpha, x \in \mathbb{F}_{2^n}$, $\mathbb{F}_{2^n}$ is the field with 2^n elements and n is even;
- $\mathrm{tr}(y) = y^{2^0} + y^{2^1} + \ldots + y^{2^{n-1}}$, $y \in \mathbb{F}_{2^n}$, $\mathrm{tr}(y)$ always belongs to $\mathbb{F}_2$;
- $0 < k < n$ and $\gcd(k, n) = 1$;
- $\alpha \notin \{y^3 \mid y \in \mathbb{F}_{2^n}\}$. Note that $\{y^3 \mid y \in \mathbb{F}_{2^n}\} \ne \mathbb{F}_{2^n}$ if n is even.

These functions are called the Kasami bent functions. Though they map $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, we can fix a basis of $\mathbb{F}_{2^n}$ (since it is a vector space over $\mathbb{F}_2$) and consider them as Boolean functions. It is well known that $\deg f = k+1$ for $0 < k < n/2$ and $\deg f = n-k+1$ for $n/2 < k < n$.

In A. Gorodilova's work [15] the properties of $D_L f$ of the Kasami functions were studied. We note the following result.

Theorem 5 (A. Gorodilova, 2013) *Let f be a Kasami bent function in n variables of degree t, $n \ge 8$ is even. Then $D_L f \not\equiv 0$ for any k-dimensional linear subspace L, where*

$$k \le \begin{cases} t-2, & \text{if } 4 \le t \le (n+3)/3; \\ t-3, & \text{if } (n+3)/3 < t \le n/2. \end{cases}$$

These derivatives for 2-dimensional L were also studied in [27]: using the derivatives, D. Sharma et al. proved that a nonquadratic Kasami bent function does not belong to the Maiorana–McFarland class.

In light of these results, it is not difficult to prove that

Theorem 6 *There exists a Kasami bent function f in n variables such that* $\#\mathrm{BS}_m(\widetilde{f}) = 0$, *where*

$$n - 2 \geq m \geq \begin{cases} n/2 + 3, & \text{if } 4 \mid n \text{ or } n = 10; \\ n/2 + 4, & \text{otherwise.} \end{cases}$$

Proof Recall that there exists a Kasami bent function in n variables of degree $n/2$ if $4 \mid n$ and of degree $n/2 - 1$ for other even n. In the first case, $\gcd(n, n/2 - 1) = 1$ allows us to construct a Kasami bent function f of degree $n/2$. In the second case, $\gcd(n, n/2 - 2) = 1$ and, similarly, there exists a Kasami function f of degree $n/2 - 1$. According to Lemma 1 and Theorem 5, these Kasami functions (even if we add an affine function) cannot have a nontrivial balanced representation by a subspace of dimension at most $n/2 - 3$ and $n/2 - 4$ respectively. The case of $n = 10$ satisfies $4 \leq t \leq (10 + 3)/3$ case of Theorem 5 and can be considered as the first case. Thus, Theorem 1 provides that $\#\mathrm{BS}_m(\widetilde{f}) = 0$, where $n - 2 \geq m \geq n - (n/2 - 3)$ for the first case and $n - 2 \geq m \geq n - (n/2 - 4)$ for the second case. □

Let us note that in Section 6.2 we consider bent functions $f \in \mathcal{B}_n$ such that $\#\mathrm{BS}_m(f) = 0$ for $m \leq n/2 + 3$. In some sense, these examples complement Theorem 6: in this section we focus on $m = n - 2, n - 3, \ldots$, in Section 6.2 we focus on $m = n/2, n/2 + 1, \ldots$. Unfortunately, at the moment there is no example of a bent function $f \in \mathcal{B}_n$, where n is arbitrary, such that $\#\mathrm{BS}_m(f) = 0$ for any $m \leq n - 2$.

6 $\mathrm{BS}_m(f_{+2})$ for the iteratively constructed bent function f_{+2}

Let us consider the simplest iterative construction of a bent function f_{+2} by $f \in \mathcal{B}_n$:

$$f_{+2}(x_1, \ldots, x_{n+2}) = f(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Recall that $f_{+2} \in \mathcal{B}_{n+2}$ if and only if $f \in \mathcal{B}_n$. Also, it holds

$$\widetilde{f_{+2}}(x_1, \ldots, x_{n+2}) = \widetilde{f}(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Since f and f_{+2} have different number of variables, let us define

$$\mathrm{pj}_n(x) = (x_1, \ldots, x_n) \text{ and } \mathrm{pj}_n(S) = \{\mathrm{pj}_n(x) \mid x \in S\},$$

where $x \in \mathbb{F}_2^{n+2}$ and $S \subseteq \mathbb{F}_2^{n+2}$. Also, $\mathbb{F}_2^n(S) = \{x \in \mathbb{F}_2^n \mid (x, 0, 0) \in S\}$.

In this section, we establish the connection between $\mathrm{BS}_{m-1}(f)$, $\mathrm{BS}_{m-2}(f)$ and $\mathrm{BS}_m(f_{+2})$.

6.1 Balanced representations of iteratively constructed functions

Recall that $f \in \mathcal{B}_n$ is normal if it has a balanced representation by some $n/2$-dimensional L. Hence, the result of this subsection (Theorem 7 and the bellow proposition) is a generalization of the normal bent function property "f is normal if and only if f_{+2} is normal" which was proven in [3] (see also [8]).

Proposition 5 *Let $f \in \mathcal{B}_n$ have a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$. Then the bent function f_{+2} has balanced representations by*

1. $L_0 = \{(x, 0, 0) \mid x \in L\}$, *i. e.* $\dim L_0 = \dim L$;
2. $L_1 = \{(x, y, 0) \mid x \in L, y \in \mathbb{F}_2\}$, *i. e.* $\dim L_1 = \dim L + 1$.

Let us establish which balanced representations of f exist if we have some balanced representation of f_{+2}.

Theorem 7 *Let $f \in \mathcal{B}_n$ and suppose that f_{+2} has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$, where $\dim L - 1 \leq \dim L' \leq \dim L$, such that f has a balanced representation by L'. Moreover, $\mathbb{F}_2^n(L) \subseteq L' \subseteq \mathrm{pj}_n(L)$ holds.*

Proof Let $x = (x_1, \ldots, x_{n+2}) \in \mathbb{F}_2^{n+2}$. For convenience, we rename the variables of both functions, that is, consider $f(x_3, \ldots, x_{n+2})$ and $f_{+2}(x) = x_1x_2 \oplus f(x_3, \ldots, x_{n+2})$, where the function f is defined on the set

$$\Gamma = \{\widetilde{x} \mid x \in \mathbb{F}_2^{n+2}\} \subseteq \mathbb{F}_2^{n+2},\ \widetilde{x} = (0, 0, x_3, \ldots, x_{n+2}).$$

We work with $\mathbb{F}_2^n(L)$ and $\mathrm{pj}_n(L)$ taking into account the new notation, i. e. $\mathrm{pj}_n(x) = \widetilde{x} \in \Gamma$ and $\mathbb{F}_2^n(L) = L \cap \Gamma$.

Suppose that f_{+2} has a balanced representation by a $(t+1)$-dimensional subspace $L \subseteq \mathbb{F}_2^{n+2}$. By Theorem 2, it is constant on each of $s^1 \oplus L, \ldots, s^m \oplus L$ which are distinct, $s^1, \ldots, s^m \in \mathbb{F}_2^{n+2}$ and $m = 2^{n-2t}$. Let $L' = L \cap \Gamma$. Since $\dim \Gamma = n$, then $\dim L' \in \{t+1, t, t-1\}$.

Case 1 $\dim L' = t + 1$. Therefore, $L = L' \subseteq \Gamma$, i. e. any coset of L' either belongs to Γ or does not intersect with Γ. Since $f(a \oplus x) = f_{+2}(a \oplus x)$ for all $x \in L', a \in \Gamma$, the function f is either constant or balanced on each coset of L' which belongs to Γ. Hence, it has balanced representation by $L' = L$. Moreover, $L' = \mathbb{F}_2^n(L)$ holds.

Case 2 $\dim L' = t$. Then for some fixed $\alpha \in L \setminus L'$ we can represent any $x \in L$ as $x = x' \oplus y\alpha$, where $x' \in L', y \in \mathbb{F}_2$. Fixing some $s \in \mathbb{F}_2^{n+2}$, it holds

$$f_{+2}(s \oplus y\alpha \oplus x') = f(\widetilde{s} \oplus y\widetilde{\alpha} \oplus x') \oplus (s_1 \oplus y\alpha_1)(s_2 \oplus y\alpha_2) = f(\widetilde{s} \oplus y\widetilde{\alpha} \oplus x') \oplus (\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2)y \oplus s_1s_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2. \quad (1)$$

Let us consider $S = (s^1 \oplus L) \cup \ldots \cup (s^m \oplus L)$. It is obvious that $\#S = m2^{t+1}$. Note that if f_{+2} is constant on $s \oplus L, s \in S$, then f_{+2} is constant on $a \oplus s \oplus L$ for $a = (\alpha_1, \alpha_2, 0, \ldots, 0) \in \mathbb{F}_2^{n+2}$ too. Indeed, $(\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2)y = (\alpha_1(s_2 \oplus \alpha_2) \oplus \alpha_2(s_1 \oplus \alpha_1) \oplus \alpha_1\alpha_2)y$ for any $y \in \mathbb{F}_2$, that is why (1) gives us

$$f_{+2}(s \oplus a \oplus y\alpha \oplus x') = f_{+2}(s \oplus y\alpha \oplus x') \oplus \alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2.$$

At the same time, Theorem 2 claims that the bent function f_{+2} cannot be constant on more than m distinct cosets. Therefore, $a \oplus S = S$. Since $a \in L \setminus L'$, it holds $(\alpha_1, \alpha_2) \neq (0, 0)$. Let us consider two subcases.

Case 2.1 $a \in L$. In this case we can suppose that $\alpha = a$. Then, fixing some $s \in S$, equality (1) transforms to

$$f_{+2}(s) = f_{+2}(s \oplus y\alpha \oplus x') = f(\widetilde{s} \oplus x') \oplus (\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2)y \oplus s_1s_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2. \quad (2)$$

On the one hand, f is constant on each $u \oplus L'$, where $u \in \widetilde{S} = \{\widetilde{s} \mid s \in S\}$. On the other hand, $f(\widetilde{s} \oplus x')$ does not depend on y. It means that $\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2 = 0$ for all

$s \in S$. Thus, for two elements of $\mathbb{F}_2^2$ given as (s_1, s_2), the equality does not hold. Therefore, $\#\widetilde{S} \geq \#S/2 = m2^t$. But in this case we have at least $m = m2^t/2^{\dim L'}$ distinct cosets of L' such that f is constant on each of them. By Theorem 2, f has a balanced representation by t-dimensional L'. Note that $\mathbb{F}_2^n(L) = L' = \mathrm{pj}_n(L)$ holds.

Case 2.2 $a \notin L$. Let us consider $L'' = L \cup (a \oplus L)$, $\dim L'' = t + 2$. Since $a \oplus S = S$, the first point of Proposition 1 provides that f_{+2} has a balanced representation by L''. To conclude the case, it is enough to note that any element $x \in L''$ can be represented as $x = x' \oplus \alpha y \oplus az = x' \oplus y(\alpha \oplus a) \oplus (z \oplus y)a = x' \oplus y\beta \oplus z'a$, where $\beta = \alpha \oplus a \in \Gamma$, $x' \in L'$, $y, z' \in \mathbb{F}_2$. Hence, we obtain that f_{+2} has a balanced representation by $(t+2)$-dimensional L''. At the same time, $\dim L'' \cap \Gamma = t + 1$ and $a \in L''$. It means that we can apply the case 2.1 to the subspace L'' and the element a. As a result, the function f has a balanced representation by $(t + 2 - 1)$-dimensional $L' \cup (\beta \oplus L') = U$. Also, $\mathbb{F}_2^n(L) \subset U \subseteq \mathrm{pj}_n(L)$ holds.

Case 3 $\dim L' = t - 1$. In this case there exist $\alpha, \beta \in L \setminus L'$ such that $(\alpha_1, \alpha_2) = (1, 0)$ and $(\beta_1, \beta_2) = (0, 1)$. Any element $x \in s^i \oplus L$, $i \in \{1, \ldots, m\}$, can be represented as $x = s^i \oplus x' \oplus y\alpha \oplus z\beta$, where $x' \in L'$, $y, z \in \mathbb{F}_2$. Without loss of generality, let us suppose that $s^i \in \Gamma$ (otherwise, we can consider $s^i \oplus \alpha$, $s^i \oplus \beta$ or $s^i \oplus \alpha \oplus \beta$ instead of s^i). Next, for any fixed $i \in \{1, \ldots, m\}$ it holds

$$f(s^i) = f_{+2}(s^i) = f_{+2}(s^i \oplus x) = f_{+2}(s^i \oplus x' \oplus y\alpha \oplus z\beta) = f(s^i \oplus x' \oplus y\widetilde{\alpha} \oplus z\widetilde{\beta}) \oplus yz \text{ for all } x' \in L' \text{ and } y, z \in \mathbb{F}_2. \quad (3)$$

Thus, f is constant on each of $s^i \oplus L'$, $s^i \oplus \widetilde{\alpha} \oplus L'$, $s^i \oplus \widetilde{\beta} \oplus L'$ and $s^i \oplus \widetilde{\alpha} \oplus \widetilde{\beta} \oplus L'$.

We consider the subspace $L'' = L' \cup (\widetilde{\alpha} \oplus \widetilde{\beta} \oplus L')$. Let us show that $\dim L'' = t$. It is equivalent to $\widetilde{\alpha} \oplus \widetilde{\beta} \notin L'$. Indeed, fixing $x' = 0$, (3) provides that

$$f(s^i) = f_{+2}(s^i) = f_{+2}(s^i \oplus \alpha \oplus \beta) = f(s^i \oplus \widetilde{\alpha} \oplus \widetilde{\beta}) \oplus 1,$$

but f is constant on $s^i \oplus L'$. It means that $\widetilde{\alpha} \oplus \widetilde{\beta} \notin L'$.

Next, we prove that f is constant on each of $s^i \oplus \widetilde{\alpha} \oplus L''$. Note that $s^i \oplus \widetilde{\alpha} \oplus L'' = (s^i \oplus \widetilde{\alpha} \oplus L') \cup (s^i \oplus \widetilde{\beta} \oplus L')$. According to (3),

$$f(s^i \oplus \widetilde{\alpha}) = f_{+2}(s^i \oplus \alpha) = f_{+2}(s^i \oplus \beta) = f(s^i \oplus \widetilde{\beta}).$$

At the same time, f is constant on both $s^i \oplus \widetilde{\alpha} \oplus L'$ and $s^i \oplus \widetilde{\beta} \oplus L'$, i. e. it is constant on their union.

The rest of the case is to prove that all $s^i \oplus \widetilde{\alpha} \oplus L''$ are distinct. Suppose that $s^i \oplus \widetilde{\alpha} \oplus s^j \oplus \widetilde{\alpha} = s^i \oplus s^j \in L''$ for $i \neq j$, where $i, j \in \{1, \ldots, m\}$. But $s^i \oplus s^j \notin L' \subseteq L$ by the choice. Therefore, $s^i \oplus s^j \in \widetilde{\alpha} \oplus \widetilde{\beta} \oplus L'$. In other words, $s^i = s^j \oplus \widetilde{\alpha} \oplus \widetilde{\beta} \oplus x'$, $x' \in L'$. By (3) and the definition of f_{+2}, we obtain that

$$f_{+2}(s^i) = f_{+2}(s^i \oplus y\alpha \oplus z\beta) = f(s^i \oplus y\widetilde{\alpha} \oplus z\widetilde{\beta}) \oplus yz = f(s^j \oplus (y \oplus 1)\widetilde{\alpha} \oplus (z \oplus 1)\widetilde{\beta} \oplus x') \oplus (y \oplus 1)(z \oplus 1) \oplus y \oplus z \oplus 1 = f_{+2}(s^j \oplus (y \oplus 1)\alpha \oplus (z \oplus 1)\beta \oplus x') \oplus y \oplus z \oplus 1 \text{ for all } y, z \in \mathbb{F}_2.$$

But $f_{+2}(s^j \oplus (y \oplus 1)\alpha \oplus (z \oplus 1)\beta \oplus x') = f_{+2}(s^j)$. Hence, $f_{+2}(s^i) = f_{+2}(s^j) \oplus y \oplus z \oplus 1$ for all $y, z \in \mathbb{F}_2$, which is a contradiction. As a result, any two of $s^i \oplus \widetilde{\alpha} \oplus L''$ are distinct and f is constant on each of them. By Theorem 2, f has a balanced representation by L''. Note that $\mathbb{F}_2^n(L) \subset L'' \subset \mathrm{pj}_n(L)$ holds. □

6.2 The connection between $\mathrm{BS}_{m-1}(f)$, $\mathrm{BS}_{m-2}(f)$ and $\mathrm{BS}_m(f_{+2})$

Recall that Theorem 1 gives us the connection between an affine subspace U, for which $f \oplus \mathrm{Ind}_U$ is a bent function, and the balanced representation of the bent function $\widetilde{f}$. It means that the results obtained in Section 6.1 can help us to establish the connection between the sets $\mathrm{BS}_m(f)$ and $\mathrm{BS}_k(f_{+2})$.

Proposition 6 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$. Then both $f_{+2} \oplus \mathrm{Ind}_{U_1}$ and $f_{+2} \oplus \mathrm{Ind}_{U_2}$ are bent functions, where*

1. $U_1 = \{(x, y, 0) \mid x \in U, y \in \mathbb{F}_2\}$, *i. e.* $\dim U_1 = \dim U + 1$;
2. $U_2 = \{(x, y, z) \mid x \in U, y, z \in \mathbb{F}_2\}$, *i. e.* $\dim U_2 = \dim U + 2$.

Theorem 8 *Let $f_{+2} \in \mathcal{B}_{n+2}$ and $f_{+2} \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_{n+2}$, where $L \subseteq \mathbb{F}_2^{n+2}$ is a linear subspace, $a \in \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$, where $\dim L - 2 \leq \dim L' \leq \dim L - 1$, such that $f \oplus \mathrm{Ind}_{\mathrm{pj}_n(a) \oplus L'} \in \mathcal{B}_n$. Moreover, $\mathbb{F}_2^n(L) \subseteq L' \subseteq \mathrm{pj}_n(L)$ holds.*

Proof By Theorem 1, $f_{+2} \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_{n+2}$ if and only if $\widetilde{f}(x) \oplus \langle a, x \rangle$ has a balanced representation by $L^\perp$. Let us consider $f_{+2}(x \oplus a)$ instead of f_{+2}:

$$f_{+2}(x \oplus a) = f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a)) \oplus (x_{n+1} \oplus a_{n+1})(x_{n+2} \oplus a_{n+2}).$$

Since $(x_{n+1} \oplus a_{n+1})(x_{n+2} \oplus a_{n+2}) = x_{n+1}x_{n+2} \oplus a_{n+2}x_{n+1} \oplus a_{n+1}x_{n+2} \oplus a_{n+1}a_{n+2}$, we can exclude $\ell(x) = a_{n+2}x_{n+1} \oplus a_{n+1}x_{n+2} \oplus a_{n+1}a_{n+2}$ from $f_{+2}(x \oplus a)$: indeed, $g \oplus \mathrm{Ind}_U \in \mathcal{B}_{n+2}$ if and only if $g \oplus \ell \oplus \mathrm{Ind}_U \in \mathcal{B}_{n+2}$.

It means that $f(\mathrm{pj}_n(\widetilde{x) \oplus \mathrm{pj}_n(a)}) \oplus x_{n+1}x_{n+2}$ has a balanced representation by $L^\perp$. According to Theorem 7, $f(\mathrm{pj}_n(\widetilde{x) \oplus \mathrm{pj}_n(a)})$ has a balanced representation by L', where $\mathbb{F}_2^n(L^\perp) \subseteq L' \subseteq \mathrm{pj}_n(L^\perp)$. Again, it implies that $f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a)) \oplus \mathrm{Ind}_{L'^\perp}(x)$ is a bent function. Consequently, $f \oplus \mathrm{Ind}_{\mathrm{pj}_n(a) \oplus L'^\perp}$ is a bent function too, where $(\mathrm{pj}_n(L^\perp))^\perp \subseteq L'^\perp \subseteq (\mathbb{F}_2^n(L^\perp))^\perp$.

To complete the proof, it is necessary to check the bounds for $L'^\perp$. The dimensions obviously satisfy the conditions. Next,

$$\begin{aligned}(\mathrm{pj}_n(L^\perp))^\perp = \{x \in \mathbb{F}_2^n \mid \langle x, y \rangle = 0 \text{ for any } y \in \mathrm{pj}_n(L^\perp)\} = \\ \{x \in \mathbb{F}_2^n \mid \langle (x, 0, 0), y \rangle = 0 \text{ for any } y \in L^\perp\} = \\ (L^\perp)^\perp \cap \{(x, 0, 0) \mid x \in \mathbb{F}_2^n\} = \mathbb{F}_2^n(L).\end{aligned}$$

We obtain that $(\mathrm{pj}_n(L))^\perp = (\mathrm{pj}_n((L^\perp)^\perp))^\perp = \mathbb{F}_2^n(L^\perp)$ from the above equality, i. e. $(\mathbb{F}_2^n(L^\perp))^\perp = \mathrm{pj}_n(L)$. As a result, $\mathbb{F}_2^n(L) \subseteq L'^\perp \subseteq \mathrm{pj}_n(L)$ holds. □

Theorem 8 allows us to preserve k zero values starting with $n/2$: if

$$\#\mathrm{BS}_{n/2}(f) = \#\mathrm{BS}_{n/2+1}(f) = \ldots = \#\mathrm{BS}_{n/2+k-1}(f) = 0, \text{ then}$$

$$\#\mathrm{BS}_{n/2+1}(f_{+2}) = \#\mathrm{BS}_{n/2+2}(f_{+2}) = \ldots = \#\mathrm{BS}_{n/2+k}(f_{+2}) = 0.$$

Computational experiments show that for the non-weakly normal bent function $f_{10} \in \mathcal{B}_{10}$ found in [20, Fact 14] the following holds.

Fact 1 For an affine subspace $U \subseteq \mathbb{F}_2^{10}$, $\dim U \leq 8$, $f_{10} \oplus \mathrm{Ind}_U \notin \mathcal{B}_{10}$ holds.

Together with Theorem 8, it implies the following:

Corollary 2 *For any $n \geq 10$, there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus \mathrm{Ind}_U \notin \mathcal{B}_n$ for any affine subspace $U \subseteq \mathbb{F}_2^n$ of dimension at most $n/2 + 3$.*

Remark 1 We do not consider the more general iterative construction $h(x, y) = f(x) \oplus g(y)$, where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^t$, for which we have the same "normal" property [8]: if g is normal, then h is normal if and only if f is normal. It is more difficult and $D_{(a,0)}D_{(0,b)}h \equiv 0$ for any $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^t$. According to Proposition 7 (see Section 6.3), $\mathrm{BS}_{n+t-2}(\widetilde{h})$ is always nonempty.

6.3 Exact number of functions in $\mathrm{BS}_n(f_{+2})$

Despite the bounds from Theorem 8, it seems impossible to obtain $\#\mathrm{BS}_m(f_{+2})$ by $\#\mathrm{BS}_{m-1}(f)$ and $\#\mathrm{BS}_{m-2}(f)$. Theorem 9 and computational experiments will clearly show this. The next proposition follows from [2, Theorem 8]. It can be proven directly by the second point of Theorem 1.

Proposition 7 (A. Canteaut, P. Charpin, 2003) *Let $f \in \mathcal{B}_n$, L be an $(n-2)$-dimensional linear subspace of $\mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{a \oplus L}$ is a bent function if and only if $D_{L^\perp}\widetilde{f} \equiv 0$.*

Let us introduce

$$K_c(f) = \#\{\text{2-dimensional linear subspace } L \mid D_L f \equiv c\},\ c \in \mathbb{F}_2.$$

Proposition 7 implies that $\#\mathrm{BS}_{n-2}(\widetilde{f}) = 4K_0(f)$.

Theorem 9 *For any $f \in \mathcal{B}_n$ it holds*

$$\begin{aligned} K_0(f_{+2}) &= 10K_0(f) + 6K_1(f) + 3 \cdot 2^n - 3, \\ K_1(f_{+2}) &= 6K_0(f) + 10K_1(f) + 3 \cdot 2^n - 2. \end{aligned}$$

Proof Let us work with a Gauss–Jordan basis (GJB) of a 2-dimensional linear subspace of $\mathbb{F}_2^{n+2}$ (see, for instance, [3]). We need to define $\mathrm{lead}(a) = i$ such that $a_i = 1$ and $a_j = 0$ for all $j < i$, where $i, j \in \{1, \ldots, n+2\}$. A pair of nonzero $a, b \in \mathbb{F}_2^{n+2}$ is a GJB of the linear subspace $\{0, a, b, a \oplus b\}$ if $\mathrm{lead}(a) > \mathrm{lead}(b)$ and $b_{\mathrm{lead}(a)} = 0$. For any linear subspace there exists a unique GJB.

Let $a = (a', \alpha), b = (b', \beta) \in \mathbb{F}_2^{n+2}$, where $a', b' \in \mathbb{F}_2^n$, $\alpha, \beta \in \mathbb{F}_2^2$. We note the following examples of GJBs:

b	0	1	1	0	1	0
a	0	0	0	1	1	0

,

b	0	1	1	0	1	0
a	0	0	0	0	0	1

.

In the first example, $\mathrm{lead}(a) = 4$, $\mathrm{lead}(b) = 2$. Also, a', b' are linearly independent, α, β are linearly dependent. In the second example, $\mathrm{lead}(a) = 6$, $\mathrm{lead}(b) = 2$. Also, a', b' are linearly dependent, α, β are linearly independent.

Let us count the number of GJBs a, b that correspond to $D_L f \equiv c$, $c \in \mathbb{F}_2$. Firstly, it is easy to see that $D_L f_{+2}(x) = D_{a'}D_{b'}f(x_1, \ldots, x_n) \oplus D_\alpha D_\beta x_{n+1}x_{n+2}$. Note that $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv d$, where $d \in \mathbb{F}_2$. It means that $D_L f_{+2} \equiv c$ if and only if $D_{a'}D_{b'}f \equiv c \oplus d$. Also, the following holds:

1. $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 1$ if and only if α, β are linearly independent;

2. $D_{a'}D_{b'}f \equiv 0$ for linearly dependent a', b'.

Next, we calculate $K_0(f_{+2})$. All the desired subspaces satisfy one of the independent cases:

Case 1 a' and b' are linearly independent. There are two subcases here:

Case 1.1 $D_{a'}D_{b'}f \equiv 0$ and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 0$. There are $K_0(f)$ possibilities to choose a GJB a', b'. According to point 1, any linearly dependent α, β can be chosen, there are exactly 10 such pairs. We obtain $10K_0(f)$ GJBs.

Case 1.2 $D_{a'}D_{b'}f \equiv 1$ and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 1$. Similarly to the previous case, there are $6K_1(f)$ distinct GJBs, since α, β are linearly independent; there are exactly 6 such pairs (α, β).

Case 2 a' and b' are linearly dependent (it holds $D_{a'}D_{b'}f \equiv 0$ by point 2) and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 0$. To form a GJB (a, b) by linearly dependent a', b', $a' = 0$ is necessary. Any nonzero vector can be chosen as b' (we do not consider $b' = 0$ since α, β are linearly dependent too). Next, any of 3 nonzero elements can be chosen as α: $(1, 0)$, $(0, 1)$ or $(1, 1)$. But $\beta_{\mathrm{lead}(\alpha)} = 0 \neq \alpha_{\mathrm{lead}(\alpha)}$, it means that the only way is $\beta = (0, 0)$. Finally, we have $3(2^n - 1)$ distinct GJBs. It means that $K_0(f_{+2}) = 10K_0(f) + 6K_1(f) + 3 \cdot 2^n - 3$.

We calculate $K_1(f_{+2})$ in the same way:

Case 1 a' and b' are linearly independent. Thus, there are two subcases:

Case 1.1 $D_{a'}D_{b'}f \equiv 0$ and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 1$, there are $6K_0(f)$ GJBs.

Case 1.2 $D_{a'}D_{b'}f \equiv 1$ and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 0$, there are $10K_1(f)$ GJBs.

Case 2 a' and b' are linearly dependent and $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 1$, i. e. α, β are linearly independent by point 1. Similarly to $K_0(f_{+2})$, $a' = 0$ is necessary. If $b' = 0$, the only way to choose (a, b) is $\alpha = (1, 0)$ and $\beta = (0, 1)$. Also, any $b' \neq 0$ can be chosen. In this case there are 3 possibilities for α: $(1, 0)$, $(0, 1)$ or $(1, 1)$. Since $\beta_{\mathrm{lead}(\alpha)} = 0$, the only way to choose linearly independent α, β is to set the rest non-leading coordinate of β to 1. Finally, we have $3(2^n - 1) + 1$ distinct GJBs.

As a result, $K_1(f_{+2}) = 6K_0(f) + 10K_1(f) + 3 \cdot 2^n - 2$. □

It can be seen that $K_0(f_{+2})$ and, as a result, $\#\mathrm{BS}_n(\widetilde{f_{+2}})$, depend on $K_0(f)$ and $K_1(f)$. Also, bounds from Theorem 8 bind $\mathrm{BS}_n(\widetilde{f_{+2}})$ only with $\mathrm{BS}_{n-2}(\widetilde{f})$: we do not consider $\mathrm{BS}_{n-1}(\widetilde{f})$ since it is trivial and has the same structure for any bent function f. Unfortunately, it looks like $K_1(f)$ has no direct connection to $\#\mathrm{BS}_{n-2}(\widetilde{f})$. Computational experiments for Maiorana–McFarland bent functions confirm this:

Fact 2 Let $f_8^i(x, y) = \langle x, \pi_i(y)\rangle$, $x, y \in \mathbb{F}_2^4$, $i \in \{1, 2\}$, and π_i be defined by

y	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$\pi_1(y)$	0100	1001	1010	0011	0101	0111	1011	1101	1100	1110	0010	1111	0001	0110	1000	0000
$\pi_2(y)$	0100	1001	1010	0011	1011	0111	0101	1100	1110	1101	0010	1111	0001	1000	0000	0110

.

Then $\#\mathrm{BS}_6(\widetilde{f_8^1}) = \#\mathrm{BS}_6(\widetilde{f_8^2})$, but $\#\mathrm{BS}_8(\widetilde{f_{8+2}^1}) \neq \#\mathrm{BS}_8(\widetilde{f_{8+2}^2})$:

	deg	K_0	K_1
f_8^1	4	43	40
f_8^2	4	43	64

Thus, it is not sufficient to know $\#\mathrm{BS}_{n-2}(f)$ to calculate $\#\mathrm{BS}_n(f_{+2})$. Nevertheless, Theorem 9 allows us to construct an infinite family of bent functions with $\#\mathrm{BS}_{n-2}(f) \neq \#\mathrm{BS}_{n-2}(\widetilde{f})$.

7 $\mathrm{BS}_m(f)$ and $\mathrm{BS}_m(\widetilde{f})$

In this section, we construct bent functions such that $\#\mathrm{BS}_m(f) \neq \#\mathrm{BS}_m(\widetilde{f})$.

Theorem 3 shows that the case of $m = n/2 + 1$ is very similar to the case of $m = n/2$: $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(\widetilde{f})$ for $m \leq n/2 + 1$. As a consequence, we have $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(\widetilde{f})$ for any $f \in \mathcal{B}_2 \cup \mathcal{B}_4 \cup \mathcal{B}_6$ and any m. It seems that the simplest example of f such that $\#\mathrm{BS}_m(f) \neq \#\mathrm{BS}_m(\widetilde{f})$ can be found in $\mathcal{B}_8$ for $m = 6$. Computational experiments show that the following fact holds.

Fact 3 Let $\xi_8(x, y) = \langle x, \pi(y)\rangle$, where $x, y \in \mathbb{F}_2^4$, and π be defined by

y	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$\pi(y)$	1001	1010	0100	0011	0101	0111	1011	1101	1100	1110	0010	1111	0001	0110	1000	0000

Then $\#\mathrm{BS}_6(\xi_8) \neq \#\mathrm{BS}_6(\widetilde{\xi_8})$. More precisely, ξ_8 and $\widetilde{\xi_8}$ have

	deg	K_0	K_1
ξ_8	4	75	80
$\widetilde{\xi_8}$	4	59	64

Now, Fact 3 and Theorem 9 allow us to construct an infinite family of Maiorana–McFarland functions f_{2k} such that $\#\mathrm{BS}_{2k-2}(f_{2k}) \neq \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$. Also, it implies that f_{2k} and $\widetilde{f_{2k}}$ are not EA-equivalent.

Corollary 3 $\#\mathrm{BS}_{2k-2}(f_{2k}) < \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$ *holds, where the function* $f_{2k} \in \mathcal{B}_{2k}$, $k \geq 4$, *is defined by*

$$f_{2k}(x) = \xi_8(x_1, \ldots, x_8) \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus \ldots \oplus x_{2k-1}x_{2k},\ x \in \mathbb{F}_2^{2k}.$$

Proof It is easy to show by induction that $K_0(\widetilde{f_{2k}}) < K_0(f_{2k})$ and $K_1(\widetilde{f_{2k}}) < K_1(f_{2k})$. The base of the induction is the function $f_8 = \xi_8$, the induction step is provided by Theorem 9. It means that $\#\mathrm{BS}_{2k-2}(f_{2k}) = 4K_0(f_{2k}) < 4K_0(f_{2k}) = \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$. □

Thus, unlike $m \leq n/2 + 1$, we obtain that $\#\mathrm{BS}_m(f)$ and $\#\mathrm{BS}_m(\widetilde{f})$ may not be equal. As a consequence, $\sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$ may not be an affine subspace.

8 Conclusion

We have considered several properties of the bent function secondary construction $f \oplus \mathrm{Ind}_L$, where f is a bent function in n variables and L is an affine subspace of arbitrary dimension. In particular, $\#\mathrm{BS}_m(f)$, where $\mathrm{BS}_m(f)$ is the set of all bent functions of the form $f \oplus \mathrm{Ind}_L$ for an m-dimensional L, has been estimated. A relationship between considered subspaces in the simplest iterative construction has been established. Examples of the "most difficult" bent functions that have empty $\mathrm{BS}_m(f)$, for different m, have been provided. It has been found that the construction properties for arbitrary subspaces are quite similar to the case of $n/2$-dimensional subspaces, thus, we have generalized some known facts. At the same time, arbitrary dimensions have some specific properties that make the construction interesting.

Note that we have not provided an example of a bent function f in n variables, where n is arbitrary, such that $\mathrm{BS}_m(f)$ is empty for any $m \leq n-2$. It is a topic for future research.

Acknowledgements We would like to thank C. Carlet and anonymous reviewers for the valuable comments. We also thank A. Gorodilova and V. Idrisova for their suggestions and helpful discussions.

References

1. Bonnetain, X., Perrin, L., Tian, S.: Anomalies and vector space search: tools for S-Box analysis. In: Galbraith, S., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019. Lecture Notes in Computer Science, 11921, pp. 196–223. Springer, Cham (2019)
2. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inform. Theory **49**(8), 2004–2019 (2003)
3. Canteaut, A., Daum, M., Dobbertin, H., Leander, G.: Finding nonnormal bent functions. Discrete Appl. Math. **154**(2), 202–218 (2006)
4. Carlet, C.: Two new classes of bent functions. In: Helleseth, T. (ed.) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, 765, pp. 77–101. Springer, Berlin, Heidelberg (1994)
5. Carlet, C.: On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions, Special Issue "Complexity Issues in Coding Theory and Cryptography" dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday. J. Complexity **20**, 182–204 (2004)
6. Carlet, C.: Boolean functions for cryptography and error correcting code. In: Crama, Y., Hammer, P.L. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
7. Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press, Cambridge (2021)
8. Carlet, C., Dobbertin, H., Leander, G.: Normal extensions of bent functions. IEEE Trans. Inform. Theory **50**(11), 2880–2885 (2004)
9. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
10. Cusick, T.W., Stanica, P. Cryptographic Boolean functions and applications, 2nd. Acad. Press. Elsevier, Amsterdam (2009)
11. Dillon, J.: Elementary Hadamard Difference Sets, PhD. dissertation. College Park, Univ Maryland (1974)
12. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with singer parameters. Finite Fields Their Appl. **10**, 342–389 (2004)
13. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: Preneel, B. (ed.) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, 1008, pp. 61–74. Springer, Berlin, Heidelberg (1995)
14. Helleseth, T., Kholosha, A.: Bent functions and their connections to combinatorics. In: Blackburn, S., Gerke, S., Wildon, M. (eds.) Surveys in Combinatorics 2013 (London Mathematical Society Lecture Note Series), pp. 91–126. Cambridge University Press, Cambridge (2013)

15. Frolova, A.: The essential dependence of Kasami bent functions on the products of variables. J. Appl. Ind. Math. **7**, 166–176 (2013)
16. Kolomeec, N.: The graph of minimal distances of bent functions and its properties. Des Codes Cryptogr **85**(3), 395–410 (2017)
17. Kolomeec, N.A., Pavlov, A.V.: Bent functions on the minimal distance. In: 2010 IEEE Region 8 international conference on computational technologies in electrical and electronics engineering (SIBIRCON), pp. 145–149 (2010)
18. Kutsenko, A.: The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun. **12**(5), 881–898 (2020)
19. Langevin, P., Leander, G.: Monomial bent function and Stickelberger's theorem. Finite Fields Their Appl. **14**, 727–742 (2008)
20. Leander, G., McGuire, G.: Construction of bent functions from near-bent functions. J. Combin. Theory. Ser. A **116**(4), 960–970 (2009)
21. Logachev, O.A., Salnikov, A.A., Yashchenko, V.V.: Boolean functions in coding theory and cryptography american mathematical society (2012)
22. Mandal, B., Stanica, P., Gangopadhyay, S., Pasalic, E.: An analysis of the $\mathcal{C}$ class of bent functions. Fundamenta Informaticae **146**, 271–292 (2016)
23. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) Advances in cryptology – EUROCRYPT '93. EUROCRYPT 1993. lecture notes in computer science, 765, pp. 386–397. Springer, Berlin (1994)
24. McFarland, R.L.: A family of difference sets in non-cyclic groups. J. Combin. Theory. Ser. A **15**, 1–10 (1973)
25. Mesnager, S., functions, B.ent.: Fundamentals and results. Springer, Berlin (2016)
26. Rothaus, O.: On bent functions. J. Combin. Theory. Ser. A **20**(3), 300–305 (1976)
27. Sharma, D., Gangopadhyay, D.: On Kasami bent function, Cryptology ePrint Archive, Report 2008/426. http://eprint.iacr.org/2008/426.pdf (2008)
28. Tokareva, N.: Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, Amsterdam (2015)
29. Yashchenko, V.: On the propagation criterion for Boolean functions and on bent functions. Probl. Peredachi Inf. **33**(1), 75–86 (1997). (in Russian)

On the number of suitable Boolean functions in constructions of filter and combining models of stream ciphers*

Tatiana Bonich, Matvey Panferov, Natalia Tokareva

Abstract

It is well known that every stream cipher is based on a good pseudorandom generator. For cryptographic purposes we are interested in generating pseudorandom sequences with the maximum possible period. A feedback register is one of the most known cryptographic primitives that is used to construct stream ciphers. In this paper we analyze periodic properties of pseudorandom sequences produced by filter and combiner generators (two known schemes of stream generators based on feedback registers). We analyze functions in these schemes which lead to pseudorandom sequences of the maximum possible period. We call such functions suitable and count the exact number of them for an arbitrary n.

Index Terms

stream cipher, filter generator, combiner generator, gamma, Boolean function

I. Introduction

SYMMETRIC ciphers usually are divided into block and stream ones. Stream ciphers are considered as more fast but not as secure as block ciphers. One of the most known cryptographic primitives that is used to construct stream ciphers is a feedback register. There are many attacks and defenses on such ciphers and counter-measures against them, see for instance [6], [4].

The properties of the pseudorandom sequence (gamma) generated by FSR are well studied in case when f is a linear function. If f is nonlinear (see [8]), there are too many open questions related to pseudorandom sequences that all are connected to analysis of nonlinear recurrent sequences, for example, see [5] for further review. That is why some nonlinear *combinations* of linear FSRs are usually considered, for instance, filter and combining models of stream generators based on LFSR (see [10]).

Let us recall a few definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A *Boolean function in n variables* is a function of the form $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A *vector of values* for a given Boolean function f is the vector $(f(x^{(1)}), \dots, f(x^{(2^n)}))$, where $x^{(1)}, \dots, x^{(2^n)}$ are binary vectors in $\mathbb{F}_2^n$ that are lexicographically ordered. Any Boolean function f can be represented uniquely in its *algebraic normal form (ANF)*:

$$f(x_1, \dots, x_n) = \bigoplus_{I \in \mathcal{P}(N)} a_I \Big(\prod_{i \in I} x_i \Big),$$

where $\mathcal{P}(N)$ is a power set of $N = \{1, \dots, n\}$ and $a_I \in \mathbb{F}_2$. For a Boolean function f the number of variables in the longest item of its ANF is called *the algebraic degree* of a function. If algebraic degree of a function f is not more than 1 then f is called *affine*. If for an affine function f it holds $f(\mathbf{0}) = \mathbf{0}$ then f is called *linear*. If algebraic degree of a function f is strictly larger than 1 then f is called *nonlinear*.

A *feedback shift register (FSR)* consists of two parts: a binary block $x = (x_1, \dots, x_n)$ of length n and a feedback function f, where f is a Boolean function in n variables. First, we fill the block x with constants, it is the *initial state* of the register. During the encryption process the register is changing its state using the feedback function. *Gamma* is a pseudorandom sequence generated by FSR. For functioning of the FSR the time is considered to be divided into clock cycles. On each clock cycle, the value of $f(x)$ is calculated first, then the state $x = (x_1, \dots, x_{n-1}, x_n)$ of the register is changed to the state $x' = (x_2, \dots, x_n, f(x))$ while the bit x_1 will be written as the first bit of the generated *gamma*. A *period* is a length of repeating part of gamma. In case when Boolean function f is linear we have *linear feedback shift register (LFSR)*. Similarly, *nonlinear feedback shift register (NLFSR)* uses nonlinear Boolean function as a feedback function.

It is known that LFSR can be also specified using a feedback polynomial. It is a polynomial of degree n defining bits to be summed. If $f(x_1, \dots, x_n) = a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n$, then the corresponding feedback polynomial is defined as $p(z) = a_1z^n + a_2z^{n-1} + \dots + a_nz + 1$, where $a_i \in \mathbb{F}_2$, $i = 1, \dots, n$. If $p(z)$ is a primitive polynomial, i.e., the primitive element of the field $GF(2^n)$ is its root, then the period of a pseudorandom sequence generated by LFSR is maximal, i.e. is equal to $2^n - 1$. As a consequence, primitive polynomials mainly are used in LSFR.

*This article was partly presented on the SEIM2020 conference.

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

There are many stream ciphers based on LFSR and NLFSR. One of them is Grain, developed in 2004 [9]. It is constructed by combining model, which is based on two shift registers, one with linear feedback and one with non-linear feedback, and a non-linear output function. Both linear and nonlinear shift register sizes are 80 bits.

Another one is A5/1 cipher that is current GSM standard [1]. It has three linear feedback shift registers of lengths 19, 22 and 23 bits with irregular clocking. The registers are clocked in a stop/go fashion using a majority rule. The output is the sum of the last bits of the three registers.

Moreover, we could mention the Gollmann cascade [7]. This cipher is the representative of combining model. It consists of a series of LFSRs that are clock-controlled by the previous LFSR. If all the LFSRs have the same length n, the linear complexity of a system with k LFSRs is equal to $n(2^n-1)^{k-1}$.

Additionally, the shrinking generator should be noted. This is also the representative of combining model. It consists of two LFSRs that are clock-controlled LFSR-1 and LFSR-2. If the output of LFSR-1 is 1, then the output of the generator is LFSR-2. If the output of LFSR-1 is 0, two bits are discarded, both LFSRs are clocked, and look new output. For instance, see [3].

Other examples of ciphers that are based on LFSR and NLFSR are Geffe generator, Jennings generator and Beth-Piper Stop-and-Go generator.

In this paper, we analyze pseudorandom sequences produced by filter and combiner generators. Namely, we study functions in these schemes that lead to pseudorandom sequences of the maximal period. We call such functions *suitable* and count the exact number of them for an arbitrary n.

II. The analysis of gamma for linear feedback shift register generators

A. Filter generators

The filter generator consists of a single shift register of length n with a linear feedback and uses a primitive polynomial to change states. A Boolean function $h(x_1,\dots,x_n)$ applied to the current state generates a pseudorandom sequence (gamma). Let us not that the number of all possible functions $h(x_1,\dots,x_n)$ is equal to 2^{2^n}. The work of the filter generator is shown in [2].

Let gamma be defined as $\gamma=(y_1,y_2,\dots,y_{2^n-1})$, where $y_1=h(x_1,\dots,x_n)$, $y_2=h(x_2,\dots,x_n,f(x_1,\dots,x_n))$, etc., and $f(x_1,\dots,x_n)$ is the feedback function. Since the number of all nonzero states is equal to 2^n-1, the maximum possible values of period of gamma is 2^n-1 too. In this paper, we would like to determine all Boolean functions h in n variables that lead to gammas with maximal period. Let us call such functions *suitable*. Functions that lead to gammas with non-maximal period we would call *unsuitable*. Note that the number of such functions does not depend on a linear feedback function. But whether the function is suitable or not for the given generator, depends on the feedback function. When we count the number of suitable functions h, we do not consider a specific set of states. We say that there is a certain number of different states used by the generator (all sets that are generated by primitive polynomials fit this definition). Next, we study which pseudorandom sequences have the maximal length. We analyze the number of unsuitable functions and the number of suitable functions. Thus, our reasonings do not affect the specific order of the states. Therefore, there will be the exact calculated number of suitable functions h for any set of states used by the generator.

Let us provide some examples of suitable and unsuitable functions. Let $n=4$ be the length of a shift register, $f(x_1,x_2,x_3,x_4)=x_1\oplus x_2$ be a feedback function and $p(z)=z^4+z^3+1$ be a corresponding primitive polynomial. Let $h_1(x_1,x_2,x_3,x_4)=x_2x_1\oplus x_3x_1\oplus x_3x_2\oplus x_4x_1\oplus x_1\oplus x_2\oplus x_3\oplus 1$ and $h_2(x_1,x_2,x_3,x_4)=x_2x_1\oplus x_3x_2\oplus x_4x_1\oplus x_1\oplus x_3\oplus 1$ be Boolean functions in n variables. We present generated gamma for these functions on Table I.

TABLE I
EXAMPLES OF SUITABLE AND UNSUITABLE FUNCTIONS

states	0001	0010	0100	1001	0011
$h_1(x_1,x_2,x_3,x_4)$	1	0	0	1	0
$h_2(x_1,x_2,x_3,x_4)$	1	0	1	1	0
states	0110	1101	1010	0101	1011
$h_1(x_1,x_2,x_3,x_4)$	0	1	0	0	1
$h_2(x_1,x_2,x_3,x_4)$	1	0	1	1	0
states	0111	1111	1110	1100	1000
$h_1(x_1,x_2,x_3,x_4)$	0	0	1	0	0
$h_2(x_1,x_2,x_3,x_4)$	1	0	1	1	0

It can be seen that h_1 generates gamma with period equal to 3 and h_2 generates gamma with period equal to 15.

Let us prove the main result for filter generators.

Theorem 1: Let $n\in\mathbb{N}$ and $2^n-1=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, where p_i are pairwise distinct prime numbers, $\alpha_i\in\mathbb{N}$, $s\in\mathbb{N}$. Then the number of suitable Boolean functions in n variables for the filter generator with LFSR based on a primitive polynomial of degree n, is equal to

$$2^{2^n}-2\sum_{\beta\in\mathbb{F}_2^s,\beta\neq 0}((-1)^{\beta_1+\dots+\beta_s+1}2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}}),$$

where $\beta = (\beta_1, \dots, \beta_s)$ and $+$ is a usual summing.

Proof: Consider sequences of length $2^n - 1$ with non-maximal period (*unsuitable* sequences). Let A_i be a set of sequences that can be divided on p_i identical subsequences, where $i = 1, \dots, s$. Then $A_i \cap A_j$ is a set of sequences that can be divided on $p_i * p_j$ identical subsequences where $i \neq j$ and $i, j = 1, \dots, s$. Then $A_i \cup A_j$ is a set of sequences that can be divided on p_i or p_j identical subsequences where $i \neq j$ and $i, j = 1, \dots, s$. Hence, all unsuitable sequences belong to the set $\cup_{i=1}^{s} A_i$ and the number of these sequences is equal to $|\cup_{i=1}^{s} A_i|$. Dividing the sequence into p_i identical subsequences, the length of the subsequence is equal to $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i - 1} \dots p_s^{\alpha_s}$. Since elements of subsequences are equal to 0 or 1 then

$$|A_i| = 2^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{(i-1)}^{\alpha_{(i-1)}} p_i^{\alpha_i - 1} p_{(i+1)}^{\alpha_{(i+1)}} \dots p_s^{\alpha_s}},$$

$$|A_i \cap A_j| = 2^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{(i-1)}^{\alpha_{(i-1)}} p_i^{\alpha_i - 1} p_{(i+1)}^{\alpha_{(i+1)}} \dots p_{(j-1)}^{\alpha_{(j-1)}} p_j^{\alpha_j - 1} p_{(j+1)}^{\alpha_{(j+1)}} \dots p_s^{\alpha_s}},$$

$$\dots$$

$$|\cap_{i=1}^{s} A_i| = 2^{p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_s^{\alpha_s - 1}}.$$

Therefore, we can compute $|\cup_{i=1}^{s} A_i|$ using the inclusion-exclusion principle:

$$\begin{aligned}
|\cup_{i=1}^{s} A_i| = \sum_{i=1}^{s} |A_i| - \sum_{1 \le i < j \le s} |A_i \cap A_j| + \\
+ \sum_{1 \le i < j < k \le s} |A_i \cap A_j \cap A_k| - \dots \\
+ (-1)^{s-1} |A_1 \cap A_2 \cap \dots \cap A_s| = \\
= \sum_{i=1}^{s} 2^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{(i-1)}^{\alpha_{(i-1)}} p_i^{\alpha_i - 1} p_{(i+1)}^{\alpha_{(i+1)}} \dots p_s^{\alpha_s}} - \\
- \sum_{1 \le i < j \le s} 2^{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{(i-1)}^{\alpha_{(i-1)}} p_i^{\alpha_i - 1} p_{(i+1)}^{\alpha_{(i+1)}} \dots p_{(j-1)}^{\alpha_{(j-1)}} p_j^{\alpha_j - 1} p_{(j+1)}^{\alpha_{(j+1)}} \dots p_s^{\alpha_s}} + \\
\dots + (-1)^{s-1} 2^{p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_s^{\alpha_s - 1}} = \\
= \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_s + 1} 2^{p_1^{\alpha_1 - \beta_1} \dots p_s^{\alpha_s - \beta_s}}),
\end{aligned}$$

where $\beta = (\beta_1, \dots, \beta_s)$.

We can write all states of our register one by one and from one state we get the second one as the next state. Consider the vector of values of a Boolean function h that generates our gamma. Since there is no zero state in our set of states (it generates the cycle of length 1), function h can take any value (0 or 1) on zero vector. That is why there are exactly two Boolean functions that generate the same sequence.

Hence, the number of unsuitable functions is equal to

$$2|\cup_{i=1}^{s} A_i| = 2 \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_s + 1} 2^{p_1^{\alpha_1 - \beta_1} \dots p_s^{\alpha_s - \beta_s}})$$

Then, the number of suitable functions is equal to

$$2^{2^n} - 2 \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_s + 1} 2^{p_1^{\alpha_1 - \beta_1} \dots p_s^{\alpha_s - \beta_s}}),$$

where $\beta = (\beta_1, \dots, \beta_s)$. ■

The results of Theorem 1 for $n = 3, \dots, 6$ are presented in the Table II.

TABLE II
NUMBER OF SUITABLE FUNCTIONS

n	3	4	5	6
suitable functions	252	65460	$2^{32} - 4$	$2^{64} - 2^{22} - 1008$
total number	256	65536	2^{32}	2^{64}

B. Combining model

Combiner generators use several linear feedback shift registers. Each register has its own length n_i and uses its own primitive polynomial for changing states. A Boolean function $h(X_1, \dots, X_m)$ generates a pseudorandom sequence gamma, where X_i is a register bit string i. The work of the combiner generator is shown in [2].

Since we do not use zero state in combiner generator, the total number of states does not exceed $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$. In this case, the maximum is reached when $gcd(n_i, n_j) = 1$, where $i, j = 1, \dots, m$, $i \neq j$, and if all LFSRs have primitive feedback polynomials. Then a Boolean function can generate a gamma with a period ranging from 1 to $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$. Boolean functions h in n variables leading to gammas of maximal period in this case are called *suitable*. Similarly, Boolean functions h in n variables leading to gammas of non-maximal period are called *unsuitable*. Notice that $gcd(2^{n_i}-1, 2^{n_j}-1) = 1$, where $i, j = 1, \dots, m$, $i \neq j$. It means that each number $(2^{n_i}-1)$ can be presented as $p_{k_1}^{\alpha_{k_1}} p_{k_2}^{\alpha_{k_2}} \dots p_{k_s}^{\alpha_{k_s}}$, where $k_1, k_2, \dots, k_s$ are integers which depend on i.

We consider a more general model of a combiner generator. This generalized combining model is applied in ciphers such as Grain [9]. Note that the classical combining model does not allow to describe a number of modern stream ciphers based on the more complicated operating with bits from different registers. In this case, the more known version of the combiner generator in which the function depends only on the last bits of the registers is included in the model we are considering. In a nonlinear model, sometimes it is more convenient to work with several smaller registers than with one large register. It should be noted that the considered model can be used not only in cases of all linear or all non-linear registers but also in cases of mixed registers (i.e. some registers are linear, some are non-linear).

Theorem 2: Let $n \in \mathbb{N}$, $m \in \mathbb{N}$, $n_1, \dots, n_m \in \mathbb{N}$, $\sum_{i=1}^{m} n_i = n$. And

$$(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

where p_i are different prime numbers, $\alpha_i \in \mathbb{N}$, $s \in \mathbb{N}$. Then the number of suitable Boolean functions in n variables for the combiner generator with LFSRs of lengths $n_1, \dots, n_m$ all based on primitive polynomials is equal to

$$2^{2^n} - 2^{2^{n_1+n_2+\dots+n_m} - (2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)} \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1+\dots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}}),$$

where $\beta = (\beta_1, \dots, \beta_s)$.

Proof: Number of unsuitable sequences for the combiner generators is equal to $\sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1+\dots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}})$. Proof of this is similar to proof of number of unsuitable sequences for the filter generators in Theorem 1. Since we use only $(2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$ states and the total number of states is equal to $2^{n_1} \cdot 2^{n_2} \dots 2^{n_m} = 2^{n_1+n_2+\dots+n_m}$, then we have $2^{n_1+n_2+\dots+n_m} - (2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)$ states, where our function can be equal to 0 or 1. Therefore, for one of these states we have two functions. Thus, the number of unsuitable Boolean functions in n variables for the combiner generators is equal to

$$2^{2^{n_1+n_2+\dots+n_m} - (2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)} \cdot \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1+\dots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}}),$$

where $\beta = (\beta_1, \dots, \beta_s)$.

Then, the number of suitable functions is equal to

$$2^{2^n} - 2^{2^{n_1+n_2+\dots+n_m} - (2^{n_1}-1)(2^{n_2}-1)\dots(2^{n_m}-1)} \sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1+\dots+\beta_s+1} 2^{p_1^{\alpha_1-\beta_1}\dots p_s^{\alpha_s-\beta_s}}),$$

where $\beta = (\beta_1, \dots, \beta_s)$.

■

The results of Theorem 2 for $n = 7$, $m = 2$, $n_1 = 3$, $n_2 = 4$ are presented in the Table III.

TABLE III
NUMBER OF SUITABLE FUNCTIONS FOR COMBINING MODEL

n_1	3
n_2	4
suitable functions	$2^{128} - 2^{58} - 2^{44} - 2^{38} + 166 * 2^{23}$
total number	2^{128}

III. Functions for models with nonlinear registers

A *nonlinear feedback shift register (NFSR)* consists of two parts: a binary vector $x = (x_1, \dots, x_n)$ of length n and a nonlinear state function $f : (x_1, \dots, x_n) \to \{0, 1\}$ in n variables.

Similarly to the linear case, let us consider the filter generator. We assume that NFSR passes over all 2^n states, i.e., it has the maximum possible period.

Theorem 3: Let $n \in \mathbb{N}$. Then the number of suitable Boolean functions in n variables for the filter generator with NFSR of the maximum possible period is equal to $2^{2^n} - 2^{2^{n-1}}$.

Proof: Maximum possible period is equal to $2^n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, where $s = 1$, $p_1 = 2$, $\alpha_1 = n$. Number of unsuitable sequences is equal to $\sum_{\beta \in \mathbb{F}_2^s, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_s + 1} 2^{p_1^{\alpha_1 - \beta_1} \dots p_s^{\alpha_s - \beta_s}})$, where $\beta = (\beta_1, \dots, \beta_s)$. Proof of this is similar to the part of the proof of Theorem 1, in which calculated the number of unsuitable sequences for the filter generators. Then the number of unsuitable sequences for the filter generator with NFSR is equal to $2^{2^{n-1}}$. Since we use all the states then the number of unsuitable sequences is equal to the number of unsuitable Boolean functions. Hence, the number of unsuitable Boolean functions in n variables for the filter generator with NFSR is equal to $2^{2^{n-1}}$. Therefore, the number of suitable functions is $2^{2^n} - 2^{2^{n-1}}$.

■

There is another question related to NFSRs: how to determine for which nonlinear feedback functions NFSR of length n generates gamma with the maximum possible period 2^n? This question is continued and still open.

Acknowledgment

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

References

[1] A. Canteaut "A5/1." "Encyclopedia of Cryptography and Security," Springer, Boston, MA, 2011.
[2] C. Carlet Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / Eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Chapter 8. pp. 257-–397.
[3] D. Coppersmith, H. Krawczyk, Y. Mansour, "The Shrinking Generator," Advances in Cryptology—CRYPTO '93 Proceedings, Springer–Verlag, 1994, pp. 22–39.
[4] N. Courtois, W. Meier "Algebraic attacks on stream ciphers with linear feedback. In: Advances in cryptology - EUROCRYPT 2003," Lecture notes in computer science, vol 2656. Springer, Heidelberg, 2003
[5] M. Glukhov, V. Elizarov, A. Nechaev, "Algebra,",vol. 2, Gelios ARV, pp. 327–333, 2003 (in Russian).
[6] J. Golić, "On the security of nonlinear filter generators. In: Fast Software Encryption," Lecture notes in computer science, vol 1039. Springer, Heidelberg, pp.173–188, 1996.
[7] D. Gollmann, "Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren," Ph.D.dissertation, Universität Linz, 1983. (In German)
[8] E. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," IEEE Trans Inform Theory 22, pp.732–736, 1976.
[9] M. Hell, T. Johansson, W. Meier "A Stream Cipher for Constrained Environments" // Int. J. Wireless Mobile Comput., vol. 2, no. 1, 2007, pp. 86–93.
[10] A. Menezes, P. C. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, pp. 191–222, 1996.

Tatiana Bonich Novosibirsk State University
Tatiana Bonich received the B.Sc. degree in mathematics from Omsk State University in 2019. In 2021 she completes her M.Sc. degree in Novosibirsk State University. Since 2019, she is a researcher of the laboratory of cryptography in Novosibirsk State University. She is currently working on analysis of pseudorandom sequences in cryptography.

Matvey Panferov Novosibirsk State University
Matvey Panferov graduated Omsk State University in 2019. Since 2019 he studies in Novosibirsk State University. Since 2019, he is a researcher of the laboratory of cryptography in Novosibirsk State University. He is interested in analysis of pseudorandom sequences in cryptography.

Natalia Tokareva Sobolev Institute of Mathematics, Novosibirsk, Russia
Natalia Tokareva received the PhD degree in mathematics from Sobolev Institute of Mathematics in 2008. Since 2014 she is a head of Cryptographic Center in Novosibirsk and a general chair of International Olympiad in Cryptography. She was a supervisor for more than 30 MS and PhD students. Her research interests include cryptographic Boolean functions, namely bent functions; symmetric cryptography and cryptanalysis in general.

УДК 519.7

ПРИМЕНЕНИЕ SAT-РЕШАТЕЛЕЙ К ЗАДАЧЕ ПОИСКА ТАБЛИЧНО ЗАДАННЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С ТРЕБУЕМЫМИ КРИПТОГРАФИЧЕСКИМИ СВОЙСТВАМИ [1]

К. В. Калгин, А. Е. Доронин

Институт математики им. Соболева СО РАН,
Новосибирский Государственный Университет, г. Новосибирск, Россия

В данной работе представлен подход к решению задачи поиска APN-функции, основанный на сведении к классической задаче о выполнимости и использовании SAT-решателей. Описано построение формул, определяющих APN-функцию. Введены два представления функции: разреженное и плотное, в которых описана задача поиска взаимно-однозначной векторной булевой функции и APN-функции. Представлено описание и реализация модернизированного switching-метода в виде SAT-задачи, который смог показать эффективность на размерностях $n = 6, 7, 8$.

Ключевые слова: *SAT-решатели, криптография, булевы функции, APN-функции, switching-метод.*

DOI 10.17223/20710410/XX/1

SAT-SOLVERS APPLICATION FOR FINDING TABLE-DEFINED VECTORIAL BOOLEAN FUNCTIONS WITH THE REQUIRED CRYPTOGRAPHIC PROPERTIES

K. V. Kalgin, A. E. Doronin

Sobolev Institute of Mathematics,
Novosibirsk State University, Novosibirsk, Russia

E-mail: kalginkv@gmail.com, artem96dor@gmail.com

In this paper we propose a method for finding an APN-function. It is based on translation into SAT-problem and using SAT-solvers. We introduce construction of several formulas defining conditions for finding APN-function. We introduce two representations of function: sparse and dense, which are used to describe the problem of finding one-to-one vectorial Boolean functions and APN-functions. We describe and implement an improved switching-method as a SAT-problem. This method showed its practical efficiency on bigger dimensions ($n = 6, 7, 8$).

Keywords: *SAT-solvers, cryptography, Boolean functions, APN-functions, switching-method.*

[1] Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2019-1613 и лаборатории криптографии JetBrains Research.

Введение

В настоящее время известно большое число открытых криптографических задач, одна из которых — поиск новых криптографических булевых функций для использования в различных шифрсистемах. Возможным подходом к решению данной задачи служит попытка записать ее в виде задачи о выполнимости и использовать SAT-решатели для поиска решений.

Задача о выполнимости (SAT- или ВЫП-задача) заключается в следующем: можно ли присвоить переменным некоторой булевой КНФ-формулы значения «истина» или «ложь» таким образом, чтобы формула стала истинной. В общем случае данная задача является NP-полной [2]. Напомним, что NP-полнота SAT-задачи означает то, что к ней можно свести все задачи из класса NP за полиномиальное время. И если найдется полиномиальный алгоритм решения NP-полной задачи, то и все остальные задачи будут решены за полиномиальное время. В настоящее время по задаче о выполнимости проводится большое количество исследований, а программы, решающие данную задачу, используются во многих областях: проверка моделей, решение задач теории расписаний, искусственный интеллект, криптография и многие другие. В связи с этим ежегодно проводятся конкурсы программ, так называемые, соревнования SAT-решателей (SAT-competition) [5].

SAT-решатель — это программа, которая проверяет выполнимость формулы, записанной в конъюнктивной нормальной форме (КНФ-формулы). Первые SAT-решатели основывались на алгоритме DPLL (алгоритм Дэвиса - Патнема - Логемана - Лавленда) [6] — полный алгоритм поиска с возвратом для решения задачи выполнимости булевых КНФ-формул. Алгоритм произвольным образом выбирает переменную, присваивает ей значение «истина», упрощает формулу и рекурсивным образом проверяет ее на выполнимость. Если алгоритм сталкивается с конфликтом (подмножеством означиваний переменных, при котором возникают ложные дизъюнкции), то алгоритм выполняет возврат к переменной и присваивает ей значение «ложь». Основное отличие DPLL от перебора в глубину — это наличие вывода значений других переменных после присваивания значения переменной на текущем шаге (constant propagation). Данный алгоритм показал высокую эффективность для ряда практических задач. Прямым продолжением алгоритма DPLL является алгоритм CDCL (Conflict-Driven-Clause-Learning) [7], который лежит в основе современных SAT-решателей. Аналогично DPLL, в алгоритме CDCL выбирается переменная и означивается в соответствии с реализованным эвристическим алгоритмом. Однако алгоритм хранит граф вывода и по ходу работы запоминает комбинации, которые не ведут к решению, тем самым позволяет эффективно отсекать подпространства наборов значений переменных, приводящих к конфликтам. Разработчики алгоритма CDCL создали SAT-решатель GRASP, который описан в работе [7]. Предложенные эвристики существенно сокращают время работ решателя на многих классах задач.

SAT-решатели используются для решения многих криптографических задач. Например, для проведения криптоанализа шифрсистем. В работе [8] рассматривается криптоанализ задачи факторизации целых чисел, на котором основана криптосистема RSA. Суть работы заключается в построении и использовании методов, которые находят приближенное решение SAT-задачи, но в результате статистических испытаний для каждого бита будет получена вероятность верного определения каждого бита. Этим методом является метод простой итерации с использованием ряда полиномиальных эвристик по улучшению его сходимости. Также используеся альтернативный способ нахождения приближенного решения SAT-задачи, заключающееся в

построении системы линейных уравнений на основе исходной формулы. Полученные данные могут быть применены с сочетании с известными SAT-решателями (например, алгоритмом локального поиска GSAT). Полученным гибридным алгоритмом удалось факторизовать число размерностью до 417 бит в двоичной записи включительно.

В работе [9] представлена гомоморфная криптосистема с открытым ключом, основанная на задаче выполнимости булевых формул. В данной системе открытым ключом является сама булева формула, секретным ключом — означивание этой формулы, при которой она станет истинной.

Работа [10] посвящена проверке обратимости векторных булевых функций. Показано, что данная задача является coNP-полной. Предлагается два подхода: с использованием SAT-решателей и бинарных диаграмм решений (BDD).

В данной работе предлагается сведение криптографической задачи поиска таблично заданных векторных булевых функций с некоторыми свойствами, такими как взаимная однозначность и дифференциальная равномерность, к задаче выполнимости. Данная задача представляется в виде КНФ-формул и подаётся на вход SAT-решателя, который в процессе своей работы проверяет формулу на выполнимость. Если она выполнима, то выводит решение.

1. Определения и обозначения

В работе были использованы следующие определения:

Определение 1. Векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется *биективной* [1], если она инъективна и сюръективна, то есть одновременно выполняются следующие условия:

1) $\forall x' \in \mathbb{Z}_2^n \; \forall x'' \in \mathbb{Z}_2^n : x' \neq x'' \to F(x') \neq F(x'')$,
2) $\forall y \in \mathbb{Z}_2^m \; \exists \mathbb{Z}_2^n \in X : F(x) = y$.

Определение 2. Векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ называется *дифференциально δ-равномерной* [3], если при любом ненулевом векторе $a \in \mathbb{Z}_2^n$ и произвольном векторе $b \in \mathbb{Z}_2^n$ уравнение

$$F(x) \oplus F(x \oplus a) = b \tag{1}$$

имеет не более δ решений, где δ — целое число.

Если $\delta = 2$, то векторная булева функция называется *APN-функцией*.

2. Задание функции

В работе представлены способы записи криптографических свойств с помощью двух представлений — разреженного и плотного.

2.1. Разреженное представление

Для задания векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ введем следующие базовые переменные:

$$f_{x,y} = 1 \iff F(x) = y, \text{ где } x, y \in \mathbb{Z}_2^n.$$

Такое представление булевой функции будем называть **разреженным** (по аналогии с разреженными матрицами). Число переменных $f_{x,y}$ равно 2^{2n}.

Теорема 1. Множество переменных $f_{x,y}$ кодирует функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ тогда и только тогда, когда следующая формула является истинной:

$$\mathbf{F}^{\mathbf{S}}(f) = \bigwedge_{x\in\mathbb{Z}_2^n} \bigwedge_{\substack{y',y''\in\mathbb{Z}_2^n \\ y'<y''}} (\overline{f_{x,y'}} \vee \overline{f_{x,y''}}) \wedge \bigwedge_{x\in\mathbb{Z}_2^n} (\bigvee_{y\in\mathbb{Z}_2^n} f_{x,y}). \tag{2}$$

Доказательство. Чтобы переменные $f_{x,y}$ задавали функцию, необходимо, чтобы для каждого элемента из множества прообразов существовал единственный образ, то есть $\forall x \in \mathbb{Z}_2^n\ \exists! y \in \mathbb{Z}_2^n$, что $f_{x,y} = 1$.

В КНФ это условие записывается в два этапа:

1) Существование образа для каждого прообраза: $\forall x\ \exists y\ f_{x,y} = 1$ или $\bigwedge\limits_{x\in\mathbb{Z}_2^n} (\bigvee\limits_{y\in\mathbb{Z}_2^n} f_{x,y})$.
2) Существование не более чем одного образа для каждого прообраза: $\forall x\ \forall y', y''\ (f_{x,y'} \to \overline{f_{x,y''}})$ или $\bigwedge\limits_{x\in\mathbb{Z}_2^n} \bigwedge\limits_{\substack{y',y''\in\mathbb{Z}_2^n \\ y'<y''}} (\overline{f_{x,y'}} \vee \overline{f_{x,y''}})$.

Объединяя данные формулы при помощи конъюнкции, получаем формулу (2). ■

Итого формула $\mathbf{F}^{\mathbf{S}}(f)$ состоит из $2^{3n-1} - 2^{2n-1}$ дизъюнкций длины 2 и 2^n дизъюнкций длины 2^n.

2.2. Плотное представление

Векторную булеву функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ всегда можно представить следующим образом: $F(x) = (F_0(x), F_1(x), \ldots, F_{n-1}(x))$, где $F_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$, $i = 0, \ldots, n-1$. Таким образом, в плотном представлении удобно ввести следующие базовые переменные:

$$fb_{x,k} = 1 \iff F_k(x) = 1, \text{ где } k = 0, \ldots, n-1,\ x \in \mathbb{Z}_2^n.$$

Такое представление булевой функции будем называть **плотным** (Буква b в обозначении fb взята от слова binary ввиду записи в данном представлении значений $f(x)$ в двоичной записи). Число переменных $fb_{x,k}$ равно $n \cdot 2^n$.

В данном представлении каждому прообразу $x \in \mathbb{Z}_2^n$ ставится в соответствие некоторый образ $y \in \mathbb{Z}_2^n$. Таким образом, наложение дополнительных условий на булевы переменные $fb_{x,k}$, как это было сделано в разреженном представлении в теореме 1, не требуется.

3. Взаимная однозначность

Поскольку для записи необходимых нам задач в определении 1 требуется равенство чисел n и m, то по свойствам функции следующие утверждения эквивалентны:

1) F биективна;
2) F инъективна;
3) F сюръективна.

Тогда определение биективной функции можно переписать следующим образом:

Утверждение 1. Векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ называется *биективной*, если выполняется одно из следующих условий:

1) $\forall x' \in \mathbb{Z}_2^n\ \forall x'' \in \mathbb{Z}_2^n : x' \neq x'' \to F(x') \neq F(x'')$,
2) $\forall y \in \mathbb{Z}_2^n\ \exists x \in \mathbb{Z}_2^n : F(x) = y$.

В далее в работе биективную булеву функцию будем называть *взаимно однозначной* булевой функцией.

Взаимная однозначность векторной булевой функции необходима, например, для использования их в качестве S-блоков в различных шифрах и криптосистемах.

3.1. Разреженное представление

Теорема 2. Множество переменных $f_{x,y}$ кодирует взаимно однозначную функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ тогда и только тогда, когда следующая формула является истинной:

$$\mathbf{P^S}(f) = \bigwedge_{y \in \mathbb{Z}_2^n} \bigwedge_{\substack{x',x'' \in \mathbb{Z}_2^n \\ x'<x''}} (\overline{f_{x',y}} \vee \overline{f_{x'',y}}) \wedge \mathbf{F^S}(f). \tag{3}$$

Доказательство. В разреженном представлении для кодирования векторной взаимно однозначной булевой функции помимо условия, задающего функцию, должно выполниться ещё одно условие, показывающее, что у каждого образа существует только один прообраз. В результате, оба условия можно записать следующим образом:

$$\begin{cases} \forall x\ \exists! y\ f_{x,y} = 1 - \text{условие для прообразов,} \\ \forall y\ \exists! x\ f_{x,y} = 1 - \text{условие для образов.} \end{cases}$$

Условие для прообразов представлено в теореме 1. Процесс получения условия для образов в КНФ разбивается на два этапа:

1) Существование хотя бы одного прообраза у каждого образа гарантирует формула $\mathbf{F^S}(f)$ из **Теоремы 1**.
2) Существование не более чем одного прообраза у каждого образа:
   $\forall y\ \forall x', x''\ (f_{x',y} \to \overline{f_{x'',y}})$ или $\bigwedge\limits_{y} \bigwedge\limits_{\substack{x',x'' \\ x'<x''}} (\overline{f_{x',y}} \vee \overline{f_{x'',y}})$, где $x', x'', y \in \mathbb{Z}_2^n$.

Поскольку эти условия должны выполняться одновременно, то значит они должны быть записаны через конъюнкцию. Таким образом мы получаем формулу (3). ■

Итого в формуле $\mathbf{P^S}(f)$ теоремы 2 содержится $2^{3n} - 2^{2n}$ дизъюнкций длины 2 и 2^n дизъюнкций длины 2^n.

3.2. Плотное представление

Запишем в данном представлении условие, задающее взаимную однозначность. Это можно сделать двумя способами: воспользовавшись соответственно первым или вторым условием из утверждения 1.

Представление через инъективность

Первое условие определения 1 означает, что все образы попарно различны, т.е. любые два вектора вида $\mathbf{fb_i} = (fb_{i,0}, \ldots, fb_{i,n-1})$ отличаются хотя бы в одной компоненте. Это условие задается следующим образом:

$$\forall i, j \neq i\ \exists k\ (fb_{i,k} \neq fb_{j,k}), \text{ где } k = 0, \ldots, n-1,\ i, j \in \mathbb{Z}_2^n.$$

Также данное условие можно записать в виде следующей формулы:

$$\mathbf{P^D_{sum}}(fb) = \bigwedge_{\substack{i,j \in \mathbb{Z}_2^n \\ i \neq j}} \bigvee_{k} (fb_{i,k} \oplus fb_{j,k}).$$

Чтобы записать данную формулу в КНФ, воспользуемся преобразованием Цейтина [4]. Для этого введем дополнительные переменные:

$$fbq_{i,j,k} = 1 \iff fb_{i,k} \oplus fb_{j,k} = 1, \text{ где } k = 0, \ldots, n-1,\ i, j \in \mathbb{Z}_2^n,\ i \neq j.$$

Число переменных $fbq_{i,j,k}$ равно $n \cdot (2^{2n} - 2^n)$.

Получим выражение, связывающее переменные $fbq_{i,j,k}$ и $fb_{i,k}$ для любых $i, j \in \mathbb{Z}_2^n,\ k = 0, \ldots, n-1$. Для этого построим таблицу истинности 1 для выражения, определяющего переменные $fbq_{i,j,k}$.

Таблица 1

Связь переменных $fbq_{i,j,k}$ и $fb_{i,k}$

$fbq_{i,j,k}$	$fb_{i,k}$	$fb_{j,k}$	значение
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Согласно алгоритму построения КНФ по таблице истинности 1 выпишем в формулу $\mathbf{SoP^D}$(Sum Of Pairs) все дизъюнкции с нулевыми значениями через конъюнкцию:

$\mathbf{SoP^D}(fb, fbq) = \bigwedge\limits_{i,j,k} (fbq_{i,j,k} \vee fb_{i,k} \vee \overline{fb_{j,k}}) \wedge (fbq_{i,j,k} \vee \overline{fb_{i,k}} \vee fb_{j,k}) \wedge (\overline{fbq_{i,j,k}} \vee fb_{i,k} \vee fb_{j,k}) \wedge (\overline{fbq_{i,j,k}} \vee \overline{fb_{i,k}} \vee \overline{fb_{j,k}})$, где $k = 0, \ldots, n-1,\ i, j \in \mathbb{Z}_2^n$.

Теорема 3. Переменные $fbq_{i,j,k}$ и $fb_{i,k}$ кодируют взаимно однозначную векторную булеву функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ тогда и только тогда, когда следующая формула является истинной:

$$\mathbf{P^D_{sum}}(fb, fbq) = \bigwedge_{\substack{i,j \in \mathbb{Z}_2^n \\ i \neq j}} \bigvee_{k=0}^{n-1} fbq_{i,j,k} \wedge \mathbf{SoP^D}(fb, fbq). \tag{4}$$

Доказательство. Напомним, что у любой пары прообразов образы должны различаться хотя бы в одной координате. Тогда в переменных $fbq_{x,y,k}$ условие взаимной однозначности представляется в таком виде: $\bigwedge\limits_{i,j} \bigvee\limits_{k} fbq_{i,j,k}$, где $k = 0, \ldots, n-1,\ i, j \in \mathbb{Z}_2^n$.

Поскольку формула $\mathbf{SoP^D}(fb, fbq)$ и полученные условия должны выполняться одновременно, они должны быть записаны через конъюнкцию. Таким образом мы получаем формулу (4). ■

Итого в формуле $\mathbf{P^D_{sum}}(fb, fbq)$ содержится $4n \cdot (2^{2n} - 2^n)$ дизъюнкций длины 3 и $2^{2n} - 2^n$ дизъюнкций длины n.

Представление через сюръективность

Второе условие определения 1 означает, что каждому образу сопоставляется единственный прообраз, т.е для любой константы y существует единственное число i, что $\mathbf{fb_i} = \mathbf{y}$, где $\mathbf{fb_i}$ — вектор двоичных переменных, и $\mathbf{y}$ — двоичное представление числа y.

Запишем данное условие при помощи логических операций:

$\bigwedge\limits_{y} \bigvee\limits_{x} (fb_{x,0}^{y_0} \wedge fb_{x,1}^{y_1} \wedge \cdots \wedge fb_{x,n-1}^{y_{n-1}})$, где $x^y = \begin{cases} x, \text{если } y = 1; \\ \overline{x}, \text{если } y = 0. \end{cases}$

Для преобразования данной формулы в КНФ воспользуемся переменными из разреженного представления $f_{x,y}$. И в самом деле:

$f_{x,y} = 1 \iff (fb_{x,0}^{y_0} \wedge fb_{x,1}^{y_1} \wedge \cdots \wedge fb_{x,n-1}^{y_{n-1}}) = 1$.

Получим выражение в КНФ, связывающее переменные $fb_{x,k}$ и $f_{x,y}$. Для этого преобразуем полученную выше формулу с помощью эквивалентных преобразований. В итоге имеем следующее выражение:

$\mathbf{SpDen}(f, fb) = \bigwedge\limits_{x,y,k} (\overline{f_{x,y}} \vee fb_{x,k}) \wedge (f_{x,y} \vee \overline{fb_{x,0}^{y_0}} \vee \cdots \vee \overline{fb_{x,n-1}^{y_{n-1}}})$, где $k = 0, \ldots, n-1,\ x, y \in \mathbb{Z}_2^n$.

Теорема 4. Переменные $f_{x,y}$ и $fb_{x,k}$ кодируют взаимно однозначную векторную булеву функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ тогда и только тогда, когда следующая формула является истинной:

$$\mathbf{P}_{\mathbf{sparse}}^{\mathbf{D}}(f, fb) = \bigwedge_{y \in \mathbb{Z}_2^n} \bigvee_{x \in \mathbb{Z}_2^n} f_{x,y} \wedge \mathbf{SpDen}(f, fb). \tag{5}$$

Доказательство. Используя новые переменные $f_{x,y}$, второе условие определения 1 записывается следующим образом: $\bigwedge\limits_{y} \bigvee\limits_{x} f_{x,y}$.

Поскольку формула выше и формула $\mathbf{SpDen}(f, fb)$ должны выполняться одновременно, то они должны быть записаны через конъюнкцию. Таким образом, получаем формулу (5). ■

Итого в формуле $\mathbf{P}_{\mathbf{sparse}}^{\mathbf{D}}(f, fb)$ содержится по $n \cdot (2^{2n} - 2^n)$ дизъюнкций длины 2 и n, а также 2^n дизъюнкций длины 2^n.

4. Дифференциальная равномерность

Дифференциальная равномерность препятствует проведению дифференциального криптоанализа блочных шифров [3]. В данной работе представлена запись дифференциальной равномерности для $\delta = 2$ (APN-функция) и $\delta = 4$. Поиск APN-функций является открытой проблемой для четных $n > 6$. Для $n = 6$ была найдена одна взаимно однозначная APN-функция или APN-перестановка. Однако нет гарантий, что такие функции существуют для $n > 6$. Потому уместно также рассмотреть случай $\delta = 4$.

4.1. Разреженное представление

В разреженном представлении дифференциальную равномерность можно записать, вводя следующие переменные:

$$d_{x,a,b} = 1 \iff F(x) \oplus F(x \oplus a) = b, \text{ где } x, a, b \in \mathbb{Z}_2^n \tag{6}$$

Число переменных $d_{x,a,b}$ равно 2^{3n}.

Из определения дифференциальной δ-равномерной функции следует, что если x — корень уравнения $F(x) \oplus F(x \oplus a) = b$, то $x \oplus a$ также является корнем уравнения. Поэтому будем считать, что x — наименьший из этих двух корней.

Для записи условия 6, используя только что введенные переменные $d_{x,a,b}$ и основные переменные $f_{x,y}$, необходимо для каждых фиксированных b, a и x просматривать всевозможные значения $F(x)$ и $F(x \oplus a)$ и проверять, равна ли их сумма значению b.Для этого рассмотрим следующие высказывания и определим, являются ли они истинными:

1) x — не корень уравнения 6, $F(x) \neq z$ и $F(x \oplus a) \neq z \oplus b$ — верно по определению дифференциальной равномерности.

2) x — не корень уравнения 6, $F(x) = z$ и $F(x \oplus a) \neq z \oplus b$ — верно, аналогично высказыванию 1).
3) x — не корень уравнения 6, $F(x) \neq z$ и $F(x \oplus a) = z \oplus b$ — верно, аналогично высказыванию 1).
4) x — не корень уравнения 6, $F(x) = z$ и $F(x \oplus a) = z \oplus b$ — неверно, потому что $F(x) \oplus F(x \oplus a) = b$, что противоречию условию "x — не корень уравнения 6".
5) x — корень уравнения 6, $F(x) \neq z$ и $F(x \oplus a) \neq z \oplus b$ — верно, потому что для аргумента x существует другое значение z, при котором $F(x) = z$ и $F(x \oplus a) = z \oplus b$.
6) x — корень уравнения 6, $F(x) = z$ и $F(x \oplus a) \neq z \oplus b$ — неверно, потому что $F(x) \oplus F(x \oplus a) \neq b$, что противоречит условию "x — корень уравнения 6".
7) x — корень уравнения 6, $F(x) \neq z$ и $F(x \oplus a) = z \oplus b$ — неверно, поскольку x — корень, значит $x \oplus a$ также является корнем уравнения 6. Дальнейшие рассуждения аналогичны высказыванию 6).
8) x — корень уравнения $F(x) \oplus F(x \oplus a) = b$ (1), $F(x) = z$ и $F(x \oplus a) = z \oplus b$ — верно по определению дифференциальной равномерности.

Эти высказывания можно записать при помощи следующей формулы:

$$d_{x,a,b} = 1 \iff \exists z \ (f_{x,z} \wedge f_{x \oplus a, z \oplus b})$$

Построим по этим данным таблицу истинности:

Таблица 2

Связь переменных $f_{x,y}$ и $d_{x,a,b}$

$d_{x,a,b}$	$f_{x,z}$	$f_{x\oplus a,z\oplus b}$	значение
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Согласно алгоритму построения КНФ по таблице истинности 2 выпишем в формулу $\mathbf{Der^S}(f, d)$ через конъюнкцию все дизъюнкции с нулевыми значениями:

$$\mathbf{Der^S}(f, d) = \bigwedge_{b,a,x,z} (f_{x,z} \vee \overline{f_{x\oplus a,z\oplus b}} \vee \overline{d_{x,a,b}}) \wedge (\overline{f_{x,z}} \vee f_{x\oplus a,z\oplus b} \vee \overline{d_{x,a,b}}) \wedge (\overline{f_{x,z}} \vee \overline{f_{x\oplus a,z\oplus b}} \vee d_{x,a,b}),$$

где $x, z, a, b \in \mathbb{Z}_2^n$, $a \neq 0$.

Теорема 5. Отображение $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ является APN-функцией тогда и только тогда, когда выполняются условия Теоремы 1, и следующая формула является истинной:

$$\mathbf{APN^S}(f, d) = \mathbf{Der^S}(f, d) \wedge \bigwedge_{\substack{b,a,x,y \in \mathbb{Z}_2^n \\ y \neq x, y \neq x \oplus a, a \neq 0}} (\overline{d_{x,a,b}} \vee \overline{d_{y,a,b}}). \tag{7}$$

Доказательство. Необходимо показать, что уравнение $F(x) \oplus F(x \oplus a) = b$ имеет два решения, либо не имеет решений. Данное требование записывается при помощи следующей формулы: $\bigwedge_{\substack{b,a,x,y \in \mathbb{Z}_2^n \\ y \neq x, y \neq x \oplus a, a \neq 0}} (\overline{d_{x,a,b}} \vee \overline{d_{y,a,b}})$.

Покажем корректность этой формулы "от противного". Предположим, что уравнение $F(x) \oplus F(x \oplus a) = b$ имеет хотя бы четыре решения x', $x' \oplus a$, x'' и $x'' \oplus a$ для некоторых ненулевых a и b. Тогда дизъюнкция $(\overline{d_{x',a,b}} \vee \overline{d_{x'',a,b}})$ равна нулю, а значит и вся формула равна нулю, что приводит к противоречию.

Поскольку формула, ограничивающая число решений уравнения $F(x) \oplus F(x \oplus a) = b$, и формула $\mathbf{Der^S}(f, d)$ должны выполняться одновременно, то они должны быть записаны через конъюнкцию. Таким образом, мы получаем формулу (7). ■

Итого в формуле $\mathbf{APN^S}(f, d)$ в общей сложности $2^{4n} - 2^{3n}$ дизъюнкций длины 3 и $2^{4n-1} - 2^{3n} - 2^{3n-1} + 2^{2n}$ дизъюнкций длины 2.

4.2. Плотное представление

Для записи дифференциальной равномерности в плотном представлении воспользуемся переменными $fbq_{x,y,k}$. Действительно, $fbq_{x,x\oplus a,k} = 1 \iff fb_{x,k} \neq fb_{x\oplus a,k}$ или, что то же самое, $fbq_{x,y,k} = 1 \iff fb_{x,k} \oplus fb_{x\oplus a,k} = 1$.

Необходимо показать, что уравнение $F(x) \oplus F(x \oplus a) = b$ имеет одну пару решений, либо не имеет решений. Воспользуемся фактом, что для любой пары векторов $\mathbf{fbq_{x,x\oplus a}} = (fbq_{x,x\oplus a,0},\ fbq_{x,x\oplus a,1}, \ldots,\ fbq_{x,x\oplus a,n-1})$ должно быть различие хотя бы в одной координате. Это можно записать следующим образом:

$$\forall a \neq 0\ \forall x, y : y \neq x, y \neq x \oplus a\ \exists k\ (fbq_{x,x\oplus a,k} \neq fbq_{y,y\oplus a,k}), \text{ где}$$
$$k = 0, \ldots, n-1,\ x, y, a \in \mathbb{Z}_2^n.$$

Запишем данный факт в виде следующей формулы:

$$\bigwedge_{a,x,y\neq x,y\neq x\oplus a} \bigvee_{k} (fbq_{x,x\oplus a,0} \oplus fbq_{y,y\oplus a,0}).$$

Воспользуемся преобразованием Цейтина для записи данной формулы вм КНФ. Введем вспомогательные переменные:

$$dbq_{x,y,a,k} = 1 \iff fbq_{x,x\oplus a,k} \oplus fbq_{y,y\oplus a,k}, \text{ где } k \in 0, \ldots, n-1,\ x, y, a \in \mathbb{Z}_2^n,\ x \neq y,$$
$$x \neq y \oplus a.$$

Число таких переменных равно $n \cdot 2^{3n-2}$.

Получим выражение, связывающее переменные $dbq_{x,y,a,k}$ и $fbq_{x,x\oplus a,k}$ для фиксированных x, y, a, k. Для этого по выражению, определяющему значение переменных $dbq_{x,y,a,k}$, построим таблицу истинности:

Таблица 3

Связь переменных $dbq_{x,y,a,k}$ и $fbq_{x,x\oplus a,k}$

$dbq_{x,y,a,k}$	$fbq_{x,x\oplus a,k}$	$fbq_{y,y\oplus a,k}$	значение
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Согласно алгоритму построения КНФ по таблице истинности 3 выпишем через конъюнкцию все дизъюнкции с нулевыми значениями:

$\mathbf{SoPEq^D}(fbq, dbq) = \bigwedge\limits_{a,x,y,k} (dbq_{x,y,a,k} \vee fbq_{x,x\oplus a,k} \vee \overline{fbq_{y,y\oplus a,k}}) \wedge (dbq_{x,y,a,k} \vee \overline{fbq_{x,x\oplus a,k}} \vee fbq_{y,y\oplus a,k}) \wedge (\overline{dbq_{x,y,a,k}} \vee fbq_{x,x\oplus a,k} \vee fbq_{y,y\oplus a,k}) \wedge (\overline{dbq_{x,y,a,k}} \vee \overline{fbq_{x,x\oplus a,k}} \vee \overline{fbq_{y,y\oplus a,k}})$, где $k = 0, \ldots, n-1,\ x, y, a \in \mathbb{Z}_2^n, a \neq 0, y \neq x, y \neq x \oplus a$.

Теорема 6. Переменные $fb_{x,k}$, $fbq_{x,x\oplus a,k}$ и $dbq_{x,y,a,k}$ кодируют APN-функцию $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ тогда и только тогда, когда следующая формула является истинной:

$$\mathbf{APN^D}(fb, fbq, dbq) = \mathbf{SoPEq^D}(fbq, dbq) \wedge \mathbf{SoP^D}(fb, fbq) \wedge \bigwedge_{\substack{a,x,y\in\mathbb{Z}_2^n \\ y\neq x, y\neq x\oplus a}} \bigvee_{k=0}^{n-1} dbq_{x,y,a,k}. \quad (8)$$

Доказательство. Напомним, что у любой пары векторов $fbq_{x,x\oplus a}$ должны быть различия хотя бы в одной координате. Тогда в переменных $dbq_{x,y,a,k}$ это условие предсталяется в таком виде:

$\bigwedge\limits_{a,x,y} \bigvee\limits_{k} dbq_{x,y,a,k}$, где $k = 0, \ldots, n-1,\ x, y, a \in \mathbb{Z}_2^n, a \neq 0, y \neq x, y \neq x \oplus a$.

Поскольку формула, ограничивающая число решений уравнения $F(x) \oplus F(x \oplus a) = b$, а также формулы $\mathbf{SoPEq^D}(fbq, dbq)$ и $\mathbf{SoP^D}(fb, fbq)$ должны выполняться одновременно, они должны быть записаны через конъюнкцию. Таким образом, мы получаем получаем формулу (8). ■

Итого в формуле $\mathbf{APN^D}(fb, fbq, dbq)$ в общей сложности $4n \cdot (2^{3n-1} - 2^{2n-1})$ дизъюнкций длины 3 и $2^{3n-1} - 2^{2n} - 2^{2n-1} + 2^n$ дизъюнкций длины n.

5. Switching-метод

Несмотря на хорошие теоретические оценки и сравнительно быструю работу на малых n ($n \leqslant 4$), описанный выше поиск неизвестных векторных булевых функций с помощью SAT-решателей работает долго для больших n ($n \geqslant 5$). Для существенного ускорения работы SAT-решателя в поиске криптографических булевых функций можно использовать полностью известные функции с некоторыми свойствами .

Switching-метод заключается в следующем. Пусть $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ — некоторая известная векторная булева функция, $F_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — её координатная функция, т.е. $F(x) = (F_1(x), \ldots, F_n(x))$, а $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$, $g \neq 0$ — неизвестная булева функция. Тогда новая векторная булева функция $G : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, на которую накладываются необходимые условия (например, APN, которое описано в разделе 4.2), вычисляется следующим образом:

$G_1(x_1, \ldots, x_n) = F_1(x_1, \ldots, x_n) \oplus c_1 \cdot g(x_1, \ldots, x_n)$;
$G_2(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) \oplus c_2 \cdot g(x_1, \ldots, x_n)$;
$\ldots$
$G_n(x_1, \ldots, x_n) = F_n(x_1, \ldots, x_n) \oplus c_n \cdot g(x_1, \ldots, x_n)$,

где $c = (c_1, \ldots, c_n) \in \mathbb{Z}_2^n$ — параметр switching-метода.

Для дальнейшего описания воспользуемся обозначением двойной производной по направлению. Напомним, что производная по направлению $D_a D_b F(x) = F(x) \oplus F(x \oplus a) \oplus F(x \oplus b) \oplus F(x \oplus a \oplus b)$. В дальнейшем будет использовать краткое обозначение $DDF(x)$. Известно, что поиск APN-функций при помощи switching-метода сводится к системе линейных уравнений. Действительно, чтобы функция G обладала свойством APN, необходимо и достаточно, чтобы выполнялось следующее утверждение:

$$\forall a \neq 0 \; \forall x, y \neq x, y \neq x \oplus a : DDG(x) \neq 0.$$

Проведем замену $G(x) = F(x) \oplus c \cdot g(x)$ и перепишем утверждение выше:

$$DDF(x) \oplus c \cdot DDg(x) \neq 0.$$

Тогда, если $DDF(x) = c$, то для сохранения свойства APN требуется $DDg(x) = 0$. А если $DDF(x) = 0$, то $DDg(x) = 1$ Таким образом, если левая часть равна c или 0, то правая часть, равная нулю и единице соответственно, записывается в систему уравнений. Каждое уравнение является линейным. Данную систему можно эффективно решить методом Гаусса, потому использование SAT-решателей здесь не является необходимым.

5.1. Модернизированный switching-метод

Интерес будет представлять модернизированный switching-метод, в котором новая векторная булева функция $G : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ строится прибавлением двух булевых функций g_1 и g_2 следующим образом:

$G_1(x_1, \ldots, x_n) = F_1(x_1, \ldots, x_n) \oplus c_1 \cdot g_1(x_1, \ldots, x_n) \oplus d_1 \cdot g_2(x_1, \ldots, x_n)$;
$G_2(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) \oplus c_2 \cdot g_1(x_1, \ldots, x_n) \oplus d_2 \cdot g_2(x_1, \ldots, x_n)$;
$\ldots$
$G_n(x_1, \ldots, x_n) = F_n(x_1, \ldots, x_n) \oplus c_n \cdot g_1(x_1, \ldots, x_n) \oplus d_n \cdot g_2(x_1, \ldots, x_n)$,
где $c = (c_1, \ldots, c_n) \neq 0, d = (d_1, \ldots, d_n) \neq 0$, $c \neq d$.

Мы будем требовать наличие у функций $g_1(x)$ и $g_2(x)$ следующих свойств:

— Функция g_1 — кубическая булева функция, т.е. имеет в своем алгебраическом представлении моном третьей степени. Функция g_2 — ненулевая произвольная булева функция. Так в перспективе можно искать новые неквадратичные и, в частности, кубические классы APN-функций, поскольку для поиска квадратичных классов существует множество других методов.
— Функции g_1 и g_2 не должны быть равны друг другу. Иначе модернизированный switching-метод сводится к классическому.
— Аффинные части функций g_1 и g_2 равны нулю. Иначе мы будем находить функции в одном и том же классе EA-эквивалентности.

5.2. Запись switching-метода в виде SAT-задачи

В работе мы рассмотрим три возможных записи switching-метода.**Первый** способ описывает прибавление функций $g_1(x)$ и $g_2(x)$ в виде алгебраической нормальной формы (АНФ):

$$g(x_1, \ldots, x_n) = \bigoplus_{b \in \mathbb{Z}_2^n} \alpha_b \cdot x^b,$$

где $\alpha_b \in \mathbb{Z}_2, x^b = x_1^{b_1} \ldots x_n^{b_n}, b = (b_1, \ldots, b_n)$, $x_i^{b_i} = \begin{cases} x_i, \text{если } b_i = 1; \\ 1, \text{если } b_i = 0. \end{cases}$

Таким образом для записи алгебраической нормальной формы функций g_1 и g_2 можно использовать следующие переменные:

$g_j\_ANF_i = 1, \iff$ коэффициент монома α_i функции $g_j(x)$ равен 1, $i \in \mathbb{Z}_{2^n}, j \in \{1, 2\}$.

Запишем все необходимые требования для функций g_1 и g_2 в виде КНФ.

Определено, что функция g_2 должна быть ненулевой. Это означает, что хотя бы один из коэффициентов при мономах АНФ равен 1. Это равносильно истинности следующей формулы: $\bigvee\limits_{i\in\mathbb{Z}_{2^n}} g_2\_ANF_i$. Аналогично записывается условие на наличие мономов третьей степени функции g_1: $\bigvee\limits_{k\in\mathbb{Z}_{2^n}} g_1\_ANF_k$, где двоичный вес числа k равен 3.

Равенство нулю аффинной части функций g_1 и g_2 можно записать следующим образом: $\bigwedge\limits_{k\in\mathbb{Z}_{2^n}} (\overline{g1\_ANF_k} \wedge \overline{g2\_ANF_k})$, где двоичный вес числа k не превосходит 1.

Для записи неравенства функций g_1 и g_2 друг другу воспользуемся следующей формулой: $\bigvee\limits_{i\in\mathbb{Z}_{2^n}} (g_1\_ANF_i \neq g_2\_ANF_i)$. Для записи в КНФ воспользуемся преобразованием Цейтина, в котором каждое неравенство записывается при помощи вспомогательных переменных.

Используя переменные $g_j\_ANF_i$, прибавление булевой функции $g_j(x)$ к функции F можно записать следующим образом:

$$\bigwedge_{x\in\mathbb{Z}_2^n} fb_{x,c_i} \oplus g_1\_ANF_{m_1}\cdot x^{m_1} \oplus g_1\_ANF_{m_2}\cdot x^{m_2} \oplus \cdots \oplus g_1\_ANF_{m_{2^n}}\cdot x^{m_{2^n}},$$

где $c_i = 1$ и $m_i \in \mathbb{Z}_2^n$. Если $d_i = 1$, то прибавление булевой функции $g_2(x)$ выполняется аналогично. Данная формула записывается в виде КНФ с помощью преобразования Цейтина, в котором результат каждого суммирования записывается при помощи вспомогательных переменных.

Условия на свойство APN записываются с помощью формулы $\mathbf{APN^D}$ из раздела 4.2.

Второй способ записать switching-метод в виде SAT задачи основан на табличном представлении булевой функции. Для этого введем следующие переменные: $g_j\_func_x = 1, \iff g_j(x) = 1,\ x \in \mathbb{Z}_{2^n}, j \in \{1,2\}$.

Данное представление позволяет записывать требуемые условия для булевых функций g_1 и g_2 лишь для некоторых мономов. Условия на функции g_1 и g_2 записываются аналогично формулам выше, только с использованием переменных $g_j\_func_x$.

Единственное исключение составляет условие кубичности функции g_1. Его можно компактно записать при помощи ранее введенных переменных $g_1\_ANF_i$. Для этого воспользуемся преобразованием Мёбиуса: $g_1\_ANF_i = \bigoplus_{x\preceq i} g_1\_func_x$. Для записи этой формулы в КНФ воспользуемся преобразованием Цейтина и для каждого суммирования введем вспомогательные переменные.

В результате операция прибавления функции $g_j(x)$ запишется так: $\bigwedge_{x\in\mathbb{Z}_2^n} fb_{x,c_i} \oplus g_1\_func_x$, где $c_i = 1$. Если $d_i = 1$, то прибавление булевой функции $g_2(x)$ выполняется аналогично. Здесь для записи в КНФ также применяется преобразование Цейтина. Свойство APN записается при помощи формулы $\mathbf{APN^D}$ из раздела 4.2.

Третий способ записи модернизированного switching-метода в виде SAT-задачи основан на системе алгебраических уравнений. Покажем, что поиск APN-функций с помощью модернизированного switching-метода сводится к решению системы нелинейных уравнений. Если воспользоваться критерием APN-функции и заменой $G(x) = F(x) \oplus c\cdot g_1(x) \oplus d\cdot g_2(x)$, то получим следующее выражение:

$$DDF(x) \oplus c \cdot DDg_1(x) \oplus d \cdot DDg_2(x) \neq 0.$$

Тогда для сохранения свойств APN рассмотрим следующие четыре случая:

1) Если $DDF(x) = c$, то $(DDg_1(x) = 1) \Rightarrow (DDg_2(x) = 1)$.
2) Если $DDF(x) = d$, то $(DDg_2(x) = 1) \Rightarrow (DDg_1(x) = 1)$.
3) Если $DDF(x) = c \oplus d$, то $(DDg_1(x) = 0) \vee (DDg_2(x) = 0)$.
4) Если $DDF(x) = 0$, то $(DDg_1(x) = 1) \vee (DDg_2(x) = 1)$.

С помощью эквивалентных преобразований булевых функций получаем следующие уравнения:

1) $(DDg_1(x)) \cdot (DDg_2(x) \oplus 1) = 0$;
2) $(DDg_1(x) \oplus 1) \cdot (DDg_2(x)) = 0$;
3) $(DDg_1(x)) \cdot (DDg_2(x)) = 0$;
4) $(DDg_1(x) \oplus 1) \cdot (DDg_2(x) \oplus 1) = 0$

Данные уравнения являются квадратичными. Поэтому для решения системы уравнений уместно использовать SAT-решатели.

Напоминм, что производная по направлению a функции $f(x)$ равна $D_a g_1(x) = g_1(x) \oplus g_1(x \oplus a)$. Заметим, что в системе уравнений часто встречаются линейная зависимость следующего вида (с точностью до константных слагаемых):

$$\begin{cases} (D_a g_1(x) \oplus D_a g_1(y)) \cdot (D_a g_2(x) \oplus D_a g_2(y)) = 0 \\ (D_a g_1(y) \oplus D_a g_1(z)) \cdot (D_a g_2(y) \oplus D_a g_2(z)) = 0 \\ (D_a g_1(x) \oplus D_a g_1(z)) \cdot (D_a g_2(x) \oplus D_a g_2(z)) = 0 \end{cases}$$

Тогда для ускорения работы SAT-решателя можно записать следующие ограничения в виде КНФ:

$$(D_a g_1(x) \oplus D_a g_1(y) \oplus D_a g_1(z)) \wedge (D_a g_2(x) \oplus D_a g_2(y) \oplus D_a g_2(z))$$

6. Результаты вычислительных экспериментов

Для получения практических результатов и оценок на размер формул для различных задач был написан генератор КНФ-формул на языке Си. Результаты были получены для задач поиска неизвестной взаимно однозначной векторной булевой функции и APN-функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ для $n = 4, 5, 6$ в плотном и разреженном представлении.

Таблица 4

Размер формул для задач one-to-one и APN (F — неизвестная функция)

		one-to-one			APN		
		переменные	дизъюнкции	литералы	переменные	дизъюнкции	литералы
Плотное	$n = 4$	544	2 040	6 240	1 744	13 860	68 880
	$n = 5$	2 640	10 416	32 240	18 760	152 520	762 600
	$n = 6$	12 480	50 400	157 248	187 872	1 531 152	7 687 008
Разреженное	$n = 4$	256	3 856	7 936	2 176	39 376	109 696
	$n = 5$	1 024	31 776	64 512	16 896	642 848	1 794 560
	$n = 6$	4 096	258 112	520 192	133 120	10 386 496	29 034 496

Сгенерированные SAT-задачи отправлялись на вход SAT-решателей Lingeling и CryptoMiniSat 5. В результате в плотном представлении полностью неизвестная APN-функция от 4 переменных вычисляется за 1.1 секунды. Для поиска APN-функции

от 5 переменных SAT-решатель работает более 15 минут. В разреженном представлении неизвестная APN-функция от 4 переменных вычисляется за 0.3 секунды. APN-функция от 5 переменных находится за 503.3 секунды или 8 минут 23.3 секунды. С большими размерностями SAT-решатель справляется за сравнительно долгое время. Также возникают трудности с генерацией формулы ввиду ее огромного размера, как можно увидеть в таблице 4.

Было проведено сравнение с поиском APN-функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ для $n = 4, 5, 6$ в плотном представлении, когда функция F известна для половины аргументов $x \in \mathbb{Z}_2^n$. Тогда в КНФ-формулу будет записано $n \cdot 2^{n-1}$ дизъюнкций длины 1, то есть переменные $fb_{x,k}$, записанные в этих дизъюнкциях, определяются однозначно и заметно упрощают КНФ-формулу при работе SAT-решателя.

Таблица 5

Размер формул для задачи APN (F — известная наполовину функция)

		APN		
		переменные	дизъюнкции	литералы
Плотное	$n = 4$	1 744	13 892	68 912
	$n = 5$	18 760	152 605	762 685
	$n = 6$	187 872	1 531 344	7 687 200

В результате в плотном представлении наполовину известная APN-функция от 4 переменных находится за 0.3 секунды. Для 5 переменных решение найдено за 43.9 секунды. Однако, как было написано ранее, известных и опубликованных частей APN-функций для 6,7,8 переменных не существует, потому такой поиск не имеет практической основы для использования.

Также приведены результаты о времени работы SAT-решателя CryptoMiniSat5 и размере файла с КНФ формулой в задаче поиска APN-функций с помощью модернизированного switching-метода в трех ранее описанных видах.

Таблица 6

Результаты для функций от 6 переменных

	Размер файла	SAT	UNSAT
АНФ	45 Мб	4 сек.	30 минут
Вектор значений	41 Мб	3 сек.	30 минут
Уравнения	1.5 Мб	0.1 сек.	1.2 сек.

Таблица 7

Результаты для функций от 7 переменных

	Размер файла	SAT	UNSAT
АНФ	439 Мб	нет данных	32 минуты
Вектор значений	447 Мб	нет данных	32 минуты
Уравнения	6 Мб	нет данных	20 сек.

В столбце UNSAT указано среднее время. Для $n = 8$ оно подсчитано приблизительно, поскольку время работы SAT-решателей на разных задачах колеблется от нескольких секунд до одного часа. В данный момент вычисления продолжаются (выполнено около 40% всех задач).

Таблица 8

Результаты для функций от 8 переменных

	Размер файла	SAT	UNSAT
Уравнения	27 Мб	нет данных	5 минут

Заключение

В данной работе представлен набор формул для поиска криптографических функций при помощи SAT-решателей. Было описано построение формул для взаимной однозначности, дифференциальной равномерности векторных булевых функций (случаев $\delta = 2$). Данный подход показывает свою эффективность уже на аналитическом этапе исследования, поскольку поиск функций с помощью SAT-решателей существенно быстрее перебора всех $2^{n \cdot 2^n}$ векторных булевых функций от n переменных.

Также был описан switching-метод поиска векторных булевых функций с заданными свойствами, а также реализован модернизированный switching-метод, который показал свою эффективность на задаче поиска APN-функции от n переменных в сравнении с «чистым» поиском функций.

ЛИТЕРАТУРА

1. *Верещагин Н. К., Шень. А.* Часть 1. Начала теории множеств // Лекции по математической логике и теории алгоритмов. 4-е изд., испр. — М.: МЦНМО, 2012. — 112 с.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М: Мир, 1982. 420 с.
3. *Городилова А. А.* От криптоанализа шифра к криптографическому свойству булевой функции // ПДМ. 2016. №3 (33).
4. *Цейтин Г. С.* О сложности вывода в исчислении высказываний. // Записки научных семинаров ЛОМИ. 1968. №8. С. 234–259.
5. `www.satcompetition.org` — SAT-competitions.
6. *Davis M., Logemann G., Loveland D.* A Machine Program for Theorem-Proving // Commun. ACM. 1962. № 5–7. С. 394–397.
7. *Marques-Silva J. P. and Sakallah K. A.* GRASP: A New Search Algorithm for Satisfiability In Proceedings of International Conference on Computer-Aided Design USA, 1996. С. 220–227.
8. *Огородников Ю. Ю.* Комбинированная атака на алгоритм RSA с использованием sat-подхода Динамика систем, механизмов и машин Омск: ОмГТУ, 2016. С. 276–284.
9. *Schmittner S. E.* A SAT-based Public Key Cryptography Scheme // IACR Cryptol. ePrint Arch. 2015. № 2015. С. 771.
10. *Wille R., Lye A., Niemann P.* Checking Reversibility of Boolean Functions // Reversible Computation: 8th International Conference Italy: RC, 2016. С. 322–337.

КАЛГИН Константин Викторович — к.ф.-м.н., м.н.с. Института математики им.Соболева СО РАН, м.н.с Института вычислительной математики и математической геофизики СО РАН, старший преподаватель Новосибирского государственного университета, г.Новосибирск. E-mail: **kalginkv@gmail.com**

ДОРОНИН Артемий Евгеньевич — аспирант Новосибирского государственного университета, г.Новосибирск. E-mail: **artem96dor@gmail.com**

Noname manuscript No.
(will be inserted by the editor)

On constructions and properties of self-dual generalized bent functions

Aleksandr Kutsenko

Received: date / Accepted: date

Abstract Bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer, are known as generalized bent (gbent) functions. Gbent functions for which it is possible to define a dual gbent function are called regular. A regular gbent function is said to be self-dual if it coincides with its dual. In this paper we explore self-dual gbent functions for even q. We consider several primary and secondary constructions of such functions. It is proved that the numbers of self-dual and anti-self dual gbent functions coincide. We give necessary and sufficient conditions for the self-duality of Maiorana–McFarland gbent functions and find Hamming and Lee distances spectrums between them. We find all self-dual gbent functions symmetric with respect to two variables and prove that self-dual gbent function can not be affine. The properties of sign functions of self-dual gbent functions are considered. Symmetries that preserve self-duality are also discussed.

Keywords Generalized Boolean functions · Self-dual bent · Maiorana–McFarland generalized bent function · Lee distance

1 Introduction

The study of Boolean functions having strong cryptographic properties is the domain of current interest, see monographies [3,5] for detail. Boolean bent functions were introduced by Rothaus [29] in 1976. Due to maximal nonlinearity they have a number of applications in cryptography and coding theory. They were used as building blocks of stream (Grain, 2004) and block (CAST, 1997) ciphers and, for instance, in 2000 T. Wada [39] established a connection between bent functions and binary constant-amplitude codewords. But despite the long history of research

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

A. Kutsenko
Sobolev Institute of Mathematics, Novosibirsk
Novosibirsk State University, Novosibirsk, Russia
E-mail: alexandrkutsenko@bk.ru

in this area there are still many open problems. Among them the exact number of bent functions as well as their complete classification seems elusive to be solved for now. One can find more details on bent functions in books [38,24].

Bent functions were initially generalized by P. V. Kumar in 1985 by considering functions of the form $\mathbb{Z}_q^n \to \mathbb{Z}_q$ with corresponding definition of bentness, see [14]. Bent functions from a finite Abelian group into a finite Abelian group were studied in [33] by V. I. Solodovnikov. Having applications of functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_4$ in code-division multiple access (CDMA) systems, K.-U Schmidt in [30] (initially appeared in preprint from 2006) generalized the notion of bentness for functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer and studied these functions for the case $q = 4$. The considered functions are named generalized bent (gbent) functions. Note that this generalization deals with the mappings of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$ called generalized Boolean functions, that are also studied from the view of obtaining linear codes with special properties, see [26]. In recent years generalized bent functions obtained much attention, in particular, for the case $q = 2^k$. In [11, 21,12,34] different constructions and properties of generalized bent functions were obtained. The connection between concepts of strong regularity of (edge-weighted) Cayley graph associated to a generalized Boolean function and gbent functions was pointed in [28]. The complete characterization of generalized bent functions from different perspectives was recently presented in [13,35,25]. A comprehensive survey on existing generalizations of bent functions can be found in [36].

For every bent Boolean function its dual bent functions is uniquely defined. It is important to note that the duality mapping is the unique known isometric mapping of the set of bent functions into itself that cannot be extended to a isometry of the whole set of all Boolean functions that preserves bentness. Self-dual bent functions form a remarkable class of bent functions since they have the direct relation to their dual bent functions and in terms of mappings can be considered as fixed points of the duality mapping. These functions were explored by C. Carlet et al. in 2010 in work [2], where a number of constructions and properties were given and the classification for small number of variables was provided. Next steps for the classification of qubic self-dual bent functions in 8 variables were made in [6], while quadratic self-dual bent functions were completely characterized in [7]. Constructions and properties of self-dual Boolean bent functions were studied in [9, 19,23]. The overview of the known metrical properties of self-dual bent functions can be found in [18].

The action of the duality mapping on bent functions within generalizations is increasingly nontrivial since it is typically defined only for the part of bent functions from corresponding generalization which are called *regular*, while more accurate work with them also demands for intermediate notation like *weak regularity* that also appears in this scope. The extension of the concept of self-duality for different generalizations of bent functions was made in several papers. The classification of quadratic self-dual bent functions of the form $\mathbb{F}_p^n \to \mathbb{F}_p$, p odd prime, was made by X.-D. Hou in [8]. In paper [4] the self-duality for bent functions within the same generalization type was studied by A. Çeşmelioğlu et al. In 2018, L. Sok. et al. [32] studied quaternary self-dual bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_4$ from the viewpoints of existence, construction, and symmetry. The relation between sign functions of quaternary self-dual bent function in n variables and two self-dual bent functions in n variables was found. Based on this it was proved that there are no quaternary self-dual bent functions in odd number of variables.

In current work we investigate constructions, symmetries and other properties of self-dual generalized bent functions $\mathbb{F}_2^n \to \mathbb{Z}_q$, when q is even. The paper is organized as follows. The next section contains the necessary notation. In section 3 several primary and secondary constructions are given. The metrical properties of self-dual gbent functions from Maiorana–McFarland class are characterized in section 4. In section 5 sign functions of self-dual gbent functions are studied. Section 6 deals with the properties of self-dual gbent functions including upper bound for the set of self-dual gbent functions, the existence of affine functions within self-dual gbent ones and characterization of self-dual gbent functions symmetric with respect to two variables. In Section 7 the construction of mappings preserving self-duality of gbent function is given.

2 Notation

Let $\mathbb{F}_2^n$ be a set of binary vectors of length n. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$, where the sign $\oplus$ denotes a sum modulo 2. Denote, following [10], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in \mathrm{GL}\,(n, \mathbb{F}_2) : LL^T = I_n \right\},$$

where L^{T} denotes the transpose of L and I_n is an identical matrix of order n over the field $\mathbb{F}_2$.

A *generalized Boolean function* f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$, the integers modulo q. The set of generalized Boolean functions in n variables is denoted by $\mathcal{GF}_n^q$, for the case $q = 2$ we use $\mathcal{F}_n$. Let $\omega = e^{2\pi i/q}$. A *sign* function of $f \in \mathcal{GF}_n^q$ is a complex valued function $F = \omega^f$, we will also refer to it as to a complex vector $\left(\omega^{f_0}, \omega^{f_1}, ..., \omega^{f_{2^n-1}}\right)$ of length 2^n, where $(f_0, f_1, ..., f_{2^n-1})$ is a vector of values of the function f.

The *Hamming weight* $\mathrm{wt}_H(x)$ of the vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates of x. The *Hamming distance* $\mathrm{dist}_H(f, g)$ between generalized Boolean functions f, g in n variables is the cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$. The Lee weight of the element $x \in \mathbb{Z}_q$ is $\mathrm{wt}_L(x) = \min\{x, q - x\}$. The Lee distance $\mathrm{dist}_L(f, g)$ between $f, g \in \mathcal{GF}_n^q$ is

$$\mathrm{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L\left(\delta(x)\right),$$

where $\delta \in \mathcal{GF}_n^q$ and $\delta(x) = f(x) + (q-1)g(x)$ for any $x \in \mathbb{F}_2^n$. For Boolean case $q = 2$ the Hamming distance coincides with the Lee distance.

The *(generalized) Walsh–Hadamard transform* of $f \in \mathcal{GF}_n^q$ is the complex valued function:

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}.$$

A generalized Boolean function f in n variables is said to be *generalized bent* (gbent) if

$$|H_f(y)| = 2^{n/2},$$

for all $y \in \mathbb{F}_2^n$ [30]. If there exists such $\widetilde{f} \in \mathcal{GF}_n^q$ that $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$, the gbent function f is said to be *regular* and $\widetilde{f}$ is called its *dual*. Note that $\widetilde{f}$ is generalized bent as well. A regular gbent function f is said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} + q/2$. Consequently, it is the case only for even q. So throughout this paper we assume that q is a positive even integer. Corresponding sets of gbent functions are denoted by $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$, respectively.

3 Constructions

In this section we present several primary and seconady constructions of self-dual gbent functions.

3.1 Direct sum

Suppose $n = n_1 + n_2 + \ldots + n_r$, where n_k are positive integers for $k = 1, 2, \ldots, r$. Let $f \in \mathcal{GF}_n^q$, consider gbent functions $f_k \in \mathcal{GF}_{n_k}^q$, $k = 1, 2, \ldots, r$. The function

$$f(x) = f_1\big(x^{(1)}\big) + f_2\big(x^{(2)}\big) + \ldots + f_r\big(x^{(r)}\big),$$

where $x^{(k)} \in \mathbb{F}_2^{n_k}$ and $x = \big(x^{(1)}, x^{(2)}, \ldots, x^{(r)}\big) \in \mathbb{F}_2^n$, is a *direct sum* of generalized Boolean functions f_k. Gbent functions obtained by a direct sum of generalized Boolean functions were studied in paper [11], it was proved that the function f is gbent if and only if all f_k are gbent functions. Here we consider self-dual bent functions obtained by this construction.

Proposition 1 *Assume all numbers p_k are even and $f_k \in \mathcal{GF}_{n_k}^q$ are gbent functions such that $\widetilde{f}_k = f_k + c_k\,(q/2)$, where $c_k \in \mathbb{F}_2$, $k = 1, 2, \ldots, r$. If there is an even number of nonzero coefficients c_k, then the function f is a self-dual gbent function in n variables.*

Proof The Walsh–Hadamard transform of f which is a direct sum of $f_k \in \mathcal{GF}_{n_k}^q$, $k = 1, 2, \ldots, r$, is given by

$$\begin{aligned} H_f(y) &= \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle} = H_{f_1}\big(y^{(1)}\big) H_{f_2}\big(y^{(2)}\big) \cdot \ldots \cdot H_{f_r}\big(y^{(r)}\big) \\ &= (-1)^{c_1 + c_2 + \ldots + c_r} 2^{\left(n_1 + n_2 + \ldots + n_r\right)/2} \omega^{\widetilde{f}_1\left(y^{(1)}\right) + \widetilde{f}_2\left(y^{(2)}\right) + \ldots + \widetilde{f}_r\left(y^{(r)}\right)} \\ &= (-1)^{c_1 + c_2 + \ldots + c_r} 2^{n/2} \omega^{f_1\left(y^{(1)}\right) + f_2\left(y^{(2)}\right) + \ldots + f_r\left(y^{(r)}\right)} \\ &= 2^{n/2} \omega^{f(y) + (q/2)\left(c_1 + c_2 + \ldots + c_r\right)} \end{aligned}$$

for all $y^{(k)} \in \mathbb{F}_2^{n_k}$ and $y = \big(y^{(1)}, y^{(2)}, \ldots, y^{(r)}\big) \in \mathbb{F}_2^n$.

3.2 Maiorana–McFarland class

Bent functions in $2k$ variables which have a representation

$$f(x,y) = \langle x, \pi(y)\rangle \oplus g(y), \quad x,y \in \mathbb{F}_2^k,$$

where $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a Boolean function in k variables, form the well known *Maiorana–McFarland* class of bent functions [22]. It is known [1] that the dual of a Maiorana–McFarland bent function $f(x,y)$ is equal to

$$\widetilde{f}(x,y) = \langle \pi^{-1}(x), y\rangle \oplus g\big(\pi^{-1}(x)\big), \quad x,y \in \mathbb{F}_2^k.$$

A generalization of this construction for the case $q = 4$ was given by Schmidt in [30]. In paper [34] this construction was given for any even q, thus, forming the following construction

$$f(x,y) = \frac{q}{2}\langle x, \pi(y)\rangle + g(y), \quad x,y \in \mathbb{F}_2^k,$$

where $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a generalized Boolean function in k variables. Its dual is

$$\widetilde{f}(x,y) = \frac{q}{2}\langle \pi^{-1}(x), y\rangle + g\big(\pi^{-1}(x)\big), \quad x,y \in \mathbb{F}_2^k.$$

In the article [2] necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions, denoted by $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$), were given. In [32] quaternary self-dual Maiorana–McFarland bent functions were studied and necessary and sufficient conditions of self-duality were obtained for them.

In the current work we generalize these results for any even q. Denote the sets of (anti-)self-dual generalized Maiorana–McFarland bent functions by $\mathrm{SB}^+_{\mathcal{M}^q}(n)$ ($\mathrm{SB}^-_{\mathcal{M}^q}(n)$ correspondingly).

Theorem 1 *A generalized Maiorana–McFarland bent function*

$$f(x,y) = \frac{q}{2}\,\langle x, \pi(y)\rangle + g(y), \;\; x,y \in \mathbb{F}_2^{n/2},$$

is (anti-)self-dual bent if and only if for any $y \in \mathbb{F}_2^{n/2}$

$$\pi(y) = L\,(y \oplus b)\,, \quad g(y) = \frac{q}{2}\,\langle b, y\rangle + d,$$

where $L \in \mathcal{O}_{n/2}, b \in \mathbb{F}_2^{n/2}$, $\mathrm{wt}\,(b)$ *is even (odd),* $d \in \mathbb{Z}_q$.

Proof Let $f(x,y) = \frac{q}{2}\,\langle x, \pi(y)\rangle \oplus g(y)$, where π is a permutation on $\mathbb{F}_2^{n/2}$, $g \in \mathcal{GF}^q_{n/2}$, $x,y \in \mathbb{F}_2^{n/2}$. By the definition of (anti-)self-duality a generalized bent function is (anti-)self-dual if it coincides with (the complement of) its dual. Then for all $x,y \in \mathbb{F}_2^n$ it must hold

$$\frac{q}{2}\,\langle x, \pi(y)\rangle + g(y) = \frac{q}{2}\langle \pi^{-1}(x), y\rangle + g\big(\pi^{-1}(x)\big) + \frac{q}{2}c, \tag{1}$$

where $c \in \mathbb{F}_2$: $c = 0$ if $f = \widetilde{f}$ and $c = 1$ if $f = \widetilde{f} + \frac{q}{2}$.

Put zero vector $x = \mathbf{0} \in \mathbb{F}_2^{n/2}$ in (11), then for any $y \in \mathbb{F}_2^n$ we have

$$g(y) = \frac{q}{2}\langle \pi^{-1}(\mathbf{0}), y\rangle + g\big(\pi^{-1}(\mathbf{0})\big) + \frac{q}{2}c.$$

The condition (11) can be transformed to

$$\frac{q}{2}\langle x, \pi(y)\rangle + \frac{q}{2}\langle \pi^{-1}(\mathbf{0}), y\rangle + g\big(\pi^{-1}(\mathbf{0})\big) = \frac{q}{2}\langle \pi^{-1}(x), y\rangle + \frac{q}{2}\langle \pi^{-1}(\mathbf{0}), \pi^{-1}(x)\rangle + g\big(\pi^{-1}(\mathbf{0})\big) + \frac{q}{2}c,$$

or, equivalently,

$$\frac{q}{2}\langle x, \pi(y)\rangle + \frac{q}{2}\langle \pi^{-1}(\mathbf{0}), y\rangle = \frac{q}{2}\langle \pi^{-1}(x), y\rangle + \frac{q}{2}\langle \pi^{-1}(\mathbf{0}), \pi^{-1}(x)\rangle + \frac{q}{2}c. \quad (2)$$

In both sides of (2) monomials of algebraic degree more than 2 can not occur, since the left part has algebraic degree at most 1 with respect to x provided that y is fixed and the right part has algebraic degree at most 1 with respect to y provided that x is fixed. Therefore, the mapping π is an affine permutation defined by $\pi(x) = L(x \oplus b)$ for any $x \in \mathbb{F}_2^n$, where L is a $(n/2) \times (n/2)$ nonsingular binary matrix, $b \in \mathbb{F}_2^{n/2}$.

Since the equality (2) should be considered by modulo q, we only care about the parity of components of both sides, thus, for any $x, y \in \mathbb{F}_2^{n/2}$ having the following equality

$$\langle x, L(y \oplus b)\rangle \oplus \langle b, y\rangle = \langle L^{-1}x \oplus b, y\rangle \oplus \langle b, L^{-1}x \oplus b\rangle \oplus c. \quad (3)$$

Putting $x \in \mathbb{F}_2^{n/2}$ to be zero vector in (3), then for any $y \in \mathbb{F}_2^{n/2}$ it must hold $\langle b, b\rangle = c$. Rewrite (3) in the form

$$\langle x, Ly \oplus \left(L^{-1}\right)^T y\rangle = \langle x, Lb \oplus \left(L^{-1}\right)^T b\rangle,$$

and consider it for a zero vector $y = \mathbf{0} =\in \mathbb{F}_2^{n/2}$:

$$\langle x, Lb \oplus \left(L^{-1}\right)^T b\rangle = 0,$$

that is $Lb \oplus \left(L^{-1}\right)^T b = \mathbf{0}$ or, equivalently, $Lb = \left(L^{-1}\right)^T b$. It means that

$$\langle x, \left(L \oplus \left(L^{-1}\right)^T\right) y\rangle = 0,$$

for any $x, y \in \mathbb{F}_2^{n/2}$. From this it follows that $L^{-1} = L^T$, that is $L \in \mathcal{O}_{n/2}$.

It follows that the number of such functions is a function of q and the cardinality of the orthogonal group.

Corollary 1 *It holds*

$$\left|\mathrm{SB}^+_{\mathcal{GM}^q}(n)\right| = \left|\mathrm{SB}^-_{\mathcal{GM}^q}(n)\right| = q \cdot 2^{n/2-1}\left|\mathcal{O}(n/2, \mathbb{F}_2)\right|.$$

3.3 Dillon functions type

In paper [21] an explicit representation of functions in a generalization of Dillon's $\mathcal{PS}_{ap}$ class to gbent functions with $q = 2^k$ was presented. By comparing the function from $\mathcal{PS}_{ap}$ in a bivariate form with its dual we obtain the following result.

Proposition 2 *Assume G_j, $j = 0, 1, ..., k-1$, be balanced Boolean functions in m variables with $G_j(0) = 0$ and $\sum_{t\in\mathbb{F}_{2^m}} \omega^{\sum_{j=0}^{k-1} 2^j G_j(t)} = 0$. Then, if $G_j(u) = G_j(1/u)$ for any $u \in \mathbb{F}_{2^m}$ (with the convention $1/0 = 0$), then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ given by*

$$f(x, y) = \sum_{j=0}^{k-1} 2^j G_j(x/y), \quad x, y \in \mathbb{F}_2^{n/2}, \tag{4}$$

is self-dual gbent in $2m$ variables.

Proof It is enough to mention that, as was shown in [21], the dual gbent function of (4) has the form

$$\widetilde{f}(x, y) = \sum_{j=0}^{k-1} 2^j G_j(y/x), \quad x, y \in \mathbb{F}_2^{n/2}.$$

3.4 Iterative construction

Let f_0, f_1, f_2, f_3 be Boolean functions in n variables. Consider a Boolean function g in $n + 2$ variables which is defined as

$$g(00, x) = f_0(x), \quad g(01, x) = f_1(x), \quad g(10, x) = f_2(x), \quad g(11, x) = f_3(x), \quad x \in \mathbb{F}_2^n.$$

It is known (Preneel et al. [27]; see also [37]) that under condition that all functions f_0, f_1, f_2, f_3 are Boolean bent functions in n variables, the mentioned function g is a bent function in $n + 2$ variables if and only if

$$\widetilde{f_0} \oplus \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3} = 1,$$

that gives the construction of a bent function in $n + 2$ variables through the concatenation of vectors of values of four bent functions in n variables [27].

Following N. Tokareva [37], we will refer to Boolean bent functions obtained by this construction as *bent iterative functions* ($\mathcal{BI}$). A construction of generalized bent functions in $n + 2$ variables obtained by a concatenation of four generalized Boolean functions on n variables was studied in [31].

Bent iterative constructions of self-dual Boolean bent functions in $n + 2$ variables, based on concatenation of 4 Boolean bent functions in n variables, were presented in [2,16]. In current work we give two constructions of generalized bent iterative functions that generalize the constructions for Boolean case:

Proposition 3 *1) Let f be a regular gbent function in n variables, then the sign function*

$$\big(F, \widetilde{F}, \widetilde{F}, -F\big),$$

where $F = \omega^f$ and $\widetilde{F} = \omega^{\widetilde{f}}$, is the sign function of a self-dual gbent function in $n+2$ variables;

2) Let f be a self-dual gbent function in n variables with the sign function F, and g be an anti-self-dual gbent function in n variables with the sign function G, then the sign function

$$\big(F, G, -G, F\big),$$

where $F = \omega^f$ and $G = \omega^g$, is the sign function of a gbent function in $n+2$ variables.

Proof Let $F = \omega^f$ be a sign function of regular gbent function f in n variables. It is clear that the function h is self-dual gbent if and only if

$$\begin{aligned}\mathcal{H}_{n+2}\begin{pmatrix} F \\ \widetilde{F} \\ \widetilde{F} \\ -F \end{pmatrix} &= \frac{1}{2}\begin{pmatrix} \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n \end{pmatrix}\begin{pmatrix} F \\ \widetilde{F} \\ \widetilde{F} \\ -F \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} \widetilde{F} + F + F - \widetilde{F} \\ \widetilde{F} - F + F + \widetilde{F} \\ \widetilde{F} + F - F + \widetilde{F} \\ \widetilde{F} - F - F - \widetilde{F} \end{pmatrix} = \begin{pmatrix} F \\ \widetilde{F} \\ \widetilde{F} \\ -F \end{pmatrix},\end{aligned}$$

Let f be a self-dual gbent function in n variables with the sign function $F = \omega^f$, and g be an anti-self-dual gbent function in n variables with the sign function $G = \omega^g$, then

$$\begin{aligned}\mathcal{H}_{n+2}\begin{pmatrix} F \\ G \\ -G \\ F \end{pmatrix} &= \frac{1}{2}\begin{pmatrix} \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n \end{pmatrix}\begin{pmatrix} F \\ G \\ -G \\ F \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} F + G - G + F \\ F - G - G - F \\ F + G + G - F \\ F - G + G + F \end{pmatrix} = \begin{pmatrix} -F \\ -G \\ G \\ -F \end{pmatrix},\end{aligned}$$

4 Hamming and Lee distance spectrums

The spectrum of Hamming distances between self-dual Maiorana–McFraland Boolean bent functions was studied in [15]. It was proved that

$$\mathrm{Sp}_H\left(\mathrm{SB}^+_{\mathcal{M}}(n) \cup \mathrm{SB}^-_{\mathcal{M}}(n)\right) = \left\{2^{n-1}\right\} \cup \bigcup_{r=0}^{n/2-1}\left\{2^{n-1}\left(1 \pm \frac{1}{2^r}\right)\right\},$$

and, if either $f, g \in \mathrm{SB}^+_{\mathcal{M}}(n)$ or $f, g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, then all distances except 2^{n-1} are attainable, and for any pair $f \in \mathrm{SB}^+_{\mathcal{M}}(n)$ and $g \in \mathrm{SB}^-_{\mathcal{M}}(n)$ it holds $\mathrm{dist}(f, g) = 2^{n-1}$.

4.1 Hamming distance spectrum

For generalized case we have

Proposition 4 *It holds*

$$\mathrm{Sp}_H\left(\mathrm{SB}^+_{\mathcal{GM}^q}(n)\cup\mathrm{SB}^-_{\mathcal{GM}^q}(n)\right)=\mathrm{Sp}_H\left(\mathrm{SB}^+_{\mathcal{M}}(n)\cup\mathrm{SB}^-_{\mathcal{M}}(n)\right).$$

Moreover, all given distances are attainable.

Proof Let $f_1,f_2\in\mathrm{SB}^+_{\mathcal{GM}^q}(n)\cup\mathrm{SB}^-_{\mathcal{GM}^q}(n)$. We have

$$f_1(x,y)=\frac{q}{2}h_1(x,y)+d_1,\quad x,y\in\mathbb{F}_2^{n/2},$$

$$f_2(x,y)=\frac{q}{2}h_2(x,y)+d_2,\quad x,y\in\mathbb{F}_2^{n/2},$$

for some $h_1,h_2\in\mathrm{SB}^+_{\mathcal{M}}(n)\cup\mathrm{SB}^-_{\mathcal{M}}(n)$ and $d_1,d_2\in\mathbb{Z}_q$. If $\mathrm{wt}\,(d_1-d_2)\notin\{0,q/2\}$, then $\mathrm{dist}_L\,(f_1,f_2)=2^n$. Otherwise, the distance coincides with some value from the spectrum for binary case so by taking $d_1,d_2=0$ and varying h_1,h_2 this spectrum can be entirely covered.

4.2 Lee distance spectrum

For binary case the Hamming distance coincides with the Lee distance, so for this case the Lee distance spectrum follows. For $q>2$ the spectrum can be obtained by using the set of attainable Hamming distances from binary case.

Theorem 2 *It holds*

$$\mathrm{Sp}_L\left(\mathrm{SB}^+_{\mathcal{GM}^q}(n)\cup\mathrm{SB}^-_{\mathcal{GM}^q}(n)\right)$$
$$=\left\{q\cdot 2^{n-2}\right\}\cup\bigcup_{w=0}^{q/2}\bigcup_{r=0}^{n/2-1}\left\{q\cdot 2^{n-2}\left(1\pm\frac{1}{2^r}\right)\mp w\cdot 2^{n-r}\right\}.$$

Moreover, all given distances are attainable.

Proof Let $f_1,f_2\in\mathrm{SB}^+_{\mathcal{GM}^q}(n)\cup\mathrm{SB}^-_{\mathcal{GM}^q}(n)$. Again, we have

$$f_1(x,y)=\frac{q}{2}h_1(x,y)+d_1,\quad x,y\in\mathbb{F}_2^{n/2},$$

$$f_2(x,y)=\frac{q}{2}h_2(x,y)+d_2,\quad x,y\in\mathbb{F}_2^{n/2},$$

for some $h_1,h_2\in\mathrm{SB}^+_{\mathcal{M}}(n)\cup\mathrm{SB}^-_{\mathcal{M}}(n)$ and $d_1,d_2\in\mathbb{Z}_q$. Denote $\mathrm{wt}_L\,(d_1-d_2)$ by w and the Hamming distance $\mathrm{dist}_H\,(h_1,h_2)$ between Boolean functions h_1,h_2 by

d. Under this notation the Lee distance between f_1 and f_2 is the function of w, d and number of variables n. Indeed,

$$\begin{aligned}
\mathrm{dist}_L(f_1,f_2) &= \sum_{x,y\in\mathbb{F}_2^{n/2}} \mathrm{wt}_L(f_1(x,y)-f_2(x,y)) \\
&= \sum_{\substack{x,y\in\mathbb{F}_2^{n/2}\\ h_1(x,y)=h_2(x,y)}} \mathrm{wt}_L(f_1(x,y)-f_2(x,y)) \\
&+ \sum_{\substack{x,y\in\mathbb{F}_2^{n/2}\\ h_1(x,y)\neq h_2(x,y)}} \mathrm{wt}_L(f_1(x,y)-f_2(x,y)) \\
&= \sum_{\substack{x,y\in\mathbb{F}_2^{n/2}\\ h_1(x,y)=h_2(x,y)}} \mathrm{wt}_L(d_1-d_2) \\
&+ \sum_{\substack{x,y\in\mathbb{F}_2^{n/2}\\ h_1(x,y)\neq h_2(x,y)}} \mathrm{wt}_L\left(d_1-d_2+\frac{q}{2}\right) \\
&= (2^n-d)\,w + d\left(\frac{q}{2}-w\right) = 2^n w - 2dw + \frac{q}{2}d.
\end{aligned}$$

If $h_1 \in \mathrm{SB}^+_{\mathcal{M}}(n)$ and $h_2 \in \mathrm{SB}^-_{\mathcal{M}}(n)$, then

$$\mathrm{dist}_L(f_1,f_2) = 2^n w - 2\cdot 2^{n-1}w + \frac{q}{2}\cdot 2^{n-1} = q\cdot 2^{n-2}.$$

From the aforementioned Hamming distance spectrum for binary case it follows that for any $r \in \{0,1,...,n/2-1\}$ there exists at least one pair of (anti-)self-dual Boolean Maiorana–McFarland bent functions in n variables at the Hamming distance $d = 2^{n-1}+2^{n-r-1}$ as well as $2^n - d = 2^{n-1}-2^{n-r-1}$. Assume r is fixed, put $d = 2^{n-1}\left(1\pm 2^{-r}\right)$ in the expression for $\mathrm{dist}_L(f_1,f_2)$:

$$\begin{aligned}
\mathrm{dist}_L(f_1,f_2) &= 2^n w - 2w\cdot 2^{n-1}\left(1\pm\frac{1}{2^r}\right) + \frac{q}{2}\cdot 2^{n-1}\left(1\pm\frac{1}{2^r}\right) \\
&= 2^n w - 2^n w \mp w\cdot 2^{n-r} + q\cdot 2^{n-2}\left(1\pm\frac{1}{2^r}\right) \\
&= q\cdot 2^{n-2}\left(1\pm\frac{1}{2^r}\right) \mp w\cdot 2^{n-r}.
\end{aligned}$$

Observation that r runs $\{0,1,...,n/2-1\}$ and w varies within the set $\{0,1,...,q/2\}$ yields the result.

Proposition 5 *The minimal Lee distance between generalized (anti-)self-dual Maiorana–McFarland bent functions in n variables is equal to $q\cdot 2^{n-3}$.*

Proof Estimate the minimal value of the term

$$D = q\cdot 2^{n-2}\left(1\pm\frac{1}{2^r}\right) \mp w\cdot 2^{n-r},$$

with $r \in \{1,2,...,n/2-1\}$ and $w \in \{0,1,...,q/2\}$. Here we exclude the case $r=0$ since then the Lee distance is equal to either $D = w\cdot 2^n \geqslant 2^n$ or $D =$

$2^{n-1}(q-2w) \geqslant 2^n$, provided that f_1, f_2 are distinct. Indeed, $r=0$ implies $d \in \{0, 2^n\}$, and the first aforementioned expression for D corresponds to $h_1 = h_2$, while the second one to $h_1 \oplus h_2 = 1$.

Consider two cases depending on sequence of the signs.

Case 1:

$$D = q \cdot 2^{n-2}\left(1+\frac{1}{2^r}\right) - w \cdot 2^{n-r} = q \cdot 2^{n-2} + 2^{n-r}\left(\frac{q}{4} - w\right).$$

Since $w \in \{0, 1, ..., q/2\}$ it follows that

$$-\frac{q}{4} \leqslant \frac{q}{4} - w \leqslant \frac{q}{4},$$

hence

$$-\frac{q}{4} \cdot 2^{n-r} \leqslant 2^{n-r}\left(\frac{q}{4} - w\right) \leqslant \frac{q}{4} \cdot 2^{n-r}.$$

Then

$$D \geqslant q \cdot 2^{n-2} - \frac{q}{4} \cdot 2^{n-r} = q \cdot 2^{n-2}\left(1 - \frac{1}{2^r}\right) \geqslant q \cdot 2^{n-3},$$

and $D_{\min} = q \cdot 2^{n-3}$, that is attainable for $r=1$ and $w = q/2$.

Case 2:

$$D = q \cdot 2^{n-2}\left(1-\frac{1}{2^r}\right) + w \cdot 2^{n-r} = q \cdot 2^{n-2} + 2^{n-r}\left(w - \frac{q}{4}\right).$$

From $w \in \{0, 1, ..., q/2\}$ it follows that

$$-\frac{q}{4} \leqslant w - \frac{q}{4} \leqslant \frac{q}{4},$$

hence

$$-\frac{q}{4} \cdot 2^{n-r} \leqslant 2^{n-r}\left(w - \frac{q}{4}\right) \leqslant \frac{q}{4} \cdot 2^{n-r}.$$

Then

$$D \geqslant q \cdot 2^{n-2} - \frac{q}{4} \cdot 2^{n-r} = q \cdot 2^{n-2}\left(1 - \frac{1}{2^r}\right) \geqslant q \cdot 2^{n-3},$$

and again $D_{\min} = q \cdot 2^{n-3}$, that is attainable for $r=1$ and $w=0$.

Thus the minimal Lee distance is equal to $q \cdot 2^{n-3}$.

In [26] it was shown that both minimal Hamming and Lee distances of generalized Reed–Muller codes $\mathrm{RM}_q(r,n)$ are equal to 2^{n-r} for any positive integer q. Therefore, it immediately follows that

Corollary 2 *The minimal Hamming distance 2^{n-2} between quadratic (generalized) bent functions is attainable on the sets of self-dual and anti-self-dual Maiorana–McFarland bent functions from $\mathcal{GM}_n^q$ only for $q=2$.*

5 Sign functions of (anti-)self-dual gbent functions

Let I_n be the identity matrix of size n and $H_n = H_1^{\otimes n}$ be the n-fold tensor product of the matrix H_1 with itself, where

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is known the Hadamard property of this matrix

$$H_n H_n^T = 2^n I_{2^n},$$

where H_n^T is transpose of H_n (it holds $H_n^T = H_n$ by symmetricity of H_n). Denote $\mathcal{H}_n = 2^{-n/2} H_n$.

Recall an orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of H_n from [2] (Lemma 5.2):

$$\mathbb{R}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

where the symbol $\oplus$ denotes a direct sum of subspaces. Consider the same decomposition

$$\mathbb{C}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

for a complex space $\mathbb{C}^{2^n}$.

As for the Boolean case (see [17]), we note that sign function of any self-dual gbent function is the eigenvector of $\mathcal{H}_n$ attached to the eigenvalue $(+1)$, that is an element from the subspace $\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big) = \mathrm{Ker}\big(H_n - 2^{n/2} I_{2^n}\big)$. The same holds for a sign function of any anti-self-dual gbent function, which obviously is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue (-1), that is an element from the subspace $\mathrm{Ker}\big(\mathcal{H}_n + I_{2^n}\big) = \mathrm{Ker}\big(H_n + 2^{n/2} I_{2^n}\big)$.

It is known that

$$\dim\big(\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)\big) = \dim\big(\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big)\big) = 2^{n-1},$$

where $\dim(V)$ is the dimension of the subspace $V \subseteq \mathbb{R}^{2^n}$. Moreover, since $\mathcal{H}_n$ is symmetric (Hermitian), the subspaces $\mathrm{Ker}\big(\mathcal{H}_n + I_{2^n}\big)$ and $\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big)$ are mutually orthogonal.

In [16] it was proved that provided $n \geqslant 4$, the linear span of sign functions of self-dual as well as anti-self-dual Boolean bent functions Boolean bent functions in n variables has dimension 2^{n-1}. The same result can be also given for gbent functions:

Theorem 3 *Let $n \geqslant 4$, then the linear span of sign functions of (anti-)self-dual gbent functions in n variables has dimension 2^{n-1}.*

Proof It is enough to mention that since q is even it holds $(-1) = \omega^{q/2} \in \{\omega, \omega^2, ..., \omega^{q-1}\}$, therefore the set of sign fuctions of (anti-)self-dual Boolean bent functions in n variables is a subset of the set of sign functions of (anti-)self-dual gbent functions in n variables. Then from [16] (Theorem 2) the dimension follows.

It is worth to note that the example of the basis of the subspace $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ can be constructed by using the functions obtained from the construction from Proposition 3.

When $n = 2$ there are two self-dual Boolean bent functions, namely x_1x_2 and $x_1x_2 \oplus 1$, which have sign functions $(1, 1, 1, -1)$ and $(-1, -1, -1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$. The set $\mathrm{SB}^-(2)$ consists of functions $x_1x_2 \oplus x_1 \oplus x_2$ and $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ with sign functions $(1, -1, -1, -1)$ and $(-1, 1, 1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$ as well. Generalization comprises solution of the system

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix} = \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix},$$

where variables are numbers $d_1, d_2, d_3, d_4 \in \mathbb{Z}_q$ in fact. It is clear that the only solution pattern is

$$\left(\omega^d, \omega^d, \omega^d, \omega^{d+q/2}\right) = \omega^d \cdot (1, 1, 1, -1) \in \mathbb{C}^4,$$

where $d \in \mathbb{Z}_q$. It means that any two sign functions of self-dual gbent functions from $\mathrm{SB}_q^+(2)$ are linearly dependent over $\mathbb{C}$ and $\left|\mathrm{SB}_q^+(2)\right| = q$.

The next result is a generalization of the similar one from [16].

Theorem 4 *Let $n \geqslant 4$ and $f \in \mathrm{SB}_q^+(n)$. For sign function $\omega^f = \left(F^{00}, F^{01}, F^{10}, F^{11}\right)$, where $F^{00}, F^{01}, F^{10}, F^{11} \in \left\{1, \omega, \omega^2, \ldots, \omega^{q-1}\right\}^{2^{n-2}}$, it holds*

$$\left\langle F^{00}, F^{01}\right\rangle + \left\langle F^{10}, F^{11}\right\rangle = 0,$$
$$\left\langle F^{00}, F^{10}\right\rangle + \left\langle F^{01}, F^{11}\right\rangle = 0.$$

Proof Let $f \in \mathrm{SB}_q^+(n)$, then by Theorem 3 there exist vectors

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2^{n-3}}) \in \mathbb{C}^{2^{n-3}},$$
$$\beta = (\beta_1, \beta_2, \ldots, \beta_{2^{n-3}}) \in \mathbb{C}^{2^{n-3}},$$
$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_{2^{n-2}}) \in \mathbb{C}^{2^{n-2}},$$

such that

$$\omega^f = \sum_{i=1}^{2^{n-3}} \alpha_i \mathbf{F}_i^n + \sum_{j=1}^{2^{n-3}} \beta_j \mathbf{G}_j^n + \sum_{k=1}^{2^{n-2}} \gamma_k \left(\mathbf{FG}\right)_k^n,$$

where the sets $S_{\mathbf{F}} = \{\mathbf{F}_i^n\}_{i=1}^{2^{n-3}}$, $S_{\mathbf{G}} = \left\{\mathbf{G}_j^n\right\}_{j=1}^{2^{n-3}}$ and $S_{\mathbf{FG}} = \left\{\left(\mathbf{FG}\right)_k^n\right\}_{k=1}^{2^{n-2}}$ are described in the proof of Theorem 2 from [16]. Consider the sets $S_{\mathbf{F}}$, $S_{\mathbf{G}}$, $S_{\mathbf{FG}}$ and denote

$$\mathbf{F}_i^n = (F_i, F_i, F_i, -F_i),$$
$$\mathbf{G}_j^n = (G_j, -G_j, -G_j, -G_j),$$
$$\left(\mathbf{FG}\right)_k^n = (A_k, -B_k, B_k, A_k),$$

where $F_i, A_k \in \mathrm{Ker}\big(\mathcal{H}_{n-2}-I_{2^{n-2}}\big)$, $G_j, B_k \in \mathrm{Ker}\big(\mathcal{H}_{n-2}+I_{2^{n-2}}\big)$, $i,j=1,2,\dots,2^{n-3}$, $k=1,2,\dots,2^{n-2}$, and define the vectors

$$\mathbf{F}=\sum_{i=1}^{2^{n-3}}\alpha_i F_i,\qquad \mathbf{G}=\sum_{j=1}^{2^{n-3}}\beta_j G_j,\qquad \mathbf{A}=\sum_{k=1}^{2^{n-2}}\gamma_k A_k,\qquad \mathbf{B}=\sum_{k=1}^{2^{n-2}}\gamma_k B_k.$$

Under this notation the sign function ω^f has the form

$$\omega^f=\begin{pmatrix}F^{00}\\F^{01}\\F^{10}\\F^{11}\end{pmatrix}=\begin{pmatrix}\mathbf{F}+\mathbf{G}+\mathbf{A}\\\mathbf{F}-\mathbf{G}-\mathbf{B}\\\mathbf{F}-\mathbf{G}+\mathbf{B}\\-\mathbf{F}-\mathbf{G}+\mathbf{A}\end{pmatrix}\in\big\{1,\omega,\omega^2,...,\omega^{q-1}\big\}^{2^n}.$$

For any $j=1,2,\dots,2^{n-2}$ denote

$$\begin{aligned}\big(\mathbf{F}+\mathbf{G}\big)_j+\mathbf{A}_j&=\omega^{t_j},\\ \big(\mathbf{F}-\mathbf{G}\big)_j-\mathbf{B}_j&=\omega^{r_j},\\ \big(\mathbf{F}-\mathbf{G}\big)_j+\mathbf{B}_j&=\omega^{l_j},\\ -\big(\mathbf{F}+\mathbf{G}\big)_j+\mathbf{A}_j&=\omega^{k_j},\end{aligned}$$

where $t_j, r_j, l_j, k_j \in \mathbb{Z}_q$. Then

$$\begin{aligned}\mathbf{A}_j&=\frac{1}{2}\big(\omega^{t_j}+\omega^{k_j}\big),\\ \mathbf{B}_j&=\frac{1}{2}\big(\omega^{l_j}-\omega^{r_j}\big),\\ \big(\mathbf{F}+\mathbf{G}\big)_j&=\frac{1}{2}\big(\omega^{t_j}-\omega^{k_j}\big),\\ \big(\mathbf{F}-\mathbf{G}\big)_j&=\frac{1}{2}\big(\omega^{r_j}+\omega^{l_j}\big).\end{aligned}$$

Note that

$$\langle\mathbf{G},\mathbf{A}\rangle=\langle\mathbf{F},\mathbf{B}\rangle=0.$$

By using this we obtain the expression for the first inner product

$$\begin{aligned}\big\langle F^{00},F^{01}\big\rangle+\big\langle F^{10},F^{11}\big\rangle&=\langle\mathbf{F}+\mathbf{G}+\mathbf{A},\mathbf{F}-\mathbf{G}-\mathbf{B}\rangle\\ &+\langle\mathbf{F}-\mathbf{G}+\mathbf{B},-\mathbf{F}-\mathbf{G}+\mathbf{A}\rangle\\ &=\langle\mathbf{F},\mathbf{F}\rangle-\langle\mathbf{F},\mathbf{G}\rangle-\langle\mathbf{F},\mathbf{B}\rangle\\ &+\langle\mathbf{G},\mathbf{F}\rangle-\langle\mathbf{G},\mathbf{G}\rangle-\langle\mathbf{G},\mathbf{B}\rangle\\ &+\langle\mathbf{A},\mathbf{F}\rangle-\langle\mathbf{A},\mathbf{G}\rangle-\langle\mathbf{A},\mathbf{B}\rangle\\ &-\langle\mathbf{F},\mathbf{F}\rangle-\langle\mathbf{F},\mathbf{G}\rangle+\langle\mathbf{F},\mathbf{A}\rangle\\ &+\langle\mathbf{G},\mathbf{F}\rangle+\langle\mathbf{G},\mathbf{G}\rangle-\langle\mathbf{G},\mathbf{A}\rangle\\ &-\langle\mathbf{B},\mathbf{F}\rangle-\langle\mathbf{B},\mathbf{G}\rangle+\langle\mathbf{B},\mathbf{A}\rangle\\ &=\langle\mathbf{A},\mathbf{F}\rangle+\langle\mathbf{F},\mathbf{A}\rangle-\langle\mathbf{G},\mathbf{B}\rangle-\langle\mathbf{B},\mathbf{G}\rangle\\ &=\langle\mathbf{A},\mathbf{F}+\mathbf{G}\rangle+\overline{\langle\mathbf{A},\mathbf{F}+\mathbf{G}\rangle}+\langle\mathbf{B},\mathbf{F}-\mathbf{G}\rangle+\overline{\langle\mathbf{B},\mathbf{F}-\mathbf{G}\rangle}\end{aligned}\tag{5}$$

while the second one has the form

$$\begin{aligned}\left\langle F^{00}, F^{10}\right\rangle + \left\langle F^{01}, F^{11}\right\rangle &= \langle \mathbf{F}+\mathbf{G}+\mathbf{A}, \mathbf{F}-\mathbf{G}+\mathbf{B}\rangle \\ &+ \langle \mathbf{F}-\mathbf{G}-\mathbf{B}, -\mathbf{F}-\mathbf{G}+\mathbf{A}\rangle \\ &= \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle + \langle \mathbf{F},\mathbf{B}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle - \langle \mathbf{G},\mathbf{G}\rangle + \langle \mathbf{G},\mathbf{B}\rangle \\ &+ \langle \mathbf{A},\mathbf{F}\rangle - \langle \mathbf{A},\mathbf{G}\rangle + \langle \mathbf{A},\mathbf{B}\rangle \\ &- \langle \mathbf{F},\mathbf{F}\rangle - \langle \mathbf{F},\mathbf{G}\rangle + \langle \mathbf{F},\mathbf{A}\rangle \\ &+ \langle \mathbf{G},\mathbf{F}\rangle + \langle \mathbf{G},\mathbf{G}\rangle - \langle \mathbf{G},\mathbf{A}\rangle \\ &+ \langle \mathbf{B},\mathbf{F}\rangle + \langle \mathbf{B},\mathbf{G}\rangle - \langle \mathbf{B},\mathbf{A}\rangle \\ &= \langle \mathbf{A},\mathbf{F}\rangle + \langle \mathbf{F},\mathbf{A}\rangle + \langle \mathbf{G},\mathbf{B}\rangle + \langle \mathbf{B},\mathbf{G}\rangle \\ &= \langle \mathbf{A},\mathbf{F}+\mathbf{G}\rangle + \overline{\langle \mathbf{A},\mathbf{F}+\mathbf{G}\rangle} - \langle \mathbf{B},\mathbf{F}-\mathbf{G}\rangle - \overline{\langle \mathbf{B},\mathbf{F}-\mathbf{G}\rangle} \end{aligned} \tag{6}$$

Consider inner in details the following inner products

$$\begin{aligned}\langle \mathbf{A},\mathbf{F}+\mathbf{G}\rangle &= \sum_{j=1}^{2^n} \mathbf{A}_j \overline{(\mathbf{F}+\mathbf{G})}_j = \frac{1}{4}\sum_{j=1}^{2^n} \left(\omega^{t_j}+\omega^{k_j}\right)\left(\overline{\omega^{t_j}}-\overline{\omega^{k_j}}\right) \\ &= \frac{1}{4}\sum_{j=1}^{2^n}\left(1-1+\omega^{k_j}\overline{\omega^{t_j}}-\omega^{t_j}\overline{\omega^{k_j}}\right) = \frac{1}{2}\mathrm{Im}\left(\sum_{j=1}^{2^n}\omega^{k_j}\overline{\omega^{t_j}}\right) i, \\ \overline{\langle \mathbf{A},\mathbf{F}+\mathbf{G}\rangle} &= -\frac{1}{2}\mathrm{Im}\left(\sum_{j=1}^{2^n}\omega^{k_j}\overline{\omega^{t_j}}\right) i, \end{aligned}$$

$$\begin{aligned}\langle \mathbf{B},\mathbf{F}-\mathbf{G}\rangle &= \sum_{j=1}^{2^n} \mathbf{B}_j \overline{(\mathbf{F}-\mathbf{G})}_j = \frac{1}{4}\sum_{j=1}^{2^n} \left(\omega^{l_j}-\omega^{r_j}\right)\left(\overline{\omega^{l_j}}+\overline{\omega^{r_j}}\right) \\ &= \frac{1}{4}\sum_{j=1}^{2^n}\left(1-1+\omega^{l_j}\overline{\omega^{r_j}}-\omega^{r_j}\overline{\omega^{l_j}}\right) = \frac{1}{2}\mathrm{Im}\left(\sum_{j=1}^{2^n}\omega^{l_j}\overline{\omega^{r_j}}\right) i, \\ \overline{\langle \mathbf{B},\mathbf{F}-\mathbf{G}\rangle} &= -\frac{1}{2}\mathrm{Im}\left(\sum_{j=1}^{2^n}\omega^{l_j}\overline{\omega^{r_j}}\right) i, \end{aligned}$$

therefore, both (5) and (6) are zero numbers.

6 Properties of self-dual gbent function

6.1 Upper bound for the number of self-dual gbent functions

Let $2^{h-1} < q \leqslant 2^h$. For any $f \in \mathcal{GF}_n^q$ it is possible to associate a unique sequence of Boolean functions $a_0, a_1, \ldots, a_{h-1} \in \mathcal{F}_n$ such that [34]

$$f(x) = a_0(x) + 2a_1(x) + \ldots + 2^{h-1}a_{h-1}(x), \quad x \in \mathbb{F}_2^n.$$

In paper [13] it was proved that for the case $q = 2^k$ and even n, provided that f is gbent its dual gbent $\widetilde{f}$ has the following form

$$\widetilde{f}(x) = b_0(x) + 2b_1(x) + \ldots + 2^{h-1}b_{h-1}(x), \quad x \in \mathbb{F}_2^n,$$

where $b_{k-1} = \widetilde{b_{k-1}}$ and the dual of $b_j = \widetilde{b_{k-1}} \oplus \big(\widetilde{b_{k-1} \oplus b_j}\big)$. If f is self-dual gbent then b_{k-1} is self-dual Boolean function and for $j = 0, 1, \ldots, k-1$ Boolean functions $\big(b_{k-1} \oplus b_j\big)$ are self-dual. It follows the statement

Proposition 6 *It holds* $\left|\mathrm{SB}^+_{2^k}(n)\right| \leqslant \left|\mathrm{SB}^+_2(n)\right|^k$.

Note that this bound is consistent with the results from the work [20].

6.2 Affinity of self-dual gbent function

In paper [31] for the case when q is divisible by 4, necessary and sufficient conditions for the bentness of generalized Boolean functions of the form

$$f(x) = \sum_{i=1}^{n} \lambda_i x_i + \lambda_0,$$

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$, were obtained. Functions from this class are referred to as *affine* functions.

It is well known that Boolean bent function and, as a consequence, self-dual Boolean bent function can not be affine. The next result shows the non-existence of self-dual gbent functions within the class of affine functions.

Theorem 5 *There are no self-dual generalized bent functions in n variables of the form*

$$f(x) = \sum_{i=1}^{n} \lambda_i x_i + \lambda_0,$$

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$.

Proof Let f be an affine gbent function in n variables (for the case q not divisible by 4 if such exists, otherwise the result follows), namely

$$f(x) = \sum_{i=1}^{n} \lambda_i x_i + \lambda_0, \quad x \in \mathbb{F}_2^n,$$

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$. It is self-dual if and only if

$$\begin{aligned} H_f(y) &= \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y \rangle} = \omega^{\lambda_0} \sum_{x \in \mathbb{F}_2^n} \omega^{\sum\limits_{i=1}^{n} \lambda_i x_i + \frac{q}{2}\langle x, y \rangle} \\ &= \omega^{\lambda_0} \prod_{i=1}^{n} \sum_{x_i \in \mathbb{F}_2} \omega^{\lambda_i x_i + \frac{q}{2} y_i x_i} = \omega^{\lambda_0} \prod_{i=1}^{n} \left(1 + \omega^{\frac{q}{2} y_i + \lambda_i}\right), \end{aligned}$$

for any $y \in \mathbb{F}_2^n$.

For every $y \in \mathbb{F}_2^n$ denote

$$\begin{aligned}\widehat{y} &= (y_1, y_2, \ldots, y_{n-1}) \in \mathbb{F}_2^{n-1},\\ P_{n-1}(\widehat{y}) &= \left(1+\omega^{\frac{q}{2}y_1+\lambda_1}\right)\left(1+\omega^{\frac{q}{2}y_2+\lambda_2}\right)\cdot\ldots\cdot\left(1+\omega^{\frac{q}{2}y_{n-1}+\lambda_{n-1}}\right),\\ a_{n-1}(\widehat{y}) &= \lambda_1 y_1 + \lambda_2 y_2 + \ldots + \lambda_{n-1}y_{n-1}.\end{aligned}$$

Then for any $y \in \mathbb{F}_2^n$ such that $y_n = 0$ it holds

$$P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})},$$

and for any $y \in \mathbb{F}_2^n$ such that $y_n = 1$:

$$P_{n-1}(\widehat{y})\left(1+\omega^{\frac{q}{2}+\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})+\lambda_n}.$$

So, for any $\widehat{y} \in \mathbb{F}_2^{n-1}$ consider the system

$$\begin{cases} P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})},\\ P_{n-1}(\widehat{y})\left(1-\omega^{\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})+\lambda_n}.\end{cases}$$

It is equivalent to

$$\begin{cases} P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})},\\ P_{n-1}(\widehat{y})\left(1-\omega^{\lambda_n}\right) = P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right)\cdot\omega^{\lambda_n}.\end{cases}$$

Thus, we obtain the relation

$$P_{n-1}(\widehat{y})\left(1-\omega^{\lambda_n}\right) = P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right)\cdot\omega^{\lambda_n},$$

and can note that $P_{n-1}(\widehat{y}) \neq 0$ since for any $y \in \mathbb{F}_2^n$ we have

$$H_f(y) = \omega^{\lambda_0}P_{n-1}(\widehat{y})\left(1+\omega^{\frac{q}{2}y_n+\lambda_n}\right),$$

and f is gbent that is $1-\omega^{\lambda_n} = \omega^{\lambda_n} + \left(\omega^{\lambda_n}\right)^2$. The solutions of this equation are $\left(-1 \pm \sqrt{2}\right)$. The norm of every of these numbers is not 1 therefore ω^{λ_n} can not be a solution.

6.3 Self-dual gbent functions symmetric with respect to two variables

A generalized Boolean function $h \in \mathcal{GF}_{n+2}^q$ is said to be symmetric with respect to two variables y and z if there exist functions $f, g, s \in \mathcal{GF}_n^q$ such that

$$h(z,y,x) = f(x) + (y \oplus z)g(x) + yzs(x), \quad y,z \in \mathbb{F}_2, x \in \mathbb{F}_2^n. \tag{7}$$

In paper [34] it was proved that a function of such form is gbent if and only if the functions $f, f+g$ are gbent and $s(x) = q/2$, $x \in \mathbb{F}_2^n$. We study the conditions for self-duality of functions of such form.

Theorem 6 *Let h be a gbent function of the form (7). Then h is self-dual if and only if f is regular gbent, $g = \widetilde{f} + (q-1)f$, and $s(x) = q/2$, $x \in \mathbb{F}_2^n$.*

Proof Let F, FG be sign functions of regular gbent functions $f, f+g$. It is clear that

$$\omega^h = \begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix}.$$

Then the function h is self-dual gbent if and only if

$$\omega^{\widetilde{h}} = \mathcal{H}_{n+2}\omega^h = \frac{1}{2}\begin{pmatrix} \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n \end{pmatrix}\begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix} = \begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix} = \omega^h.$$

Consider the system

$$\begin{aligned} \omega^{\widetilde{h}} &= \frac{1}{2}\begin{pmatrix} \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n \end{pmatrix}\begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} \mathcal{H}_n F + \mathcal{H}_n(FG) + \mathcal{H}_n(FG) + \mathcal{H}_n F \\ \mathcal{H}_n F - \mathcal{H}_n(FG) + \mathcal{H}_n(FG) - \mathcal{H}_n F \\ \mathcal{H}_n F + \mathcal{H}_n(FG) - \mathcal{H}_n(FG) - \mathcal{H}_n F \\ \mathcal{H}_n F - \mathcal{H}_n(FG) - \mathcal{H}_n(FG) + \mathcal{H}_n F \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} \widetilde{F} - \widetilde{F} + 2\widetilde{FG} \\ 2\widetilde{F} - \widetilde{FG} + \widetilde{FG} \\ 2\widetilde{F} + \widetilde{FG} - \widetilde{FG} \\ -2\widetilde{FG} \end{pmatrix} = \begin{pmatrix} \widetilde{FG} \\ \widetilde{F} \\ \widetilde{F} \\ -\widetilde{FG} \end{pmatrix}. \end{aligned}$$

Writing

$$\begin{pmatrix} \widetilde{FG} \\ \widetilde{F} \\ \widetilde{F} \\ -\widetilde{FG} \end{pmatrix} = \begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix},$$

we see that $\widetilde{f} = f + g$, or, equivalently, $g = \widetilde{f} + (q-1)f$.

Thus, we have

$$h(z, y, x) = f(x) + (z \oplus y)\left[\widetilde{f}(x) + (q-1)f(x)\right] + \frac{q}{2}zy.$$

7 Symmetries

In paper [6] (see also [2]) it was shown that the mapping

$$f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c, x\rangle \oplus d, \tag{8}$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$, preserves self-duality of a bent function. The group which consists of mappings of such form is called an *extended orthogonal group* and denoted by $\overline{\mathcal{O}}_n$ [6]. It is known that this group is a subgroup of $\mathrm{GL}(n+2, \mathbb{F}_2)$ [6].

In paper [17] known results were generalized within isometric mappings from the set of all mappings of all Boolean functions in $n \geqslant 4$ variables into itself, which preserve the Hamming distance. Namely it was proved the group of automorphisms of self-dual Boolean bent functions coincides with the extended orthogonal group.

In paper [32] it was proved that the mappings of the form

$$f(x) \longrightarrow f\left(Lx\right) + d,$$

where $L \in \mathcal{O}_n$, $d \in \mathbb{Z}_4$, preserve self-duality of a quaternary self-dual gbent function.

In current work we set the form (8) for generalized case. The following result provides the construction of mappings of such form preserving the (anti-)self-duality of a Boolean function.

Theorem 7 *The mapping of the set of all generalized Boolean functions in n variables to itself of the form*

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) + \frac{q}{2}\langle c, x\rangle + d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{Z}_q$, preserves (anti-)self-duality of a gbent function.

Proof Let $f \in \mathrm{SB}_q^+(n) \cup \mathrm{SB}_q^-(n)$ that is $\widetilde{f} = f + \frac{q}{2}\varepsilon$ for some $\varepsilon \in \mathbb{F}_2$. Consider a function $g(x) = f\left(L\left(x \oplus c\right)\right) + \frac{q}{2}\langle c, x\rangle + d$, where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{Z}_q$. Its generalized Walsh–Hadamard transform is

$$\begin{aligned}
H_g(y) &= \sum_{x \in \mathbb{F}_2^n} \omega^{g(x)}(-1)^{\langle x, y\rangle} = \sum_{x \in \mathbb{F}_2^n} \omega^{f(L(x\oplus c)) + \frac{q}{2}\langle c, x\rangle + d + \frac{q}{2}\langle x, y\rangle} \\
&= \omega^d \sum_{x \in \mathbb{F}_2^n} \omega^{\frac{q}{2}\langle x, y\oplus c\rangle + f(L(x\oplus c))} = \omega^d \sum_{z \in \mathbb{F}_2^n} \omega^{\frac{q}{2}\left\langle L^{-1}z \oplus c, y\oplus c\right\rangle + f(z)} \\
&= \omega^{d + \frac{q}{2}\langle c, y\rangle + \frac{q}{2}\langle c, c\rangle} \sum_{z \in \mathbb{F}_2^n} \omega^{\frac{q}{2}\langle z, L(y\oplus c)\rangle + f(z)} \\
&= \omega^{d + \frac{q}{2}\langle c, y\rangle} 2^{n/2} \omega^{\widetilde{f}(L(y\oplus c))} = 2^{n/2}\omega^{f(L(y\oplus c)) + \frac{q}{2}\langle c, y\rangle + d + \frac{q}{2}\varepsilon} \\
&= 2^{n/2}\omega^{g(y) + \frac{q}{2}\varepsilon} = 2^{n/2}\omega^{\widetilde{g}(y)},
\end{aligned}$$

hence $\widetilde{g}(y) = g(y) + \frac{q}{2}\varepsilon$ for any $y \in \mathbb{F}_2^n$.

By using the mappings of this form we can clarify, for instance, the classification of quaternary self-dual bent functions in 4 variables given in [32] and formed by 8 classes. Namely, the representatives with vectors of values (0330302132010110) and (3123231322030300) from the classes 4 and 5 respectively are related by the transformation

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2}\langle c, x\rangle + d,$$

where

$$L = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix}, \quad c = (1001), \quad d = 3.$$

Table 1 Classification of quaternary self-dual bent functions in 4 variables

Representative from equivalence class	Size
0220202022000000	24
2022220222020200	64
0330313133110110	48
0330302132010110	120
1321213122010100	96
0220213023100000	48
Number of quaternary self-dual bent functions in four variables	400

The representatives with vectors of values (2022220222020200) and (2123230332121210) from the classes 2 and 7 respectively are related by the transformation

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2}\langle c, x\rangle + d,$$

where

$$L = \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad c = (0101), \quad d = 1.$$

Thus, the classification of quaternary self-dual bent functions in 4 variables is given in the Table 1.

By a slight change of the parameters mentioned in Theorem 7, it is possible to obtain the class of mapping that define a bijection between self-dual and anti-self-dual gbent functions in n variables.

Proposition 7 *The mapping of the set of all generalized Boolean functions in n variables to itself of the form*

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

with

$$\pi(x) = L\,(x \oplus c)\,, \quad g(x) = \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, $d \in \mathbb{Z}_q$, is a bijection between the sets $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$.

Proof Let $f \in \mathrm{SB}_q^+(n) \cup \mathrm{SB}_q^-(n)$ and $\widetilde{f} = f + \frac{q}{2}\varepsilon$ for some $\varepsilon \in \mathbb{F}_2$. One can show that for $g(x) = f\,(L\,(x \oplus c)) + \frac{q}{2}\langle c, x\rangle + d$, where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, $d \in \mathbb{Z}_q$, it holds $H_g(y) = 2^{n/2}\omega^{\widetilde{g}(y)+q/2}$, $y \in \mathbb{F}_2^n$.

From the existence of such bijections it follows that the cardinalities of the sets of self-dual and anti-self-dual gbent functions coincide.

Corollary 3 *It holds $\left|\mathrm{SB}_q^+(n)\right| = \left|\mathrm{SB}_q^-(n)\right|$.*

8 Conclusion

In current paper self-dual generalized bent functions were explored. A group of primary and secondary constructions was presented. The general form of self-dual Maiorana–McFarland gbent functions and their metrical properties were studied. The non-existence of affine self-dual gbent functions was shown. We also gave the description of self-dual gbent functions symmetric with respect to two variables. The properties of sign functions of self-dual gbent functions were considered.

It is interesting to find other symmetries, if any, distinct from the ones that were found in this work. It involves the study of the automorphisms gropus of the considered gbent functions with respect to Hamming or Lee metrics. The study of connection with self-dual Boolean functions also seems to be a promising task.

References

1. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. p. 257–397. Cambridge University Press, Cambridge (2010)
2. Carlet C., Danielsen L.E., Parker M.G., Solé P.: Self-dual bent functions, Int. J. Inform. Coding Theory, **1**, 384–399 (2010)
3. Carlet C.: Boolean Functions for Cryptography and Coding Theory, 620 p., Cambridge University Press (2020)
4. Çeşmelioğlu A., Meidl W. Pott A.: On the dual of (non)-weakly regular bent functions and self-dual bent functions. Adv. Math. Commun. **7**(4), 425–440 (2013)
5. Cusick T.W., Stănică P.: Cryptographic Boolean functions and applications, 288 p., Acad. Press, London, (2017)
6. Feulner T., Sok L., Solé P., Wassermann A.: Towards the Classification of Self-Dual Bent Functions in Eight Variables. Des. Codes Cryptogr. **68**(1), 395–406 (2013)
7. Hou X.-D.: Classification of self dual quadratic bent functions, Des. Codes Cryptogr. **63**(2), 183–198 (2012)
8. Hou X.-D.: Classification of p-ary self dual quadratic bent functions, p odd. Journal of Algebra **391**, 62–81 (2013)
9. Hyun J.Y., Lee H., Lee Y.: MacWilliams duality and Gleason-type theorem on self-dual bent functions. Des. Codes Cryptogr. **63**(3), 295–304 (2012)
10. Janusz G.J.: Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl. **13**(3), 450–491 (2007)
11. Hodžić S., Pasalic E.: Generalized Bent Functions — Some General Construction Methods and Related Necessary and Sufficient Conditions. Cryptogr. Commun. **7**(4), 469–483 (2015)
12. Hodžić S., Pasalic E.: Construction methods for generalized bent functions. Discrete Appl. Math. **238**, 14–23 (2018)
13. Hodžić S., Meidl W., Pasalic E.: Full Characterization of Generalized Bent Functions as (Semi)-Bent Spaces, Their Dual, and the Gray Image. IEEE Trans. Inform. Theory **64**(7), 5432–5440 (2018)
14. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Series A **40**, 90–107 (1985)
15. Kutsenko A.V.: The Hamming Distance Spectrum Between Self-Dual Maiorana–McFarland Bent Functions. Journal of Applied and Industrial Math. **12**(1), 112–125 (2018)
16. Kutsenko A.: Metrical properties of self-dual bent functions. Des. Codes Cryptogr. **88**(1), 201–222 (2020)
17. Kutsenko A.: The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun. **12**(5), 881–898 (2020)
18. Kutsenko A., Tokareva N.: Metrical properties of the set of bent functions in view of duality. Applied Discrete Math. №49, 18–34 (2020)
19. Luo G., Cao X., Mesnager S.: Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun. **11**(6), 1261–1273 (2019)
20. Sok L., Shi M., Solé. P.: Decomposition of bent generalized Boolean functions. https://arxiv.org/abs/1611.06357v1.

21. Martinsen T., Meidl W., Stănică P.: Partial spread and vectorial generalized bent functions. Des. Codes Cryptogr. **85**(1), 1–13 (2017)
22. McFarland R.L., A family of difference sets in non-cyclic groups. J. Combin. Theory. Ser. A **15**(1), 1–10 (1973)
23. Mesnager S.: Several New Infinite Families of Bent Functions and Their Duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014)
24. Mesnager S.: Bent Functions: Fundamentals and Results, 544 p., Springer, Berlin (2016)
25. Mesnager S., Tang C., Qi Y., Wang L., Wu B., Feng K.: Further Results on Generalized Bent Functions and Their Complete Characterization. IEEE Trans. Inform. Theory **64**(7), 5441–5452 (2018)
26. Paterson K.G. Generalized Reed–Muller Codes and Power Control in OFDM Modulation. IEEE Trans. Inform. Theory **46**(1), 104–120, (2000)
27. Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J.: Propagation characteristics of Boolean functions. In: Advances in Cryptology-EUROCRYPT. Lecture Notes in Computer Science, **473**, pp. 161–173. Springer, Berlin (1990)
28. Riera C., Stănică P., Gangopadhyay S.: Generalized bent Boolean functions and strongly regular Cayley graphs. Discrete Appl. Math. **283**, 367–374 (2020)
29. Rothaus O.S.: On bent functions. J. Combin. Theory. Ser. A **20**(3), 300–305 (1976)
30. Schmidt K.-U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inform. Theory **55**(4), 1824–1832 (2009)
31. Singh B.K.: On cross-correlation spectrum of generalized bent functions in generalized Maiorana–McFarland class. Information Sciences Letters **2**(3), 139–145 (2013)
32. Sok L., Shi M., Solé. P.: Classification and Construction of quaternary self-dual bent functions. Cryptogr. Commun. **10**(2), 277–289 (2018)
33. Solodovnikov V.I.: Bent functions from a finite Abelian group into a finite Abelian group. Discret. Math. Appl. **12**(2), 111–126 (2002)
34. Stănică P., Martinsen T., Gangopadhyay S., Singh B. K.: Bent and generalized bent Boolean functions. Des. Codes Cryptogr., **69**(1), 77–94 (2013)
35. Tang C., Xiang C., Qi Y., Feng K.: Complete Characterization of Generalized Bent and 2^k-Bent Boolean Functions. IEEE Trans. Inform. Theory **63**(7), 4668–4674 (2017)
36. Tokareva N.N.: Generalizations of bent functions — a survey. J. Appl. Ind. Math. **5**(1), 110–129 (2011)
37. Tokareva N.N.: On the number of bent functions from iterative constructions: lower bounds. Adv. Math. Commun. **5**(4), 609–621 (2011)
38. Tokareva N.: Bent Functions, Results and Applications to Cryptography, 230 p., Acad. Press. Elsevier (2015)
39. Wada T.: Characteristic bit sequences applicable to constant amplitude orthogonal multicode systems. IEICE Trans. Fundamentals **E83-A**(11), 2160–2164, (2000)

О НЕЛИНЕЙНОСТИ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ ОБОБЩЕННОЙ КОНСТРУКЦИЕЙ ДОББЕРТИНА

И. А. Сутормин[1]

[1] Институт математики им. С. Л. Соболева, пр. Академика Коптюга, 4. 630090 Новосибирск, Россия

E-mail: ivan.sutormin@gmail.com

Аннотация. В работе предложено обобщение конструкции Доббертина 1995 г. для сбалансированных булевых функций, обладающих высокой нелинейностью. Исследован спектр Уолша-Адамара предложенных функций. Доказана точная верхняя оценка на спектральный радиус (нижняя оценка нелинейности), и показан способ построения сбалансированной функции от $2n$ переменных со спектральным радиусом равным $2^n + 2^k R$ при помощи сбалансированной функции от $n - k$ переменных со спектральным радиусом равным R.

Ключевые слова: булевы функции, бент-функции, сбалансированность, нелинейность, спектральный радиус.

Введение

В различных криптографических алгоритмах часто используются булевы функции. Нелинейность — одно из основных для них свойств. Оно показывает, насколько хорошо функцию можно приблизить некоторой аффинной функцией, работать с которой значительно проще. Шифр может стать уязвимым к линейному криптоанализу при низкой нелинейности даже одной его части. Примером криптографического алгоритма, скомпрометированного своими компонентами с низкой нелинейностью, может послужить старый стандарт шифрования США — DES. Описание линейного криптоанализа для этого шифра можно найти в [1].

В случае четного числа переменных n известна максимальная возможная для булевой функции нелинейность: $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. Она достигается на функциях, называемых бент-функциями. Они были впервые описаны О. Ротхаусом [2] в 1976 г. В СССР в 60-е годы В. Елисеев и О. Степченков также занимались изучением этого класс функций. Подробную информацию о бент-функциях и других криптографических функциях можно найти в монографиях Н. Токаревой [3], S. Mesnager [4],

Работа выполнена в рамках государственного задания ИМ СО РАН (проект № 0314-2019-0017) при поддержке Российского Фонда Фундаментальных Исследований (проект 20–31–70043) и лаборатории криптографии JetBrains Research.

C. Carlet [5], T. Cusick , P. Stanica [6] и О. Логачева, А. Сальникова, С. Смышляева, В. Ященко [7].

В практических целях также часто требуется, чтобы функция была сбалансированной – принимала значения 0 и 1 одинаково часто. Идеально было бы использовать сбалансированную функцию с максимальной возможной нелинейностью, но бент-функции не сбалансированы. Для максимального значения нелинейности сбалансированных функций существует асимптотическая оценка [8], но точное значение неизвестно. Наилучшие нижние оценки этого значения получены как следствие конкретных конструкций сбалансированных функций [9–14].

Одна из таких конструкций, предложенная в 1995 г. Х. Доббертином [15] , основана на модификации нормальных бент-функций — функций от $2n$ переменных, постоянных на некотором аффинном подпространстве L размерности n. Спектральный радиус R_f — один из возможных параметров, через который можно выразить нелинейность функции: $N_f = 2^{n-1} - \frac{R_f}{2}$, именно его для этой конструкции удобно оценивать. Суть конструкции заключается в замене значений бент-функции на подпространстве L значениями сбалансированной функции θ от n переменных. У сбалансированной функции Θ, имеющей конструкцию Доббертина, спектральный радиус равен $R_\Theta = 2^n + R_\theta$, а нелинейность, соответственно, $N_\Theta = 2^{2n-1} - 2^{n-1} - \frac{R_\theta}{2}$. Также в [15] была сформулирована не опровергнутая до сих пор гипотеза о несуществовании сбалансированных функций с нелинейностью выше, чем можно получить при помощи этой конструкции. Простая структура конструкции Доббертина позволяет модифицировать ее для получения новых конструкций функций с хорошими криптографическими свойствами. Пример такого обобщения конструкции на случай векторных булевых функций можно найти в [16].

Данная работа посвящена новому обобщению конструкции Доббертина. Для этого используется класс бент-функций с близкими к нормальности свойствами. Функции, принадлежащие этому классу, постоянны на некотором подпространстве размерности 2^{n-k} и на $2^{2k} - 1$ его сдвигах, $0 \leqslant k \leqslant n-2$. С их помощью в работе построено обобщение конструкции Доббертина. Результатом работы является оценка спектрального радиуса для полученой сбалансированной функции Θ от $2n$ переменных:

$$R_\Theta \leqslant 2^n + \sum_{y \in I_0 \cup I_1} R_{\theta_y},$$

здесь θ_y — набор 2^{2k} произвольных сбалансированных функций от $n-k$ переменных, требуемых для конструкции. Также доказанно, что неравенство в этой оценке достигается при “неудачном” выборе θ_y, и найден набор функций для которого оценка спектрального радиуса принимает

вид

$$R_\Theta = 2^n + 2^k R_\theta,$$

где θ — произвольная сбалансированная функция от $n-k$ переменных, по которой определяются все θ_y. К сожалению, наилучший результат в данной оценке достигается при $k = 0$, то есть в случае, описанном Доббертином.

1. Определения

Введем необходимые определения и обозначения. Обозначим через $\mathbb{F}_2^n$ векторное пространство размерности n над полем из двух элементов $\mathbb{F}_2$. Далее, при работе с элементами $\mathbb{F}_2^n$, знаком $+$ будем обозначать покомпонентное сложение по модулю 2. Нулевой вектор будет обозначаться $\mathbf{0}$. Для двух двоичных векторов x, y введем обозначение $\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$. Функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2$ называется *булевой функцией*. *Расстоянием Хэмминга* между двумя булевыми функциями называется количество аргументов, на которых их значения отличаются. Расстояние Хэмминга от функции до класса функций — минимальное из расстояний Хэмминга от нее до одного из представителей этого класса. *Аффинная функция* — функция вида $\langle a, x\rangle + c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$. Функция называется *сбалансированной*, если она принимает значения 0 и 1 одинаково часто.

Преобразование Уолша-Адамара $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ для булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ определяется как

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle x,a\rangle}.$$

Спектральным радиусом булевой функции f называется

$$R_f = \max_{a \in \mathbb{F}_2^n} |W_f(a)|.$$

Нелинейностью — расстояние Хэмминга от функции f до класса аффинных функций. Она равна

$$N_f = 2^{n-1} - \frac{R_f}{2}.$$

Бент-функции — функции от n переменных, все коэффициенты Уолша-Адамара которых равны $\pm 2^{n/2}$. Они существуют только при четном n. На бент-функциях достигается максимальная возможная нелинейность. Функция $\widetilde{f}$, заданная равенством

$$W_f(y) = 2^{\frac{n}{2}} (-1)^{\widetilde{f}(y)},$$

называется *дуальной* к бент-функции f. Известно, что такая функция также будет являться бент-функцией.

Булевы функции f и g от n переменных *аффинно эквивалентны*, если для всех x выполнено $g(x) = f(Ax + b)$, где A — невырожденная двоичная матрица размера $n \times n$, а b — двоичный вектор размерности n. Известно, что аффинная эквивалентность сохраняет нелинейность и сбалансированность булевых функций. Непустое множество $M \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых $x, y \in M$ выполнено $x + y \in M$. Сдвиги элементов $x \in M$ на постоянную $a \in \mathbb{F}_2^n$ — всевозможные суммы вида $a + x$, образуют *аффинное подпространство* той же размерности.

Булева функция от $2n$ переменных называется *нормальной*, если она постоянна на некотором аффинном подпространстве L размерности n. Известно (см. [15]), что любая такая бент-функция аффинно эквивалентна функции $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, постоянной на $L = \{(x, \mathbf{0}) \mid x \in \mathbb{F}_2^n\}$ и равной некоторой сбалансированной $f_y : \mathbb{F}_2^n \to \mathbb{F}_2$ на $\{(x, y) \mid x \in \mathbb{F}_2^n\}$ где $y \in \mathbb{F}_2^n$, $y \neq \mathbf{0}$.

2. Конструкция Доббертина

Идея конструкции Доббертина для высоконелинейных сбалансированных функций заключается в замене значений нормальной бент-функции f от $2n$ переменных на всем подпространстве L на значения некоторой сбалансированной $\theta : \mathbb{F}_2^n \to \mathbb{F}_2$. Результатом такой замены будет функция

$$\Theta(x, y) = \begin{cases} \theta(x), & \text{если } y = \mathbf{0}, \\ f(x, y), & \text{иначе.} \end{cases}$$

Получившаяся функция — сбалансирована, ее коэффициенты Уолша-Адамара вычисляются по формуле:

$$W_\Theta(a, b) = \begin{cases} 0, & \text{если } a = \mathbf{0}, \\ W_f(a, b) + W_{\theta(a)}, & \text{иначе.} \end{cases}$$

Спектральный радиус функции Θ выражается через спектральный радиус функции θ:

$$R_\Theta = 2^n + R_\theta.$$

Это позволяет оценить минимальный возможный спектральный радиус сбалансированной функции от $2n$ переменных через спектральный радиус сбалансированной функции от n переменных:

$$RB(2n) \leqslant 2^n + RB(n).$$

Здесь $RB(n) = \min\{R_f \mid f : \mathbb{F}_2^n \to \mathbb{F}_2, f \text{ — сбалансированная}\}$. В [15] также была сформулирована не опровергнутая до сих пор гипотеза о несуществовании сбалансированных функций с нелинейностью выше, чем можно получить при помощи этой конструкции.

3. Обобщение конструкции Доббертина

Мы рассматриваем обобщение конструкции Доббертина, использующее функции с близкими к нормальности свойствами, а именно бент-функции от $2n$ переменных, принимающие постоянное значение на 2^{2k} сдвигах некоторого подпространства L размерности $n-k$, здесь $0 \leqslant k \leqslant n-2$. Так как аффинная эквивалентность сохраняет нелинейность и сбалансированность, мы можем без ограничения общности рассматривать такую бент-функцию в виде $f : \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{n+k} \to \mathbb{F}_2$, для которой существуют подмножества $I_0, I_1 \subset \mathbb{F}_2^{n+k}$, мощности $|I_0| = 2^{2k-1} + 2^{k-1}$, $|I_1| = 2^{2k-1} - 2^{k-1}$, для которых справедливо

$$\begin{array}{l} f(x,y) = 0, \quad \text{при } y \in I_0, \\ f(x,y) = 1, \quad \text{при } y \in I_1. \end{array} \tag{1}$$

Из [18] (Theorem 2.2) и [17] (Proposition 7) известно, что тогда f сбалансированна при любом фиксированном $y \notin I_0 \cup I_1$. Отметим, что $||I_0| - |I_1|| = 2^k$ легко следует из максимальной нелинейности бент-функций, а при прибавлении к такой функции тождественной единицы мы получим бент-функцию, равную еденице на $2^{2k-1} + 2^{k-1}$ сдвигах L и нулю на $2^{2k-1} - 2^{k-1}$ сдвигах. Все приведенные далее утверждения для функций вида (1) верны и для их отрицания.

Представление (1) прямо связано с конструкцией вида $\widetilde{f} + Ind_{L^\perp}$ [17–19].

В работе [20] описано представление бент-функций в виде линейного разветвления:

$$f(x,y) = \langle \Phi(y), x \rangle + \psi(y).$$

Необходимым условием для того, чтобы f была бент-функцией является условие на функцию $\Phi : \mathbb{F}_2^{n+k} \to \mathbb{F}_2^{n-k}$:

$$\forall \alpha \in \mathbb{F}_2^{n-k} \ |\Phi^{-1}(\alpha)| = 2^{2k}.$$

То есть f должна быть постоянна ровно на 2^{2k} различных сдвигах $L = \left\{(x, \mathbf{0}) \mid x \in \mathbb{F}_2^{n-k}\right\}$. Любая такая функция имеет вид (1).

Используя бент-функцию $f(x,y)$, имеющую представление (1), и набор из 2^{2k} произвольных сбалансированных функций $\theta_y : \mathbb{F}_2^{n-k} \to \mathbb{F}_2$, можно построить сбалансированную функцию $\Theta : \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{n+k} \to \mathbb{F}_2$, имеющую конструкцию, подобную конструкции высоконелинейных сбалансированных функций Доббертина:

$$\Theta(x,y) = \begin{cases} \theta_y(x), & \text{при } y \in I_0 \cup I_1, \\ f(x,y), & \text{иначе.} \end{cases}$$

Несложно заметить, что при $k = 0$ описанная конструкция полностью совпадает с конструкцией Доббертина.

4. Свойства спектра Уолша-Адамара используемых бент-функций

Установим несколько полезных свойств спектра Уолша-Адамара функций вида (1).

Лемма 1. *Пусть f — функция вида (1). Тогда для любого $b \in \mathbb{F}_2^{n+k}$ выполнено*

$$W_f(\mathbf{0}, b) = 2^{n-k}\left(\sum_{y\in I_0}(-1)^{\langle b,y\rangle} - \sum_{y\in I_1}(-1)^{\langle b,y\rangle}\right).$$

Доказательство.

$$W_f(\mathbf{0}, b) = \sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{f(x,y)+\langle b,y\rangle}$$

$$= \sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y\rangle}\left(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\right)$$

$$= \sum_{y\in I_0}(-1)^{\langle b,y\rangle}\left(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\right) + \sum_{y\in I_1}(-1)^{\langle b,y\rangle}\left(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\right)$$

$$+ \sum_{y\notin I_0\cup I_1}(-1)^{\langle b,y\rangle}\left(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\right) = \sum_{y\in I_0}(-1)^{\langle b,y\rangle}\cdot 2^{n-k}$$

$$- \sum_{y\in I_1}(-1)^{\langle b,y\rangle}\cdot 2^{n-k} + \sum_{y\notin I_0\cup I_1}(-1)^{\langle b,y\rangle}\left(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\right).$$

Так как f сбалансирована при $y \notin I_0\cup I_1$, сумма $\sum\limits_x(-1)^{f(x,y)}$ в последнем слагаемом равна 0 для любого y. Лемма 1 доказана.

В общем случае поиск подходящих подмножеств I_0 и I_1, для которых f — бент-функция, может быть очень сложной задачей. Поэтому интересным следствием Леммы 1 является необходимый признак их выбора.

Следствие 1. *Для того, чтобы функция вида (1) являлась бент-функцией необходимо, чтобы для подмножеств I_0 и I_1 и любого $b \in \mathbb{F}_2^{n+k}$ было выполнено*

$$\left|\sum_{y\in I_0}(-1)^{\langle b,y_i\rangle} - \sum_{y\in I_1}(-1)^{\langle b,y_i\rangle}\right| = 2^k.$$

Лемма 2. *Пусть f — функция вида (1). Тогда для любого $a \in \mathbb{F}_2^{n-k}$, $a \neq \mathbf{0}$ и $b \in \mathbb{F}_2^{n+k}$ выполнено*

$$W_f(a,b) = \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \notin I_0 \cup I_1} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}.$$

Доказательство.

$$W_f(a,b) = \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle} + \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_1} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle} + \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \notin I_0 \cup I_1} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}.$$

Преобразовывая

$$\sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle} = \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{\langle a,x\rangle+\langle b,y\rangle} = \left(\sum_{x \in \mathbb{F}_2^{n-k}} (-1)^{\langle a,x\rangle} \right) \left(\sum_{y \in I_0} (-1)^{\langle b,y\rangle} \right),$$

получаем множитель $\sum\limits_{x \in \mathbb{F}_2^{n-k}} (-1)^{\langle a,x\rangle}$, равный 0.

Аналогично можно показать, что

$$\sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_1} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle} = 0.$$

Лемма 2 доказана.

Лемма 3. *Пусть f — функция вида (1), тогда для любого $a \in \mathbb{F}_2^{n-k}$, $a \neq \mathbf{0}$ произведение $W_f(a,b) \cdot W_f(\mathbf{0},b)$ при различных значениях $b \in \mathbb{F}_2^{n+k}$ принимает как значение 2^{2n}, так и значение -2^{2n}.*

Доказательство. Воспользовавшись Леммами 1 и 2, преобразуем сумму:

$$2^{k-n}\sum_{b\in\mathbb{F}_2^{n+k}} W_f(a,b)\cdot W_f(\mathbf{0},b)$$

$$=\sum_{b\in\mathbb{F}_2^{n+k}}\left(\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}\right)\left(\sum_{z\in I_0}(-1)^{\langle b,z\rangle}-\sum_{z\in I_1}(-1)^{\langle b,z\rangle}\right)$$

$$=\sum_{b\in\mathbb{F}_2^{n+k}}\left(\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}\right)\left(\sum_{z\in I_0\cup I_1}(-1)^{f(x,z)+\langle b,z\rangle}\right)$$

$$=\sum_{b\in\mathbb{F}_2^{n+k}}\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}\sum_{z\in I_0\cup I_1}(-1)^{f(x,y)+f(x,z)+\langle a,x\rangle+\langle b,y+z\rangle}$$

$$=\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}\sum_{z\in I_0\cup I_1}(-1)^{f(x,y)+f(x,z)+\langle a,x\rangle}\left(\sum_{b\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y+z\rangle}\right).$$

Заметим, что $\sum\limits_{b\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y+z\rangle}=0$, так как $y\neq z$. Следовательно, вся сумма $\sum\limits_b W_f(a,b)\cdot W_f(\mathbf{0},b)=0$, что возможно только если произведения $W_f(a,b)\cdot W_f(\mathbf{0},b)$ меняют знак при изменении b. Лемма 3 доказана.

5. Свойства спектра Уолша-Адамара полученных сбалансированных функций

Теорема 1. *Функция, имеющая предложенную конструкцию, является сбалансированной функцией, и ее коэффициенты Уолша-Адамара вычисляются по формуле:*

$$W_\Theta(a,b)=\begin{cases}W_f(a,b)+\sum\limits_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a), & \text{если } a\neq\mathbf{0},\\ 0, & \text{иначе.}\end{cases}$$

Доказательство. Сбалансированность функции очевидна. Преобразуем ее выражение для спектра Уолша-Адамара:

$$W_\Theta(a,b)=\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{\Theta(x,y)+\langle a,x\rangle+\langle b,y\rangle}$$

$$=\sum_{y\in I_0\cup I_1}\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{\theta_y(x)+\langle a,x\rangle+\langle b,y\rangle}+\sum_{y\notin I_0\cup I_1}\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}.$$

Прибавим и отнимем от выражения $\sum\limits_{y\in I_0\cup I_1}\sum\limits_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}$. Тогда оно примет вид:

$$\sum_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a)+W_f(a,b)-\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{\langle a,x\rangle}\left(\sum_{y\in I_0}(-1)^{\langle b,y\rangle}-\sum_{y\in I_1}(-1)^{\langle b,y\rangle}\right).$$

Так как $\sum\limits_{x\in\mathbb{F}_2^{n-k}}(-1)^{\langle a,x\rangle}=0$ при $a\neq\mathbf{0}$ и $W_{\theta_y}(\mathbf{0})=0$, то

$$W_\Theta(a,b)=\begin{cases}W_f(a,b)+\sum\limits_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a), & a\neq\mathbf{0},\\ W_f(\mathbf{0},b)-2^{n-k}\left(\sum\limits_{y\in I_0}(-1)^{\langle a,x\rangle+\langle b,y\rangle}-\sum\limits_{y\in I_1}(-1)^{\langle a,x\rangle+\langle b,y\rangle}\right), & a=\mathbf{0}.\end{cases}$$

По Лемме 1 верно $W_f(\mathbf{0},b)=2^{n-k}\left(\sum\limits_{y\in I_0}(-1)^{\langle a,x\rangle+\langle b,y\rangle}-\sum\limits_{y\in I_1}(-1)^{\langle a,x\rangle+\langle b,y\rangle}\right)$.
Следовательно $W_\Theta(\mathbf{0},b)=0$. Теорема 1 доказана.

6. Оценки спектрального радиуса

Нас интересуют функции с высокой нелинейностью, а значит, с как можно более низким спектральным радиусом. Для функции, полученной при помощи конструкции Доббертина, $R_\Theta=2^n+R_\theta$. Из Теоремы 1 следует следующее утверждение о спектральном радиусе функции, имеющей предложенную конструкцию.

Следствие 2. *Для спектрального радиуса Θ верно:*

$$R_\Theta\leqslant 2^n+\sum_{y\in I_0\cup I_1}R_{\theta_y}.$$

При этом всегда можно выбрать θ_y, при которых оценка достигаеся.

Доказательство. Преобразуя выражение для коэффициентов Уолша-Адамара из Теоремы 1, можно получить оценку:

$$\begin{aligned}R_\Theta&=\max_{a,b}\Big|W_f(a,b)+\sum_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a)\Big|\\&\leqslant\max_{a,b}|W_f(a,b)|+\sum_{y\in I_0\cup I_1}\max_a|W_{\theta_i}(a)|=2^n+\sum_{y\in I_0\cup I_1}R_{\theta_y}.\end{aligned}$$

Так как f — бент-функция, все ее коэффициенты Уолша-Адамара равны $\pm2^n$. Зафиксируем некоторую сбалансированную функцию θ. Выберем

$a = \widetilde{a}$, для которого $|W_\theta(\widetilde{a})| = \max_a(|W_\theta(a)|) = R_\theta$. Тогда, взяв все θ_y равными θ, получим:

$$W_\Theta(\widetilde{a}, \mathbf{0}) = W_f(\widetilde{a}, \mathbf{0}) + \sum_{y \in I_0 \cup I_1} W_\theta(\widetilde{a}) = W_\theta(\widetilde{a}) + 2^{2k} W_\theta(\widetilde{a}),$$

а взяв все $\theta_y = \theta + 1$, аналогично получим $W_\Theta(\widetilde{a}, \mathbf{0}) = W_\theta(\widetilde{a}) - 2^{2k} W_\theta(\widetilde{a})$. Вне зависимости от знаков $W_\theta(\widetilde{a})$ и $W_\Theta(\widetilde{a}, \mathbf{0})$ в одном из этих случаев, знаки перед коэффициентами одинаковые, и в неравенстве $R_\Theta \leqslant 2^n + \sum_{i=1}^{2^{2k}} R_{\theta_y}$ достигается равенство. Следствие 2 доказано.

Возникает вопрос: можно ли более "удачным" выбором θ_y гарантировать спектральный радиус меньше, чем в худшем случае?

Теорема 2. *Пусть θ — сбалансированная функция от $n-k$ переменных, $\theta_y = \theta$ при $y \in I_0$, и $\theta_y = \theta \oplus 1$ при $y \in I_1$. Тогда*

$$R_\Theta = 2^n + 2^k R_\theta.$$

Доказательство. Преобразуем выражение коэффициентов Уолша-Адамара при $a \neq \mathbf{0}$ для такого выбора функций:

$$W_\Theta(a,b) = W_f(a,b) + \sum_{y \in I_0} (-1)^{\langle b,y \rangle} W_\theta(a) + \sum_{y \in I_1} (-1)^{\langle b,y \rangle} \big(-W_\theta(a)\big)$$

$$= W_f(a,b) + W_\theta(a) \left(\sum_{y \in I_0} (-1)^{\langle b,y \rangle} - \sum_{y \in I_1} (-1)^{\langle b,y \rangle} \right).$$

Тогда согласно Лемме 1

$$W_\Theta(a,b) = W_f(a,b) + W_\theta(a) \cdot 2^{k-n} W_f(\mathbf{0}, b).$$

По Лемме 3 произведение $W_f(a,b) \cdot W_f(\mathbf{0},b)$ для фиксированного $a \neq \mathbf{0}$ меняет знак при изменении значений b. Следовательно, для каждого ненулевого a существует b, для которого $W_f(a,b)$ и $W_f(\mathbf{0},b)$ имеют как одинаковые, так и разные знаки. Тогда, вне зависимости от $W_\theta(a)$, спектральный радиус Θ равен:

$$R_\Theta = \max_{a,b} |W_f(a,b) + \sum_{y \in I_0} (-1)^{\langle b,y \rangle} W_\theta(a) + \sum_{y \in I_1} (-1)^{\langle b,y \rangle} \big(- W_\theta(a)\big)|$$

$$= \max_{a \neq \mathbf{0}, b} |W_f(a,b) + W_\theta(a) \cdot 2^{k-n} W_f(0,b)| = 2^n + \max_{a \neq \mathbf{0}} |W_\theta(a)| \cdot 2^k.$$

Также $W_\theta(\mathbf{0}) = 0$, значит максимум на нем достигаться не может, и спектральный радиус равен:

$$R_\Theta = 2^n + 2^k \cdot R_\theta.$$

Теорема 2 доказана.

В работе [8] доказано, что

$$\lim_{m\to\infty} \frac{RB(m)}{2^{\frac{m}{2}}} = 1.$$

Взяв в качестве θ функцию с $R_\theta \approx 2^{\frac{n-k}{2}}$, получим, что спектральный радиус функции Θ из Теоремы 2 выражается следующим образом:

$$R_\Theta \approx 2^n + 2^k \cdot 2^{\frac{n-k}{2}} = 2^n + 2^{\frac{n+k}{2}}.$$

Видно, что наилучший результат достигается при $k = 0$, то есть в случае, описанном Доббертином.

7. Заключение

В работе построено обобщение конструкции Доббертина при помощи класса бент-функций с близкими к нормальности свойствами. Также были доказаны некоторые свойства спектра Уолша-Адамара для функций, принадлежащих этому классу, и найдена точная нижняя оценка их нелинейности. Однако максимальная возможная нелинейность для построенных таким образом функций остается неизвестной.

ЛИТЕРАТУРА

1. **Matsui M.** Linear cryptanalysis method for DES cipher. // Advances in Cryptology: CRYPTO '93. Heidelberg: Springer, 1994. P. 386–397. (Lect. Notes Comput. Sci.; Vol. 765).
2. **Rothaus O.** On «bent» functions // J. of Combinatorial Theory, Series A. 1976. Vol. 20, No. 3. P. 300–305.
3. **Tokareva N. N.** Bent Functions, Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 220 p.
4. **Mesnager S.** Binary bent functions: fundamentals and results. Heidelberg: Springer, 2016. 540 p.
5. **Carlet C.** Boolean functions for cryptography and error-correcting codes. // Boolean models and methods in math., comput. sci., and engineering, chapter 8. UK: Cambridge University Press, 2010. P. 257-397.
6. **Cusick T., Stanica P.** Cryptographic Boolean Functions and Applications. Acad. Press, Elsevier, 2009. 248 p.
7. **Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
8. **Schmidt K.** Asymptotically optimal Boolean functions // J. of Combinatorial Theory, Series A. 2019. Vol. 164. P. 50–59.
9. **Seberry J., Zhang X., Zheng Y.** Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics // Advances in Cryptology: CRYPTO '93. Springer-Verlag, 1994. P. 49–60. (Lect. Notes Comput. Sci.; Vol. 773).

10. **Carlet C.** On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities. // Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2006. Proc. (Las Vegas, NV, USA, February 20–24, 2006) Heidelberg: Springer, 2006. P 1–23. (Lect. Notes Comput. Sci.; Vol. 3857).
11. **Wang Q., Tan C. H.** Properties of a Family of Cryptographic Boolean Functions Sequences and Their Applications // SETA 2014: 8th Int. Conf. (Melbourne, VIC, Australia, November 24—28). P. 34–46, 2014.
12. **Tang D., Maitra S.** Construction of n-Variable ($n \equiv 2 \bmod 4$) BalancedBoolean Functions With Maximum Absolute Value in Autocorrelation Spectra $< 2^{\frac{n}{2}}$ // IEEE Transactions on Information Theory. 2018. Vol. 64, No. 1. P. 393—402.
13. **Kavut S., Maitra S., Tang D.** Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile // Designs Codes and Cryptography. 2019. Vol. 87. P. 261—276.
14. **Patterson N. J., Wiedemann D. H.** The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276 // IEEE Transactions on Information Theory. 1983. Vol. 29, No. 3. P 354–356.
15. **Dobbertin H.** Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption: Second Int. Workshop. Proc. (Leuven, Belgium, December 14—16, 1994). Heidelberg: Springer, 1995. P. 61—74. (Lect. Notes Comput. Sci.; Vol. 1008).
16. **Fomin D.** New classes of 8-bit permutations based on a butterfly structure // Math. Aspects of Cryptography. 2019. Vol. 10, No. 2. P. 169—180.
17. **Kolomeec N.** The graph of minimal distances of bent functions and its properties. // Designs, Codes and Cryptography. 2017. Vol. 85, No. 3. P. 395–410.
18. **Kolomeec N.** On properties of a bent function secondary construction // The 5th Int. Workshop on Boolean Functions and their Appl. (BFA-2020). (Loen, Norway, September 15–17, 2020). P. 23–26.
19. **Carlet C.** Two new classes of bent functions // Advances in Cryptology: CRYPTO '93. 1994. P. 77—101. (Lect. Notes Comput. Sci.; Vol. 765).
20. **Ященко В. В.** О критерии распространения для булевых функций и о бент-функциях. // Проблемы передачи информации. 1997. Т. 33, С. 75—86.

ЛИТЕРАТУРА

1. **Matsui M.** Linear cryptanalysis method for DES cipher. Advances in Cryptology, Eurocrypt 1993., Lecture Notes in Computer Science. V. 765, Springer-Verlag pp. 386–397, 1994.
2. **Rothaus O.** On «bent» functions // Journal of Combinatorial Theory Series A. V. 20. No. 3. pp. 300–305. 1976.
3. **Tokareva N. N.** Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
4. **Mesnager S.** Binary bent functions: fundamentals and results. Springer Verlag, 2016.

5. **Carlet C.** Boolean functions for cryptography and error-correcting codes. In: Boolean models and methods in mathematics, computer science, and engineering, chap. 8. UK: Cambridge University Press; 2010. pp. 257-397.
6. **Cusick T.** Stanica P. Cryptographic Boolean Functions and Applications. Elsevier, 2009.
7. **Logachev O. A., Sal'nikov A. A., Smyshljaev S. V., Jashhenko V. V.** Boolean functions in coding theory and cryptology. 2-nd ed. MCCME, 2012. [Russian]
8. **Schmidt K.** Asymptotically optimal Boolean functions // Journal of Combinatorial Theory. Series A. V. 164 pp. 50–59, 2019
9. **Seberry J., Zhang X., Zheng Y.** Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics, Advances in Cryptology: CRYPTO '93, Lecture Notes in Computer Science V. 773, Springer-Verlag pp. 49–60, 1994.
10. **Carlet C.** On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities. In: Fossorier M.P.C., Imai H., Lin S., Poli A. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2006. Lecture Notes in Computer Science. V. 3857. Springer, Berlin, Heidelberg. pp 1–23. 2006.
11. **Wang Q., Tan C. H.** Properties of a Family of Cryptographic Boolean Functions Sequences and Their Applications, SETA 2014: 8th International Conference Melbourne, VIC, Australia, November 24–28, pp. 34–46, 2014.
12. **Tang D., Maitra S.** Construction of n-Variable ($n \equiv 2 \bmod 4$) BalancedBoolean Functions With Maximum Absolute Value in Autocorrelation Spectra $< 2^{\frac{n}{2}}$ // IEEE Transactions on Information Theory. V. 64. No. 1. pp. 393—402, 2018.
13. **Kavut S., Maitra S., Tang D.** Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile // Designs Codes and Cryptography. V. 87, pp. 261—276, 2019.
14. **Patterson N. J., Wiedemann D. H.** The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276 // IEEE Transactions on Information Theory, V. 29. No. 3. pp 354–356, 1983.
15. **Dobbertin H.** Construction of bent functions and balanced Boolean functions with high nonlinearity, Fast Software Encryption: Second International Workshop. Proceedings, Leuven, Belgium, December 14–16, 1994, Springer-Verlag pp. 61–74, 1995.
16. **Fomin D.** New classes of 8-bit permutations based on a butterfly structure // Mathematical Aspects of Cryptography, V. 10, Issue 2, pp. 169–180, 2019
17. **Kolomeec N.** The graph of minimal distances of bent functions and its properties. // Designs, Codes and Cryptography, V. 85. No. 3. pp. 395–410, 2017.
18. **Kolomeec N.** On properties of a bent function secondary construction // Conference abstracts The 5th International Workshop on Boolean Functions and their Applications (BFA-2020). Loen, Norway, September 15-17, pp. 23–26, 2020. Abstracts are available here `https://boolean.w.uib.no/files/2020/09/BFA_2020_abstracts_numbered.pdf`

19. Carlet C. Two new classes of bent functions // Lecture Notes in Computer Science V. 765. pp. 77—101, 1994.

20. Jashhenko V. V. On a propagation criteria for boolean functions and bent functions. // Problems of Information Transmission. V. 33, pp. 75—86, 1997. [Russian]

На правах рукописи

Куценко Александр Владимирович

САМОДУАЛЬНЫЕ БЕНТ-ФУНКЦИИ И ИХ МЕТРИЧЕСКИЕ СВОЙСТВА

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2020

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Новосибирский национальный исследовательский государственный университет».

Научный руководитель: кандидат физико-математических наук, с.н.с. **Токарева Наталья Николаевна**

Официальные оппоненты: **Фомичев Владимир Михайлович,** доктор физико-математических наук, профессор, Финансовый университет при Правительстве Российской Федерации, профессор.

Панкратова Ирина Анатольевна, кандидат физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет», заведующий лабораторией компьютерной криптографии.

Ведущая организация: Институт проблем информационной безопасности факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный университет имени М. В. Ломоносова».

Защита состоится 24 марта 2021 г. в 16 ч. 00 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академи наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук и на сайте http://math.nsc.ru.

Автореферат разослан «__» _____ 2021 г.

Ученый секретарь
диссертационного совета
Д 003.015.01,
д.ф.-м.н. Шамардин Юрий Владиславович

Общая характеристика работы

Актуальность темы. Настоящая работа посвящена булевым функциям от чётного числа переменных, обладающим свойством максимальной нелинейности — бент-функциям. Данный класс функций имеет многочисленные приложения в таких областях как криптография, комбинаторика, теория кодирования. Исследуется отображение, которое каждой бент-функции ставит в соответствие дуальную к ней бент-функцию. Изучаются метрические, а также комбинаторные свойства неподвижных точек данного отображения — самодуальных бент-функций.

Приведём необходимые определения.

Пусть $\mathbb{F}_2^n$ — пространство двоичных векторов с n координатами. *Весом Хэмминга* вектора $x \in \mathbb{F}_2^n$ называется количество его координат, отличных от 0. *Расстоянием Хэмминга* $\operatorname{dist}(x,y)$ между двумя векторами $x,y \in \mathbb{F}_2^n$ называется количество координат, в которых эти векторы различаются. Легко видеть, что расстояние Хэмминга является метрикой на $\mathbb{F}_2^n$. *Булевой функцией* от n переменных называется произвольное отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. Множество булевых функций от n переменных обозначается через $\mathcal{F}_n$. *Характеристическим вектором* (характеристической последовательностью) булевой функции $f \in \mathcal{F}_n$ называется вектор

$$F \equiv (-1)^f = \left((-1)^{f_0},(-1)^{f_1},\ldots,(-1)^{f_{2^n-1}}\right) \in \{\pm 1\}^{2^n},$$

где $(f_0,f_1,\ldots,f_{2^n-1}) \in \mathbb{F}_2^{2^n}$ — вектор значений (таблица истинности) функции f. *Весом Хэмминга* $\operatorname{wt}(f)$ булевой функции f называется вес Хэмминга её вектора значений. *Расстояние Хэмминга* $\operatorname{dist}(f,g)$ между двумя булевыми функциями $f,g \in \mathcal{F}_n$ определяется как число векторов пространства $\mathbb{F}_2^n$, на которых данные функции принимают различные значения. Символом $\oplus$ обозначим сложение по модулю 2. Для пары векторов $x,y \in \mathbb{F}_2^n$ через $\langle x,y\rangle$ обозначается значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша—Адамара* булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x,y\rangle}, \ \ y \in \mathbb{F}_2^n.$$

Нелинейностью булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от функции f до множества всех аффинных булевых функций от n переменных — мера удалённости функции от множества аффинных и, как следствие, линейных булевых функций. Соответственно, использование функций,

обладающих высокой нелинейностью, в качестве компонент блочных и поточных шифров увеличивает стойкость к линейному криптоанализу[1] — одному из основных статистических видов криптоанализа блочных шифров. Например, функции, обладающие максимально возможной нелинейностью, были использованы в качестве составных элементов в поточном шифре Grain (2004) и блочном шифре CAST (1997).

Булева функция f от чётного числа переменных n называется **бент-функцией**, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. В случае чётного n на бент-функциях, и только на них, достигается максимальное значение нелинейности $2^{n-1} - 2^{n/2-1}$. Множество бент-функций от n переменных обозначается через $\mathcal{B}_n$. Отметим, что для случая нечётного числа переменных нахождение максимального значения нелинейности является известной открытой проблемой теории кодирования, связанной с поиском радиуса покрытия кода Рида — Маллера первого порядка. Термин «бент-функция» предложил американский математик O. S. Rothaus, который исследовал данные функции в 60х годах прошлого века, при этом первая работа по данной теме была опубликована в 1976 году[2]. Тем не менее, известно[3], что булевы функции, обладающие аналогичными свойствами, в это же время также исследовались в Советском Союзе — математиками В. А. Елисеевым и О. П. Степченковым, которые использовали термин «минимальная функция».

Для более детального знакомства со свойством нелинейности, а также другими важными криптографическими свойствами можно порекомендовать книги О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко[4] и T. W, Cusick, P. Stănică[5], а также книгу C. Carlet[6] . Описанию известных результатов и открытых вопросов, связанных с бент-функциями и их обобщениями, посвящены монографии Н. Н. Токаревой[7] и S. Mesnager[8].

---

[1] M. Matsui. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology — EUROCRYPT '93. 1994. P. 386—397. Part of the Lecture Notes in Computer Science book series (LNCS, volume 765).

[2] O. S. Rothaus. On "bent" functions // J. Combin. Theory, Ser. A. 1976. Vol. 20, no. 3. P. 300—305.

[3] А. С. Кузьмин, В. Т. Марков, А. А. Нечаев, В. Шишкин, А. Б. Шишков. Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информации. 2008. Т. 44, № 1. С. 15—37.

[4] О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Ященко. Булевы функции в теории кодирования и криптологии. ЛЕНАНД, 2015. 576 с.

[5] T. W. Cusick, P. Stănică. Cryptographic Boolean Functions and Applications. 2nd ed. Acad. Press, 2017. 288 p.

[6] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Cambridge Univ. Press, 2020. 620 p.

[7] N. Tokareva. Bent Functions: Results and Applications to Cryptography. Acad. Press, 2015. 220 p.

[8] S. Mesnager. Bent functions: Fundamentals and results. Springer, 2016. 544 p.

Всюду далее считается, что n — чётное натуральное число. Для каждой бент-функции $f \in \mathcal{B}_n$ соотношением

$$W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}, \ y \in \mathbb{F}_2^n$$

единственным образом определяется булева функция $\widetilde{f}$ от того же числа переменных. Функция $\widetilde{f}$ называется **дуальной** к бент-функции f. Булева функция $\widetilde{f}$ также является бент-функцией, кроме того, для неё справедливо соотношение $\widetilde{\widetilde{f}} = f$. Таким образом, множество бент-функций от n переменных, отличных от своих дуальных, разбивается на пары $(f, \widetilde{f})$, каждая из которых состоит из бент-функции и дуальной к ней. Функцию $\widetilde{f}$ впервые в своих работах отметили O. S. Rothaus и J. F. Dillon[9] в 70х годах прошлого века.

Матрицей Сильвестра — Адамара называется квадратная матрица порядка 2^n, обозначаемая H_n, определяемая следующими рекуррентными соотношениями:

$$H_0 = (1), \qquad H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, n \geqslant 2.$$

Данная матрица тесно связана с дискретным преобразованием Уолша и имеет различные приложения в комбинаторике и квантовой информатике. Нетрудно видеть, что она является симметричной, кроме того, она позволяет получить описание преобразования Уолша — Адамара булевой функции в матрично-векторной форме[10]. В терминах характеристических векторов и матрицы Сильвестра — Адамара бент-функцию можно определить следующим образом: пусть n — чётное число, тогда $f \in \mathcal{F}_n$ — бент-функция, если $H_n(-1)^f \in \{\pm 2^{n/2}\}^{2^n}$. Характеристический вектор дуальной функции $\widetilde{f}$ однозначным образом находится из условия

$$H_n(-1)^f = 2^{n/2}(-1)^{\widetilde{f}}.$$

Отображение дуальности определяется на множестве бент-функций от n переменных и действует по правилу $f \to \widetilde{f}$. В терминах характеристических векторов оно имеет следующую эквивалентную форму: $(-1)^f \to (-1)^{\widetilde{f}}$. Известно, что оно сохраняет расстояние Хэмминга, то есть является изометричным отображением множества бент-функций[11]. Стоит отметить, что на данный момент отображение дуальности является единственным известным отображением, которое обладает таким свойством и при этом не расширяется до изометрии на множестве всех булевых функций от n переменных. Также

[9] J. F. Dillon. Elementary Hadamard difference sets : PhD thesis. Univ. of Maryland, 1974.

[10] В. Н. Сачков. Введение в комбинаторные методы дискретной математики. 2-е изд. М. : МЦНМО, 2004. 424 с.

[11] C. Carlet. Two New Classes of Bent Functions // Advances in Cryptology — EUROCRYPT '93. 1994. P. 77–101. Part of the Lecture Notes in Computer Science book series (LNCS, volume 765).

заметим, что отображение, действующее из множества характеристических векторов булевых функций от n переменных в пространство $\mathbb{R}^{2^n}$ по правилу

$$(-1)^f \longrightarrow \frac{1}{2^{n/2}} H_n (-1)^f, \ \ f \in \mathcal{F}_n,$$

обладает тем свойством, что бент-функции от n переменных являются в точности теми функциями, образ характеристических векторов которых снова является характеристическим вектором булевой функции.

Исследованию того, как изменяются основные характеристики бент-функции под действием отображения дуальности, а также изучению его действия на конкретные классы бент-функций, посвящено большое количество работ. В частности, в работе[12] получено соотношение, связывающее алгебраические степени бент-функции и дуальной к ней. В статье[13] доказано, что бент-функция разложима в сумму двух бент-функций в том и только в том случае, когда таким свойством обладает дуальная к ней. Связь между коэффициентами числовой нормальной формы (Numerical Normal Form) бент-функции и дуальной к ней изучалась в работах[14,15]. Хорошо известно, что отображение дуальности сохраняет расширенную аффинную эквивалентность: дуальные расширенно аффинно эквивалентных бент-функций также расширенно аффинно эквивалентны. Действие отображения дуальности на некоторые классы бент-функций, например, класс Мэйорана — МакФарланда и класс Диллона $\mathcal{PS}_{ap}$, может быть описано относительно просто, в то время как во многих других случаях нахождение дуальной функции и исследование её свойств является нетривиальной задачей. Этим вопросам посвящены, например, работы[16,17], в которых изучалось действие отображения дуальности на бент-функции из класса Нихо. Было показано, что дуальные к ним функции уже не принадлежат данному классу. Функции, являющиеся дуальными к бент-функциям из некоторых других мономиальных классов, изучались в работах[18,19,20]. В частности,

[12] X.-D. Hou. New constructions of bent functions // J. Combin. Inform. System Sci. 2000. Vol. 25. P. 173—189.

[13] Н. Н. Токарева. О разложении дуальной бент-функции в сумму двух бент-функций // Прикл. дискрет. матем. 2014. 4(26). С. 59—61.

[14] C. Carlet, P. Guillot. A new representation of Boolean functions // Proceedings of AAECC'13. 1999. P. 94—103. Part of the Lecture Notes in Computer Science book series (LNCS, volume 1719).

[15] X.-D. Hou, P. Langevin. Results on bent functions // J. Comb. Theory Ser. A. 1997. Vol. 80. P. 232—246.

[16] C. Carlet, T. Helleseth, A. Kholosha, S. Mesnager. On the dual of bent functions with 2^r Niho exponents // 2011 IEEE International Symposium on Information Theory (ISIT). 2011. P. 703—707.

[17] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, S. Mesnager. Further Results on Niho Bent Functions // IEEE Trans. Inform. Theory. 2012. Vol. 58, no. 11. P. 6979—6985.

[18] N. G. Leander. Monomial bent functions // IEEE Trans. Inform. Theory. 2006. Vol. 52, no. 2. P. 738—743.

[19] P. Langevin, G. Leander. Monomial bent functions and Stickelberger's theorem // Finite Fields Appl. 2008. Vol. 14, no. 3. P. 727—742.

[20] P. Langevin, G. Leander, G. McGuire. Kasami bent function are not equivalent to their duals // Finite Fields and Applications: Eighth International Conference on Finite Fields and Applications. Contemp. Math. Vol. 461. 2008. P. 187—197.

было получено, что дуальные функции бент-функций Касами не являются мономиальными, тогда как дуальная функция (квадратичной) бент-функции с показателем Голда является квадратичной.

Важной метрической характеристикой отображения дуальности является расстояние Хэмминга между бент-функцией и дуальной к ней — количество позиций, в которых меняются вектор значений и характеристический вектор бент-функции под действием данного отображения. Величина $\mathrm{dist}(f,\widetilde{f})$ полностью характеризуется *отношением Рэлея булевой функции*. Для $f \in \mathcal{F}_n$ отношением Рэлея называется величина

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle}.$$

Описание всех бент-функций, находящихся на определённом расстоянии от своей дуальной функции или, другими словами, классификация бент-функций в терминах значений отношения Рэлея, является открытой проблемой. В работе[21] можно найти характеризацию для бент-функций от малого числа переменных, а также ряд свойств отношения Рэлея и его вид для некоторых известных классов бент-функций.

Бент-функция f называется **самодуальной**, если она совпадает со своей дуальной, то есть $f = \widetilde{f}$. Таким образом, самодуальные бент-функции являются *неподвижными точками* отображения дуальности. Бент-функция f называется **анти-самодуальной**, если она совпадает с отрицанием свой дуальной, то есть $f = \widetilde{f} \oplus 1$. Понятия *дуальной бент-* (dual bent) и *анти-дуальной бент-* (anti-dual bent) функций, по существу, аналоги определений самодуальной и анти-самодуальной бент-функций, соответственно, предложили B. Preneel и др. в работе[22]. Более общее понятие *самодуальной бент-функции на конечной абелевой группе* было введено О. А. Логачевым, А. А. Сальниковым, В. В. Ященко[23].

Из определения самодуальности следует, что характеристический вектор самодуальной бент-функции является собственным вектором матрицы H_n, соответствующим собственному числу $2^{n/2}$. В свою очередь, характеристический вектор анти-самодуальной бент-функции является собственным вектором, соответствующим собственному числу $\left(-2^{n/2}\right)$. Таким образом, вопрос характеризации самодуальных и анти-самодуальных бент-функций тесно связан с перечислением и исследованием свойств собственных векторов матрицы Сильвестра — Адамара, координаты которых суть числа ± 1.

[21] L. E. Danielsen, M. G. Parker, P. Solé. The Rayleigh quotient of bent functions // Cryptography and Coding. 2009. P. 418—432. Part of the Lecture Notes in Computer Science book series (LNCS, volume 5921).

[22] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle. Propagation characteristics of Boolean functions // Advances in Cryptology — EUROCRYPT '90. 1991. P. 161—173. Part of the Lecture Notes in Computer Science book series (LNCS, volume 473).

[23] О. А. Логачев, А. А. Сальников, В. В. Ященко. Бент-функции на конечной абелевой группе // Дискрет. матем. 1997. Т. 9, № 4. С. 3—20.

Стоит отметить, что в случае чётного числа переменных на (анти-)самодуальных бент-функциях, и только на них, достигается максимальное (соответственно, минимальное) значение отношения Рэлея булевой функции. Для случая нечётного числа переменных поиск максимального значения отношения Рэлея булевой функции является открытым вопросом, что позволяет говорить о некоторой аналогии с известной проблемой поиска максимального значения нелинейности булевой функции для случая нечётного числа переменных.

Открытой проблемой является полная характеризация и описание классов эквивалентности самодуальных и анти-самодуальных бент-функций. Этому и другим вопросам, связанным с самодуальными и анти-самодуальными бент-функциями, посвящён ряд работ российских и зарубежных авторов. В частности, данные классы бент-функций были отражены в работах таких исследователей, как C. Carlet, X.-D. Hou, P. Solé, В. А. Зиновьев, J. Rifà, S. Mesnager, T. Helleseth, B. Preneel и др.

В частности, в работе C. Carlet и др.[24] был получен ряд конструкций, а также описаны некоторые свойства самодуальных бент-функций. Представлена классификация самодуальных бент-функции от $2,4,6$ переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность. Показано, что расстояние Хэмминга между самодуальной и анти-самодуальной бент-функциями от n переменных равно 2^{n-1}. Рассмотрены свойства характеристического вектора самодуальной бент-функции. В работе X.-D. Hou[25] приведена классификация всех квадратичных самодуальных бент-функций относительно действия ортогональной группы, основанная, в том числе, на классификации инволютивных симплектических матриц. Классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность, можно найти в статье[26]. Верхняя оценка количества самодуальных бент-функций, полученная на основе их взаимосвязи с формально самодуальными бент-функциями, представлена в работе[27]. В статьях S. Mesnager[28], а также J. Rifà и В. А. Зиновьева[29] предложены алгебраические и комбинаторные конструкции самодуальных бент-функций. Алгебраическим

[24] C. Carlet, L. E. Danielsen, M. G. Parker, P. Solé. Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. Vol. 1. P. 384—399.

[25] X.-D. Hou. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. Vol. 63, no. 2. P. 183—198.

[26] T. Feulner, L. Sok, P. Solé, A. Wassermann. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. Vol. 68, no. 1. P. 395—406.

[27] J. Y. Hyun, H. Lee, Y. Lee. MacWilliams duality and Gleason-type theorem on self-dual bent functions // Des. Codes Cryptogr. 2012. Vol. 63, no. 3. P. 295—304.

[28] S. Mesnager. Several New Infinite Families of Bent Functions and Their Duals // IEEE Trans. Inform. Theory. 2014. Vol. 60, no. 7. P. 4397—4407.

[29] J. Rifà, V. A. Zinoviev. On binary quadratic symmetric bent and almost bent functions. arXiv:1211.5257v3.

конструкциям бент-функций и самодуальных бент-функций, основанным на использовании инволюций, посвящены работы[30,31].

Целью данной работы является исследование взаимосвязи между свойствами отображения дуальности и его неподвижных точек — самодуальных бент-функций, а также изучение метрических свойств самодуальных бент-функций. В работе доказано, что множества характеристических векторов самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, которая определяет отображение дуальности в терминах характеристических векторов. Доказано, что не существует изометричного отображения множества всех булевых функций от n переменных в себя, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней функцию. Таким образом, отображение дуальности не может быть доопределено до изометричного отображения всех булевых функций от n переменных в себя. Полностью описана группа автоморфизмов множества самодуальных бент-функций от $n \geqslant 4$ переменных. Доказано, что изометричное отображение всех булевых функций от $n \geqslant 4$ переменных в себя сохраняет расстояние между каждой бент-функцией и дуальной к ней, если и только если оно является элементом группы автоморфизмов множества самодуальных бент-функций от n переменных. Данные результаты позволяют говорить о тесной связи свойств отображения дуальности и метрических свойств самодуальных бент-функций. Исследованы метрические свойства самодуальных бент-функций. Получена итеративная конструкция самодуальных бент-функций, позволяющая по паре из произвольной самодуальной и анти-самодуальной бент-функций от n переменных построить 4 самодуальных бент-функции от $n + 2$ переменных.

Основные положения, выносимые на защиту:

1. Доказано, что множества характеристических векторов самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.
2. Описаны группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных.
3. Установлено, что группа автоморфизмов множества самодуальных бент-функций совпадает с множеством изометричных отображений всех булевых функций от $n \geqslant 4$ переменных в себя, сохраняющих расстояние Хэмминга между каждой бент-функцией и дуальной к ней.
4. Доказано, что множество булевых функций, максимально удалённых от множества самодуальных (анти-самодуальных) бент-функций

[30] R. S. Coulter, S. Mesnager. Bent Functions From Involutions Over $\mathbb{F}_{2^n}$ // IEEE Trans. Inform. Theory. 2018. Vol. 64, no. 4. P. 2979—2986.

[31] G. Luo, X. Cao, S. Mesnager. Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. 2019. Vol. 11, no. 6. P. 1261—1273.

от $n \geqslant 4$ переменных, совпадает с множеством анти-самодуальных (самодуальных) бент-функций от n переменных. Таким образом, доказана метрическая регулярность множества (анти-)самодуальных бент-функций от n переменных.

5. Найден полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана – МакФарланда.

Научная новизна и значимость: Работа носит теоретический характер. Все результаты диссертации являются новыми и снабжены полными доказательствами. Полученные результаты могут быть использованы для дальнейшего изучения свойств отображения дуальности, а также самодуальных и анти-самодуальных бент-функций. Например, для поиска спектра расстояний Хэмминга между самодуальными бент-функциями, классификации самодуальных бент-функций относительно изометричных отображений, сохраняющих самодуальность.

Методология и методы исследования. В диссертации используются комбинаторные методы и методы дискретного анализа, аппарат линейной алгебры. Для изучения метрических свойств самодуальных бент-функций используется соответствие между характеристическими векторами самодуальных и анти-самодуальных бент-функций и собственными векторами матрицы Сильвестра – Адамара.

Апробация работы. Результаты работы докладывались на следующих конференциях и семинарах: Международная конференция «Sequences and Their Applications (SETA 2020)» (г. Санкт-Петербург, 2020 г.), Международная конференция «Boolean Functions and their Applications (BFA 2019, BFA 2020)» (Италия, г. Флоренция, 2019 г.; Норвегия, г. Лоен, 2020 г.), Симпозиум «Современные тенденции в криптографии (CTCrypt 2019, CTCrypt 2020)» (Калининградская область, г. Светлогорск, 2019 г.; Московская область, 2020 г.), Международный семинар «Дискретная математика и ее приложения» (Россия, г. Москва, 2016 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография (SIBECRYPT)» (г. Новосибирск, 2015 г.; г. Новосибирск, 2016 г.; г. Красноярск, 2017 г.; г. Абакан, 2018 г.; г. Томск, 2019 г.), семинар исследовательского центра Selmer Center in Secure Communication (Норвегия, г. Берген, февраль 2020 г.), семинары «Дискретный анализ», «Теория кодирования», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ, семинар отдела теоретической кибернетики ИМ СО РАН.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель работы.

Первая глава является обзором известных результатов по свойствам отображения дуальности, отношения Рэлея, а также самодуальным и анти-самодуальным бент-функциям. Приведены известные комбинаторные и алгебраические конструкции самодуальных и анти-самодуальных бент-функций, а также алгоритмы перечисления всех самодуальных и анти-самодуальных бент-функций от n переменных, степень которых не превосходит заранее фиксированного числа. Рассмотрены известные результаты по классификации самодуальных бент-функций от $n \leqslant 8$ переменных. Описана классификация квадратичных самодуальных бент-функций. Перечислены верхние оценки количества самодуальных бент-функций, а также нижние оценки, полученные на основе известных конструкций.

Через $\mathrm{SB}^+(n)$ обозначим множество самодуальных бент-функций от n переменных, а через $\mathrm{SB}^-(n)$ — множество анти-самодуальных бент-функций от n переменных.

Обзор главы 1 опубликован в [4].

Во **второй главе** изучаются комбинаторные свойства бент-функций.

Пусть f_0,f_1,f_2,f_3 — бент-функции от n переменных. Рассмотрим булеву функцию f от $n+2$ переменных, определённую следующим образом:

$$f(00,x) = f_0(x), \quad f(01,x) = f_1(x), \quad f(10,x) = f_2(x), \quad f(11,x) = f_3(x), \ x \in \mathbb{F}_2^n.$$

Теорема 1. *Бент-функция f от $n+2$ переменных, определённая указанным выше способом, является самодуальной тогда и только тогда, когда существует пара бент-функций $g_1,g_2 \in \mathcal{B}_n$ и булева функция $h \in \mathcal{F}_n$ такие, что*

$$f_0 = \widetilde{g}_2, \qquad f_1 = \widetilde{g_1 \oplus h}, \qquad f_2 = \widetilde{g}_1, \qquad f_3 = \widetilde{g_2 \oplus h} \oplus 1,$$

и функции g_1,g_2,h удовлетворяют следующей системе

$$\begin{cases} h = g_1 \oplus g_2 \oplus \widetilde{g}_1 \oplus \widetilde{g}_2, \\ \widetilde{g_1 \oplus h} = \widetilde{g}_1 \oplus h, \\ \widetilde{g_2 \oplus h} = \widetilde{g}_2 \oplus h, \\ g_1 \oplus \widetilde{g}_2 = h\,(g_1 \oplus g_2)\,. \end{cases}$$

Данный результат описывает самодуальные бент-функции от $n+2$ переменных, вектор значений которых является конкатенацией четырёх векторов значений бент-функций от n переменных.

Как было сказано ранее, действие отображения дуальности на бент-функцию $f \in \mathcal{B}_n$ может быть представлено в виде умножения характеристического вектора данной функции на матрицу Сильвестра — Адамара. С использованием итеративных конструкций самодуальных бент-функций, получаемых с помощью Теоремы 1, доказана следующая

Теорема 2. *Множества характеристических векторов самодуальных бент-функций и анти-самодуальных бент-функций от $n \geqslant 4$ переменных линейно порождают собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным числам $2^{n/2}$ и $(-2^{n/2})$, соответственно.*

Таким образом, множества самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных полностью характеризуют собственные подпространства матрицы Сильвестра — Адамара. Пусть $f \in \mathcal{B}_n$ — произвольная бент-функция, и F^+, $F^- \in \mathbb{R}^{2^n}$ — проекции её характеристического вектора $(-1)^f$ на собственные подпространства матрицы Сильвестра — Адамара, соответствующие собственным значениям $2^{n/2}$ и $(-2^{n/2})$. Тогда действие отображения дуальности на функцию f описывается схемой

$$F^+ + F^- = (-1)^f \longrightarrow (-1)^{\widetilde{f}} = F^+ - F^-,$$

при этом в силу Теоремы 2 проекции F^+ и F^- есть линейные комбинации характеристических векторов самодуальных и анти-самодуальных бент-функций от n переменных.

Результаты главы 2 опубликованы в [2; 4; 10; 13; 15].

В **третьей главе** изучаются свойства отображения дуальности, полностью описываются группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций. Устанавливается связь между данными группами и метрическими свойствами отображения дуальности.

Отображение, определённое на множестве булевых функций, называется *изометричным*, если оно сохраняет расстояние Хэмминга.

Как было отмечено ранее, отображение дуальности $f \to \widetilde{f}$ сохраняет расстояние Хэмминга.

Утверждение 5. *При $n \geqslant 4$ не существует изометричного отображения множества всех булевых функций от n переменных в себя, отличного от тождественного, обладающего тем свойством, что каждая самодуальная бент-функция от n переменных является его неподвижной точкой.*

Данный результат позволяет сделать вывод о том, что не существует изометричного отображения множества всех булевых функций от n переменных в себя, которое каждой бент-функции от n переменных ставит в соответствие дуальную к ней функцию. Таким образом, отображение дуальности не может быть доопределено до изометричного отображения всех булевых функций от n переменных в себя.

Группой автоморфизмов фиксированного множества булевых функций $M \subseteq \mathcal{F}_n$ называется группа изометричных отображений множества всех булевых функций от n переменных в себя, оставляющих множество M на месте. Она обозначается через $\mathrm{Aut}\,(M)$.

Через $\mathrm{GL}\,(n,\mathbb{F}_2)$ обозначается *полная линейная группа* порядка n над полем $\mathbb{F}_2$. *Ортогональной группой* порядка n над полем $\mathbb{F}_2$ называется группа

$$\mathcal{O}_n = \left\{L \in \mathrm{GL}\,(n,\mathbb{F}_2) : LL^{\mathrm{T}} = I_n\right\},$$

где I_n — единичная матрица порядка n над полем $\mathbb{F}_2$. Группа преобразований, действующих на множестве всех булевых функций от n переменных по правилу

$$f(x) \longrightarrow f(L(x \oplus c)) \oplus \langle c,x\rangle \oplus d,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{F}_2$, называется *расширенной ортогональной группой* и обозначается $\overline{\mathcal{O}}_n$.

Теорема 3. *Для $n \geqslant 4$ справедливо*

$$\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^{-}(n)\right) = \overline{\mathcal{O}}_n.$$

Таким образом, все изометричные отображения, сохраняющие (анти-)самодуальность, полностью характеризуются расширенной ортогональной группой. В частности, отсюда следует, что существующий подход к классификации самодуальных бент-функций является самым общим в рамках изометричных отображений множества всех булевых функций от n переменных, сохраняющих самодуальность.

Для случая $n \geqslant 4$ полностью охарактеризованы изометричные отображения множества всех булевых функций от n переменных в себя, меняющие местами множества самодуальных и анти-самодуальных бент-функций от n переменных. Наличие данных изометричных соответствий во многих случаях позволяет тривиальным образом переносить утверждения, касающиеся метрических свойств самодуальных бент-функций, на анти-самодуальные бент-функции, и наоборот.

Изометричное отображение φ множества всех булевых функций от n переменных в себя будем называть *перестановочным с отображением дуальности*, если оно переводит множество бент-функций от n переменных в себя, и для каждой бент-функции $f \in \mathcal{B}_n$ выполняется

$$\widetilde{\varphi(f)} = \varphi(\widetilde{f}).$$

С использованием отношения Рэлея булевой функции получено полное описание изометричных отображений, оставляющих класс бент-функций от $n \geqslant 4$ переменных на месте и сохраняющих расстояние Хэмминга между каждой бент-функцией и дуальной к ней, также охарактеризованы все отображения, перестановочные с отображением дуальности.

Теорема 4. *Пусть φ — изометричное отображение множества всех булевых функций от $n \geqslant 4$ переменных в себя. Тогда следующие условия эквивалентны:*

1) *φ перестановочно с отображением дуальности;*
2) *φ является элементом группы автоморфизмов множества бент-функций от n переменных и сохраняет расстояние Хэмминга между каждой бент-функцией и дуальной к ней;*
3) *φ является элементом группы автоморфизмов множества самодуальных бент-функций от n переменных.*

Таким образом, множество изометричных отображений, сохраняющих расстояние между бент-функцией и дуальной к ней, совпадает с группой автоморфизмов самодуальных бент-функций. Это позволяет говорить о наличии тесной связи между свойствами отображения дуальности и метрическими свойствами (анти-)самодуальных бент-функций.

Результаты главы 3 опубликованы в [2–4; 9; 11–14].

В **четвёртой главе** найдено минимальное расстояние между самодуальными бент-функциями, а также описаны множества булевых функций, максимально удалённых от множеств (анти-)самодуальных бент-функций.

Утверждение 14. *Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между различными самодуальными бент-функциями от n переменных равно $2^{n/2}$.*

С использованием данного утверждения, а также известных изометричных взаимно однозначных соответствий между множествами самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных, доказано, что минимальное расстояние Хэмминга между различными анти-самодуальными бент-функциями от $n \geqslant 4$ переменных также равно $2^{n/2}$.

Для случая $n = 2$ имеем $\mathrm{SB}^+(2) = \{x_1x_2,\, x_1x_2 \oplus 1\}$ — данные функции являются отрицаниями друг друга и находятся на расстоянии 2^n. Но при $n \geqslant 4$ расстояние $2^{n/2}$, являющееся минимальным расстоянием между различными бент-функциями от n переменных, достижимо также и на (анти-)самодуальных бент-функциях.

Охарактеризованы множества булевых функций, находящихся на максимальном удалении от множеств (анти-)самодуальных бент-функций.

Теорема 5. *Пусть $n \geqslant 4$, тогда*
- *Множество булевых функций, максимально удалённых от множества самодуальных бент-функций от n переменных, совпадает с множеством анти-самодуальных бент-функций от n переменных;*
- *Множество булевых функций, максимально удалённых от множества анти-самодуальных бент-функций от n переменных, совпадает с множеством самодуальных бент-функций от n переменных.*

Множество векторов, максимально удалённых от множества $A \subseteq \mathbb{F}_2^n$, обозначается через $\widehat{A}$. Множество A называется *метрически регулярным*, если $\widehat{\widehat{A}} = A$. Множество булевых функций называется *метрически регулярным*,

если метрически регулярным является соответствующее ему множество векторов значений.

Теорема 6. *Множества самодуальных и анти-самодуальных бент-функций от n переменных являются метрически регулярными множествами.*

Используя двойственность между самодуальными и анти-самодуальными бент-функциями, вытекающую из приведённых выше результатов, можно определить данные функции в метрическом смысле: самодуальная бент-функция от $n \geqslant 4$ переменных — это булева функция от n переменных, максимально удалённая от множества анти-самодуальных бент-функций от n переменных. Аналогичное утверждение можно сформулировать для анти-самодуальных бент-функций.

Результаты главы 4 опубликованы в [2; 4; 10; 13; 14].

В **пятой главе** исследуются расстояния Хэмминга между самодуальными бент-функциями из одного известного класса.

Бент-функции от n переменных, представимые в виде

$$f(x,y) = \langle x,\pi(y)\rangle \oplus g(y), \;\; x,y \in \mathbb{F}_2^{n/2},$$

где π — перестановка на множестве $\mathbb{F}_2^{n/2}$, а g — булева функция от $n/2$ переменных, формируют хорошо известный *класс Мэйорана — МакФарланда* (1973). Данная конструкция является одной из первых конструкций бент-функций, её мощность даёт хорошую нижнюю оценку количества данных функций.

Через $\mathrm{SB}^+_{\mathcal{M}}(n)$ обозначим множество самодуальных бент-функций от n переменных из класса Мэйорана — МакФарланда, а через $\mathrm{SB}^-_{\mathcal{M}}(n)$ — множество анти-самодуальных бент-функций от n переменных из данного класса.

Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Теорема 7. *Пусть $f,g \in \mathrm{SB}^+_{\mathcal{M}}(n) \cup \mathrm{SB}^-_{\mathcal{M}}(n)$, тогда если*

- *$f \in \mathrm{SB}^+_{\mathcal{M}}(n)$, а $g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, то $\mathrm{dist}(f,g) = 2^{n-1}$;*
- *$f,g \in \mathrm{SB}^+_{\mathcal{M}}(n)$ или $f,g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, то при $n = 2$ имеем $\mathrm{dist}(f,g) = 2^n$ (если $f \neq g$), а при $n \geqslant 4$ справедливо*

$$\mathrm{dist}(f,g) \in \left\{2^{n-1},\, 2^{n-1} \pm 2^{n-r-1}\right\},\; r = 0,1,\ldots,n/2-1,$$

и все приведённые расстояния достижимы.

Из Теоремы 7 следует, что при $n \geqslant 4$ минимальное расстояние Хэмминга между рассматриваемыми различными функциями составляет 2^{n-2}.

Результаты главы 5 опубликованы в [1; 6; 7; 13; 14].

Благодарности. Я выражаю искреннюю благодарность своему научному руководителю Наталье Николаевне Токаревой за постановку интересных задач, положивших начало моим исследованиям, постоянную и всестороннюю поддержку, а также ценные советы и замечания, позволившие по-новому взглянуть

на многие вопросы, рассматриваемые в работе. Приношу свою благодарность руководителю лаборатории дискретного анализа Института математики им. С. Л. Соболева СО РАН Александру Андреевичу Евдокимову и её сотрудникам, в частности, Николаю Александровичу Коломейцу и Владимиру Николаевичу Потапову, за внимание к работе, ценные советы и предложения. Хотелось бы выразить благодарность рецензентам моих статей и тезисов за указание ценных замечаний и дополнений, позволивших улучшить качество работ. Выражаю признательность коллективу исследовательского центра Selmer Center in Secure Communication (Норвегия, г. Берген) за проявленный интерес к полученным результатам, а также полезные замечания. Выражаю благодарность Денису Станиславовичу Кротову, взявшему на себя труд прочитать текст рукописи. Отдельно хотелось бы поблагодарить своих коллег — Анастасию Александровну Городилову, Валерию Александровну Идрисову и Алексея Константиновича Облаухова за интересную и плодотворную совместную работу, а также дружескую атмосферу.

Публикации. Результаты по теме диссертации изложены в 15 печатных изданиях, 4 из которых изданы в журналах, рекомендованных ВАК, а также индексируемых Web of Science и Scopus, 11 — в тезисах докладов.

Объем и структура работы. Диссертация состоит из введения, пяти глав и заключения. Полный объем диссертации 134 страниц текста с 9 таблицами. Список литературы содержит 100 наименований.

В **заключении** приведены основные результаты работы.

Публикации автора по теме диссертации

1. А. В. Куценко. Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана-МакФарланда // Дискретный анализ и исследование операций. — 2018. — Т. 25, № 1. — С. 98—119. — Перевод: A. V. Kutsenko. The Hamming distance spectrum between self-dual Maiorana–McFarland bent functions // Journal of Applied and Industrial Mathematics. — 2018. Vol. 12, no. 1. — P. 112–125.
2. A. Kutsenko. Metrical properties of self-dual bent functions // Designs, Codes and Cryptography. — 2020. — Vol. 88, no. 1. — P. 201—222.
3. A. Kutsenko. The group of automorphisms of the set of self-dual bent functions // Cryptography and Communications. — 2020. — Vol. 12, no. 5. — P. 881—898.
4. A. Kutsenko, N. Tokareva. Metrical properties of the set of bent functions in view of duality // Прикладная дискретная математика. — 2020. — № 49. — С. 18–34.
5. А. В. Куценко. О самодуальных булевых бент-функциях // Прикладная дискретная математика. Приложение. — 2015. — № 8. — С. 34–35.

6. А. В. Куценко. О расстоянии Хэмминга между самодуальными булевыми бент-функциями // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова. — 2016. — С. 386—388.

7. А. В. Куценко. О множестве расстояний Хэмминга между самодуальными бент-функциями // Прикладная дискретная математика. Приложение. — 2016. — № 9. — С. 29—30.

8. А. В. Куценко. О свойствах изометричных отображений множества бент-функций // Тезисы докладов Международной конференции «Математика в современном мире», посвящённой 60-летию Института математики им. С. Л. Соболева. — 2017. — С. 439.

9. А. В. Куценко. О некоторых свойствах известных изометричных отображений множества бент-функций // Прикладная дискретная математика. Приложение. — 2017. — № 10. — С. 43—44.

10. А. В. Куценко. О некоторых свойствах самодуальных бент-функций // Прикладная дискретная математика. Приложение. — 2018. — № 11. — С. 44—46.

11. А. В. Куценко. Изометричные отображения множества всех булевых функций в себя, сохраняющие самодуальность и отношение Рэлея // Прикладная дискретная математика. Приложение. — 2019. — № 12. — С. 55—58.

12. A. Kutsenko. Isometric Mappings of the Set of all Boolean Functions into Itself which Preserve Self-duality and the Rayleigh Quotient // Proceedings of the 4th workshop Boolean Functions and their Applications (BFA 2019), Florence, Italy, June 16-21, 2019. — 2019.

13. А. В. Куценко. О метрических свойствах множества самодуальных бент-функций // Прикладная дискретная математика. Приложение. — 2020. — № 13. — С. 21—27.

14. A. Kutsenko. On metrical properties of self-dual generalized bent functions // Proceedings of the 5th workshop Boolean Functions and their Applications (BFA 2020), Loen, Norway, September 15-17, 2020. — 2020.

15. A. Kutsenko. On constructions and properties of self-dual generalized bent functions // Proceedings of the 11th International Conference on Sequences and Their Applications (SETA 2020), Saint-Petersburg, September 22-25, 2020. — 2020.

Куценко Александр Владимирович

Самодуальные бент-функции и их
метрические свойства

Автореф. дис. на соискание учёной степени
кандидата физико-математических наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж ___ экз.
Типография _____

На правах рукописи

Облаухов Алексей Константинович

Метрически регулярные множества в булевом кубе: конструкции и свойства

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2020

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН).

Научный руководитель: кандидат физико-математических наук
Токарева Наталья Николаевна

Официальные оппоненты: **Фомичёв Владимир Михайлович,**
доктор физико-математических наук, профессор,
Финансовый университет при Правительстве Российской Федерации, профессор.

Панкратова Ирина Анатольевна,
кандидат физико-математических наук, доцент,
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет», заведующий лабораторией компьютерной криптографии.

Ведущая организация: Институт проблем информационной безопасности факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный университет имени М.В.Ломоносова».

Защита состоится 24 марта 2021 г. в 17 часов на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук и на сайте math.nsc.ru.

Отзывы на автореферат в двух экземплярах, заверенные печатью учреждения, просьба направлять по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4, ученому секретарю диссертационного совета Д 003.015.01.

Автореферат разослан __ _____ 2021 года.

Ученый секретарь
диссертационного совета
Д 003.015.01,
д-р физ.-мат. наук Ю. В. Шамардин

Общая характеристика работы

Актуальность и степень разработанности темы исследования. В данной работе изучаются метрические свойства подмножеств пространства $\mathbb{F}_2^n$ (часто называемого *булевым кубом* размерности n), в частности, свойство метрической регулярности и связанные с ним понятия и объекты.

Приведём несколько необходимых определений.

Пусть $\mathbb{F}_2^n = \{0,1\}^n$ — множество двоичных наборов длины n, рассматриваемое как векторное пространство над полем $\mathbb{F}_2$. *Расстоянием Хэмминга* между двумя двоичными векторами называется число таких координат, в которых эти векторы различаются. *Радиусом покрытия* $\rho(X)$ множества $X \subseteq \mathbb{F}_2^n$ называется наибольшее из расстояний от векторов $\mathbb{F}_2^n$ до множества X. Назовём *метрическим дополнением* $\widehat{X}$ множества X множество всех векторов $\mathbb{F}_2^n$, находящихся на максимальном возможном расстоянии от данного множества. Множество называется *метрически регулярным*, если его второе метрическое дополнение (метрическое дополнение метрического дополнения, $\widehat{\widehat{X}}$) совпадает с ним самим.

Задача изучения метрического дополнения множества тесно связана с задачами покрытия и упаковки, как в булевом кубе, так и в других метрических пространствах. *Задача упаковки сфер* в евклидовом пространстве $\mathbb{R}^n$ заключается в поиске наиболее плотного расположения одинаковых сфер в пространстве при условии, что никакие две сферы не перекрываются. *Задача покрытия сферами* требует найти наименее плотное расположение сфер, при котором объединение объёмов всех сфер покрывает пространство целиком.

Задачи покрытия и упаковки в пространстве $\mathbb{R}^n$ очень часто решаются при помощи решётчатых упаковок. *Решёткой* называется подмножество евклидова пространства $\mathbb{R}^n$, образующее группу по сложению, а *решётчатой упаковкой* называется множество сфер, центры которых лежат в узлах соответствующей решётки. *Глубокой дырой* решётки называется точка пространства, удалённая на максимальное возможное расстояние от узлов решётки. Таким образом, множество всех глубоких дыр решётки есть не что иное, как её метрическое дополнение.

Метрическое дополнение решётки используется[1] для итеративного построения упаковок сфер в пространстве $\mathbb{R}^n$. Пусть $X \subseteq \mathbb{R}^n$ — решётка, а Λ — упаковка сфер в $\mathbb{R}^n$, соответствующая решётке X. *Слоем сфер* в пространстве $\mathbb{R}^{n+1}$ назовём множество сфер таких, что их центры лежат на гиперплоскости $\mathbb{R}^n$ в узлах решётки X, а сечение данных сфер гиперплоскостью совпадает с упаковкой Λ. Построим плотную упаковку сфер в $\mathbb{R}^{n+1}$ путём складывания подобных слоёв друг на друга. Расположим соседние слои таким образом, чтобы множество центров X упаковки Λ одного слоя было расположено напротив

[1] Conway J. H., Sloane N. J. A. Sphere packings, lattices and groups // Springer Science & Business Media. — 2013. — Т. 290.

подмножества точек $\widehat{X}$ другого слоя. При подобном расположении всех слоёв сфер друг относительно друга во многих случаях получается достаточно плотная упаковка в пространстве $\mathbb{R}^{n+1}$. В случае, если $\widehat{X}$ имеет существенно большую мощность, чем X, иногда таким способом возможно построить несколько неэквивалентных друг другу упаковок. Большое количество известных плотных (в том числе наиболее плотных) упаковок сфер построено при помощи данной итеративной конструкции из более простых упаковок меньших размерностей.

Метрическое дополнение решётки также рассматривалось при нахождении радиуса покрытия одной из наиболее известных решёток — решётки Лича[2,3] Λ_{24}. Данная решётка порождает наиболее плотную упаковку шаров[4] в пространстве $\mathbb{R}^{24}$, а также имеет[5] наибольшее возможное в данном пространстве контактное число (максимальное количество шаров, одновременно соприкасающихся с шаром такого же размера).

Вскоре после открытия данной решётки Дж. Лич высказал гипотезу, что её радиус покрытия равен радиусу упаковки $e(\Lambda_{24})$, умноженному на $\sqrt{2}$. В 1982 году С. Нортон доказал оценку $\rho(\Lambda_{24}) \leqslant 1.452\ldots \cdot e(\Lambda_{24})$, а чуть позже, в том же году, гипотеза была доказана Дж. Конвеем, Р. Паркером и Н. Слоэном[6]. Доказательство заключается в исследовании метрического дополнения решётки: авторы установили, что существует 23 неэквивалентных класса глубоких дыр, и поставили в соответствие каждому классу одну из так называемых решёток Нимайера, радиус покрытия каждой из которых равен $\sqrt{2}$.

Нетрудно заметить, что точки метрического дополнения любого множества в евклидовом пространстве являются вершинами так называемых *областей Дирихле* (*областей диаграммы Вороного*) данного множества.

Задачи вычисления радиуса покрытия и плотной упаковки сфер активно изучаются также в пространстве двоичных векторов $\mathbb{F}_2^n$, снабжённом метрикой Хэмминга. *Двоичным кодом* называется произвольное подмножество пространства $\mathbb{F}_2^n$. Пусть $C \subseteq \mathbb{F}_2^n$ — двоичный код. *Кодовым расстоянием* d называется кратчайшее из расстояний между векторами кода C. *Радиусом упаковки* $e(C)$ кода $C \subseteq \mathbb{F}_2^n$ называется наибольшее число e такое, что сферы радиуса e с центрами в векторах кода C не пересекаются. Радиус упаковки кода $e(C)$ равен $\lfloor \frac{d-1}{2} \rfloor$ и отражает количество ошибок, потенциально возникших при передаче

[2]Leech J. Notes on sphere packings // Canadian Journal of Mathematics. — 1967. — Т. 19. — С. 251–267.

[3]Lepowsky J., Meurman A. An E8-approach to the Leech lattice and the Conway group // Journal of Algebra. — 1982. — Т. 77. — №. 2. — С. 484–504.

[4]Cohn H., Kumar A., Miller S. D., Radchenko D., Viazovska M. The sphere packing problem in dimension 24 // Annals of Mathematics. — 2017. — С. 1017–1033.

[5]Odlyzko A. M., Sloane N. J. A. New bounds on the number of unit spheres that can touch a unit sphere in n dimensions // Journal of Combinatorial Theory, Series A. — 1979. — Т. 26. — №. 2. — С. 210–214.

[6]Conway J. H., Parker R. A., Sloane N. J. A. The covering radius of the Leech lattice // Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences. — 1982. — Т. 380. — №. 1779. — С. 261–290.

кодированной информации, которые может исправить данный код. *Параметрами кода* называют тройку $(n,|C|,d)$, отражающую его длину, мощность и кодовое расстояние. Код C называется *линейным*, если он является линейным подпространством булева куба, т.е. если сумма любых двух векторов кода лежит в нём же. Для линейных кодов параметрами кода называют тройку $[n,k,d]$, где k обозначает размерность кода как линейного подпространства булева куба $\mathbb{F}_2^n$.

Минимизация мощности двоичного кода при заданном радиусе покрытия, как и двойственная к ней задача минимизации радиуса покрытия при заданной мощности, имеют разнообразные приложения как в теории кодирования информации, так и в других областях математики. В книге "Covering codes" Дж. Коэна и др.[7] приводятся оценки оптимальных параметров покрывающих двоичных кодов, а также обзор различных конструкций покрывающих кодов. Помимо этого, изучается радиус покрытия кодов из многих известных семейств, таких как коды Рида-Маллера, коды БЧХ, коды Рида-Соломона и др.

Метрическую регулярность можно рассматривать как одно из расширений понятия *совершенности* кода. Код $C \subseteq \mathbb{F}_2^n$ называется *совершенным*, если шары радиуса $e(C)$ покрывают всё пространство $\mathbb{F}_2^n$, то есть радиус покрытия кода равен радиусу упаковки. Легко видеть, что всякий совершенный код является метрически регулярным. Совершенные коды имеют наилучшие параметры для кодирования информации. В то же время, количество различных наборов параметров, которыми могут обладать нетривиальные совершенные коды, невелико, что было доказано в работах В. Зиновьева, В. Леонтьева[8] и А. Тиетвайнена[9]. Так, каждый нетривиальный двоичный совершенный код имеет параметры кода Хэмминга $[2^r-1, 2^r-r-1,3]$ или кода Голея $[23,12,7]$.

Одним из ослаблений совершенных кодов являются так называемые почти совершенные коды[10]. Код называется *почти совершенным*, если его мощность достигает модифицированной границы Джонсона. К. Линдстрём в 1977 году установил, что все двоичные почти совершенные коды уже найдены, а всякий почти совершенный код над полем другого размера является совершенным[11]. Тем самым, все почти совершенные коды описаны в работе Дж. Гётельса и С. Сновера[12], а представленные в ней конструкции приводят к метрически регулярным кодам: тривиальные коды повторений, укороченные коды Хэмминга, коды Препарата и др.

---

[7] Cohen G., Honkala I., Litsyn S., Lobstein A. Covering codes // Elsevier. — 1997. — Т. 54.

[8] Зиновьев В. А., Леонтьев В. К. О совершенных кодах // Проблемы передачи информации. — 1972. — Т. 8. — №. 1. — С. 26–35.

[9] Tietäväinen A. On the nonexistence of perfect codes over finite fields // SIAM Journal on Applied Mathematics. — 1973. — Т. 24. — №. 1. — С. 88–96.

[10] Goethals J. M., Snover S. L. Nearly perfect binary codes // Discrete Mathematics. — 1972. — Т. 3. — №. 1-3. — С. 65–88.

[11] Lindström K. All nearly perfect codes are known // Information and Control. — 1977. — Т. 35. — №. 1. — С. 40–47.

[12] см. 10

Почти совершенные коды являются подмножеством полностью регулярных кодов[13]. Одно из определений таких кодов гласит, что код C называется *полностью регулярным*, если любой вектор $x \in C_i$ находится на расстоянии 1 от a_i векторов из множества C_{i-1} и от b_i векторов из множества C_{i+1}. Здесь $C_i = \{x \in \mathbb{F}_2^n \,|\, d(x,C) = i\}$ — множество векторов на расстоянии i от кода, а числа a_i, b_i зависят лишь от расстояния i, но не зависят от выбора кодового слова. Из этого определения легко следует, что всякий полностью регулярный код является метрически регулярным. Обратное в общем случае неверно — контрпримером является метрически регулярный код $\{(000),(011)\}$ в $\mathbb{F}_2^3$, не являющийся полностью регулярным. Обзор конструкций и свойств полностью регулярных кодов можно найти в работе Ж. Боржеса, Д. Рифа и В. Зиновьева[14].

С другой стороны, почти совершенные коды содержатся во множестве *квази-совершенных* кодов[15]. Код называется *квази-совершенным*, если его радиус покрытия на единицу больше радиуса упаковки. Класс квази-совершенных кодов достаточно велик, и в общем случае квази-совершенный код не является метрически регулярным: тривиальным контрпримером является код $\{(00),(01),(10)\}$ в $\mathbb{F}_2^2$. Изучаются также другие усиления квази-совершенных кодов — например, равномерно упакованные коды (включая равномерно упакованные коды в сильном и слабом смыслах)[16,17,18], некоторые из которых являются полностью регулярными, и, следовательно, метрически регулярными.

Булевой функцией f от m переменных называется произвольное отображение из $\mathbb{F}_2^m$ в $\mathbb{F}_2$. *Вектором значений* булевой функции называется двоичный вектор длины 2^m, содержащий значения данной функции на всех булевых векторах длины m, упорядоченных некоторым образом. Расстояние между булевыми функциями определяется как расстояние между их векторами значений. *Аффинной булевой функцией* от m переменных называется функция вида $a_1x_1 + a_2x_2 + \ldots + a_mx_m + c$, где $a_i, c \in \mathbb{F}_2$. Здесь и далее при проведении операций с булевыми векторами/функциями, знаком "+" обозначается сложение в поле $\mathbb{F}_2$ (по модулю 2). *Код Рида-Маллера порядка k от m переменных* определяется как множество всех функций (либо их векторов значений), алгебраическая степень которых не превосходит k; в частности,

[13] Delsarte P. An algebraic approach to the association schemes of coding theory // Philips Res. Rep. Suppl. — 1973. — Т. 10. — С. vi+–97.

[14] Боржес Ж., Рифа Д., Зиновьев В. А. О полностью регулярных кодах // Проблемы передачи информации. — 2019. — Т. 55. — №. 1. — С. 3–50.

[15] Gorenstein D., Peterson W. W., Zierler N. Two-error correcting Bose-Chaudhuri codes are quasi-perfect // Information and Control. — 1960. — Т. 3. — №. 3. — С. 291–294.

[16] Семаков Н. В., Зиновьев В. А., Зайцев Г. В. Равномерно упакованные коды // Проблемы передачи информации. — 1971. — Т. 7. — №. 1. — С. 38–50.

[17] Бассалыго Л. А., Зайцев Г. В., Зиновьев В. А. О равномерно упакованных кодах // Проблемы передачи информации. — 1974. — Т. 10. — №. 1. — С. 9–14.

[18] van Tilborg H. C. A., Goethals J. M. Uniformly packed codes // Philips Research Reports. — 1975. — Т. 30. — С. 9–36.

множество аффинных булевых функций является кодом Рида-Маллера первого порядка. Код Рида-Маллера порядка k от m переменных имеет параметры $[2^m, \sum_{i=0}^{k} \binom{m}{i}, 2^{m-k}]$.

Задача исследования и классификации метрически регулярных множеств в булевом кубе была впервые поставлена Н. Токаревой[19] при изучении метрических свойств бент-функций[20]. Булева функция f от чётного числа переменных m называется *бент-функцией*, если она находится на максимальном возможном расстоянии $2^{m-1} - 2^{\frac{m}{2}-1}$ от множества аффинных функций. Иными словами, множество бент-функций — это метрическое дополнение множества аффинных функций. Бент-функции имеют разнообразные применения в криптографии, теории кодирования и комбинаторике[21,22]. В 2010 году Н. Токарева доказала, что множество аффинных функций является метрическим дополнением множества бент-функций[23], и тем самым установила, что множества аффинных функций и бент-функций являются метрически регулярными.

Изучением метрических дополнений и метрически регулярных множеств занимаются как отечественные, так и зарубежные авторы. Так, в одной из своих работ[24], П. Станица, Т. Сасао и Дж. Батлер вводят понятие *множеств функций разбиения* и изучают метрические дополнения и метрическую регулярность таких множеств. Множество $\mathcal{S}$ булевых функций называется *множеством функций разбиения* относительно разбиения $\mathcal{U}$ пространства $\mathbb{F}_2^m$, если каждая функция из $\mathcal{S}$, будучи ограниченной на любой класс из разбиения $\mathcal{U}$, является постоянной (то есть все векторы класса отображаются либо в 0, либо в 1), и все функции, соответствующие каждой возможной комбинации значений на классах, включены в множество $\mathcal{S}$. Множества функций разбиения включают, например, множество симметрических функций, поворотно-симметрических (rotation symmetric) функций, анти-самодуальных функций и другие.

Авторы явно вычисляют радиус покрытия, описывают метрическое дополнение произвольного множества функций разбиения и доказывают его метрическую регулярность. Затем авторы переходят к изучению множеств симметрических и поворотно-симметрических функций. Они вычисляют радиусы покрытия для обоих множеств, описывают множество максимально асимметрических функций (метрическое дополнение множества симметрических функций) и вычисляют количество таких функций. Авторы описывают

[19] Tokareva N. Duality between bent functions and affine functions // Discrete mathematics. — 2012. — Т. 312. — №. 3. — С. 666–670.

[20] Rothaus O. S. On “bent” functions // Journal of Combinatorial Theory, Series A. — 1976. — Т. 20. — №. 3. — С. 300–305.

[21] Tokareva N. Bent functions: results and applications to cryptography // Academic Press. — 2015.

[22] Mesnager S. Bent Functions: Fundamentals and Results // Springer International Publishing. – 2016.

[23] Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Mathematics and Applications. — 2010. — Т. 20. — №. 5-6. — С. 655–664.

[24] Stănică P., Sasao T., Butler J. T. Distance duality on some classes of Boolean functions // Journal of Combinatorial Mathematics and Combinatorial Computing. — 2018. — Т. 107. — С. 181–198.

весовое распределение максимально асимметрических функций и их алгебраические степени, а затем приводят классификацию всех булевых функций относительно расстояния до множества симметрических функций.

А. Куценко изучались метрические свойства двух подклассов бент-функций, называемых *самодуальными* и *анти-самодуальными* бент-функциями. В одной из своих работ[25] автор доказывает, что множество самодуальных бент-функций является метрическим дополнением множества анти-самодуальных бент-функций и наоборот, устанавливая тем самым метрическую регулярность обоих множеств. Другие метрические свойства бент-функций (например, свойства графа минимальных расстояний между бент-функциями) также изучались Н. Коломейцем[26,27].

Целью данной работы является изучение свойства метрической регулярности и связанных понятий:

1. Описание конструкций метрически регулярных множеств; оценка количества метрически регулярных множеств.
2. Получение оценок мощности метрически регулярных множеств и их метрических дополнений.
3. Изучение свойств и вида метрических дополнений линейных кодов; изучение метрической регулярности линейных кодов.

Научная новизна и значимость работы: Все результаты, представленные в работе, являются новыми. Работа носит теоретический характер. Полученные конструкции и теоретические результаты могут быть применены при дальнейших исследованиях метрически регулярных множеств, а также при исследовании свойств бент-функций и различных линейных кодов.

Методология и методы исследования. В работе применялись методы комбинаторики, дискретного анализа и теории кодирования. Для выдвижения гипотез и проверки некоторых частных случаев были использованы компьютерные эксперименты.

Основные положения, выносимые на защиту:

1. Представлены различные конструкции метрически регулярных множеств: доказана сходимость операции взятия метрического дополнения, получены итеративные конструкции строго метрически регулярных множеств и найдено число множеств, полученных при помощи данных конструкций.
2. Показано, что задача поиска наибольшего по мощности метрически регулярного множества сводится к задаче поиска наименьшего покрывающего кода радиуса 1.

---

[25] Kutsenko A. Metrical properties of self-dual bent functions // Designs, Codes and Cryptography. — 2020. — Т. 88. — №. 1. — С. 201–222.

[26] Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. — 2009. — Т. 6. — №. 2. — С. 5–20.

[27] Kolomeec N. The graph of minimal distances of bent functions and its properties // Designs, Codes and Cryptography. — 2017. — Т. 85. — №. 3. — С. 395–410.

3. Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения, зависящая от радиуса покрытия множества. Представлены конструкции семейств метрически регулярных множеств большой мощности, получена нижняя оценка мощности наибольшего метрически регулярного множества при заданном радиусе покрытия.
4. Получена общая характеризация первого и второго метрических дополнений линейных кодов.
5. Доказана метрическая регулярность кодов Рида-Маллера $\mathcal{RM}(k,m)$ для $k = 0$, $k \geqslant m - 3$, а также кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. Описаны метрические дополнения всех перечисленных кодов, за исключением кода $\mathcal{RM}(2,6)$.

Апробация работы. Основные результаты работы докладывались на научных семинарах Института математики им. С.Л. Соболева СО РАН: «Криптография и криптоанализ», «Дискретный анализ» и «Теория кодирования»; на научном семинаре исследовательской группы Selmer Center (г. Берген, Норвегия, 2019, 2020); а также на международной конференции «Boolean Functions and their Applications (BFA)» (2019, 2020), на всероссийской конференции «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» Sibecrypt (2015, 2017, 2018) и на Международной студенческой конференции МНСК (2015-2018).

Публикации. Основные результаты по теме диссертации изложены в работах [1–10], из них 5 статей опубликованы в журналах из списка ВАК.

Объем и структура работы. Диссертация состоит из введения, 5 глав, заключения и приложения. Полный объём диссертации составляет 93 страницы, включая 1 рисунок и 5 таблиц. Список литературы содержит 64 наименования.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель исследования, излагается научная новизна и практическая значимость представляемой работы.

В **первой главе** приводятся необходимые определения. Вводятся понятия метрического дополнения множества, метрической регулярности и строгой метрической регулярности. Приводятся примеры, иллюстрирующие введённые понятия.

Во **второй главе** предложены различные конструкции метрически регулярных множеств.

Напомним, что метрическое дополнение множества X обозначается $\widehat{X}$.

Утверждение 2.1. *Пусть X — произвольное подмножество пространства $\mathbb{F}_2^n$. Рассмотрим следующую последовательность множеств: $X_0 = X$,*

$X_{k+1} = \widehat{X}_k$ *для* $k \geqslant 0$. *Тогда существует число* $M \leqslant n$ *такое, что для любого* $m \geqslant M$ *множество* X_m *является метрически регулярным.*

Данное утверждение показывает, что из произвольного подмножества булева куба можно построить метрически регулярное множество, причём не более, чем за n операций нахождения метрического дополнения.

Представлены итеративные конструкции строго метрически регулярных множеств. Пусть $X \subseteq \mathbb{F}_2^n$ — произвольное подмножество булева куба. Множество X называется *строго метрически регулярным*, если сумма расстояний $d(y,X) + d(y,\widehat{X})$ постоянна для всех векторов $y \in \mathbb{F}_2^n$ и равна радиусу покрытия множества X. *Послойным представлением* пространства $\mathbb{F}_2^n$ относительно множества X называется множество слоёв, определённых следующим образом:

$$X_k := \{y \in \mathbb{F}_2^n \mid d(y,X) = k\}, k = 0,1,\ldots,r.$$

Доказана следующая теорема.

Теорема 2.4. *Пусть* $A \subseteq \mathbb{F}_2^n$ *— строго метрически регулярное множество с радиусом покрытия* $r > 0$. *Пусть* $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant r$ *— некоторая последовательность индексов. Тогда объединение* $C = \bigcup\limits_{k=1}^{s} A_{i_k}$ *является строго метрически регулярным множеством тогда и только тогда, когда существует число* $q > 0$ *такое, что выполняются следующие условия:*

1. *для любого* $k \in \{1,\ldots,s-1\}$ *разность* $i_{k+1} - i_k$ *равна* 1, $2q$ *или* $2q+1$;
2. *для любого* $k \in \{2,\ldots,s-1\}$ *как минимум одна из разностей* $i_{k+1} - i_k, i_k - i_{k-1}$ *больше единицы;*
3. i_1 *равно либо* q, *либо* 0, *и если* $i_1 = 0$, *а* i_2 *существует, то* $i_2 - i_1 = 2q$ *или* $2q+1$;
4. i_s *равно либо* $r-q$, *либо* r, *и если* $i_s = r$, *а* i_{s-1} *существует, то* $i_s - i_{s-1} = 2q$ *или* $2q+1$;

При выполнении указанных условий число q *является радиусом покрытия множества* C.

Затем подсчитывается количество различных строго метрически регулярных множеств, которые можно получить при помощи данной конструкции.

Теорема 2.5. *Пусть* $A \subseteq \mathbb{F}_2^n$ *— строго метрически регулярное множество с радиусом покрытия* $r > 0$. *Количество* $G_q(r)$ *различных строго метрически регулярных множеств с радиусом покрытия* q, *которые можно построить объединением слоёв послойного представления пространства относительно множества* A, *применяя теорему 2.4, можно вычислить при помощи следующих рекуррентных формул:*

$$G_q(r) = \begin{cases} G_q(r-q) + G_q(r-q-1), & \text{при } r > q, \\ 2, & \text{при } r = q, \\ 0, & \text{при } 0 \leqslant r < q. \end{cases}$$

Характеристическое уравнение данной рекуррентной последовательности имеет вид $x^{q+1} = x + 1$. Данное уравнение не разрешимо в радикалах при $q \geqslant 4$, однако разрешимо при меньших q.

Результаты второй главы опубликованы в работах [2, 3, 8].

Третья глава посвящена оценкам мощностей метрически регулярных множеств.

Показано, что всякое метрически регулярное множество вкладывается в метрически регулярное множество с радиусом покрытия 1. Исходя из этого факта доказывается, что задача нахождения наибольшего метрически регулярного множества сводится к задаче нахождения наименьшего покрывающего кода радиуса 1.

Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения при фиксированном радиусе покрытия.

Теорема 3.4. *Пусть $A \subseteq \mathbb{F}_2^n$ — метрически регулярное множество с радиусом покрытия r. Тогда*

$$|A| + |\widehat{A}| \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

При помощи конструкций из главы 2 строятся семейства больших строго метрически регулярных множеств, размер которых позволяет оценить мощность наибольшего метрически регулярного множества с заданным радиусом покрытия в булевом кубе заданной размерности.

Теорема 3.6. *Пусть A — наибольшее метрически регулярное множество с радиусом покрытия r в булевом кубе размерности n ($n \geqslant 2r$), и пусть s — остаток от деления $n+1$ на $2r+1$. Тогда*

$$|A| \geqslant \max\left\{2^n\left(\frac{2}{2r+1} - \frac{2}{\sqrt{n-s+1}}\right), 2^{n-2r}\binom{2r}{r}\right\}. \qquad (1)$$

Результаты третьей главы опубликованы в работах [2, 3, 7, 8].

В **четвёртой главе** рассматриваются свойства метрических дополнений линейных подпространств (линейных кодов) булева куба.

Описывается общий вид метрического дополнения линейного подпространства.

Лемма 4.1. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, a — двоичный вектор длины n и $d(a,L) = k$. Тогда для любого вектора y из смежного класса*

$a + L$ имеет место $d(y,L) = k$, и, следовательно, множество $\widehat{L}$ является объединением смежных классов подпространства L.

Известно, что радиус покрытия линейного подпространства размерности k в булевом кубе размерности n не превышает $n - k$. Рассматривается канонический базис подпространства и с его помощью доказываются следующие утверждения.

Теорема 4.4. *Пусть L — линейное подпространство размерности k. Равенство $\rho(L) = n - k$ достигается тогда и только тогда, когда веса всех векторов канонического базиса подпространства L не превосходят 2. Метрическое дополнение $\widehat{L}$ состоит в этом случае из одного смежного класса пространства L.*

Теорема 4.5. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k, $wt(e_i^*) \leq 3$ для всех векторов e_i^* из канонического базиса и существует индекс j такой, что $wt(e_j^*) = 3$. Тогда $\rho(L) = n - k - 1$ тогда и только тогда, когда $supp(e_i^*) \cap supp(e_j^*) \neq \emptyset$ для всех i,j таких, что $wt(e_i^*) = wt(e_j^*) = 3$. При этом метрическое дополнение $\widehat{L}$ состоит из одного, двух или трёх смежных классов L, в зависимости от мощности пересечения носителей всех векторов канонического базиса веса 3.*

Приводится характеристика второго метрического дополнения линейного подпространства булева куба.

Теорема 4.7. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $x \in \widehat{\widehat{L}}$ тогда и только тогда, когда $\widehat{L}$ инвариантно относительно сдвига на x, т.е. $\widehat{L} = x + \widehat{L}$.*

При помощи теорем 4.5 и 4.7 строится пример линейного подпространства булева куба, не являющегося метрически регулярным.

Результаты четвёртой главы опубликованы в работах [1, 6].

В **пятой главе** рассматривается известное семейство линейных кодов — коды Рида-Маллера.

Метрическая регулярность кодов $\mathcal{RM}(1,m)$ при чётных m была установлена Н. Токаревой[28]. Естественно, что изучение множества наиболее удалённых от кода векторов требует знания радиуса покрытия кода. Среди кодов высоких порядков, радиусы покрытия известны для кодов $\mathcal{RM}(k,m)$ при $k \geqslant m - 3$. Радиус покрытия кода $\mathcal{RM}(1,m)$ неизвестен при нечётных $m > 7$, однако вычислен[29,30] для кода $\mathcal{RM}(1,5)$ и для кода $\mathcal{RM}(1,7)$. В 1981 году, Дж. Шац

[28] Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Mathematics and Applications. — 2010. — Т. 20. — №. 5-6. — С. 655–664.

[29] Berlekamp E., Welch N. Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code // IEEE Transactions on Information Theory. — 1972. — Т. 18. — №. 1. — С. 203–207.

[30] Mykkeltveit J. The covering radius of the $(128, 8)$ Reed-Muller code is 56 // IEEE Transactions on Information Theory. — 1980. — Т. 26. — №. 3. — С. 359–362.

определил[31] радиус покрытия кода $\mathcal{RM}(2,6)$, а совсем недавно К. Ванг вычислил[32] радиус покрытия кода $\mathcal{RM}(2,7)$. При $m > 7$, радиус покрытия кода $\mathcal{RM}(2,m)$ на данный момент неизвестен.

В данной главе доказывается метрическая регулярность кодов Рида-Маллера $\mathcal{RM}(k,m)$ для $k = 0$, $k \geqslant m - 2$. Затем, опираясь на метод нахождения радиуса покрытия кода $\mathcal{RM}(m-3,m)$, описанный в книге "Covering codes" Коэном и др., описывается метрическое дополнение и устанавливается метрическая регулярность кодов Рида-Маллера порядка $m - 3$ от m переменных. Также в данной главе доказывается метрическая регулярность кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. В совокупности с результатом Н. Токаревой о метрической регулярности множества аффинных функций, тем самым устанавливается метрическая регулярность всех кодов Рида-Маллера, радиус покрытия которых известен, за исключением двух: $\mathcal{RM}(1,7)$ и $\mathcal{RM}(2,7)$. Высказывается гипотеза о метрической регулярности всех кодов Рида-Маллера.

Результаты пятой главы опубликованы в работах [4, 5, 9, 10].

В **заключении** приведены основные результаты работы.

В **приложении А** содержатся выкладки и таблицы, необходимые для доказательства леммы 5.17 из раздела 5.8 главы 5.

Благодарности

Автор выражает благодарность научному руководителю Токаревой Н. Н. за научное руководство: постановку интересных задач, обсуждение результатов, помощь в подготовке статей и выступлений и поддержку на протяжении всего обучения и работы. Также автор благодарит А. Куценко, А. Городилову, Н. Коломейца и всю команду Криптографического центра (Новосибирск) за поддержку и обсуждение результатов. Автор признателен коллективу исследовательской группы Selmer Center (Норвегия) за предоставленную возможность стажировки и плодотворную работу.

[31] Schatz J. The second order Reed-Muller code of length 64 has covering radius 18 // IEEE Transactions on Information Theory. — 1981. — Т. 27. — №. 4. — С. 529–530.

[32] Wang Q. The covering radius of the Reed-Muller code $RM(2,7)$ is 40 // Discrete Mathematics. — 2019. — Т. 342. — №. 12. — Статья 111625.

Публикации автора по теме диссертации

[1] Облаухов А. К. О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. — 2016. — Т. 23. — №. 3. — С. 93–106. (Перевод: Oblaukhov A. K. Metric complements to subspaces in the Boolean cube // Journal of Applied and Industrial Mathematics. — 2016. — Т. 10. — №. 3. — С. 397–403.)

[2] Oblaukhov A. K. Maximal metrically regular sets // Сибирские электронные математические известия. — 2018. — Т. 15. — С. 1842–1849.

[3] Oblaukhov A. A lower bound on the size of the largest metrically regular subset of the Boolean cube // Cryptography and Communications. — 2019. — Т. 11. — №. 4. — С. 777–791.

[4] Oblaukhov A. K. On metric complements and metric regularity in finite metric spaces // Прикладная дискретная математика. — 2020. — №. 49. — С. 35–45.

[5] Oblaukhov A. On metric regularity of Reed-Muller codes // Designs, Codes and Cryptography. — 2020. Опубликована онлайн. DOI: 10.1007/s10623-020-00813-z

[6] Облаухов А. К. О некоторых метрических свойствах линейных подпространств булева куба // Прикладная дискретная математика. Приложение. — 2015. — №. 8. — С. 13–15.

[7] Облаухов А. К. О максимальных метрически регулярных множествах // Прикладная дискретная математика. Приложение. — 2017. — №. 10. — С. 23–24.

[8] Облаухов А. К. Нижняя оценка мощности наибольшего метрически регулярного подмножества булева куба // Прикладная дискретная математика. Приложение. — 2018. — №. 11. — С. 14–16.

[9] Oblaukhov A. Metrically regular subsets of the Boolean cube // Тезисы международной конференции “Boolean Functions and their Applications (BFA) 2019”.

[10] Oblaukhov A. Metric regularity of Reed-Muller codes // Тезисы международной конференции “Boolean Functions and their Applications (BFA) 2020”.

Облаухов Алексей Константинович

Метрически регулярные множества в булевом кубе: конструкции и свойства

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Типография _____

The duality mapping and unitary operators acting on the set of all generalized Boolean functions

Aleksandr Kutsenko[1,2] and Anastasiya Gorodilova[1]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia
[2]Novosibirsk State University, Novosibirsk, Russia
alexandrkutsenko@bk.ru, gorodilova@math.nsc.ru

Abstract

Functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer, are known as generalized Boolean functions. Bent functions within this generalization are called generalized bent (gbent). A gbent function is said to be regular if it is possible to define its dual gbent function. A duality mapping is the mapping that transforms every regular gbent function to its dual gbent. A regular gbent function is said to be self-dual if it coincides with its dual. In this paper we define the action of linear operator $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ on the set of all generalized Boolean functions in n variables via their sign functions. The characterization of unitary operators that transform the set of all generalized Boolean functions in n variables into itself is provided. We also study the properties if sign functions of self-dual gbent functions.

Keywords: Duality mapping, Generalized bent function, Self-dual bent

1 Introduction

The study of Boolean functions having strong cryptographic properties is the domain of current interest, see monographies [2, 4] for detail. Boolean bent functions were introduced by O. Rothaus [26] in 1976. Due to maximal nonlinearity they have a number of applications in cryptography and coding theory. There are still many open problems. Among them the exact number of bent functions as well as their complete classification that seem elusive to be solved for now. One can find more details on bent functions in books [33, 22].

The **duality mapping** is a mapping that transforms every (regular generalized) bent function to its dual (generalized) bent. For the Boolean case for every bent function its dual bent function is uniquely defined. It is important to note that the duality mapping is the unique known isometric mapping of the set of bent functions into itself that cannot be extended to a isometry of the whole set of all Boolean functions that preserves bentness. The action of

the duality mapping on bent functions within generalizations is increasingly nontrivial since it is typically defined only for the part of bent functions from corresponding generalization which are called *regular*, while more accurate work with them also demands for intermediate notation like *weak regularity* that also appears in this scope.

Self-dual bent functions that are fixed points of the duality mapping form a remarkable class of bent functions since they have the direct relation to their dual bent functions. The definition of self-duality initially was in paper [18] by O.A. Logachev, A.A. Sal'nikov and V.V. Yashchenko. In more details these functions were explored by C. Carlet et al. in 2010 in work [1], where a number of constructions and properties were given and the classification for small number of variables was provided. Next steps for the classification of qubic self-dual bent functions in 8 variables were made in [5], while quadratic self-dual bent functions were completely characterized in [8]. Constructions and properties of self-dual Boolean bent functions were studied in [10, 13, 21]. The overview of the known metrical properties of self-dual bent functions can be found in [17]. The extension of the concept of self-duality for different generalizations of bent functions was made in several papers. The classification of quadratic self-dual bent functions of the form $\mathbb{F}_p^n \to \mathbb{F}_p$, p odd prime, was made by X.-D. Hou in [9]. In paper [3] the self-duality for bent functions within the same generalization type was studied by A. Çeşmelioğlu et al. In 2018 in paper [28] L. Sok. et al. studied quaternary self-dual bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_4$ from the viewpoints of existence, construction, and symmetry. The relation between sign functions of quaternary self-dual bent function in n variables and two self-dual bent functions in n variables was found. Based on this it was proved that there are no quaternary self-dual bent functions in odd number of variables.

In this paper we define the action of linear operator $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ on the generalized Boolean functions in n variables via their sign functions. We study the interconnection between unitary operators that transform the set of all generalized Boolean functions in n variables into itself and the duality mapping. The paper os organised as follows. In Section 2 necessary definitons and notation are given. In Section 3 properties of sign functions of self-dual gbent functions are considered. The main results are in Section 4, namely, Section 4.1, where unitary operators under consideration are characterized.The question whether the duality mapping can be described by the considered set of operators is partially studied in Section 5 The conclusion is in Section 6.

2 Notation

Let $\mathbb{F}_2^n$ be a set of binary vectors of length n. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$, where the sign $\oplus$ denotes a sum modulo 2. Denote, following [11], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in \mathrm{GL}\left(n, \mathbb{F}_2\right) : LL^T = I_n \right\},$$

where L^{T} denotes the transpose of L and I_n is an identical matrix of order n over the field $\mathbb{F}_2$.

A *generalized Boolean function* f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$, the integers modulo q. The set of generalized Boolean functions in n variables is denoted by $\mathcal{GF}_n^q$, for the case $q = 2$ we use $\mathcal{F}_n$. Let $\omega = e^{2\pi i/q}$. A *sign* function of $f \in \mathcal{GF}_n^q$ is a complex valued function $F = \omega^f$, we will also refer to it as to a complex vector $\left(\omega^{f_0}, \omega^{f_1}, \ldots, \omega^{f_{2^n-1}}\right)$ of length 2^n, where $(f_0, f_1, \ldots, f_{2^n-1})$ is a vector of values of the function f.

The *Hamming weight* $\mathrm{wt}_H(x)$ of the vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates of x. The *Hamming distance* $\mathrm{dist}_H(f, g)$ between generalized Boolean functions f, g in n variables is the cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$. The Lee weight of the element $x \in \mathbb{Z}_q$ is $\mathrm{wt}_L(x) = \min\{x, q - x\}$. The Lee distance $\mathrm{dist}_L(f, g)$ between $f, g \in \mathcal{GF}_n^q$ is

$$\mathrm{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L\left(\delta(x)\right),$$

where $\delta \in \mathcal{GF}_n^q$ and $\delta(x) = f(x) + (q-1)g(x)$ for any $x \in \mathbb{F}_2^n$. For Boolean case $q = 2$ the Hamming distance coincides with the Lee distance.

The *(generalized) Walsh–Hadamard transform* of $f \in \mathcal{GF}_n^q$ is the complex valued function:

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}.$$

A generalized Boolean function f in n variables is said to be *generalized bent* (gbent) if

$$|H_f(y)| = 2^{n/2},$$

for all $y \in \mathbb{F}_2^n$ [27]. If there exists such $\widetilde{f} \in \mathcal{GF}_n^q$ that $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$, the gbent function f is said to be *regular* and $\widetilde{f}$ is called its *dual*. Note that $\widetilde{f}$ is generalized bent as well. A regular gbent function f is said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} + q/2$. Consequently, it is the case only for even q. So throughout this paper we assume that q is

a positive even integer. Corresponding sets of gbent functions are denoted by $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$, respectively.

The *duality mapping* is a mapping that transforms every regular gbent function to its dual one. Thus, it is essentially defined only on regular gbent functions.

3 Eigenvectors of the duality mapping

In this section properties of sign functions of (anti-)self-dual gbent functions will be studied and the connection with the duality mapping will be explicitely pointed.

Let I_n be the identity matrix of size n and $H_n = H_1^{\otimes n}$ be the n-fold tensor product of the matrix H_1 with itself, where

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

This matrix is known as Sylvester Hadamard matrix. It is known the Hadamard property of this matrix

$$H_n H_n^T = 2^n I_{2^n},$$

where H_n^T is transpose of H_n (it holds $H_n^T = H_n$ by symmetricity of H_n). Denote $\mathcal{H}_n = 2^{-n/2} H_n$.

By using Sylvester Hadamard matrix it is possible to define the duality mapping as follows

$$\omega^f \longrightarrow \mathcal{H}_n \omega^f = \omega^{\widetilde{f}},$$

where f is a regular gbent function in n variables. Thus, sign functions if self-dual gbent functions are eigenvectors of the aforementioned linear operator that correspond to the eigenvalue 1. At the same time sign functions if anti-self-dual gbent functions are eigenvectors of the aforementioned linear operator that correspond to the eigenvalue (-1). In terms of subspaces these facts imply that sign functions belong to the spaces $\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big) = \mathrm{Ker}\big(H_n - 2^{n/2} I_{2^n}\big)$ and $\mathrm{Ker}\big(\mathcal{H}_n + I_{2^n}\big) = \mathrm{Ker}\big(H_n + 2^{n/2} I_{2^n}\big)$ correspondingly.

Recall an orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of H_n from [1] (Lemma 5.2):

$$\mathbb{R}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

where the symbol $\oplus$ denotes a direct sum of subspaces. Consider the same decomposition

$$\mathbb{C}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

for a complex space $\mathbb{C}^{2^n}$. It is known that

$$\dim\big(\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)\big) = \dim\big(\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big)\big) = 2^{n-1},$$

where $\dim(V)$ is the dimension of the subspace $V \subseteq \mathbb{C}^{2^n}$. Moreover, since $\mathcal{H}_n$ is symmetric (Hermitian), the subspaces $\mathrm{Ker}\big(\mathcal{H}_n + I_{2^n}\big)$ and $\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big)$ are mutually orthogonal.

In [15] it was proved that provided $n \geqslant 4$, the linear span of sign functions of self-dual as well as anti-self-dual Boolean bent functions Boolean bent functions in n variables has dimension 2^{n-1}. The same result can be also given for gbent functions:

Proposition 1. *Let $n \geqslant 4$ be an evem number, then the linear span of sign functions of (anti-)self-dual gbent functions in n variables has dimension 2^{n-1}.*

Proof. It is enough to mention that since q is even it holds $(-1) = \omega^{q/2} \in \left\{\omega, \omega^2, \ldots, \omega^{q-1}\right\}$, therefore the set of sign fuctions of (anti-)self-dual Boolean bent functions in n variables is a subset of the set of sign functions of (anti-)self-dual gbent functions in n variables. □

It is worth to note that the example of the basis of the subspace $\mathrm{Ker}\big(\mathcal{H}_n - I_{2^n}\big)$ can be constructed by using the functions obtained via iterative constructions from [1] and [15].

When $n = 2$ there are two self-dual Boolean bent functions, namely x_1x_2 and $x_1x_2 \oplus 1$, which have sign functions $(1, 1, 1, -1)$ and $(-1, -1, -1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$. The set $\mathrm{SB}^-(2)$ consists of functions $x_1x_2 \oplus x_1 \oplus x_2$ and $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ with sign functions $(1, -1, -1, -1)$ and $(-1, 1, 1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$ as well. Generalization comprises solution of the system

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix} = \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix},$$

where variables are numbers $d_1, d_2, d_3, d_4 \in \mathbb{Z}_q$ in fact. It is clear that the only solution pattern is

$$\left(\omega^d, \omega^d, \omega^d, \omega^{d+q/2}\right) = \omega^d \cdot (1, 1, 1, -1) \in \mathbb{C}^4,$$

where $d \in \mathbb{Z}_q$. It means that any two sign functions of self-dual gbent functions from $\mathrm{SB}_q^+(2)$ are linearly dependent over $\mathbb{C}$ and $\left|\mathrm{SB}_q^+(2)\right| = q$.

4 Unitary operators and eigenvectors of the duality mapping

In this section we define an action of linear operator $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ on a (generalized) Boolean function in n variables and characterize all unitary operators which transform the set of all (generalized) Boolean functions in n variables into itself and preserve self-duality, thus generalizing in some way the results from [16] on isometric mappings which preserve self-duality of a Boolean bent function and those, which define bijections between the sets of self-dual and anti-self-dual Boolean bent functions.

4.1 Linear operators and generalized Boolean functions

Throught this section we will use standard basis of the space $\mathbb{C}^{2^n}$, which consists of the vectors $\{e_i\}_{i=1}^{2^n} \subset \mathbb{C}^{2^n}$, where e_i has 1 on th i-th position, the rest are zeros.

Let $\varphi : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ be linear operator with matrix A in standard basis of the space $\mathbb{C}^{2^n}$. We shall say that φ *transforms* the generalized Boolean function $f \in \mathcal{GF}_n^q$ with sign function F to the generalized Boolean function $f' \in \mathcal{GF}_n^q$ if the sign function F' of f' is equal to AF, that is $F' = AF = \varphi(F)$. This also comprises the definition of the duality mapping via the Sylvester Hadamard matrix (see Section 3).

Recall that a linear operator φ is said to be *unitary* if $\varphi\varphi^\dagger = \varphi^\dagger\varphi = id$, where $\varphi^\dagger$ is a Hermitian adjoint operator of φ. The matrix of φ is called unitary in this case. Denote by $\mathcal{U}_n^q$ the set of unitary operators $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ which transform the set of generalized Boolean functions in n variables $\mathcal{GF}_n^q$ into itself.

The next result characterizes the set $\mathcal{U}_n^q$. The matrix is called *monomial* or *generalized permutation* if it has exactly one nonzero entry in every row (column).

Theorem 1. *Operators from $\mathcal{U}_n^q$ are characterized by monomial matrices with nonzero elements from the set $\left\{1, \omega, \omega^2, \ldots, \omega^{q-1}\right\}$ and only them.*

Proof. It is obvious that operators with monomial matrices of such form transform the set of q-ary generalized Boolean functions in n variables into itself. Moreover every such matrix is unitary.

Now assume $\varphi \in \mathcal{U}_n^q$ and let $U = (u_{ij})_{i,j=1}^{2^n}$ be its matrix in the canonical basis. Denote by $v_0 \in \mathbb{C}^{2^n}$ a vector with all ones and by $v_i \in \mathbb{C}^{2^n}, i = 1, 2, \ldots, 2^n$, a vector which has 1 on the i-th position, the rest are (-1). Let

$v_{ij} \in \mathbb{C}^{2^n}, i, j = 1, 2, \ldots, 2^n, (i \neq j)$, be a vector which has 1 on the i-th and j-th positions, the rest are (-1)

Fix some $i, j, k \in \{1, 2, \ldots, 2^n\}, (i < j)$. Denote $(Uv_0)_k = \omega^{d_0}, (Uv_i)_k = \omega^{d_i}$, $(Uv_j)_k = \omega^{d_j}$ and $(Uv_{ij})_k = \omega^{d_{ij}}$ for some $d_0, d_i, d_j, d_{ij} \in \mathbb{Z}_q$. Their addition yields

$$\begin{aligned}
(Uv_0)_k + (Uv_i)_k &= 2u_{ki} = \omega^{d_0} + \omega^{d_i}, \\
(Uv_0)_k + (Uv_j)_k &= 2u_{kj} = \omega^{d_0} + \omega^{d_j}, \\
(Uv_0)_k + (Uv_{ij})_k &= 2\left(u_{ki} + u_{kj}\right) = \omega^{d_0} + \omega^{d_{ij}}.
\end{aligned}$$

After grouping of these items we see that

$$u_{ki} = \frac{\omega^{d_0} + \omega^{d_i}}{2}, \quad u_{kj} = \frac{\omega^{d_0} + \omega^{d_j}}{2}, \quad u_{ki} + u_{kj} = \frac{\omega^{d_0} + \omega^{d_{ij}}}{2},$$

that is

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_0} + \omega^{d_j} = \omega^{d_0} + \omega^{d_{ij}},$$

or, equivalently,

$$\omega^{d_0} + \omega^{d_i} + \omega^{d_j} = \omega^{d_{ij}}.$$

Its is clear that it is the case only if $\omega^{d_{ij}}$ coincides with one of three numbers $\omega^{d_0}, \omega^{d_i}, \omega^{d_j}$ and the rest two are the same numbers with opposite signs, that is always possible since q is even.

Basically there are two variants:

Case 1: If $\omega^{d_{ij}} = \omega^{d_0}$ and $\omega^{d_i} + \omega^{d_j} = 0$, then the k-th row of U is

$$U_k = \left(u_{k1}, \ldots, u_{k,i-1}, \frac{\omega^{d_0} - \omega^{d_j}}{2}, u_{k,i+1}, \ldots, u_{k,j-1}, \frac{\omega^{d_0} + \omega^{d_j}}{2}, u_{k,j+1}, \ldots, u_{k,2^n}\right).$$

But in this case

$$\begin{aligned}
|u_{ki}|^2 + |u_{kj}|^2 &= \frac{1}{4}\left(\left|\omega^{d_0} - \omega^{d_j}\right|^2 + \left|\omega^{d_0} + \omega^{d_j}\right|^2\right) \\
&= \frac{1}{4}\left[\left(\omega^{d_0} - \omega^{d_j}\right)\left(\overline{\omega^{d_0}} - \overline{\omega^{d_j}}\right) + \left(\omega^{d_0} + \omega^{d_i}\right)\left(\overline{\omega^{d_0}} + \overline{\omega^{d_j}}\right)\right] \\
&= \frac{1}{4}\left(\omega^{d_0}\overline{\omega^{d_0}} - \omega^{d_0}\overline{\omega^{d_j}} - \omega^{d_j}\overline{\omega^{d_0}} + \omega^{d_j}\overline{\omega^{d_j}}\right) \\
&+ \frac{1}{4}\left(\omega^{d_0}\overline{\omega^{d_0}} + \omega^{d_0}\overline{\omega^{d_j}} + \omega^{d_j}\overline{\omega^{d_0}} + \omega^{d_j}\overline{\omega^{d_j}}\right) \\
&= \frac{1}{4}\left(2 \cdot \omega^{d_0}\overline{\omega^{d_0}} + 2 \cdot \omega^{d_j}\overline{\omega^{d_j}}\right) = \frac{1}{4}(2 + 2) = 1,
\end{aligned}$$

and since U is unitary that implies $\|U_k\|^2 = 1$ for any $k \in \{1, 2, \ldots, 2^n\}$, we derive that all components of U_k except, maybe,

$$u_{ki} = \frac{\omega^{d_0} - \omega^{d_j}}{2},$$

$$u_{kj} = \frac{\omega^{d_0} + \omega^{d_j}}{2},$$

are necessarily equal to zero.

Case 2: Without loss of generality assume that $\omega^{d_{ij}} = \omega^{d_i}$ and $\omega^{d_0} + \omega^{d_j} = 0$, then $u_{kj} = 0$.

Thus for any distinct $i, j \in \{1, 2, \ldots, 2^n\}$ either at least one of items u_{ki}, u_{kj} of the k-th row U_k is zero or in this row there are at most two nonzero items, whose form was considered in Case 1.

If for any row only Case 2 is met, the matrix is obviously monomial. So assume that some row of U, say k-th (in fact, then U has at least two rows of such form), has the form which is described in Case 1.

Consider vector (sign function) $F \in \mathbb{C}^{2^n}$ whose coordinates for $l = 1, 2, \ldots, 2^n$ are defined by

$$F_l = \begin{cases} \omega^{r_1}, & l = i, \\ \omega^{r_2}, & l = j, \\ 1, & \text{otherwise}, \end{cases}$$

where $r_1, r_2 \in \mathbb{Z}_q$ such that $r_1 < r_2$ and $r_2 - r_1 \neq q/2$, denote $\Delta r = r_2 - r_1$. We have

$$(UF)_k = u_{ki}\omega^{r_1} + u_{kj}\omega^{r_2} = \omega^{r_1}\left(\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2}\omega^{\Delta r}\right) = \omega^{s+r_1},$$

for some $s \in \mathbb{Z}_q$. It is clear that it holds if and only if

$$\frac{\omega^{d_0} - \omega^{d_j}}{2} + \frac{\omega^{d_0} + \omega^{d_j}}{2}\omega^{\Delta r} = \omega^s.$$

Recall some trigonometric identities. For any real α, β it holds:

$$\begin{aligned} \cos\alpha + \cos\beta &= 2\cos\left(\frac{\alpha+\beta}{2}\right)\cos\left(\frac{\alpha-\beta}{2}\right), \\ \cos\alpha - \cos\beta &= -2\sin\left(\frac{\alpha+\beta}{2}\right)\sin\left(\frac{\alpha-\beta}{2}\right), \\ \sin\alpha \pm \sin\beta &= 2\sin\left(\frac{\alpha\pm\beta}{2}\right)\cos\left(\frac{\alpha\mp\beta}{2}\right), \\ \sin(\alpha \pm \beta) &= \sin\alpha\cos\beta \pm \cos\alpha\sin\beta, \\ \sin 2\alpha &= 2\cos\alpha\sin\alpha. \end{aligned}$$

Consider doubled real part of ω^s:

$$\begin{aligned}2\mathrm{Re}\left(\omega^s\right) &= \cos\left(\frac{2\pi d_0}{q}\right) - \cos\left(\frac{2\pi d_j}{q}\right) \\ &+ \cos\left(\frac{2\pi\left(d_0+\Delta r\right)}{q}\right) + \cos\left(\frac{2\pi\left(d_j+\Delta r\right)}{q}\right) \\ &= 2\cos\left(\frac{\pi\left(2d_0+\Delta r\right)}{q}\right)\cos\left(\frac{\pi\Delta r}{q}\right) \\ &- 2\sin\left(\frac{\pi\left(2d_j+\Delta r\right)}{q}\right)\sin\left(\frac{\pi\Delta r}{q}\right),\end{aligned}$$

and doubled imaginary part of ω^s:

$$\begin{aligned}2\mathrm{Im}\left(\omega^s\right) &= \sin\left(\frac{2\pi d_0}{q}\right) - \sin\left(\frac{2\pi d_j}{q}\right) \\ &+ \sin\left(\frac{2\pi\left(d_0+\Delta r\right)}{q}\right) + \sin\left(\frac{2\pi\left(d_j+\Delta r\right)}{q}\right) \\ &= 2\sin\left(\frac{\pi\left(2d_0+\Delta r\right)}{q}\right)\cos\left(\frac{\pi\Delta r}{q}\right) \\ &+ \sin\left(\frac{\pi\Delta r}{q}\right)\cos\left(\frac{\pi\left(2d_j+\Delta r\right)}{q}\right).\end{aligned}$$

For simplicity denote $\alpha = \pi\Delta r/q, \beta = \pi\left(2d_0+\Delta r\right)/q$ and $\gamma = \pi\left(2d_j+\Delta r\right)/q$. Since ω^s is a root of unity, its norm is equal to 1, hence

$$\begin{aligned}\mathrm{Re}^2\left(\omega^s\right) + \mathrm{Im}^2\left(\omega^s\right) &= \cos^2\alpha\cos^2\beta - 2\cos\alpha\sin\alpha\cos\beta\sin\gamma + \sin^2\alpha\sin^2\gamma \\ &+ \cos^2\alpha\sin^2\beta + 2\cos\alpha\sin\alpha\sin\beta\cos\gamma + \sin^2\alpha\cos^2\gamma \\ &= \cos^2\alpha\left(\cos^2\beta+\sin^2\beta\right) + \sin^2\alpha\left(\cos^2\gamma+\sin^2\gamma\right) \\ &+ 2\cos\alpha\sin\alpha\left(\sin\beta\cos\gamma - \cos\beta\sin\gamma\right) \\ &= 1 + \sin\left(2\alpha\right)\sin\left(\beta-\gamma\right) = 1,\end{aligned}$$

that is

$$\sin\left(2\alpha\right)\sin\left(\beta-\gamma\right) = 0.$$

Let the firt sine is zero, that is

$$2\alpha = \frac{2\pi\Delta r}{q} = \pi m,$$

for some $m \in \mathbb{Z}$. Then $\Delta r = mq/2$ but since $\Delta r \in \{1, 2, \ldots, q-1\}$, it is the case only for $\Delta r = q/2$, that is a contradiction with the choice of r_1, r_2.

If the second sine is zero, namely

$$\beta - \gamma = \frac{2\pi\,(d_0 - d_j)}{q} = \pi m',$$

for some $m' \in \mathbb{Z}$, again we have either $d_0 = d_j$ or $|d_0 - d_j| = q/2$ since $|d_0 - d_j| \in \{0, 1, \ldots, q-1\}$. But then either $\omega^{d_0} - \omega^{d_j} = 0$ or $\omega^{d_0} + \omega^{d_j} = 0$, that is in the k-th row there is exactly one nonzero element. □

List below some apparent properties of $\mathcal{U}_n^q$ which can be derived from Theorem 1:

Proposition 2. *Every operator from $\mathcal{U}_n^q$ preserves Lee and Hamming distance between generalized Boolean functions and Euclidian distance between their sign functions.*

Proposition 3. *The cardinality of $\mathcal{U}_n^q$ is the following*

$$|\mathcal{U}_n^q| = 2^n! \cdot q^{2^n}.$$

4.2 Matrix representation and connection with Markov's theorem for Boolean case

A mapping φ of the set of all Boolean functions in n variables to itself is called *isometric* if it preserves the Hamming distance between functions, that is

$$\mathrm{dist}_H(\varphi(f), \varphi(g)) = \mathrm{dist}_H(f, g),$$

for any $f, g \in \mathcal{F}_n$. The set of all isometric mappings of the set of all Boolean functions in n variables to itself in [16] was denoted by $\mathcal{I}_n$.

From Markov's theorem (1956) it follows that the general form of isometric mappings of all Boolean functions in n variables to itself is

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$ [19].

Theorem 1 can be reformulated in terms of mappings of (generalized) Boolean functions:

Theorem 2. *The action of any operator from $\mathcal{U}_n^q$ on the set $\mathcal{GF}_n^q$ is uniquely represented in the form*

$$f(x) \longrightarrow f\,(\pi(x)) + g(x),$$

where π is a permuation on $\mathbb{F}_2^n$ and $g \in \mathcal{GF}_n^q$.

Following [16] denote such operator by $\varphi_{\pi,g} \in \mathcal{U}_n^q$. So, for binary case we immediately obtain correspondence between $\mathcal{U}_n^2$ and $\mathcal{I}_n$:

Corollary 1. *For $q = 2$ there is an one-to-one correspondence between the set $\mathcal{U}_n^q$ and the set of isometric mappings of all Boolean functions in n variables into itself ($\mathcal{I}_n$), defined by Markov's theorem.*

Thus the considered set $\mathcal{U}_n^q$ is a some kind of generalization of the set $\mathcal{I}_n$ comprising the framework of sign functions.

Denote by $\{\mathbf{v}_k\}_{k=0}^{2^n-1}$ all binary vectors of length n considered in the lexicographical order.

By Theorem 1, provided that the (standard) basis is fixed, there is an one-to-one correspondence between $\mathcal{U}_n^q$ and the set of monomial matrices of order $2^n \times 2^n$ with nonzero elements from the set $\left\{1, \omega^1, \omega^2, \ldots, \omega^{q-1}\right\}$. Indeed, consider arbitrary mapping $\varphi_{\pi,g} \in \mathcal{U}_n^q$. Let it transforms a function $f \in \mathcal{GF}_n^q$ with sign function

$$F = \left(\omega^{f(\mathbf{v}_0)}, \omega^{f(\mathbf{v}_1)}, \ldots, \omega^{f(\mathbf{v}_{2^n-1})}\right) \in \mathbb{C}^{2^n},$$

to $f' \in \mathcal{GF}_n^q$ with sign function

$$F' = \left(\omega^{f'(\mathbf{v}_0)}, \omega^{f'(\mathbf{v}_1)}, \ldots, \omega^{f'(\mathbf{v}_{2^n-1})}\right) \in \mathbb{C}^{2^n},$$

that is $F' = UF$, where U is a matrix of $\varphi_{\pi,g}$. Namely this matrix is

$$k\begin{pmatrix} & & & j & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ & & & \vdots & & & \\ \ldots & 0 & \ldots & \omega^{g(\mathbf{v}_{k-1})} & \ldots & 0 & \ldots \\ & & & \vdots & & & \\ & & & 0 & & & \\ & & & \vdots & & & \end{pmatrix},$$

in which in the k-th row a nonzero element $\omega^{g(\mathbf{v}_{k-1})}$ is in the j-th column, where $(j-1)$ is a number with binary representation $\pi(\mathbf{v}_{k-1})$. So the k-th component of the vector $F' = UF$ is equal to

$$\omega^{f'(\mathbf{v}_{k-1})} = \omega^{f(\pi(\mathbf{v}_{k-1}))} \cdot \omega^{g(\mathbf{v}_{k-1})} = \omega^{f(\pi(\mathbf{v}_{k-1}))+g(\mathbf{v}_{k-1})},$$

for any $k \in \{1, 2, \ldots, 2^n\}$, that is equivalent to

$$f'(x) = f(\pi(x)) + g(x), \quad x \in \mathbb{F}_2^n.$$

4.3 The Rayleigh quotient of (generalized) Boolean function

In this subsection operators from the set $\mathcal{U}_n^q$, which preserve and change the sign of the Rayleigh quotient (Rayleigh ratio) of the Sylvester Hadamard matrix defined for every generalized Boolean function in n variables, are studied.

In [1] *the Rayleigh quotient* S_f of a Boolean function $f \in \mathcal{F}_n$ was defined as

$$S_f = \sum_{x,y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x,y \rangle} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} W_f(y),$$

and when $f \in \mathcal{B}_n$ the *normalized Rayleigh quotient* N_f is a number

$$N_f = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \widetilde{f}(x)} = 2^{-n/2} S_f.$$

It is known [1] (Theorem 3.1) that the value of S_f is at most $2^{3n/2}$ with equality if and only if f is self-dual bent, and at least $\left(-2^{3n/2}\right)$ with equality if and only if f is anti-self-dual bent.

All isometric mappings from the set $\mathcal{I}_n$ that preserve the Rayleigh quotient of every Boolean function in n variables (or change its sign) were characterized in [16]. It was made by showing the direct link between perserving the Rayleigh quoient and preserving the self-duality. Also it was proved that bijectivity between the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ is correlated with the change of sign of the Rayleigh quoient.

In [28] the authors studied the Rayleigh quotient of generalized Boolean (bent) functions from $\mathcal{GF}_n^4$. For a generalized Boolean function $f \in \mathcal{GF}_n^4$ they defined

$$R(f) = 2^{-n} \sum_{x,y \in \mathbb{F}_2^n} i^{f(x)-f(y)} (-1)^{\langle x,y \rangle},$$

and proved, see [28] (Theorem 7), the bound $-2^{n/2} \leqslant R(f) \leqslant 2^{n/2}$ with equalities if and only if f is self-dual quaternary bent $(+2^{n/2})$ or self-dual quaternary bent $(-2^{n/2})$.

Define *the Rayleight quotient* R_f of (generalized) Boolean function $f \in \mathcal{GF}_n^q$ as follows

$$R_f = 2^{-n} \sum_{x,y \in \mathbb{F}_2^n} \omega^{f(x)-f(y)} (-1)^{\langle x,y \rangle}.$$

The matrix-vector representation the Rayleight quotient for a generalized Boolean function $f \in \mathcal{FG}_n^q$ with sign function F is

$$R_f = 2^{-n} \sum_{x \in \mathbb{F}_2^n} \overline{\omega^{f(x)}} \sum_{y \in \mathbb{F}_2^n} \omega^{f(y)} (-1)^{\langle x,y \rangle} = \frac{\langle F, H_n F \rangle}{\langle F, F \rangle}.$$

By the same technique as in the proof of [28] (Theorem 7) it is possible to prove that the same bound $-2^{n/2} \leqslant R_f \leqslant 2^{n/2}$ holds with equalities met if and only if f is self-dual gbent $(+2^{n/2})$ or anti-self-dual gbent $(-2^{n/2})$.

The mentioned correlation with preserving of self-duality and bijectivity for Boolean case also stands for the Rayleigh quotient of generalized Boolean function.

Theorem 3. *For $n \geqslant 4$ an operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$*

- *preserves the Rayleigh quotient if and only if it preserves (anti-)self-duality;*
- *changes the sign of the Rayleigh quotient if and only if it is a bijection between the sets $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$.*

The proofs of these statements are similar to those provided in [16] (Theorems 3 and 4) and are omitted.

It also follows that

Corollary 2. *An operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$, which preserves the Rayleigh quotient or changes the sign of the Rayleigh quotient, also preserves gbentness.*

5 The duality mapping and unitary operators

In this section for the case of even n we study the question if there exists an operator from the set $\mathcal{U}_n^q$, that transforms every regular gbent function to its dual gbent function.

Theorem 4. *If n is an even number, then in $\mathcal{U}_n^q$ there is no such operator which assigns the dual bent function to every regular bent function from the set $\mathcal{GB}_n^q$.*

Proof. Consider the following set of gbent functions:

$$B = \left\{ \frac{q}{2} f | f \in \mathcal{B}_n \right\} \subset \mathcal{GB}_n^q.$$

It is clear that all gbent functions from B are regular ones with the values from the set $\{0, q/2\}$. Assume the desired operator exists, let it be

$$\varphi_{\pi,g} : f(x) \longrightarrow f\left(\pi(x)\right) + g(x),$$

for some permutation π and generalized Boolean function $g \in \mathcal{GF}_n^q$. Then, in order to transform gebnt functions from the set B to their duals, the

function g also must have values in $\{0, q/2\}$. It means that in fact we have a reduction to Boolean case, since all considered generalized Boolean functions, namely that ones from the set B and the function g, have values from the set $\{0, q/2\}$.

Then non-existence of isometric mapping of the set of all Boolean functions in n variables into itself which assigns to every bent functions its dual implies non-existence of the considered unitary operator. It is known [14] that there is no such isometric mapping, hence the result follows.

□

Thus, Theorem 4 is a generalization of the known result of non-existence for the Boolean case, but here we consider all mappings from the set $\mathcal{U}_n^q$.

It is interesting to study the same question for the case of an odd number of variables n.

6 Conclusion

In this paper the action of linear operators of the form $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ on the generalized Boolean functions in n variables via their sign functions was defined. The interconnection between unitary operators that transform the set of all generalized Boolean functions in n variables into itself and the duality mapping was studied. The known classification of quaternary self-dual bent functions is clarified. It follows that the set $\mathcal{U}_n^q$ can be seen as an initial expansion of the set of automorphisms of the Boolean functions in n variables to generalized Boolean functions. For the future study it can be interesting to go beyond the set $\mathcal{U}_n^q$ that is to consider operators that transform some desired subsets of Boolean functions into itself but not neccesarily all generalized Boolean functions. Examples of such problems deal with gbent or self-dual gbent functions. The question of determing the connection between the set $\mathcal{U}_n^q$ and duality mapping for odd n is an open one.

Acknowledgments. The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (project no. 20-31-70043) and Laboratory of Cryptography JetBrains Research.

References

[1] Carlet C., Danielson L.E., Parker M.G., Solé. P., "Self-dual bent functions", *Int. J. Inform. Coding Theory*, **1** (2010), 384–399.

[2] Carlet C., *Boolean Functions for Cryptography and Coding Theory*, Cambridge Univ. Press, London, 2020, 620.

[3] Çeşmelioğlu A., Meidl W. Pott A., "On the dual of (non)-weakly regular bent functions and self-dual bent functions", *Adv. Math. Commun.*, **7**:4 (2013), 425–440.

[4] Cusick T.W., Stănică P., *Cryptographic Boolean functions and applications*, Acad. Press, London, 2017, 288.

[5] Feulner T., Sok L., Solé P., Wassermann A., "Towards the Classification of Self-Dual Bent Functions in Eight Variables", *Des. Codes Cryptogr.*, **68**:1 (2013), 395–406.

[6] Gangopadhyay S., Poonia V.S., Aggarwal D., Parekh R., "Generalized Boolean Functions and Quantum Circuits on IBM-Q", 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019.

[7] Hodžić S., Meidl W., Pasalic E., "Full Characterization of Generalized Bent Functions as (Semi)-Bent Spaces, Their Dual, and the Gray Image", *IEEE Trans. Inform. Theory*, **64**:7 (2018), 5432–5440.

[8] Hou X.-D., "Classification of self dual quadratic bent functions", *Des. Codes Cryptogr.*, **63**:2 (2012), 183–198.

[9] Hou X.-D., "Classification of p-ary self dual quadratic bent functions, p odd", *Journal of Algebra*, **391** (2013), 62–81.

[10] Hyun J.Y., Lee H., Lee Y., "MacWilliams duality and Gleason-type theorem on self-dual bent functions", *Des. Codes Cryptogr.*, **63**:3 (2012), 295–304.

[11] Janusz G.J., "Parametrization of self-dual codes by orthogonal matrices", *Finite Fields Appl.*, **13**:3 (2007), 450–491.

[12] Kumar P.V., Scholtz R.A., Welch L.R., "Generalized bent functions and their properties", *J. Comb. Theory Series A*, **40** (1985), 90–107.

[13] Luo G., Cao X., Mesnager S., "Several new classes of self-dual bent functions derived from involutions", *Cryptogr. Commun.*, **11**:6 (2019).

[14] Kutsenko A.V., "On some properties of known isometric mappings of the set of bent functions", *Prikl. Diskr. Mat. Suppl. (Applied Discrete Math. Supplement)*, **10** (2020), 43–44.

[15] Kutsenko A., "Metrical properties of self-dual bent functions", *Des. Codes Cryptogr.*, **88**:1 (2020), 201–222.

[16] Kutsenko A., "The group of automorphisms of the set of self-dual bent functions", *Cryptogr. Commun.*, **12**:5 (2020), 881–898.

[17] Kutsenko A., Tokareva N., "Metrical properties of the set of bent functions in view of duality", *Prikl. Diskr. Mat. (Applied Discrete Math.)*, **49** (2020), 18–34.

[18] Logachev O.A., Sal'nikov A.A., Yashchenko V.V., "Bent functions on a finite Abelian group", *Discrete Math. Appl.*, **7**:6 (1997), 547–564.

[19] Markov A. A., "On transformations without error propagation", *Selected Works, Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, MTsNMO, Moscow*, 2003, 70–93, In Russian.

[20] Martinsen T., Meidl W., Stănică P., "Partial spread and vectorial generalized bent functions", *Des. Codes Cryptogr.*, **85**:1 (2017), 1–13.

[21] Mesnager S., "Several New Infinite Families of Bent Functions and Their Duals", *IEEE Trans. Inf. Theory*, **60**:7 (2014), 4397–4407.

[22] Mesnager S., *Bent Functions: Fundamentals and Results,*, Springer, Berlin, 2016, 544 p.

[23] Mesnager S., Tang C., Qi Y., Wang L., Wu B., Feng K., "Further Results on Generalized Bent Functions and Their Complete Characterization", *IEEE Trans. Inform. Theory*, **64**:7 (2018), 5441–5452.

[24] Paterson K.G., "Generalized Reed–Muller Codes and Power Control in OFDM Modulation", *IEEE Trans. Inform. Theory*, **46**:1 (2000), 104–120.

[25] Riera C., Stănică P., Gangopadhyay S., "Generalized bent Boolean functions and strongly regular Cayley graphs", *Discrete Appl. Math.*, **283** (2020), 367–374.

[26] Rothaus O.S., "On bent functions", *J. Combin. Theory. Ser. A*, **20**:3 (1976), 300–305.

[27] Schmidt K.-U., "Quaternary constant-amplitude codes for multicode CDMA", *IEEE Trans. Inform. Theory*, **55**:4 (2009), 1824–1832.

[28] Sok L., Shi M., Solé. P., "Classification and Construction of quaternary self-dual bent functions", *Cryptogr. Commun.*, **10**:2 (2018), 277–289.

[29] Solodovnikov V.I., "Bent functions from a finite Abelian group into a finite Abelian group", *Discret. Math. Appl.*, **12**:2 (2002), 111–126.

[30] Stănică P., Martinsen T., Gangopadhyay S., Singh B. K., "Bent and generalized bent Boolean functions", *Des. Codes Cryptogr.*, **69**:1 (2013), 77–94.

[31] Tang C., Xiang C., Qi Y., Feng K., "Complete characterization of generalized bent and2k-bent Boolean functions", *IEEE Trans. Inform. Theory*, **63** (2017), 4668–4674.

[32] Tokareva N.N., "Generalizations of bent functions — a survey", *J. Appl. Ind. Math.*, **5**:1 (2011), 110–129.

[33] Tokareva N., *Bent Functions, Results and Applications to Cryptography*, Acad. Press. Elsevier, 2015, 230.

[34] Wada T., "Characteristic bit sequences applicable to constant amplitude orthogonal multicode systems", *IEICE Trans. Fundamentals*, **E83-A**:11 (2000), 2160–2164.

On derivatives of Boolean bent functions

Shaporenko Alexander

Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia
JetBrains Research, Novosibirsk, Russia
shaporenko.alexandr@gmail.com

Abstract

In this paper, the property of affine functions to be derivatives of bent functions is studied. The importance of Boolean bent functions in symmetric cryptography stems from linear cryptanalysis of stream ciphers. In that context bent functions are the ones which are the worst approximated by affine functions. There are also connections between bent functions and distinct objects of coding theory such as Reed-Muller and Kerdock codes. Recall, that a bent function is a Boolean function f in n variables (n is even) such that for any nonzero vector y its derivative $D_y f(x) = f(x) \oplus f(x \oplus y)$ is balanced, i.e., it takes values 0 and 1 equally often. Whether every balanced function is a derivative of a some bent function or not is an open problem. In this paper, special case of this problem was studied. It was proven that every nonconstant affine function in n (even) variables is a derivative of $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ bent functions, where $\mathcal{B}_n$ is a set of all bent functions in n variables. Iterative lower bound for the number of bent functions is presented.

Keywords: Boolean functions, bent functions, derivatives of a bent function, lower bound for the number of bent functions.

1 Introduction

A Boolean function in even number of variables is called *bent* if it has maximal nonlinearity [1]. Nonlinearity is an important property in cryptography. Ciphers using functions with high nonlinearity as components are more resistant to linear cryptanalysis [2] because bent functions are badly approximated by affine functions. Bent functions were used in design of the block cipher CAST as coordinate functions of S-blocks [3]. The nonlinear feedback polynomial of the NFSR (nonlinear feedback shift register) of the stream cipher Grain is constructed as the sum of a linear function and a bent function [4]. There are also connections between bent functions and distinct objects of coding theory such as *Reed-Muller and Kerdock codes* [5]. In coding theory,

there is a well-known task of determining the covering radius for the *Reed-Muller code* $RM(l, n)$. This task is related (if the code has order 1) to the task of finding the most nonlinear Boolean functions [6, 7]. Special sets of quadratic bent functions allow one to construct Kerdock codes [8] that are optimal and have large code distances that grow with the code lengths [9, 10]. This very optimality of Kerdock codes is caused by extremal properties of bent functions.

Another definition of a bent function is the following. It is a Boolean function f in n variables (n is even) such that for any nonzero vector y its derivative $D_y f(x) = f(x) \oplus f(x \oplus y)$ is balanced, i.e., it takes values 0 and 1 equally often [5]. In [11] it was shown that every balanced function is a derivative of a some bent function for $n \leqslant 6$ (n even). Whether it is true for every even n is an open problem. We will study this problem for the case of affine functions.

2 Necessary definitions and statements

Let $\mathbb{Z}_2 = \{0, 1\}$. Denote by $\mathbb{Z}_2^n$ the n-dimensional vector space over $\mathbb{Z}_2$. Let us denote by $\oplus$ the addition modulo 2. We will also use the following inner product:

$$\langle x, y \rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n.$$

A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called *a Boolean function* in n variables. A Boolean function f is called *affine* if it can be represented as $l_{a,b}(x) = \langle a, x \rangle \oplus b$, where $a \in \mathbb{Z}_2^n$ and $b \in \mathbb{Z}_2$. A Boolean function is called *balanced* if it takes values 0 and 1 equally often.

Let us recall a well known fact.

Lemma 1. *An affine function $l_{a,b}(x) = \langle a, x \rangle \oplus b$, where $a \in \mathbb{Z}_2^n$ (nonzero) and $b \in \mathbb{Z}_2$, is balanced.*

The Hamming weight $wt(f)$ of a Boolean function f is the number of vectors $x \in Z_2^n$ such that $f(x) = 1$. For nonconstant affine functions it is equal to 2^{n-1}. We denote by $dist(f, g)$ *the Hamming distance* between two Boolean functions f and g; it is the number of positions in which their vectors of values differ:

$$dist(f, g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}|.$$

Every Boolean function f in n variables can be associated with its *support*:

$$\mathrm{supp}(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}.$$

A Boolean function $D_y f(x) = f(x) \oplus f(x \oplus y)$ is called a *derivative* of a Boolean function f in n variables in *the direction* y, where $y \in \mathbb{Z}_2^n$.

Lemma 2. *A Boolean function f in n variables is a derivative of a some Boolean function g in n variables in nonzero direction y if and only if $f(x) \oplus f(x \oplus y) = 0$ for all $x \in \mathbb{Z}_2^n$.*

Proof. ($\Rightarrow$) One can see that $D_y g(x) = g(x) \oplus g(x \oplus y) = D_y g(x \oplus y)$ for all $x \in \mathbb{Z}_2^n$. Therefore, $f(x) = f(x \oplus y)$ for all $x \in \mathbb{Z}_2^n$.

($\Leftarrow$) Let i be the first nonzero coordinate of y. Define a Boolean function g in the following way $g(x) = x_i f(x)$ for all $x \in \mathbb{Z}_2^n$. Then

$$D_y g(x) = x_i f(x) \oplus (x_i \oplus 1) f(x \oplus y) = f(x) \text{ for all } x \in \mathbb{Z}_2^n.$$

Therefore, f is a derivative of g in the direction y. □

The *nonlinearity* of a Boolean function f in n variables is the Hamming distance N_f from this function to the set of all affine functions, i.e., $N_f = \min\limits_{a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2} dist(f, l_{a,b})$.

A *bent function* is a Boolean function in an even number of variables that has the maximal nonlinearity, i.e., $N_f = 2^{n-1} - 2^{n/2-1}$. Denote by $\mathcal{B}_n$ a set of all bent functions in n variables.

The Walsh-Hadamard transform of a Boolean function f in n variables is the integer-valued function on $\mathbb{Z}_2^n$ defined as

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \text{ for every } y \in \mathbb{Z}_2^n.$$

For a bent function f, the *dual function* $\tilde{f}$ in n variables is defined by the equality $W_f(y) = 2^{n/2}(-1)^{\tilde{f}(y)}$. This definition is correct since $W_f(y) = \pm 2^{n/2}$ for any vector y if f is a bent function [5].

Lemma 3. *(see, for instance, [5]) A Boolean function f in n variables is bent if and only if for any nonzero vector y its derivative $D_y f(x) = f(x) \oplus f(x \oplus y)$ is balanced or equivalently it holds*

$$\sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} = 0, \text{ for any nonzero } y.$$

Lemma 4. *Let $l_{a,b}(x) = \langle a, x \rangle \oplus b$, where $a \in \mathbb{Z}_2^n$, a is nonzero, and $b \in \mathbb{Z}_2$. There are $2^{n-1} - 1$ nonzero directions for which $l_{a,b}$ is a derivative of a some Boolean function. Namely, these directions are exactly those nonzero vectors y such that $\langle a, y \rangle = 0$.*

Proof. If $\langle a, y\rangle = 0$ then

$$l_{a,b}(x) \oplus l_{a,b}(x \oplus y) = \langle a, x\rangle \oplus b \oplus \langle a, x \oplus y\rangle \oplus b = \langle a, y\rangle = 0.$$

Therefore, it follows from Lemma 2 that the function $l_{a,b}$ is a derivative of a some Boolean function in the direction y. It is known that there exist 2^{n-1} different nonzero vectors y such that $\langle a, y\rangle = 0$ if a is nonzero. Since $\langle a, 0\rangle = 0$ as well, the statement is proved. □

Lemma 5. *Let l be a nonconstant affine function that is a derivative of bent functions g and g' in distinct nonzero directions y and y', respectively. Then $g \neq g'$.*

Proof. Suppose that $g = g'$ is a bent function such that $D_y g(x) = D_{y'} g(x) = l(x)$ for $y \neq y'$. Then for every $x \in \mathbb{Z}_2^n$ it holds

$$\begin{aligned} &D_y g(x) \oplus D_{y'} g(x) = \\ &= g(x) \oplus g(x \oplus y) \oplus g(x) \oplus g(x \oplus y') = \\ &= g(x \oplus y) \oplus g(x \oplus y') = \\ &= g(x \oplus y) \oplus g(x \oplus y \oplus (y' \oplus y)) = \\ &= D_{y' \oplus y} g(x \oplus y) = 0, \end{aligned}$$

which contradicts Lemma 3. □

3 Affine functions as derivatives of bent functions

In what follows we suppose that n is even.

Theorem 1. *Any nonconstant affine function $l_{a,b}$ in n variables is a derivative of $(2^{n-1} - 1)|\mathcal{B}_{n-2}|^2$ bent functions in $n \geq 4$ variables.*

Proof. Let $l_{a,b}(x) = \langle a, x\rangle \oplus b$ be an affine function in $n \geq 4$ variables, where $a \in \mathbb{Z}_2^n$ is nonzero and $b \in \mathbb{Z}_2$. Suppose that $l_{a,b}$ is a derivative of some Boolean function in the direction y'.

Let i be the number of the first nonzero coordinate of y' and j be the number such that $j \neq i$ and x_j is an essential variable for $l_{a,b}$. Let us show that such j always exists. Suppose the opposite. Then $l_{a,b}(x) = x_i \oplus b$ and $D_{y'} l_{a,b}(x) = l_{a,b}(x) \oplus l_{a,b}(x \oplus y') = 1$, for every $x \in \mathbb{Z}_2^n$, which by Lemma 2 contradicts the fact that $l_{a,b}$ is a derivative of g in the direction y'.

Without loss of generality, let $i = 1$ and $j = 2$. It follows from Lemma 2 that $l_{a,b}(x) = l_{a,b}(x \oplus y')$ and hence

$$x \in \mathrm{supp}(l_{a,b}) \iff x \oplus y' \in \mathrm{supp}(l_{a,b}). \tag{1}$$

Note that for any Boolean function g in n variables that has $\ell_{a,b}$ as its derivative in the direction y' it holds that

$$g(x) \oplus g(x \oplus y') = l_{a,b}(x). \tag{2}$$

It follows from (1) and (2) that any Boolean function g, such that $D_{y'}g(x) = \ell_{a,b}(x)$, has the following representation

$$\begin{aligned}
&g(0, x_2, \bar{x}) = f_0(\bar{x}), && (0, x_2, \bar{x}) \in \mathrm{supp}(l_{a,b}),\\
&g(1, x_2 \oplus y'_2, \bar{x} \oplus \bar{y'}) = f_0(\bar{x}) \oplus 1, && (1, x_2 \oplus y'_2, \bar{x} \oplus \bar{y'}) \in \mathrm{supp}(l_{a,b}),\\
&g(0, x_2, \bar{x}) = f_1(\bar{x}), && (0, x_2, \bar{x}) \notin \mathrm{supp}(l_{a,b}),\\
&g(1, x_2 \oplus y'_2, \bar{x} \oplus \bar{y'}) = f_1(\bar{x}), && (1, x_2 \oplus y'_2, \bar{x} \oplus \bar{y'}) \notin \mathrm{supp}(l_{a,b}),
\end{aligned}$$

where

$$\bar{z} = (z_3, \ldots, z_n), \text{for } z_k \in \mathbb{Z}_2$$

and f_0, f_1 are some Boolean functions in $n-2$ variables. Therefore, by considering different Boolean functions in $n-2$ variables as f_0 and f_1, we can get all Boolean functions in n variables that have $\ell_{a,b}$ as its derivative in the direction y'.

Let f_0 and f_1 be bent functions and g be defined as above. Denote by $M = \{x \in \mathbb{Z}_2^n : x_1 = 0\}$. Thus, $x \in M \iff x \oplus y' \in \mathbb{Z}_2^n \backslash M$.

Let us show that g is bent by checking that $D_y g(x)$ is balanced for every nonzero $y \neq y'$.

Suppose that $b = 0$. Then $l_{a,b}(x \oplus y) = l_{a,b}(x) \oplus l_{a,b}(y)$ and from (1) and (2) we have

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus g(x \oplus y)} =\\
&= \sum_{\substack{x \in M\\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x \oplus y') \oplus g(x \oplus y \oplus y')} +\\
&+ \sum_{\substack{x \in M\\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x \oplus y') \oplus g(x \oplus y \oplus y')} =
\end{aligned}$$

$$\begin{aligned}
&= \sum_{\substack{x \in M\\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x) \oplus g(x \oplus y) \oplus l_{a,b}(x) \oplus l_{a,b}(x \oplus y)} +\\
&+ \sum_{\substack{x \in M\\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x) \oplus g(x \oplus y) \oplus l_{a,b}(x) \oplus l_{a,b}(x \oplus y)} =
\end{aligned}$$

$$= \sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus l_{a,b}(y)} +$$
$$+ \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus l_{a,b}(y)}.$$

There are two cases:

Case 1. If $l_{a,b}(y) = 1$. Then

$$\sum_{x\in\mathbb{Z}_2^n} (-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= \sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus 1} +$$
$$+ \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus 1} = 0.$$

Case 2. If $l_{a,b}(y) = 0$. Then $l_{a,b}(x\oplus y) = 1 \iff l_{a,b}(x) = 1$.
Suppose that $y_1 = 0$. Then

$$g(0, x_2\oplus y_2, \bar{x}\oplus\bar{y}) = f_0(\bar{x}\oplus\bar{y}), \qquad (0, x_2, \bar{x}) \in \mathrm{supp}(l_{a,b}),$$
$$g(0, x_2\oplus y_2, \bar{x}\oplus\bar{y}) = f_1(\bar{x}\oplus\bar{y}), \qquad (0, x_2, \bar{x}) \notin \mathrm{supp}(l_{a,b}),$$

and

$$\sum_{x\in\mathbb{Z}_2^n} (-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= \sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)} +$$
$$+ \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= 2\Big(\sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} + \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x)\oplus g(x\oplus y)} \Big) =$$
$$= 2\Big(\sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}} (-1)^{f_0(\bar{x})\oplus f_0(\bar{x}\oplus\bar{y})} + \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}} (-1)^{f_1(\bar{x})\oplus f_1(\bar{x}\oplus\bar{y})} \Big). \qquad (3)$$

Let us show that $\bar{y} \neq 0$. Since y is nonzero, then $\bar{y} = 0$ only if $y_2 = 1$. But in that case $l_{a,b}(y) = 1$ since x_2 is an essential variable for $l_{a,b}$ and $b = 0$.

Note that if $(a_1, a_2, \bar{x}) \in \mathrm{supp}(l_{a,b})$ then $(a_1, a_2 \oplus 1, \bar{x}) \notin \mathrm{supp}(l_{a,b})$, where $a_1, a_2 \in \mathbb{Z}_2$, since x_2 is essential for $l_{a,b}$. Therefore,

$$\{\bar{x} : (0, x_2, \bar{x}) \in \mathrm{supp}(l_{a,b})\} = \{\bar{x} : (0, x_2, \bar{x}) \notin \mathrm{supp}(l_{a,b})\} = \mathbb{Z}_2^{n-2}, \qquad (4)$$

and since f_0 and f_1 are bent it follows from Lemma 3 that

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus g(x \oplus y)} = \\
&= 2\Big(\sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} + \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = \\
&= 2\Big(\sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} + \sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = 0.
\end{aligned}$$

Suppose that $y_1 = 1$. Then

$$\begin{aligned}
g(1, x_2 \oplus y_2, \bar{x} \oplus \bar{y}) &= f_0(\bar{x} \oplus \bar{y} \oplus \bar{y'}) \oplus 1, \qquad && (0, x_2, \bar{x}) \in \mathrm{supp}(l_{a,b}), \\
g(1, x_2 \oplus y_2, \bar{x} \oplus \bar{y}) &= f_1(\bar{x} \oplus \bar{y} \oplus \bar{y'}), && (0, x_2, \bar{x}) \notin \mathrm{supp}(l_{a,b}),
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus g(x \oplus y)} = \\
&= \sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x) \oplus g(x \oplus y)} + \\
&+ \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + (-1)^{g(x) \oplus g(x \oplus y)} = \\
&= 2\Big(\sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} + \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{g(x) \oplus g(x \oplus y)} \Big) = \\
&= 2\Big(\sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y} \oplus \bar{y'}) \oplus 1} + \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y} \oplus \bar{y'})} \Big). \qquad (5)
\end{aligned}$$

Therefore, if $\bar{y'} \neq \bar{y}$, then from (4) and since f_0 and f_1 are bent it follows

from Lemma 3 that

$$\sum_{x\in\mathbb{Z}_2^n}(-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= 2\Big(\sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}}(-1)^{f_0(\bar{x})\oplus f_0(\bar{x}\oplus\bar{y}\oplus\bar{y'})\oplus 1} + \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}}(-1)^{f_1(\bar{x})\oplus f_1(\bar{x}\oplus\bar{y}\oplus\bar{y'})}\Big) =$$
$$= 2\Big(\sum_{\bar{x}\in\mathbb{Z}_2^{n-2}}(-1)^{f_0(\bar{x})\oplus f_0(\bar{x}\oplus\bar{y}\oplus\bar{y'})\oplus 1} + \sum_{\bar{x}\in\mathbb{Z}_2^{n-2}}(-1)^{f_1(\bar{x})\oplus f_1(\bar{x}\oplus\bar{y}\oplus\bar{y'})}\Big) = 0.$$

If $\bar{y'} = \bar{y}$, then from (4) we have that

$$\sum_{x\in\mathbb{Z}_2^n}(-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= 2\Big(\sum_{\bar{x}\in\mathbb{Z}_2^{n-2}}(-1)^{f_0(\bar{x})\oplus f_0(\bar{x})\oplus 1} + \sum_{\bar{x}\in\mathbb{Z}_2^{n-2}}(-1)^{f_1(\bar{x})\oplus f_1(\bar{x})}\Big) =$$
$$= 2\big(-2^{n-2} + 2^{n-2}\big) = 0.$$

It follows from Lemma 3 that g is bent.

If $b = 1$ then

$$\sum_{x\in\mathbb{Z}_2^n}(-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= \sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}}(-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus l_{a,b}(y)\oplus 1} +$$
$$+ \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}}(-1)^{g(x)\oplus g(x\oplus y)} + (-1)^{g(x)\oplus g(x\oplus y)\oplus l_{a,b}(y)\oplus 1},$$

and to show that g is bent it is sufficient to switch Cases 1 and 2. It is worth to elaborate on the case when $b = 1$, $\ell_{a,b}(y) = 1$ and $y_1 = 0$. If $\bar{y} = 0$ then from (3) we get

$$\sum_{x\in\mathbb{Z}_2^n}(-1)^{g(x)\oplus g(x\oplus y)} =$$
$$= 2\Big(\sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}}(-1)^{f_0(\bar{x})\oplus f_0(\bar{x}\oplus\bar{y})} + \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}}(-1)^{f_1(\bar{x})\oplus f_1(\bar{x}\oplus\bar{y})}\Big) =$$
$$= 2\Big(\sum_{\substack{x\in M\\ x\in \mathrm{supp}(l_{a,b})}}(-1)^{f_0(\bar{x})\oplus f_0(\bar{x})} + \sum_{\substack{x\in M\\ x\notin \mathrm{supp}(l_{a,b})}}(-1)^{f_1(\bar{x})\oplus f_1(\bar{x})}\Big) = 2^n$$

and hence $D_y g(x)$ is not balanced. Let us show that this case is not possible. Since y is nonzero, then $\bar{y} = 0$ only if $y_2 = 1$. But in that case $l_{a,b}(y) = 1 \oplus b = 0$ since x_2 is an essential variable for $l_{a,b}$ and $b = 1$.

Now let us show that if g is bent then f_0 and f_1 are bent. Suppose the opposite. Let f_0 is not bent. Then it follows from Lemma 3 that there is exist a nonzero vector $\bar{y}$ such that $D_{\bar{y}} f_0(\bar{x})$ is not balanced.

Note that there is always a nonzero vector $y = (0, y_2, \bar{y}) \notin \mathrm{supp}(l_{a,b})$, since x_2 is essential for $l_{a,b}$ and hence either $(0, a, \bar{y}) \notin \mathrm{supp}(l_{a,b})$ or $(0, a \oplus 1, \bar{y}) \notin \mathrm{supp}(l_{a,b})$, where $y_2, a \in \mathbb{Z}_2$.

Suppose that $b = 0$. Then from (3), (4) and since g is bent

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus g(x \oplus y)} = \\
&= 2\Big(\sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} + \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = \\
&= 2\Big(\sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} + \sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = 0,
\end{aligned}$$

and hence

$$\sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} = - \sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})}. \tag{6}$$

From (1) we know that $(1, y_2 \oplus y_2', \bar{y} \oplus \bar{y'}) \notin \mathrm{supp}(l_{a,b})$. Therefore, from (5), (4) and since g is bent

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_2^n} (-1)^{g(x) \oplus g(x \oplus y \oplus y')} = \\
&= 2\Big(\sum_{\substack{x \in M \\ x \in \mathrm{supp}(l_{a,b})}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y}) \oplus 1} + \sum_{\substack{x \in M \\ x \notin \mathrm{supp}(l_{a,b})}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = \\
&= 2\Big(\sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y}) \oplus 1} + \sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})} \Big) = 0,
\end{aligned}$$

and hence

$$\sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_0(\bar{x}) \oplus f_0(\bar{x} \oplus \bar{y})} = \sum_{\bar{x} \in \mathbb{Z}_2^{n-2}} (-1)^{f_1(\bar{x}) \oplus f_1(\bar{x} \oplus \bar{y})}. \tag{7}$$

Consequently, (6) and (7) contradict each other, since $D_{\bar{y} f_0(\bar{x})}$ is not balanced.

If $b = 1$ it is sufficient to consider a nonzero vector $(0, y_2 \oplus 1, \bar{y}) \in \mathrm{supp}(l_{a,b})$.

Note that for different $\{f_0, f_1\}$ and $\{f'_0, f'_1\}$ we get different g. Since f_0 and f_1 are arbitrary bent functions in $n-2$ variables there are $|\mathcal{B}_{n-2}|^2$ bent functions g for which $l_{a,b}$ is a derivative in the direction y'.

It follows from Lemma 5 that for different directions y' we get different bent funcions that have $l_{a,b}$ as its derivative. Therefore, it follows from Lemma 4 that there are $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ bent functions that have $l_{a,b}$ as the derivative. □

4 Iterative lower bound

Theorem 1 gives us an iterative lower bound.

Theorem 2. *For even $n \geq 2$ it holds $|\mathcal{B}_{n+2}| \geqslant (2^{n+2}-2)|\mathcal{B}_n|^2$.*

Proof. Let l a be nonconstant affine function in $n+2$ variables. It follows from Theorem 1 that there are $(2^{n+1}-1)|\mathcal{B}_n|^2$ bent functions in $n+2$ variables that have l as its derivative. Therefore, $|\mathcal{B}_{n+2}| \geqslant (2^{n+1}-1)|\mathcal{B}_n|^2$.

Let us show that it is not possible for some bent function to have both l and $l \oplus 1$ as its derivatives. Suppose that $g(x)$ is a bent and $D_y = l(x)$ and $D_{y'} = l(x) \oplus 1$ for $y \neq y'$. Then for every $x \in \mathbb{Z}_2^n$

$$\begin{aligned}
&D_y g(x) \oplus D_{y'} g(x) = \\
&= g(x) \oplus g(x \oplus y) \oplus g(x) \oplus g(x \oplus y') = \\
&= g(x \oplus y) \oplus g(x \oplus y') = \\
&= g(x \oplus y) \oplus g(x \oplus y \oplus (y' \oplus y)) = \\
&= D_{y' \oplus y} g(x \oplus y) = l(x) \oplus l(x) \oplus 1 = 1,
\end{aligned}$$

which contradicts Lemma 3. Thus, we can multiply our bound by 2. □

Let us compare this iterative lower bound with other known. We have this iterative lower bound from [12]

$$|\mathcal{B}_{n+2}| \geqslant 6|\mathcal{B}_n|^2 - 8|\mathcal{B}_n|$$

but it is not better than the following one.

Proposition 1. *(Climent et al, [13]) For even $n \geq 2$ it holds*

$$|\mathcal{B}_{n+2}| \geqslant 6|\mathcal{B}_n|^2 + 2^{n+2}(2^n - 3)|\mathcal{B}_n|.$$

The Iterative lower bound from Proposition 1 is worse than one from Theorem 2 for every even $n \leq 8$. See Table 1.

Variables	4	6	8	10
Bent	896	5 425 430 528	$2^9\times$ 193 887 869 660 028 067 003 488 010 240 $\approx 2^{106.29}$	?
Proposition 1	512	5 562 368	176 611 863 208 449 277 952 $\approx 2^{68}$	$\approx 2^{215}$
Theorem 2	896	49 774 592	7 476 565 289 195 207 131 136 $\approx 2^{72.6}$	$\approx 2^{222.5}$
Proposition 3	512	322 961 408	$\approx 2^{87.35}$	$\approx 2^{262.16}$

Table 1: Number of bent functions constructed with different methods

Proposition 2. *(Canteaut et al, [14], Tokareva [15]) Let functions f_0, f_1, and f_2 be bent functions in n variables. Then function g defined as*

$$g(0,0,x) = f_0(x), \qquad g(0,1,x) = f_1(x),$$
$$g(1,0,x) = f_2(x), \qquad g(1,1,x) = f_3(x),$$

is a bent function in $n+2$ variables if and only if f_3 is a bent function in n variables and $\tilde{f}_0 \oplus \tilde{f}_1 \oplus \tilde{f}_2 \oplus \tilde{f}_3 = 1$.

Bent functions that can be obtained by Proposition 2 are called *bent iterative* functions. Let $\mathcal{BI}_{n+2}$ denote the class of all such functions in $n+2$ variables.

The following iterative lower bound is based on Proposition 2. It was proven by the author [15] in 2011. For now it is the best iterative lower bound for the number of bent functions.

Proposition 3. *(Tokareva, [15]) For even $n \geq 2$ it holds*

$$|\mathcal{B}_{n+2}| \geqslant |\mathcal{BI}_{n+2}| \geq |\mathcal{B}_n|^4/|X_n|,$$

where X_n is the set of all Boolean functions in n variables that can be represented as the sum of two distinct bent functions.

The Iterative lower bound from Theorem 2 is not better than one from Proposition 3 when $n \geq 6$. See Table 1.

5 Conclusion and open problems

In [11] it was shown that every balanced function f in n variables is a derivative of a some bent function for $n \leqslant 6$ (n even). Whether it is true for nonaffine balanced functions for every even n is an open problem.

Iterative lower bound from Theorem 2 theoretically can be improved if we consider more then two affine functions l and $l \oplus 1$. Unfortunately, it is hard to keep track of bent functions that were already counted because it is possible that $D_y g(x) = l(x)$ and $D_{y'} g(x) = h(x)$, where $h \neq l$, $h \neq l \oplus 1$ and $y \neq y'$.

We also can consider bent functions that do not have affine derivatives. Such functions of degree 3 were studied for example in [14]. Although, the number of such functions was not presented.

6 Acknowledgement

The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Laboratory of Cryptography JetBrains Research.

References

[1] Rothaus O. S., "On 'bent' functions", *J. Combinat. Theory A*, **20**:3 (1976), 300–305.

[2] Matsui M., "Linear Cryptanalysis Method for DES cipher", *Advances in Cryptology*, EUROCRYPT 1993., Springer, Berlin, Heidelberg, 386–397.

[3] Adams C., "Constructing symmetric ciphers using the CAST design procedure", *Proc. Design, Codes, and Cryptography*, **12**:3 (1997), 283–316.

[4] Hell M., Johansson T., Maximov A., and Meier W., "A stream cipher proposal: Grain-128", *IEEE International Symposium on Information Theory*, 2006, 1614–1618.

[5] Tokareva N., *Bent functions: results and applications to cryptography*, Acad. Press. Elsevier, 2015.

[6] Kavut S., Maitra S., Yucel MD., "Search for Boolean functions with excellent profiles in the rotation symmetric class", *IEEE Trans Inform Theory*, **53**:5 (2007), 1743–1751.

[7] Maitra S., Sarkar P., "Maximum nonlinearity of symmetric Boolean functions on odd number of variables", *IEEE Trans Inform Theory*, **48**:9 (2002), 2626-2630.

[8] Kerdock AM., "A class of low-rate non-linear binary codes", *Inform Control*, **20**:2 (1972), 182-187.

[9] Delsarte P., "An algebraic approach to the association schemes of coding theory", *Ph.d. thesis*, 1973.

[10] Sidelnikov V. M., "On extremal polynomials used in code size estimation", *Probl Inf Transm*, **16**:3 (1980), 174-186.

[11] Tokareva N. N., "On the set of derivatives of a boolean bent function", *Applied Discrete Mathematics. Supplement*, **9** (2016), 327–350.

[12] Climent JJ, Garcia FJ, Requena V., "On the construction of bent functions of n + 2 variables from bent functions of n variables", *Adv Math Commun*, **2**:4 (2008), 421–431.

[13] Climent JJ, Garcia FJ, Requena V, "A construction of bent functions of n + 2 variables from a bent function of n variables and its cyclic shifts", *Algebra*, 2014.

[14] Canteaut A, Charpin P., "Decomposing bent functions", *IEEE Trans Inform Theory*, **49**:8 (2003), 2004–2019.

[15] Tokareva N. N., "On the number of bent functions from iterative constructions: lower bounds and hypotheses", *Adv Math Commun*, **5**:4 (2011), 609–621.

Algebraic cryptanalysis of round-reduced lightweight ciphers SIMON and SPECK

Aleksandr Kutsenko[1,2], Natalia Atutova[1,2], Darya Zyubina[1,2], Ekaterina Maro[3] and Stepan Filippov[4]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia
[2]Novosibirsk State University, Novosibirsk, Russia
[3]Southern Federal University, Taganrog, Russia
[4]Saint Petersburg State University, Saint Petersburg, Russia
alexandrkutsenko@bk.ru, atutova.n@yandex.ru, zyubinadarya@gmail.com, eamaro@sfedu.ru, filippowstepan@yandex.ru

Abstract

This paper presents algebraic attacks on SIMON and SPECK, two families of lightweight block ciphers having LRX- and ARX-structures respectively. They were presented by the U.S. National Security Agency in 2013 and later standardized by ISO as a part of the RFID air interface standard. We algebraically encode the ciphers and try to solve the underlying systems with different SAT solvers, methods based on the linearization and for the first time apply to these ciphers the approaches that use the sparsity of the considered systems of equations. The linearization parameters in systems of equations for both of the ciphers are estimated. A comparison of the efficiency of the used methods is provided.

Keywords: algebraic cryptanalysis, block cipher, lightweight, SIMON, SPECK

Lightweight cryptography is a research direction of current interest. This is due to the fact that the impact and the usage of RFID tags, FPGAs, smartcards, mobile phones, sensor networks and other cryptographic algorithms for resource-constrained devices continuously grows and becomes more and more important. Lightweight cryptographic primitives are designed to be both efficient and secure for limited resources. In this case the problem of obtaining the trade-off between the security and efficiency, measured by different metrics, appears.

There were developed a number of lightweight block and stream ciphers, hash functions with a purpose of obtaining the aforementioned trade-off. For example, lightweight block ciphers designs include, but are not limited to, HIGHT [1], KATAN [2], KLEIN [3], Piccolo [4] and PRESENT [5].

In 2013, the NSA introduced the specifications of lightweight block cipher families SIMON and SPECK that were claimed to be flexible enough to provide

excellent performance in both hardware and software environments. SIMON has been optimized for performance on hardware devices, and SPECK for performance in software. But it was emphasized that both families performed exceptionally well in both hardware and software, providing the platform flexibility required by future applications. As of October 2018, the Simon and Speck ciphers have been standardized by ISO as a part of the RFID air interface standard, International Standard ISO/29167-21 (Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications) and International Standard ISO/29167-22 (Information technology — Automatic identification and data capture techniques — Part 22: Crypto suite SPECK security services for air interface communications), that makes them available for use by commercial entities.

There are no specific cryptanalytic results nor analysis provided in the specification document. However, later there appeared a couple of works related to the cryptanalysis of these ciphers. Mostly differential attacks are under consideration. For instance, in paper [6] differential cryptanalysis of round-reduced SIMON and SPECK was considered. The attacks on up to slightly more than half the number of rounds were described and the drawback of the intensive optimizations in these ciphers was concluded.

The considered ciphers are representatives of LRX- and ARX- structures of block ciphers, the core of them is the explicit usage of nonlinear algebraic operations instead of S-boxes. It leads to the problem of algebraic analysis of these ciphers. Algebraic analysis of SIMON was made by Raddum in [7]. Combined algebraic and truncated differential cryptanalysis on reduced-round SIMON appeared in paper of Courtois et al. [8]. The resistance of SIMON-64/128 with respect to algebraic attacks was studied by using a SAT solver and ElimLin algorithm. In article [9] the usage of SAT-solvers for algebraic cryptanalysis of ARX-structures was discussed. Recently, in paper [10] the attack on up to 13 rounds with 8 chosen plaintexts by fixing 4 and 6 key bits for Simon-32/64 and Simon-64/128 was presented.

In current work we study and compare the efficiency of different types of algebraic attacks on round-reduced SIMON and SPECK. The analysis is provided via different SAT solvers usage as well as methods of solving systems of polynonomial equations, based on the linearization routine. The methods that exploit the sparsity of the systems of equations (The Raddum-Semaev description of the system and the Algorithm) are also considered. This is the first attempt to analyze the resiliense of SPECK cipher to different algebraic attacks outside the SAT-solvers usage. The conclusion on the obtained results

is given.

1 SIMON and SPECK families of ciphers

1.1 General description of SIMON

SIMON is a family of lightweight block ciphers for an optimal hardware performance, presented in [11]. Simon has structure of classical Feistel scheme, in each round $2n$-bit input of the round is divided into two n-bit halves. Each round of SIMON applies a non-linear, non-bijective round function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ to the left half L of the state. The output of F is added using XOR to the right half R along with a round key k, and the two halves are swapped. The round function F is defined as

$$F(x) = (S^8(x) \odot S^1(x)) \oplus S^2(x), \quad x \in \mathbb{F}_2^n,$$

where $S^j(x)$ denotes left rotation of $x \in \mathbb{F}_2^n$ by j positions and the symbol $\odot$ is for binary operation AND.

We introduce a new variable for each output of the bitwise operation $\odot$, then to describe T rounds we get $n(T-2)$ quadratic equations in $n(T-2)+k$ unknowns. Where n is a word size, T is a number of rounds and k is a key length.

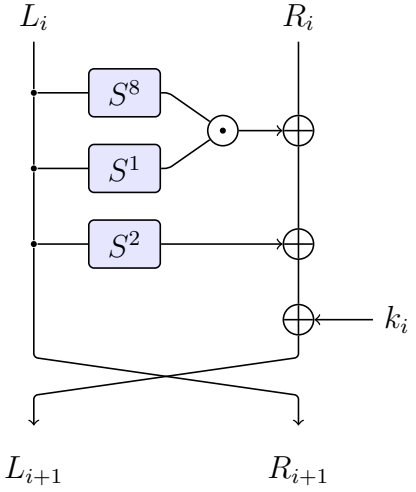


Figure 1: Round function of SIMON

The key schedule of SIMON is described as a function that operates on two, three or four n-bit word registers, depending on the size of the general key. It performs two rotations to the right: $S^{-3}(x)$ and $S^{-1}(x)$ and XOR the results together with a fixed constant $c = 2^n - 4$ and five constant sequences depending on the version of the specification. These constant sequences are

obtained by using three square matrices of order 5 over the field $\mathbb{F}_2$, and a linear feedback shift register where the first two are of period 31 and the last three have the period 62. The general secret key consists of m key words, each of n bits length, where $m \in \{2, 3, 4\}$.

1.1.1 Key schedules

The first m keys are set, each consisting of n bits. The sequence of keys is calculated recursively ($c = 2^n - 4$ is a constant, and z_j is a fixed periodical sequence, exact value see in [11]). The value of m depends on the values of the block size $2n$ and the number of rounds T (Table 1)

$$k_{i+m} = \begin{cases} c \oplus (z_j)_i \oplus k_i \oplus \left(I \oplus S^{-1}\right) S^{-3} k_{i+1}, \text{ for } m = 2, \\ c \oplus (z_j)_i \oplus k_i \oplus \left(I \oplus S^{-1}\right) S^{-3} k_{i+2}, \text{ for } m = 3, \\ c \oplus (z_j)_i \oplus k_i \oplus \left(I \oplus S^{-1}\right) (S^{-3} k_{i+3} \oplus k_{i+1}), \text{ for } m = 4. \end{cases}$$

Block size $2n$	**Key size** mn	**Word size** n	**Key words** m	**const seq**	**Rounds** T
32	**64**	16	4	z_0	32
48	**72**	24	3	z_0	36
	96		4	z_1	36
64	**96**	32	3	z_2	42
	128		4	z_3	44
96	**96**	48	2	z_2	52
	144		3	z_3	54
128	**128**	64	2	z_2	68
	192		3	z_3	69
	256		4	z_4	72

Table 1: SIMON parameters

1.2 General description of SPECK

SPECK is a family of lightweight block ciphers for excellent performance in both hardware and software, but have been optimized for performance on microcontrollers. This family was also presented in paper [11]. In each round $2n$-bit input of the round is divided into two n-bit halves. Each round of SPECK applies a non-linear round function is defined as

$$R_k(x, y) \to \left(\left(S^{-\alpha}(x) + y\right) \oplus k, S^{\beta}(y) \oplus \left(S^{-\alpha}(x) + y\right) \oplus k\right),$$

where $S^j(x)$ denotes left rotation (if $j > 0$) by j positions and right rotation (if $j < 0$) of $x \in \mathbb{F}_2^n$, the symbol «+» is an addition modulo 2^n. The parameters have following values: $\alpha = 7$ and $\beta = 2$ if $n = 16$ (block size is equal to 32) and $\alpha = 8$ and $\beta = 3$ otherwise.

On the first round there will be only $2n$ equations because initially we set two n-bit words. On the next encryption rounds, $2 \cdot (8n - 3)$ equations are added each time (for $m = 1$ $7n - 3$ equations are added on key schedules and $8n - 3$ on a round function) and $3n$ unknowns. Starting from the second round, 3 unknowns are added due to the key schedule. When constructing a system of equations, we substitute the input and output cipher before the first round and after the last (L_0, R_0, L_n, R_n), so the number of unknowns is reduced by $4n$. The final formulas for the number of equations and the number of unknowns are

$$e = \begin{cases} (7n-3)(T-1) + (8n-3)(T-1) + 2n, & \text{for } m = 1, \\ 2(8n-3)(T-1) + 2n, & \text{for } m = 2, 3, 4, \end{cases}$$

$$u = \begin{cases} n(5T-4), & \text{for } m = 1, \\ n(6T-5), & \text{for } m = 2, 3, 4. \end{cases}$$

where e is a number of equations, u is a number of variables, n is a word size, T is a number of rounds.

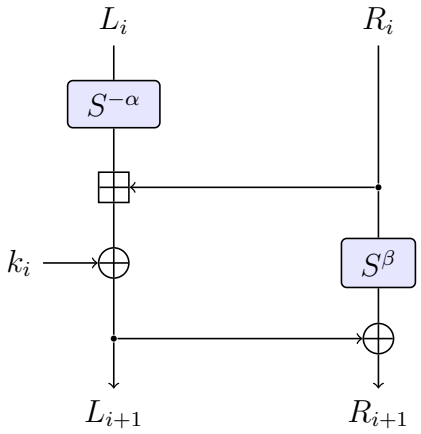


Figure 2: Round function of SPECK

1.2.1 Key schedules

The SPECK key schedules use the round function to generate round keys. Let $K = (l_{m-2}, \ldots, l_0, k_0)$ be a key for a SPECK, where $l_i, k_0 \in \mathbb{F}_2^n$, $m \in \{2, 3, 4\}$. The value of m depends on the values of the block size $2n$ and the number of rounds T (Table 2). Keys k_i and l_i are defined as

$$l_{i+m-1} = (k_i + S^{-\alpha} l_i) \oplus i,$$

$$k_{i+1} = S^{\beta} k_i \oplus l_{i+m-1}$$

Block size $2n$	**Key size** mn	**Word size** n	**Key words** m	**Rot** α	**Rot** β	**Rounds** T
32	**64**	16	4	7	2	22
48	**72**	24	3	8	3	22
	96		4			23
64	**96**	32	3	8	3	26
	128		4			27
96	**96**	48	2	8	3	28
	144		3			29
128	**128**	64	2	8	3	32
	192		3			33
	256		4			34

Table 2: SPECK parameters

Conducting cryptanalysis on a small number of rounds (such as 3 and 4) with selecting standard characteristics (Table 2) is not sensible since the keys are not built on the basis of the original ones and there will be no connection between them. Therefore, in this work we consider the cipher with $m = 1$ for $T \in \{3, 4\}$.

1.2.2 Addition modulo 2^n

The round function of the Speck cipher is nonlinear, this property in SPECK is provided by the addition operation modulo 2^n, which is the part of the encryption algorithm. It is possible to obtain a redefined system of $6n - 3$ linearly independent algebraic equations that completely describe the operation under consideration [12]. One of them will be linear while the rest

are quadratic.

$$\begin{cases} w_0x_{i+\alpha} = x_\alpha x_{i+\alpha} \oplus y_0x_{i+\alpha}\ ,\ i = \overline{1, n-1} \\ w_0y_i = x_\alpha y_i \oplus y_0y_i\ ,\ i = \overline{0, n-1} \\ w_0w_i = x_\alpha w_i \oplus y_0w_i\ ,\ i = \overline{0, n-1} \\ w_1x_\alpha = x_{1+\alpha}x_\alpha \oplus y_1x_\alpha \oplus x_\alpha y_0 \\ w_1y_0 = x_{1+\alpha}y_0 \oplus y_1y_0 \oplus x_\alpha y_0 \\ w_i = x_{i+\alpha} \oplus y_i \oplus x_{i-1+\alpha} \oplus y_{i-1} \oplus x_{i-1+\alpha}y_{i-1} \oplus x_{i-1+\alpha}w_{i-1} \oplus \\ y_{i-1}w_{i-1}, i = \overline{2, n-1} \\ w_i(x_{i-1+\alpha} \oplus y_{i-1}) = x_{i-1+\alpha}x_{i+\alpha} \oplus x_{i-1+\alpha}y_i \oplus x_{i-1+\alpha} \oplus x_{i-1+\alpha}w_{i-1} \oplus \\ x_{i+\alpha}y_{i-1} \oplus y_{i-1}y_i \oplus y_{i-1} \oplus y_{i-1}w_{i-1}\ ,\ i = \overline{2, n-1} \\ w_i(x_{i-1+\alpha} + w_{i-1}) = x_{i-1+\alpha}x_{i+\alpha} \oplus x_{i-1+\alpha}y_i \oplus x_{i-1+\alpha} \oplus x_{i+\alpha}w_{i-1} \oplus y_iw_{i-1} \oplus \\ x_{i-1+\alpha}w_{i-1}\ ,\ i = \overline{2, n-1} \\ w_0 = x_{\alpha\ mod\ n} \oplus y_0 \\ w_1 = x_{1+\alpha} \oplus y_1 \oplus x_\alpha y_0 \end{cases}$$

2 Attacks based on linearization

2.1 Pure linearization

The idea of this method is to assign every monomial from the initial system with a new variable. The system after the assignment becomes a linear one. The obtained system is solved via different methods, for instance Gaussian elimination, and solutions of linear system are checked for being solutions for the initial nonlinear system of equations.

The efficiency of linearization depends on the rank r of the system whereas the number of different monomials in the initial system defines the number of variables n' in the system of linear equations. The set of solutions is not empty, so it is $2^{n'-r} > 0$, hence in order to estimate the performance one should analyze the bounds for the values of n' and r.

The analysis of this attack (see [13]) shows that the rank of the system is expected to be sufficiently large if $m \approx n^2/2$. Estimation of the required number of operations and time complexity of the attack can be provided by taking into account the number of different monomials in the system of equations that describe the considered cipher and varying its rank.

2.1.1 Number of different monomials in SIMON's system of equations

Considering the encryption algorithm, we can estimate the number of monomials for each round. With the introduction of new variables, the estimate is $6nT$, where n is the word length, T is the number of rounds. The estimate was obtained based on the fact that for each operation new variables are introduced (xor, plus, plus, addition with key) and taking into account the re-designation when replacing L_{i+1} and R_{i+1}.

In addition, an estimation of the number of variables without reassignment (introduction of new variables) was carried out in order to assess the effectiveness of the linearization method. When analyzing a small number of rounds without introducing new variables, it was noticed that every four rounds, the number of variables decreases when added using R_i. Thus, a recurrence relation was obtained for the number of variables, taking into account the decrease every four rounds. Let $P(T)$ be the number of variables on the T-th round, where n is a word size.

$$P(T) = \begin{cases} 4 \cdot n, & T = 1 \\ 7 \cdot n, & T = 2 \\ n\big(P^2(T-2) + P(T-2) + 1\big), & \text{if } T \text{ is divisible by 4} \\ n\big(P^2(T-2) + P(T-1) + P(T-2) + 1\big), & \text{otherwise.} \end{cases}$$

In practice, an estimate for the number of variables with $n = 16$, $T = 32$ was found, excluding the key stage, it is about 2^{68}. Thus, we found that changing the variables significantly reduces the amount of computation.

For the case when new variables are introduced on every round and the degree is at most 2, the formula without monomials that come from the key schedule equations (all equations are linear), is

$$M \leqslant 6nT,$$

where M is a number of monomials, n is a word size, T is a number of rounds.

Block size $2n$	**Word size** n	**Rounds** T	**Num. of monomials**	**Rank of the linearized system**	**Num. of unknowns with key schedule**
32	16	32	$\approx 2^{11.6}$	$\approx 2^{8.9}$	$\approx 2^{9}$
48	24	36	$\approx 2^{12.3}$	$\approx 2^{9.7}$	$\approx 2^{9.7}$
64	32	42	$\approx 2^{13}$	$\approx 2^{10.3}$	$\approx 2^{10.4}$
		44	$\approx 2^{13}$	$\approx 2^{10.4}$	$\approx 2^{10.4}$
96	48	52	$\approx 2^{13.9}$	$\approx 2^{11.2}$	$\approx 2^{11.3}$
		54	$\approx 2^{13.9}$	$\approx 2^{11.3}$	$\approx 2^{11.3}$
128	64	68	$\approx 2^{14.7}$	$\approx 2^{12}$	$\approx 2^{12.1}$
		69	$\approx 2^{14.7}$	$\approx 2^{12}$	$\approx 2^{12.1}$
		72	$\approx 2^{14.8}$	$\approx 2^{12.1}$	$\approx 2^{12.2}$

Table 3: Parameters of SIMON's system of equations

By using these data the estimates of cryptographic strength with respect to linearization can be made. In fact it defined by the complexity of the search in the set of the solutions of obtained system of equations and the complexity of obtaining the solutions by Gauss elimination. The complexity of the search is about $2^{n'-r}$, where n' is the number of monomials (variables in lonearized system) and r is the rank of linearized system.

For real specifications, for instance for 32 rounds block size and 32 rounds number of monomials (variables in linearized system) is about $2^{11.5}$ while the rank is about 2^9. For 96 block size and 52 rounds the number of monomials (variables in linearized system) is about 2^{14} while the rank is about 2^{11} It is clear that the obtained estimates are unfeasible in comparison with brute force.

2.1.2 Number of different monomials in Speck's system of equations

The main method of withholding degree is the introduction of new variables for the output bits of nonlinear operations. In this case the degree will then not exceed 2. New variables are introduced with each new round: cipher text (x_i, y_i), key (k_i, l_i), variables describing addition modulo 2^n.

In the system of equations that describes an addition modulo 2^n (section 1.2.2), there are total $5(7n-8)$ monomials. In practice, it was found out that the unique monomials in the system of equations of addition modulo 2^n is at most $25n - 18$. As a result, the number of unique monomials per Speck round is at most $28n - 18$ per each round.

The final formula for estimating the number of monomials, excluding such ones that come from the key schedule equations (all equations are linear), is

$$M \leqslant (28n - 18)T,$$

where M is the number of monomials, n is the word size, T is the number of rounds.

Block size $2n$	Rounds T	Num. of monomials	Rank of the system without key sch.	Rank of the system with key schedule	Num. of unknowns without key sch.	Num. of unknowns with key schedule
32	22	$\approx 2^{13.2}$	$\approx 2^{11.4}$	$\approx 2^{12.4}$	$\approx 2^{9.95}$	$\approx 2^{11}$
48	22	$\approx 2^{13.8}$	$\approx 2^{12}$	$\approx 2^{13}$	$\approx 2^{10.5}$	$\approx 2^{11.6}$
	23	$\approx 2^{13.9}$	$\approx 2^{12.1}$	$\approx 2^{13.1}$	$\approx 2^{10.6}$	$\approx 2^{11.7}$
64	26	$\approx 2^{14.5}$	$\approx 2^{12.7}$	$\approx 2^{13.7}$	$\approx 2^{11.2}$	$\approx 2^{12.3}$
	27	$\approx 2^{14.5}$	$\approx 2^{12.8}$	$\approx 2^{13.7}$	$\approx 2^{11.3}$	$\approx 2^{12.3}$
96	28	$\approx 2^{15.2}$	$\approx 2^{13.4}$	$\approx 2^{14.4}$	$\approx 2^{11.9}$	$\approx 2^{13}$
	29	$\approx 2^{15.2}$	$\approx 2^{13.4}$	$\approx 2^{14.4}$	$\approx 2^{12}$	$\approx 2^{13}$
128	32	$\approx 2^{15.8}$	$\approx 2^{14}$	$\approx 2^{15}$	$\approx 2^{12.6}$	$\approx 2^{13.6}$
	33	$\approx 2^{15.8}$	$\approx 2^{14.1}$	$\approx 2^{15.1}$	$\approx 2^{12.6}$	$\approx 2^{13.6}$
	34	$\approx 2^{15.9}$	$\approx 2^{14.1}$	$\approx 2^{15.1}$	$\approx 2^{12.6}$	$\approx 2^{13.6}$

Table 4: Parameters of Speck's system of equations

As well as in the previous section by using obtained estimates the complexity of the linearization attack can be analyzed. For real specifications, for instance for 32 rounds block size and 32 rounds number of monomials (variables in linearized system) is about 2^{13} while the rank is about 2^9. For 96 block size and 28 rounds the number of monomials (variables in linearized system) is about 2^{15} while the rank is about 2^{13} It is clear that the obtained estimates are unfeasible in comparison with brute force as well.

2.2 XL-attack

This attack was introduced in [14, 15]. It takes a system of m polynomial equations in n unknowns, of degree d and outputs its solution or solutions, if the equations have sufficient rank.

- 1: Select degree $D > d$. Usually $D = d + 1$.
- 2: Make a list S of all monomials of degree $D - d$ or less, including the monomial 1, which has degree 0.
- 3: Multiply all equations by every element of S. (Since there were m equations before this step, there are $m|S|$ equations after it).
- 4: Linearize the system.
- 5: Solve the obtained system via linear algebra.

For the case $d = 2$ and $D = d + 1$ the analysis of this attack (see [13]) shows that the uique solution is likely to be found if $m \approx n^2/6$.

2.3 ElimLin

The ElimLin algorithm appeared in [16] (see also its analysis in [17]). Its point is the search of hidden linear equations existing in the ideal generated by the given system of equations. This algorithm is composed of two sequential steps:

1 : Gaussian Elimination: Discover all the linear equations in the linear span of initial equations.

2 : Substitution: Variables are iteratively eliminated.

In more details it can be described as follows.

INPUT: A system of degree 2 polynomial equations. OUTPUT: Either, a solution or solutions to the system, if the equations have sufficient rank, or if not, then a reduced system of equations in fewer variables than the original, to be solved by some other method.

1 : D is an empty set.

2 : Linearize the system of equations.

3 : Perform Gaussian Elimination to result in Reduced Row Echelon Form.

4 : Let ℓ be the number of all-linear equations found.

1 : If $\ell = 0$, STOP.

2 : If $\ell > 0$.

1 : For $i = 1, 2, \ldots, \ell$

1 : Move all the variables and constants, but one, to one side of the equal sign.

2 : Substitute this redefinition of a variable into the other equations, thus eliminating one variable.

2 : Substitute this redefinition of a variable into the other definitions in D.

2 : Add the definition to D.

2 : Goto Step 3, "Perform Gaussian Elimination."

2.4 Results

In the Table 5 we give the results for the pure linearization, the XL-method and the ElimLin method that allow to compare SIMON and SPECK from that perspective. For XL-method the value of the resulting degree D was chosen to 3.

A search on the key space key is 2^{16} (when $n = 16$, $m = 1$). As we can see in the table 5 the linearization method from round 4 and 5 onwards gives worse results than a brute force attack. Using the pure linearization method for T at least 4 and XL-method for at least 5 rounds (cipher SIMON) does not improve the search for a solution in comparison with brute force.

	Simon parameters	**Number of equations**	**Number of variables**	**Number of monomials**	**Number of solutions**
Pure linearization	$T = 3$, $m = 1$	48	32	48	4, only one corresponds to the key
XL-method	$T = 3$, $m = 1$	1584	32	992	1
Pure linearization	$T = 4$, $m = 1$	64	48	80	65536
XL-method	$T = 4$, $m = 1$	3136	48	2616	256, only one corresponds to the key
Pure linearization	$T = 5$, $m = 1$	80	64	112	2^{32}
XL-method	$T = 5$, $m = 1$	5200	64	5008	2^{336}
	Speck parameters				
Pure linearization	$T = 3$, $m = 1$	500	176	1236	—
XL-method	$T = 3$, $m = 1$	88500	176	185216	—

Table 5: Results for attaks based on linearization

	Parameters	**(Equations, Linear equations)**	**(Equations, Linear equations after ElimLin applied)**
Simon	$T = 3$, $m = 1$	(48, 32)	(48, 32)
Simon	$T = 5$, $m = 1$	(80, 32)	(80, 48)
Speck	$T = 3$, $m = 1$	(500, 132)	(307, 137)
Speck	$T = 5$, $m = 2$	(1032, 296)	(654, 297)

Table 6: Results for ElimLin

3 Attack based on SAT solvers

3.1 SAT

The Boolean satisfiability problem (SAT) is a decision problem, in which for an arbitrary Boolean formula the question is whether there exists such assignment of variables that the formula has value True. This problem is known to be NP-hard.

SAT solvers are a powerful computational tools to test the hardness of certain problems, they have successfully been used to test hardness assump-

tions [18]. There are several examples of the usage of SAT solvers in a scope of algebraic cryptanalysis. The first SAT-based cryptanalysis was provided by Massacci et al. in [19]. In that work the Data Encryption Standard (DES) was attacked with a usage of DPLL-based SAT solvers.

SAT-based cryptanalysis implies two stages: on the first stage a SAT encoding is provided, for instance the translation of the given ANF system to CNF. There are some tools for converting cryptographic tasks into CNF: Grain-of-Salt [20], URSA [21], SAW [22], Transalg [23], Bosphorus [24]. We use anf2cnf [25] convertor from PolyBoRi library integrated at Sage. On the second stage the obtained SAT instance is solved using SAT solving algorithm. For cryptographic systems often applied such SAT-solvers as CryptoMiniSat [26] and Lingeling (with its parallel versions Plingeling and Treengeling) [27].

For addition information about overview and state-of-art on SAT solvers and their applications to cryptanalysis we recommended to refer to paper [23].

3.2 Results

In this section the results on the usage of SAT solvers for attack on reduced-round versions of Simon and Speck ciphers are given. We apply SAT solvers CryptoMiniSat (in Sage ver. 6.10) and Lingeling, Plingeling, Treengeling at PC with following features: Core i5-4690 CPU 3.5 GHz (x4), 12Gb RAM.

Choosing the tools for solving SAT problem was make in favor of Lingeling family solvers and CryptoMiniSat based on rating SAT Competition 2018 [28], 2020 [29]. The CryptoMiniSat solver was originally developed for solving SAT problems related to cryptographic structures and has been widely used in scientific literature for analyzing methods based on SAT solving. Plingeling and CryptoMiniSat solvers were included in the top-3 parallel tracks (only for SAT) SAT Competition 2018, which is presumably about the effectiveness of their subsequent use on multiprocessor systems.

Experimental result of SAT solving for 3 to 10 round Simon and 3 to 6 round Speck are presented at Tables 7 and 8. Two ANF generation form for Simon were examined: all round keys are independent variables and all round keys are represented by key schedule algorithm.

SIMON parameters	Num. of equations	Num. of unknowns	SAT parameters	SAT	Time (RAM)
$T = 3$, $m = 1$ (with round key)	80	80	96 lit., 432 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	0.17 sec. 0.01 sec., 0.1 MB 1.1 sec., 0.7 MB 0.50 sec., 0.05 MB
$T = 5$, $m = 2$ (with round key)	128	128	192 lit., 1136 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	8.43 sec. 0.9 sec., 2.0 MB 2.9 sec., 21.0 MB 2.36 sec., 10 MB
$T = 5$, $m = 2$ (key schedule)	80	80	176 lit., 1710 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	15.79 sec. 1.4 sec., 2.0 MB 2.2 sec., 15.4 MB 0.86 sec., 3 MB
$T = 7$, $m = 2$ (with round key)	192	192	320 lit., 2064 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	287.31 sec. 3687.9 sec., 45.9 MB 212.7 sec., 103.3 MB 681.14 sec., 77 MB
$T = 7$, $m = 2$ (key schedule)	112	112	320 lit., 3632 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	101.23 sec. 1867.2 sec., 38.0 MB 229.5 sec., 99.2 MB 389.84 sec., 62 MB
$T = 8$, $m = 2$ (with round key)	224	224	384 lit., 2528 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- 69811.9 sec., 120.5 MB 4775.5 sec., 260.3 MB 12702.81 sec., 182 MB
$T = 8$, $m = 2$ (key schedule)	128	128	368 lit., 4448 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	51533.67 sec. 845.4 sec., 26.6 MB 1188.8 sec., 169.2 MB 4426.12 sec., 95 MB
$T = 9$, $m = 2$ (key schedule)	144	144	480 lit., 6448 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- >260174.3 sec., >180.7 MB 47799.2 sec., 620.3 MB 24547.91 sec., 172 MB
$T = 10$, $m = 2$ (key schedule)	160	160	560 lit., 8096 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- - 17554.9 sec., 458.8 MB 60776.91 sec., 234 MB
$T = 11$, $m = 2$ (key schedule)	176	176	640 lit., 9648 clause	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- -

Table 7: Results for SAT solvers on SIMON

Speck parameters	Num. of equations	Num. of unknowns	SAT parameters	SAT	Time (RAM)
$T = 3$, $m = 1$	500	176	1460 lit., 11020 clause	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	0.56 sec. 0.9 sec., 9.6 MB 0.97 sec., 4 MB 0.2 sec., 1.9 MB
$T = 4$, $m = 2$	782	320	2492 lit., 17380 clause	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	21.4 sec. 3.0 sec., 17.3 MB 8.25 sec., 15 MB 61.4 sec., 14.8 MB
$T = 5$, $m = 2$	1032	416	3312 lit., 23184 clause	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	- - 14448.17 sec., 278 MB -
$T = 6$, $m = 2$	1282	512	4132 lit., 28988 clause	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	- - 123353.82 sec., 546 MB -

Table 8: Results for SAT solvers on SPECK

4 The Raddum–Semaev Method

4.1 The representation of the system os equations

This approach to solving sparse polynomial systems of equations over $\mathbb{F}_2$ was introduced by Hårvard Raddum and Igor Semaev, its general description was presented in [30]. The analysis and some properties one can find in paper [31].

Its core is the following. To i-th equation $f_i(x) = 0$ from the initial system of equations a subset if variables $X_i \subseteq X$ and the list $L_i \subseteq \mathbb{F}_2^{|X_i|}$ of vectors are associated. The set X_i is the set of all variables from which the Boolen function f essentially depends. The list L_i consists of all configurations that are in fact solutions of the equation $f_i(x) = 0$ (it is expected that the cardinality of $|L_i|$ is about $2^{|X_i|-1}$). Every pair $\big(X_i, L_i\big)$ can be considered as a single vertex in a graph. This set of vertices is said to be upper set [13]. The other type of vertices (lower set) is defined by the pairs $\big(X_i \cap X_j, L'_{ij}\big)$ each of which is obtained via the intersection of variables ffrom i-th and j-th equations, whereas the list L'_{ij} is a set of all possible combinations for tha variables from $X_i \cap X_j$ that is a space $\mathbb{F}_2^{|X_i \cap X_j|}$. The edges are drawn from the vertex $\big(X_i \cap X_j, L'_{ij}\big)$ to every of vertices $\big(X_i, L_i\big)$ and $\big(X_j, L_j\big)$. If there is a pair of vertices with the same intersection that is already considered in the graph, two edges are added instead of introducing the new vertex.

The sparsity in variables plays an important role since the lists L_{ij} comprise all possible combinations from the intersections of two particular equatuions. Here, we discuss a form of sparsity when only a limited numberof variables actually appear in each equation. If this number is large the computationsl cost can be nonfeasible. Together with that, all solutions of the equations from the initial system should be considered.

4.2 Agreeing-Gluing Algorithm

The processing and the search of the solution is performed via the so called Agreeing procedure. This routine takes two adjacent vertices and updates their lists by removing vectors that have different subvectors for common variables. It starts chain-reaction with another vertices that were agreed before such update, so the algorithm proceeds them again that leads to the reducing of their lists.

In practise it is often the case when all vertices are in agreement state while there are still a lot of redundant configarations in their lists, that makes the search of the solution hard from this point. For such situations a Gluing

procedure is performed. For two pairs $\big(X_1, L_1\big)$ and $\big(X_2, L_2\big)$ two sets of variables $Z = X_1 \cup X_2$ and $Y = X_1 \cap X_2$ are defined by the rule $U = \{a_1, b, a_2\}$ with $(a_1, b) \in L_1$, $(b, a_2) \in L_2$, $a_i = X_i \setminus Y$ and b belongs to Y. Then the vector (a_1, b, a_2) is the gluing of (a_1, b) and $\{b, a_2\}$. After the gluing the new vertex is not agreed with its neighbours so the Agreement procedure can start.

There is also another technique used for re-starting the Agreement procedure that is known as Splitting. Its idea is that the list of the vertex is splitted into two parts one of which is temporarily discarded. If there is no solution at the end of the work of the Algorithm, the another partition is considered.

The criteria for stop is the situation when there is an only one item in every list, but in practise it is enough to have small number of vectors in the lists after the Agreeing-Gluing Algorithm.

As results for the usage of this Algorithm to attack SIMON and SPECK we give only maximal number of rounds for which the Algorithm finished in feasible time. It is worth mention that time complexity depends heavily on the heuristics used to start the Agreement process whether it is (partial) Splitting or Gluing. The choice of vertices for Gluing can also comprise some analysis of current state of the graph.

4.3 SIMON

For the cipher SIMON, the maximum number of variables in each equation depends on the number of rounds and keys. For 6 variables, the number of equations will correspond to $n(T-2) + n(T-m)$.

Number of variables	**Number of equations**
6	$2(T-1)(2n-4)$
5	$2(T-1)n$
4	$6(T-1)n + (T-2)n$
3	$2(n+1)(T-1)$
2	$3n$

Table 9: Number of variables for each equation for SIMON

It shows that for $T \geqslant 16$ it becomes rather costly to perform the Agreeng-Gluing algorithm.

Within current work the Agreeing-Gluing Algorithm was run on SIMON for up to 9 rounds.

Simon parameters	**Num. of equations**	**Num. of unknowns**	**Upper set Lower set**
$T = 7$, $m = 2$	112	112	112 800
$T = 8$, $m = 2$	128	128	128 1072
$T = 9$, $m = 2$	144	144	144 1600

Table 10: Parameters for the Raddum-Semaev Algorithm on SIMON

4.4 SPECK

By introducing of new variables on each round of SPECK cipher, the number of different variables on each round does not increase. The maximum number of variables that occur in a single equation is 6. Furthermore, the number of equations and the number of variables on each round can be represented as a Table 11 for $m = 1$ and as a Table 12 for $m = 2, 3, 4$.

Number of variables	**Number of equations**
6	$2(T-1)(2n-4)$
5	$2(T-1)n$
4	$6(T-1)n + (T-2)n$
3	$2(n+1)(T-1)$
2	$3n$

Table 11: Number of variables for each equation for SPECK, $m = 1$

Number of variables	**Number of equations**
6	$2(T-1)(2n-4)$
5	$2(T-1)n$
4	$6(T-1)n + (T-2)n$
3	$2(n+1)(T-1)$
2	$(T-1)n + 3n$

Table 12: Number of variables for each equation for SPECK, $m = 2, 3, 4$

The Agreeing-Gluing Algorithm was run on SPECK for up to 6 rounds.

Speck parameters	**Num. of equations**	**Num. of unknowns**	**Upper set Lower set**
$T = 3$, $m = 1$	500	176	500 558
$T = 4$, $m = 2$	782	320	782 749
$T = 5$, $m = 2$	1032	416	1032 1005
$T = 6$, $m = 2$	1282	512	1282 1229

Table 13: Parameters for the Raddum-Semaev Algorithm on SPECK

5 Conclusion

The goal of current work was to analyze and compare the efficiency of different types of algebraic attacks under the same conditions on two instances of LRX- and ARX- ciphers that are based on the explicit usage of logical operations. This is the first attempt to estimate the resilience of the cipher SPECK to algebraic cryptanalysis via different methods.

Experimental results show that algebraic analysis techniques is perspective way for modern cipher's robustness analysis (especially for lightweight ciphers). Two approaches at algebraic analysis as linearization methods and reduction to SAT-problem for SIMON and SPECK ciphers are presented. The usage of the the Raddum–Semaev Algorithm was also analyzed.

The results of algebraic analysis show that including of extra nonlinear operation (like addition modulo 2^n) leads to an extremely increase of time and memory complexity of algebraic attack. Therefore observed methods more efficiently applicable for SIMON cryptanalysis then for SPECK encryption algorithm. At the same time the sparsity of the system for SPECK seems to be extremely lower than for SIMON that leads to the idea that the usage of techniques that exploit sparsity is a goal worth pursuing.

Further directions of research are: theoretical complexity assessments of algebraic analysis for full-round Simon and Speck ciphers, experimental usage of other ANF-to-CNF converters and efficient SAT-solvers, observe and develop methods to combine linearization and SAT techniques to improve efficiency of analysis. The usage and comparison of other methods of solving systems of Boolean equations is also a direction for the future research.

Acknowledgments. The work was carried out within the framework

of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Laboratory of Cryptography JetBrains Research. The first author was supported by Russian Foundation for Basic Research (project no. 20-31-70043).

The authors cordially thank Sergey Agievich and Natalia Tokareva for the advice and the attention to work and also the anonymous referees for their valuable comments and suggestions which led to the improvement of this paper.

References

[1] Hong D. et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device", *Lecture Notes in Computer Science*, CHES 2006: Cryptographic Hardware and Embedded Systems — CHES 2006, **4249**, 2006, 46–59.

[2] De Canniére C., Dunkelman O., Knezevic M., "KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers", *Lecture Notes in Computer Science*, CHES 2009: Cryptographic Hardware and Embedded Systems — CHES 2009, **5747**, 2009, 272–288.

[3] Gong Z., Nikova S., Law Y.W., "KLEIN: A New Family of Lightweight Block Ciphers", *Lecture Notes in Computer Science*, RFIDSec 2011: RFID. Security and Privacy, **7055**, 2012, 1–18.

[4] Shibutani K., Isobe T., Hiwatari H., Mitsuda A., Akishita T., Shirai T., "*Piccolo*: An Ultra-Lightweight Blockcipher", *Lecture Notes in Computer Science*, CHES 2011: Cryptographic Hardware and Embedded Systems — CHES 2011, **6917**, 2011, 342–357.

[5] Bogdanov A. et al., "PRESENT: An Ultra-Lightweight Block Cipher", *Lecture Notes in Computer Science*, CHES 2007: Cryptographic Hardware and Embedded Systems — CHES 2007, **4727**, 2007, 450–466.

[6] Abed F., List E., Lucks S., Wenzel J., "Differential Cryptanalysis of Round-Reduced Simon and Speck", *Lecture Notes in Computer Science*, FSE 2014: Fast Software Encryption, **8540**, 2015, 525–545.

[7] Raddum H., "Algebraic Analysis of the Simon Block Cipher Family", *Lecture Notes in Computer Science*, LATINCRYPT 2015: Progress in Cryptology — LATINCRYPT 2015, **9230**, 2015, 157–169.

[8] Courtois N, Mourouzis T, Song G, Sepehrdad P, Susil P., "Combined Algebraic and Truncated Differential Cryptanalysis on Reduced-round Simon", 11th International Conference on Security and Cryptography, 2014, 399–404.

[9] Andrzejczak M., Dudzic W., "SAT Attacks on ARX Ciphers with Automated Equations Generation", *Infocommunications Journal*, **11**:4 (2019), 2–7.

[10] Yeo S.L., Le D.-P., Khoo K., "Improved algebraic attacks on lightweight block ciphers", *Jour. of Cryptogr. Engineering*, **11** (2021), 1–19.

[11] Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L., "The Simon and Speck Families of Lightweight Block Ciphers", *NSA Research Directorate*, 2013.

[12] Courtois N. T.,Debraize B., "Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0", *Lecture Notes in Computer Science*, ICICS 2008: Information and Communications Security, **5308**, 2008, 328–344.

[13] Bard G., *Algebraic Cryptanalysis*, Springer, 2009, 356 pp.

[14] Courtois N., Shamir A., Patarin J., Klimov A., "Efficient algorithms for solving overdefined systems of multivariate polynomial equations", *Lecture Notes in Computer Science*, EUROCRYPT 2000, **1807**, ed. B. Preneel, 2000, 392–407

[15] Courtois N., "The security of cryptographic primitives based on multivariate algebraic problems", MQ, MinRank, IP, HFE. Ph.D. thesis, Paris VI (2001). Available at http://www.nicolascourtois.net/phd.pdf.

[16] Courtois, N., Bard, G.V., "Algebraic cryptanalysis of the data encryption standard", *Lecture Notes in Computer Science*, IMA International Conference on Cryptography and Coding Theory, **4887**, ed. S.D. Galbraith, 2007, 152–169.

[17] Courtois N., Sepehrdad P., Susil P., Vaudenay S., "Elimlin algorithm revisited", *Lecture Notes in Computer Science*, FSE 2012: Fast Software Encryption, **7549**, 2012, 306–325.

[18] Soos M., Nohl K., Castelluccia C., "Extending SAT Solvers to Cryptographic Problems", *Lecture Notes in Computer Science*, SAT 2009: Theory and Applications of Satisfiability Testing — SAT 2009], **5584**, 2009, 244–257.

[19] Massacci F., Marraro L., "Logical cryptanalysis as a SAT-problem: Encoding and analysis", *Journal of Automated Reasoning*, **24** (2000), 165–203.

[20] Grain of Salt https://www.msoos.org/grain-of-salt/.

[21] Janicic P., "URSA: A System for Uniform Reduction to SAT", *Logical Methods in Computer Science*, **8** (2012).

[22] Carter K., Foltzer A., Hendrix J., Huffman B., Tomb A., "SAW: The software analysis workbench", 2013 ACM SIGAda Annual Conference on High Integrity Language Technology (HILT), 2013, 15–18.

[23] Semenov A., Otpuschennikov I., Gribanova I., Zaikin O., Kochemazov S., "Translation of Algorithmic Descriptions of Discrete Functions to SAT with Applications to Cryptanalysis Problems", *Logical Methods in Computer Science*, **16**:1 (2020).

[24] Choo D., Soos M., Chai K.M.A., Meel K. S., "Bosphorus: Bridging ANF and CNF Solvers", 2019 Design, Automation, Test in Europe Conference Exhibition (DATE), 2019.

[25] "An ANF to CNF Converter using a Dense/Sparse Strategy", https://doc.sagemath.org/html/en/reference/sat/sage/sat/converters/polybori.html.

[26] Soos M., "The CryptoMiniSat 5 set of solvers at SAT competition 2016", *SAT Competition 2016 — Solver and Benchmark Descriptions*, 2016.

[27] Biere A., "CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT Entering the SAT Competition 2017", Proceedings of SAT Competition 2017 — Solver and Benchmark Descriptions, **B-2017-1 of Department of Computer Science Series of Publications B** (2017), 14–15.

[28] Heule M.J.H., Järvisalo M.J., Suda M. (eds.), "Proceedings of SAT Competition 2018 — Solver and Benchmark Descriptions", **B-2018-1** (2018).

[29] "Proceedings of SAT Competition 2020 — Solver and Benchmark Descriptions", **B-2020-1** (2020).

[30] Raddum H., Semaev I., "New technique for solving sparse equation systems", Cryptology ePrint Archive, 2006/475.

[31] Semaev I., "On solving sparse algebraic equations over finite fields", *Des. Codes Cryptogr.*, **49**:1–3 (2008), 47–60.

Анализ стойкости стандартов легковесной криптографии для систем связи по радиоинтерфейсу к алгебраическим атакам[1]

Куценко Александр Владимирович, *аспирант, Новосибирский государственный университет, мл. научн. сотр, Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, alexandrkutsenko@bk.ru*

Атутова Наталья Дмитриевна*, студентка, Новосибирский государственный университет, г. Новосибирск, n.atutova@g.nsu.ru*

Зюбина Дарья Александровна*, студентка, Новосибирский государственный университет, г. Новосибирск, d.zyubina@g.nsu.ru*

Маро Екатерина Александровна, *кандидат технических наук, доцент, Южный федеральный университет, г. Таганрог, eamaro@sfedu.ru*

Филиппов Степан Дмитриевич*, студент, Санкт-Петербургский государственный университет, г. Санкт-Петербург, filippowstepan@yandex.ru*

Аннотация

Легковесные криптографические примитивы предназначены для обеспечения эффективности и безопасности при существенных ограничениях на объем используемых ресурсов. В настоящее время одними из стандартов легковесной криптографии для систем связи по радиоинтерфейсу с помощью радиочастотной идентификация являются предложенные АНБ США в 2013 году блочные шифры Simon и Speck. В настоящей работе проводится алгебраический криптоанализ легковесных криптографических примитивов на примере шифров Simon и Speck с сокращенным числом раундов. На основе полученных результатов делается вывод об эффективности алгебраических атак на рассматриваемые шифры. При проведении алгебраического криптоанализа рассмотрен ряд известных подходов, в основе которых лежит метод линеаризации, получены теоретические оценки на эффективность использования данного метода. Рассмотрена эффективность подхода, заключающегося в использовании SAT-решателей различных типов.

Ключевые слова: блочный шифр, легковесная криптография, алгебраический криптоанализ, Simon, Speck.

Введение

Легковесная криптография является актуальным направление исследований, представляющим интерес в настоящее время. Это связано с тем, что влияние и использование RFID-меток, ПЛИС, смарт-карт, мобильных телефонов, сенсорных сетей и других устройств с ограничениями на используемые ресурсы постоянно растет и приобретает всё большую важность. Соответственно, возникает задача, связанная с разработкой и анализом криптографических алгоритмов, эффективных при условиях работы, предполагающих ограничения на используемые ресурсы. Легковесные криптографические примитивы предназначены для обеспечения эффективности и безопасности при ограниченном объеме ресурсов. В этом случае возникает проблема поиска компромисса между безопасностью и эффективностью, измеряемой с помощью различных метрик.

1 Работа первых трёх авторов выполнена в рамках государственного задания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research. Работа первого автора выполнена при поддержке Российского Фонда Фундаментальных Исследований (проект № 20-31-70043).

За последние годы был разработан ряд легковесных блочных и поточных шифров, а также хэш-функций с целью получения вышеупомянутого компромисса. Список легковесных блочных шифров включает такие шифры как HIGH [1], KATAN [2], KLEIN [3], Piccolo [4] и PRESENT [5].

В 2013 году Агентство национальной безопасности США представило семейства Simon и Speck легковесных блочных шифров для обеспечения хорошей аппаратной и программной производительности. Шифр Simon был оптимизирован для аппаратной реализации, в то время как Speck - для программной. При этом было подчеркнуто, что оба семейства эффективны как для программной, так и для аппаратной реализации, что обеспечивает гибкость, необходимую для различных приложений. По состоянию на октябрь 2018 года шифры Simon и Speck были стандартизированы Международной организацией по стандартизации (ISO) в рамках следующих стандартов легковесной криптографии для систем связи по радиоинтерфейсу RFID (радиочастотной идентификации):

- Международный стандарт ISO/IEC 29167-21:2018
  Информационные технологии. Методы автоматической идентификации и сбора данных. Часть 21. Службы безопасности набора криптографического алгоритма SIMON для систем связи по радиоинтерфейсу;
- Международный стандарт ISO/IEC 29167-22:2018
  Информационные технологии. Методы автоматической идентификации и сбора данных. Часть 22. Службы безопасности набора криптографического алгоритма SPECK для систем связи по радиоинтерфейсу,

что делает их доступными для использования коммерческими организациями.

В документе, опубликованном разработчиками, не было указано результатов криптоанализа данных шифров. Однако позже появились несколько работ, в которых анализировалась устойчивость данных шифров к некоторым видам статистических и аналитических атак. Например, в статье [6] рассматривался разностный криптоанализ шифров Simon и Speck с уменьшенным числом раундов. Был сделан вывод о наличии определённых недостатков.

Рассмотренные шифры являются представителями LRX- и ARX- структур блочных шифров, в основе которых является использование нелинейных алгебраических операций вместо S-блоков. Это обуславливает интерес к алгебраическому криптоанализу данных шифров. Основная идея алгебраического криптоанализа состоит в составлении сложной системы булевых уравнений, описывающих преобразование шифра. Система строится на основе полностью известного алгоритма шифрования. Зашифрование на секретном, неизвестном криптоаналитику ключе некоторого количества открытых текстов позволяет провести означивание системы – подстановку в уравнения системы битов открытого текста и соответствующего ему шифртекста. На следующем этапе осуществляется решение данной системы булевых уравнений с помощью различных методов. Неизвестными являются биты ключа - они соответствуют решению.

Первая попытка провести алгебраический анализ шифра Simon была сделана в работе [7]. Комбинация алгебраического и усеченного разностного криптоанализа шифра Simon от малого числа раундов была рассмотрена в работе [8]. Алгебраические атаки были представлены использованием SAT-решателя, а также алгоритма ElimLin. Относительно недавно опубликована статья [9], в которой рассмотрены алгебраические атаки на легковесные шифры Simon и Present с помощью SAT-решателей.

В настоящей работе мы изучаем и сравниваем эффективность алгебраических атак на легковесные блочные шифры на примере LRX- и ARX- шифров Simon и Speck с сокращенным числом раундов. Анализ осуществляется с помощью различных SAT-

решателей, а также методов решения систем полиномиальных уравнений, основанных на процедуре линеаризации. На основе полученных результатов делается вывод об эффективности рассмотренных алгебраических атак на данные шифры, а также сравнении стойкости шифров Simon и Speck.

1. Семейства шифров Simon и Speck

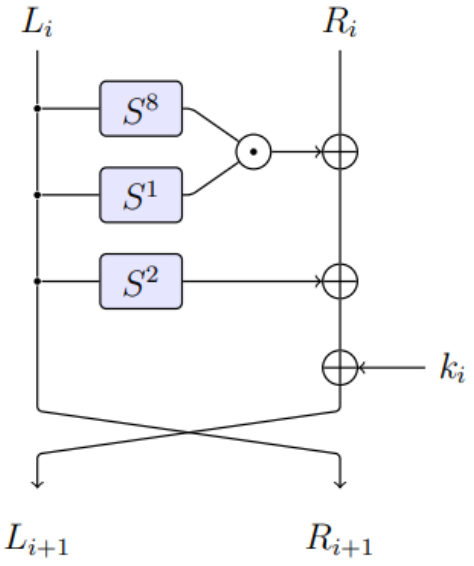
1.1 Общее описание шифра Simon

Simon – это семейство легковесных блочных шифров, разработанных для оптимальной аппаратной реализации [10]. Семейство имеет структуру классической схемы Фейстеля, в каждом раунде $2n$-битовый вход раунда делится на две -битовые половины. Раунд применяет нелинейную, необратимую функцию раунда F: $F_2^n \to F_2^n$ применяемую к левой половине L. К выводу функции применяется операция XOR с правой половиной R и ключом k и две половины меняются местами. Функция F определяется как

$$F(x) = \left(S^8(x) \odot S^1(x)\right) \oplus S^2(x), \; x \in F_2^n$$

где $S^j(x)$ обозначает левый сдвиг x на j позиций, символом $\odot$ обозначено побитовая операция логического умножения, а символ $\oplus$ обозначает бинарную операцию сложения по модулю 2.

Вводя новую переменную для каждого выхода побитовой операции $\odot$ для описания T раундов получаем $n \cdot (T-2)$ квадратичных уравнений с $n \cdot (T-2) + k$ неизвестными, где n - размер слова, T - количество раундов, а k - длина ключа.



Раундовая функция шифра Simon

Ключевое расписание Simon описывается как функция, которая работает с двумя, тремя или четырьмя -разрядными регистрами слов, в зависимости от размера общего ключа. Она выполняет два сдвига вправо: $S^{-3}(x)$ и $S^{-1}(x)$ и выполняет XOR результатов вместе с фиксированной константой $c = 2^{n-4}$ и пятью заданными последовательностями в зависимости от версии спецификации. Эти постоянные последовательности получаются с помощью трех квадратных матриц порядка 5 над полем F_2 и регистра сдвига с линейной обратной связью, где первые две имеют период

31, а последние три имеют период 62. Общий секретный ключ состоит из m ключевых слов, каждое из которых имеет длину n битов, где $m \in \{2,3,4\}$.

1.1.1 Ключевое расписание

Устанавливаются первые m ключей, каждый из которых состоит из n битов.

Последовательность ключей вычисляется рекурсивно ($c = 2^{n-4}$ - постоянная, а z_j - фиксированная периодическая последовательность, см. [10]. Значение m зависит от размера блока $2n$ и количества раундов T. (Таблица 1)

$$k_{\{i+m\}} = \begin{cases} c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+1}, m = 2 \\ c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+2}, m = 3 \\ c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})(S^{-3}k_{i+3} \oplus k_{i+1}), m = 4 \end{cases}$$

Размер блока $2n$	**Размер ключа** mn	**Размер слова** n	**Ключи** m	**Константа**	**Раунды** T
32	**64**	16	4	z_0	32
48	**72**	24	3	z_0	36
	96		4	z_1	36
64	**96**	32	3	z_2	42
	128		4	z_3	44
96	**96**	48	2	z_2	52
	144		3	z_3	54
128	**128**	64	2	z_2	68
	192		3	z_3	69
	256		4	z_4	72

Таблица 1 – Параметры Simon

1.2 Общее описание Speck

Speck - семейство легковесных блочных шифров, разработанных для эффективной программной реализации и оптимизированных для работы на микроконтроллерах [10]. В каждом раунде $2n$-битовый вход раунда делится на две - битовые половины. Каждый раунд Speck применяет нелинейную круглую функцию, которая определяется как

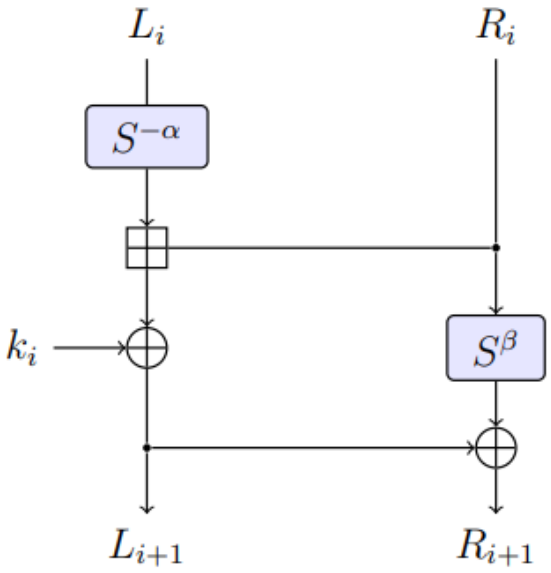
$$R_k(x, y) \to \Big((S^{-\alpha}(x) + y) \oplus k, S^{\beta}(y) \oplus (S^{-\alpha}(x) + y) \oplus k\Big),$$

где $S^j(x)$ обозначает побитовый сдвиг влево (если $j > 0$) на позиции j и побитовый сдвиг вправо (если $j < 0$), символ + является сложением по модулю2^n. Параметры имеют следующие значения $\alpha = 7$ и $\beta = 2$, если n = 16 (размер блока = 32) и $\alpha = 8$ и $\beta = 3$ в противном случае.

В раунде шифрования каждый раз добавляются $8n - 2$ уравнений и $3n$ неизвестных. Начиная со второго раунда, $8n - 2$ новых уравнений и $3n$ неизвестных добавляются из-за ключевого расписания. При построении системы уравнений мы подставляем входной и выходной шифр перед первым и после последнего раундов (L_0, R_0, L_n, R_n), поэтому число неизвестных уменьшается на $4n$. Окончательная формула для числа уравнений и числа неизвестных

$$e = (8n - 3)(2T - 1) - (6n - 3),$$
$$u = n(6T - 4),$$

где e - число уравнений, u - число неизвестных, n - размер слова, T - число раундов.



Раундовая функция шифра Speck

1.2.1 Ключевое расписание

Ключевое расписание шифра Speck использует раундовую функцию для генерации раундовых ключей. Пусть $K = (l_{m-2}, \ldots, l_0, k_0)$ - ключ для Speck. Значение m зависит от значений размера блока $2n$ и количества раундов T (таблица 2). Ключи k_i и l_i определяются как

$$l_{i+m-1} = (k_i + S^{-\alpha} l_i) \oplus i,$$
$$k_{i+1} = S^{\beta} k_i \oplus l_{i+m-1}$$

Размер блока $2n$	**Размер ключа** mn	**Размер слова** n	**Ключи** m	**Сдвиг** α	**Сдвиг** β	**Раунды** T
32	**64**	16	4	7	2	22
48	**72**	24	3	8	3	22
	96		4			23
64	**96**	32	3	8	3	26
	128		4			27
96	**96**	48	2	8	3	28
	144		3			29
128	**128**	64	2	8	3	32
	192		3			33
	256		4			34

Таблица 2 – Параметры Speck

Проведение криптоанализа на небольшом количестве раундов (например, 3 и 4) с выбором стандартных спецификаций (таблица 2) нецелесообразно, так как ключи не строятся на основе исходных и между ними не будет никакой связи. Поэтому в данной работе для $T \in \{3,4\}$ предполагается $m = 1$.

1.2.2 Сложение по модулю 2^n

Раундовая функция шифра Speck нелинейна, то есть она не может быть описана исключительно линейными алгебраическими уравнениями. Это свойство Speck обеспечивается операцией сложения по модулю 2^n, которая является частью алгоритма шифрования. Можно получить переопределенную систему из $6n-3$ линейно независимых алгебраических уравнений, полностью описывающих рассматриваемую операцию [11]. Одно из них будет линейным, а остальные - квадратичными.

$$
\begin{cases}
w_0 x_{i+\alpha} = x_\alpha x_{i+\alpha} \oplus y_0 x_{i+\alpha}, \overline{i=1,n-1} \\
w_0 y_i = x_\alpha y_i \oplus y_0 y_i, \overline{i=0,n-1} \\
w_0 w_i = x_\alpha w_i \oplus y_0 w_i, \overline{i=0,n-1} \\
w_1 x_\alpha = x_{1+\alpha} x_\alpha \oplus y_1 x_\alpha \oplus x_\alpha y_0 \\
w_1 y_0 = x_{1+\alpha} y_0 \oplus y_1 y_0 \oplus x_\alpha y_0 \\
w_i = x_{i+\alpha} \oplus y_i \oplus x_{i-1+\alpha} \oplus y_{i-1} \oplus x_{i-1+\alpha} y_{i-1} \oplus x_{i-1+\alpha} w_{i-1} \oplus y_{i-1} w_{i-1}, \overline{i=2,n-1} \\
w_i(x_{i-1+\alpha} \oplus y_{i-1}) = x_{i-1+\alpha} x_{1+\alpha} \oplus x_{i-1+\alpha} y_i \oplus x_{i-1+\alpha} \oplus x_{i-1+\alpha} w_{i-1} \oplus x_{1+\alpha} y_{i-1} \oplus y_{i-1} y_i \\
\oplus y_{i-1} \oplus y_{i-1} w_{i-1}, \overline{i=2,n-1} \\
w_i(x_{i-1+\alpha} \oplus w_{i-1}) = x_{i-1+\alpha} x_{1+\alpha} \oplus x_{i-1+\alpha} y_i \oplus x_{i-1+\alpha} \oplus x_{i+\alpha} w_{i-1} \oplus y_i w_{i-1} \oplus x_{i-1+\alpha} w_{i-1}, \\
\overline{i=2,n-1}
\end{cases}
$$

2. Атаки, основанные на линеаризации

2.1 Простая линеаризация

Идея этого метода состоит в том, чтобы присвоить каждому одночлену исходной системы новую переменную. После операции присваивания система становится линейной. Полученная система решается различными методами, например, методом исключения Гаусса, после этого решения системы линейных уравнений проверяются на то, что они являются решениями исходной нелинейной системы уравнений.

Эффективность линеаризации зависит от ранга r системы, тогда как количество различных одночленов в исходной системе определяет количество переменных n' в системе линейных уравнений. Набор решений не пустой, поэтому он равен $2^{n'-r} > 0$, поэтому для оценки производительности необходимо проанализировать границы для значений n' и r.

Анализ этой атаки (см., например, [12]) показывает, что ранг системы с большой вероятностью будет достаточно большим при $m \approx n^2/2$. Оценить необходимое количество операций и временную сложность атаки можно, учитывая количество различных одночленов в системе уравнений, описывающих рассматриваемый шифр, и варьируя ранг системы.

2.1.2 Количество различных мономов системы уравнений шифра Simon

Рассматривая алгоритм шифрования, можем оценить количество одночленов для каждого раунда. С введением новых переменных оценка составит $6nT$, где n - длина слова, T - количество раундов. Оценка была получена исходя из того, что для каждой операции вводятся новые переменные и также повторное обозначение при замене L_{i+1} и R_{i+1}.

Кроме того, была проведена оценка количества переменных без переназначения (введения новых переменных), чтобы оценить эффективность метода линеаризации. При анализе небольшого количества раундов без введения новых переменных было

сделано наблюдение, что каждые четыре раунда количество переменных уменьшается при сложении с R_i.

Таким образом, можно получить рекуррентное соотношение для числа переменных изменяемой части с учетом сокращения переменных каждые четыре раунда. Пусть $P(T)$ - количество переменных на раунде T:

$$P(T) = \begin{cases} 4n, n = 1 \\ 7n, n = 2 \\ n(P^2(T-2) + P(T-2) + 1), n \vdots 4 \\ n(P^2(T-2) + P(T-1) + P(T-2) + 1), \text{иначе.} \end{cases}$$

На практике была найдена оценка количества переменных $\approx 2^{72}$ для $n = 16$, $T = 32$, исключая ключевой этап. Таким образом, выявлено, что ввод новых переменных значительно сокращает объем вычислений.

Окончательная формула для оценки количества одночленов, исключая те, которые происходят из ключевых уравнений расписания (все уравнения линейны), имеет следующий вид:

$$M \leq 6nT,$$

где M - количество одночленов, n - размер слова, T - количество раундов.

Размер блока $2n$	**Размер слова** n	**Раунды T**	**Кол-во мономов**	**Кол-во уравнений**	**Кол-во неизвестных без ключ. расписания**
32	16	32	$\approx 2^{11.585}$	$\approx 2^{8.9069}$	$\approx 2^{8.9542}$
48	24	36	$\approx 2^{12.34}$	$\approx 2^{9.6724}$	$\approx 2^{9.7142}$
64	32	42	$\approx 2^{12.977}$	$\approx 2^{10.322}$	$\approx 2^{10.358}$
		44	$\approx 2^{13.044}$	$\approx 2^{10.392}$	$\approx 2^{10.426}$
96	48	52	$\approx 2^{13.87}$	$\approx 2^{11.229}$	$\approx 2^{11.257}$
		54	$\approx 2^{13.925}$	$\approx 2^{11.285}$	$\approx 2^{11.313}$
128	64	68	$\approx 2^{14.672}$	$\approx 2^{12.044}$	$\approx 2^{12.066}$
		69	$\approx 2^{14.693}$	$\approx 2^{12.066}$	$\approx 2^{12.087}$
		72	$\approx 2^{14.755}$	$\approx 2^{12.129}$	$\approx 2^{12.15}$

Таблица 3 – Параметры системы уравнений шифра Simon

2.1.2 Количество различных мономов системы уравнений шифра Speck

Основным методом удержания степени является введение новых переменных для выходных битов нелинейных операций. В этом случае степень не будет превышать 2. С каждым новым раундом вводятся новые переменные: текст (x_i, y_i), ключ (k_i, l_i), переменные, описывающие сложение по модулю 2^n.

В системе уравнений, описывающей сложение по модулю 2^n (раздел 1.2.2), имеется всего $5(7n - 8)$ мономов. На практике оказалось, что всего различных мономов в системе уравнений сложения по модулю 2^n не более, чем $25n - 18$. В результате количество различных мономов на каждом раунде шифра Speck не превышает $28n - 18$.

Итоговая формула для оценки числа одночленов, исключая такие, которые образуются из генерации ключей (все уравнения линейны), имеет вид

$$M \leq (28n - 18)T,$$

где M – количество мономов, n – размер слова, T – количество раундов.

Размер блока $2n$	**Число раундов** T	**Кол-во мономов**	**Кол-во уравненинии й без ключевого расписания**	**Кол-во уравнений с ключевым расписанием**	**Кол-во неизвестны х без ключевого расписания**	**Кол-во неизвестных с ключевым расписанием**
32	22	$\approx 2^{13.2}$	$\approx 2^{11.4}$	$\approx 2^{12.4}$	$\approx 2^{9.95}$	$\approx 2^{11}$
48	22	$\approx 2^{13.81}$	$\approx 2^{12}$	$\approx 2^{13.03}$	$\approx 2^{10.5}$	$\approx 2^{11.59}$
	23	$\approx 2^{13.88}$	$\approx 2^{12.1}$	$\approx 2^{13.09}$	$\approx 2^{10.6}$	$\approx 2^{11.65}$
64	26	$\approx 2^{14.47}$	$\approx 2^{12.7}$	$\approx 2^{13.7}$	$\approx 2^{11.2}$	$\approx 2^{12.25}$
	27	$\approx 2^{14.5}$	$\approx 2^{12.75}$	$\approx 2^{13.74}$	$\approx 2^{11.27}$	$\approx 2^{12.3}$
96	28	$\approx 2^{15.2}$	$\approx 2^{13.4}$	$\approx 2^{14.4}$	$\approx 2^{11.9}$	$\approx 2^{12.94}$
	29	$\approx 2^{15.23}$	$\approx 2^{13.44}$	$\approx 2^{14.44}$	$\approx 2^{11.96}$	$\approx 2^{13}$
128	32	$\approx 2^{15.79}$	$\approx 2^{14}$	$\approx 2^{15}$	$\approx 2^{12.52}$	$\approx 2^{13.56}$
	33	$\approx 2^{15.84}$	$\approx 2^{14.04}$	$\approx 2^{15.04}$	$\approx 2^{12.57}$	$\approx 2^{13.6}$
	34	$\approx 2^{15.88}$	$\approx 2^{14.08}$	$\approx 2^{15.08}$	$\approx 2^{12.62}$	$\approx 2^{13.64}$

Таблица 4 – Параметры системы уравнений шифра Speck

2.2 XL-атака

Данная атака была представлена в работах [13,14]. На вход поступает система из m полиномиальных уравнений от n неизвестных степени d, на выходе ее решения, если уравнения имеют достаточный ранг.

1. Выбрать степень $D > d$. Обычно $D = d + 1$.
2. Составить список S всех одночленов степени $D - d$ или меньше, включая одночлен 1 степени 0.
3. Умножить уравнения исходной системы на каждый элемент из множества S. (Поскольку до этого шага было m уравнений, после него будет $m|S|$ уравнений).
4. Линеаризовать систему.
5. Решить полученную систему линейных уравнений.

Для случая $d = 2$ и $D = d + 1$ анализ этой атаки [12] показывает, что единственное решение, вероятно, будет найдено, если $m \approx n^2/6$m.

2.3 ElimLin

Алгоритм ElimLin появился в работе [15] (анализ можно найти в [16]). Его суть - поиск скрытых линейных уравнений, существующих в идеале, порожденном рассматриваемой системой уравнений. Этот алгоритм состоит из двух последовательных шагов:

1. Исключение Гаусса: поиск линейных уравнений в линейной оболочке исходной системы уравнений.
2. Замена: переменные итеративно удаляются.

Более подробно это можно описать следующим образом.

1. ВХОД: Система полиномиальных уравнений степени 2.
2. ВЫХОД: решение, либо решения системы, если уравнения имеют достаточный ранг. В противном случае приведенная система

уравнений с меньшим количеством переменных, чем исходная, должна быть решена с помощью другого метода.

2.5 Результаты

В таблицах 5,6 приведены результаты для простой линеаризации, XL-метода и ElimLin. Полученные данные позволяют сравнить эффективность этих методов для шифров Simon и Speck. Для XL-метода выбрано значение степени $D = 3$.

	Параметры Simon	**Кол-во уравнений**	**Кол-во переменных**	**Кол-во мономов**	**Кол-во решений**
Линеаризация	$T = 3, m = 1$	48	32	48	4
XL-метод	$T = 3, m = 1$	1584	32	992	1
Линеаризация	$T = 4, m = 1$	64	48	80	65536
XL-метод	$T = 4, m = 1$	3136	48	2616	256
	Параметры Speck				
Линеаризация	$T = 3, m = 1$	500	176	1236	—
XL-метод	$T = 3, m = 1$	88500	176	185216	—

Таблица 5 – Результаты атак, основанных на линеаризации

	Параметры	**(Кол-во ур-ний, Кол-во лин. ур-ний)**	**(Кол-во ур-ний, Кол-во лин. ур-ний после ElimLin)**
Simon	$T = 3, m = 1$	(48, 32)	(48, 32)
Simon	$T = 5, m = 1$	(80, 32)	(80, 48)
Speck	$T = 3, m = 1$	(500, 132)	(307, 137)
Speck	$T = 5, m = 2$	(1032, 296)	(654, 297)

Таблица 6 – Результаты ElimLin

3. Атаки основанные на SAT решателях

3.1 SAT

Задача булевой выполнимости (SAT) — это задача решения, в которой для произвольной булевой формулы возникает вопрос, существует ли такое значение переменных, что формула имеет значение “Истина”. Данная задача является NP-трудной.

SAT решатели — это мощный вычислительный инструмент для проверки вычислительной трудности определенных задач [16]. Существует несколько примеров использования SAT-решателей в области алгебраического криптоанализа. Первый криптоанализ на основе SAT был представлен в [17]. В этой работе стандарт шифрования данных DES был атакован с использованием SAT-решателей на основе DPLL.

Криптоанализ на основе SAT предполагает два этапа: на первом этапе выполняется кодирование в SAT форму, например перевод данной системы из алгебраической нормальной формы (АНФ, полином Жегалкина) в конъюнктивную нормальную форму (КНФ). Существуют некоторые инструменты для автоматизированного преобразования криптографических задач в КНФ: Grain-of-Salt [19], URSA [20], SAW [21], Transalg [22], Bosphorus [23]. Мы используем конвертер anf2cnf [24] из библиотеки PolyBoRi, интегрированной в Sage. На втором этапе полученный экземпляр SAT-задачи решается с помощью SAT-решателя. Для криптографических систем часто применяются такие SAT-решатели, как CryptoMiniSat [25] и Lingering (с его параллельными версиями Plingeling и Treengeling) [26].

Дополнительную информацию о современном положении дел и развитии подходов на основе SAT-решателей, а также их приложениях к криптоанализу можно найти в работе [21].

3.2 Результаты

В этом разделе приведены результаты использования SAT-решателей для реализации алгебраической атаки на шифры Simon и Speck с сокращенным числом раундов. Мы применяем SAT-решатели CryptoMiniSat (в Sage ver. 6.10) и Lingeling, Plingeling, Treengeling на ПК со следующими параметрами: Core i5-4690 CPU 3,5 ГГц (x4), 12 Гб оперативной памяти. Экспериментальные результаты решения SAT для 3-10-го раунда Simon и 3-6-го раунда Speck представлены в таблицах 7 и 8. Были рассмотрены два генератора систем уравнений в форме АНФ для шифра Simon: в одном все раундовые ключи являются независимыми переменными, в другом все раундовые ключи представлены алгоритмом ключевого расписания.

Параметры Simon	**Кол-во ур-ний**	**Кол-во неизв.**	**Параметры КНФ**	**SAT**	**Время (RAM)**
$T = 8, m = 2$	128	128	368 лит., 4448 клоз.	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- 845.4 с., 26.6 MB 1188.8 с., 169.2 MB 4426.12 с., 95 MB
$T = 9, m = 2$	144	144	480 лит., 6448 клоз.	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- - 47799.2 с., 620.3 MB -
$T = 10, m = 2$	160	160	560 лит., 8096 клоз.	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- - 17554.9 с., 458.8 MB -
$T = 11, m = 2$	176	176	640 лит., 9648 клоз.	CryptoMiniSat (SageMath) Lingeling Plingeling Treengeling	- - - -

Таблица 7 – Результаты применения SAT-решателя для шифра Simon

Параметры Speck	**Кол-во ур-ний**	**Кол-во неизв.**	**Параметры КНФ**	**SAT**	**Время (RAM)**
$T = 3,\ m = 1$	500	176	1460 лит., 11020 клоз.	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	0.56 с. 0.9 с., 9.6 MB 0.97 с., 4 MB 0.2 с., 1.9 MB
$T = 4,\ m = 2$	782	320	2492 лит., 17380 клоз.	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	21.4 с. 3.0 с., 17.3 MB 8.25 с., 15 MB 61.4 с., 14.8 MB
$T = 5,\ m = 2$	1032	416	3312 лит., 23184 клоз.	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	- - 14448.17 с., 278 MB -
$T = 6,\ m = 2$	1282	512	4132 лит., 28988 клоз.	CryptoMiniSat (SageMath) Plingeling Treengeling Lingeling	- - 123353.82 с., 546 MB -

Таблица 8 – Результаты применения SAT-решателя для шифра Speck

Заключение

Как показывают экспериментальные результаты, методы алгебраического анализа являются перспективным подходом к анализу устойчивости современных шифров, в частности, легковесных шифров. В работе рассмотрены два основных подхода к алгебраическому анализу: подход, в основе которого лежит процесс линеаризации, а также подход, заключающийся в использовании SAT-решателей.

Полученные результаты показывают, что включение дополнительных нелинейных операций (например, операцию сложения по модулю 2^n) значительно увеличивает временную сложность, а также использование памяти ЭВМ. Из этого можно сделать вывод, что рассмотренные методы алгебраических атак более эффективны при проведении криптоанализа шифра Simon, чем для алгоритма шифрования Speck.

Дальнейшие направления исследований: теоретические оценки сложности алгебраического анализа для полнораундовых шифров Simon и Speck, экспериментальное использование других трансляторов ANF-to-CNF и эффективных SAT-решателей, наблюдение и разработка методов объединения линеаризации и методов SAT для повышения эффективности анализа. Также стоит рассмотреть другие методы решения систем булевых уравнений, например, подход метод Раддума-Семаева.

Литература

[1] Hong D. et al., “HIGHT: A New Block Cipher Suitable for Low-Resource Device”, Lecture Notes in Computer Science, CHES 2006: Cryptographic Hardware and Embedded Systems — CHES 2006, 4249, 2006, 46–59.

[2] De Canni´ere C., Dunkelman O., Knezevic M., “KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers”, Lecture Notes in Computer Science, CHES 2009: Cryptographic Hardware and Embedded Systems — CHES 2009, 5747, 2009, 272–288.

[3] Gong Z., Nikova S., Law Y.W., “KLEIN: A New Family of Lightweight Block Ciphers”, Lecture Notes in Computer Science, RFIDSec 2011: RFID. Security and Privacy, 7055, 2012, 1–18.

[4] Shibutani K., Isobe T., Hiwatari H., Mitsuda A., Akishita T., Shirai T., “Piccolo: An UltraLightweight Blockcipher”, Lecture Notes in Computer Science, CHES 2011: Cryptographic Hardware and Embedded Systems — CHES 2011, 6917, 2011, 342–357.

[5] Bogdanov A. et al., “PRESENT: An Ultra-Lightweight Block Cipher”, Lecture Notes in Computer Science, CHES 2007: Cryptographic Hardware and Embedded Systems — CHES 2007, 4727, 2007, 450–466.

[6] Abed F., List E., Lucks S., Wenzel J., “Differential Cryptanalysis of Round-Reduced Simon and Speck”, Lecture Notes in Computer Science, FSE 2014: Fast Software Encryption, 8540, 2015, 525–545.

[7] Raddum H., “Algebraic Analysis of the Simon Block Cipher Family”, Lecture Notes in Computer Science, LATINCRYPT 2015: Progress in Cryptology — LATINCRYPT 2015, 9230, 2015, 157–169. 14

[8] Courtois N, Mourouzis T, Song G, Sepehrdad P, Susil P., “Combined Algebraic and Truncated Differential Cryptanalysis on Reduced-round Simon”, 11th International Conference on Security and Cryptography, 2014, 399–404.

[9] Yeo S.L., Le D.-P., Khoo K. “Improved algebraic attacks on lightweight block ciphers”, Journal of Cryptographic Engineering, 11, 1–19 (2021).

[10] Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L., “The Simon and Speck Families of Lightweight Block Ciphers”, NSA Research Directorate, 2013.

[11] Courtois N. T.,Debraize B., “Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0”, Lecture Notes in Computer Science, ICICS 2008: Information and Communications Security, 5308, 2008, 328–344.

[12] Bard G., Algebraic Cryptanalysis, Springer, 2009, 356 pp.

[13] Courtois N., Shamir A., Patarin J., Klimov A., “Efficient algorithms for solving overdefined systems of multivariate polynomial equations”, Lecture Notes in Computer Science, EUROCRYPT 2000, 1807, ed. B. Preneel, 2000, 392–407

[14] Courtois N., “The security of cryptographic primitives based on multivariate algebraic problems”, MQ, MinRank, IP, HFE. Ph.D. thesis, Paris VI (2001). Available at http://www.nicolascourtois.net/phd.pdf.

[15] Courtois, N., Bard, G.V., “Algebraic cryptanalysis of the data encryption standard”, Lecture Notes in Computer Science, IMA International Conference on Cryptography and Coding Theory, 4887, ed. S.D. Galbraith, 2007, 152–169.

[16] Courtois N., Sepehrdad P., Susil P., Vaudenay S., “Elimlin algorithm revisited”, Lecture Notes in Computer Science, FSE 2012: Fast Software Encryption, 7549, 2012, 306–325.

[17] Soos M., Nohl K., Castelluccia C., “Extending SAT Solvers to Cryptographic Problems”, Lecture Notes in Computer Science, SAT 2009: Theory and Applications of Satisfiability Testing — SAT 2009, 5584, 2009, 244–257.

[18] Massacci F., Marraro L., “Logical cryptanalysis as a SAT-problem: Encoding and analysis”, Journal of Automated Reasoning, 24 (2000), 165–203.

[19] Grain of Salt https://www.msoos.org/grain-of-salt/.

[20] Janicic P., “URSA: A System for Uniform Reduction to SAT”, Logical Methods in Computer Science, 8 (2012).

[21] Carter K., Foltzer A., Hendrix J., Huffman B., Tomb A., “SAW: The software analysis workbench”, 2013 ACM SIGAda Annual Conference on High Integrity Language Technology (HILT), 2013, 15–18.

[22] Semenov A., Otpuschennikov I., Gribanova I., Zaikin O., Kochemazov S., “Translation of Algorithmic Descriptions of Discrete Functions to SAT with Applications to Cryptanalysis Problems”, Logical Methods in Computer Science, 16:1 (2020).

[23] Choo D., Soos M., Chai K.M.A., Meel K. S., “Bosphorus: Bridging ANF and CNF Solvers”, 2019 Design, Automation Test in Europe Conference Exhibition (DATE), 2019.

[24] “An ANF to CNF Converter using a Dense/Sparse Strategy”, https://doc.sagemath.org/html/en/reference/sat/sage/sat/converters/polybori.html.

[25] Soos M., “The CryptoMiniSat 5 set of solvers at SAT competition 2016”, SAT Competition 2016 — Solver and Benchmark Descriptions, 2016.

[26] Biere A., “CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT Entering the SAT Competition 2017”, Proceedings of SAT Competition 2017 — Solver and Benchmark Descriptions, B-2017-1 of Department of Computer Science Series of Publications B (2017), 14–15.

УДК 519.7 DOI 10.17223/2226308X/X/1

ГИБРИДНЫЙ ПОДХОД К ПОИСКУ БУЛЕВЫХ ФУНКЦИЙ С ВЫСОКОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ НА ОСНОВЕ ЭВРИСТИЧЕСКИХ МЕТОДОВ[1]

Н. Д. Атутова

В настоящее время одним из перспективных и развивающихся методов анализа шифров является алгебраический криптоанализ. Для успешного противостояния шифров такому виду атак в их структуре необходимо использовать функции с высокой алгебраической иммунностью. В работе предложен комбинированный подход к поиску булевых функций с высокой алгебраической иммунностью на основе эвристических методов, в частности, генетического алгоритма и алгоритма Hill Climbing. Для булевых функций от $n \leqslant 8$ переменных были проведены вычислительные эксперименты, продемонстрировавшие эффективность предлагаемого подхода.

Ключевые слова: *Генетический алгоритм, алгоритм Hill Climbing, алгебраическая иммунность, нелинейность, эвристики*

Развивающийся интерес к криптоанализу повышает потребность в улучшении стойкости шифров. Для защиты от статистических и аналитических методов криптоанализа для построения компонент шифра необходимо использовать булевы функции, обладающие хорошими криптографическими характеристиками. В 2003 году N.Courtois и W.Meier в [1] предложили новый метод криптоанализа шифров, названный алгебраическим криптоанализом. Высокая алгебраическая иммунность помогает противостоять такому криптоанализу.

Целью работы является построение булевых функций с максимальной алгебраической иммунностью – характеристикой, повышающей стойкость шифра к алгебраическим атакам.

Алгебраическая иммунность булевой функции f ($AI(f)$) — минимальное число d такое, что существует булева функция g степени d не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$, где функции f и g — функции от равного числа переменных. Известно, что для любой функции f от n переменных справедливо $AI(f) \leqslant \lceil \frac{n}{2} \rceil$.

Задача полного описания класса булевых функций, обладающих максимальной алгебраической иммунностью, а также получения новых конструкций таких функций, является открытой проблемой.

Существует три способа нахождения функций с высокой алгебраической иммунностью: полный перебор, алгебраическое конструирование и эвристики. При росте числа переменных множество булевых функций растёт дважды экспоненциально, что ухудшает эффективность полного перебора. Алгебраическое построение заведомо сужает множество решений. Перспективным является подход, использующий эвристические методы, в основе которых лежит структурированный перебор с параметрами для достижения желаемого результата. В работе предлагается рассмотреть применение эвристических методов, в частности, генетического алгоритма и алгоритма Hill Climbing. Специфика применения данных алгоритмов для поиска булевых функций с высокими

[1]Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации номер 075-15-2019-1613 и лаборатории криптографии JetBrains Research.

значениями нелинейности впервые была описана в [3]. Также, были получены теоретические результаты применения этих алгоритмов для функций от 16 переменных. Эффективность эвристических методов была продемонстрирована в ряде работ: в [4] исследована возможность применения алгоритма имитации отжига для поиска функций с высокой нелинейностью и низкой автокорреляцией; в [5] реализован генетический алгоритм для поиска бент-функций и сбалансированных функций; в работе [6] приведены последние результаты применения гибридного генетического алгоритма для построения сбалансированной булевой функции с оптимальными криптографическими характеристиками.

Для достижения максимального значения алгебраической иммунности реализованы два алгоритма.

Генетический алгоритм – это метод поиска, аналогичный естественному отбору в природе. Для получения более жизнеспособных потомков, к особям из начальной популяции итерационно применяется скрещивание и мутация. Последовательно происходит полное обновление популяции потомками, обладающими наибольшими значениями целевой функцией. В терминах нашей задачи:

– Особь – вектор значений булевой функции;

– Начальная популяция – случайное множество особей, без ограничений;

– Скрещивание – однородный кроссинговер. На вход поступают булевы функции f и g, представленные своими векторами значений $(f_0, f_1, ..., f_{2^{n-1}})$ и $(g_0, g_1, ..., g_{2^{n-1}})$, соответственно. На выходе булева функция h, вектор значений $(h_0, h_1, ..., h_{2^{n-1}})$ которой определяется следующим образом: если $f_i = g_i$, то $h_i = f_i$, если $f_i \neq g_i$, то h_i принимается равным значению f_i или g_i с одинаковой вероятностью, где $i = 0, 1, ..., 2^{n-1}$. Введём некоторые ограничения на скрещивание. Для этого нам потребуется расстояние Хэмминга.

Расстоянием Хэмминга ($dist(f, g)$) между булевыми функциями f и g от n переменных называется число координат, в которых различаются их векторы значений.

Если $dist(f, g) > 2^{n-1}$, то вместо вектора значений функции g рассматривается вектор, полученный инверсией всех битов вектора значений функции g. В рамках работы вероятность выполнения операции скрещивания принималась равной 0.8.

– Мутация - перестановка двух случайных различных битов вектора значений входной функции;

– Целевая функция – алгебраическая иммунность;

В работе представлены экспериментальные результаты применения генетического алгоритма для булевых функций при $n = 4, 6, 8$ (*Таблица 1*), где целевой функцией является алгебраическая иммунность. Алгоритм повышает её значения до максимальной теоретической оценки для всех особей популяции. Подсчитано количество полученных функций с максимальным значением целевой функции, получаемых на каждой итерации при каждом обновлении популяции.

Hill Climbing – иттерационный алгоритм, который начинается с произвольного решения задачи, а затем пытается найти лучшее решение путём пошагового изменения одного из элементов решения. В рамках рассматриваемой задачи также используется понятие нелинейности – характеристики, повышающей стойкость к линейному криптоанализу [2]. Используем следующие определения:

$$W_f(y) = \sum_x (-1)^{f(x) \oplus \langle x, y \rangle} \ , \ y \in \mathbb{F}_2^n$$

преобразование Уолша-Адамара булевой функции f, где $\langle x, y\rangle = x_1y_1 \oplus ... \oplus x_ny_n,\ y \in \mathbb{F}_2^n$

С помощью преобразования Уолша-Адамара можно определить следующую числовую характеристику:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{y\in\mathbb{F}_2^n}|W_f(y)|.$$

Величину N_f называют *нелинейностью* булевой функции. При чётном числе переменных n максимально возможное значение нелинейности равно $2^{n-1} - 2^{(n/2)-1}$. В случае нечетного n точное значение максимальной нелинейности неизвестно.

Алгоритм для повышения нелинейности описан в [3]. На вход поступает вектор значений булевой функции. Алгоритм итеративно пытается его улучшить, изменяя одну из координат. На каждой итерации коэффициенты Уолша-Адамара разбиваются на множества и последовательно происходит проверка условий на повышение значения целевой функции. В настоящей работе Hill Climbing применяется для поддержания высокой нелинейности после мутации потомков на каждой итерации генетического алгоритма.

Известно следующее соотношение, связывающее нелинейность и алгебраическую иммунность булевой функции [7]

$$N_f \geqslant 2\sum_{i=0}^{AI(f)-2}\binom{n-1}{i}.$$

Соотношение определяет верхнюю границу на алгебраическую иммунность. При этом, если нелинейность булевой функции достаточно высока, то верхняя граница на алгебраическую иммунность увеличивается. В рамках данной работы при поиске булевых функций с максимальной алгебраической иммунностью на каждой итерации поддерживалось высокое значение нелинейности для получаемых потомков с помощью алгоритма Hill Climbing. Проведённые эксперименты показали повышение эффективности генетического алгоритма при применении Hill Climbing для поддержания высокой нелинейности, к потомкам на каждой итерации генетического алгоритма. Результаты экспериментов для $n = 4, 6, 8$ представлены в Таблице 1.

n	P	T	min, среднее значение, max $AI(f)$ в исходной популяции	min, среднее значение, max $AI(f)$ после применения ГА	Количество функций с max $AI(f)$ при применении ГА	Количество функций с max $AI(f)$ при применении ГА + Hill Climbing
4	10	20	(0, 1.1, 2)	(2, 2, 2)	609	715
6	10	20	(0, 1.6, 3)	(3, 3, 3)	649	718
8	10	20	(1, 2.5, 4)	(4, 4, 4)	683	703
8	20	20	(1, 2.75, 4)	(4, 4, 4)	2864	2989

Таблица 1

Результаты применения ГА и Hill Climbing

Для параметров используются следующие обозначения: n – число переменных, P – размер популяции, T – число итераций.

Таким образом, в работе представлены результаты применения генетического алгоритма и Hill Climbing для поиска функций с высокими значениями алгебраической

иммунности для $n \leqslant 8$. Подсчитано количество найденных функций и проверена эффективность предложенного скомбинированного подхода из двух алгоритмов.

Полученные булевы функции могут быть использованы при поиске векторных булевых функций с высокой компонентной алгебраической иммунностью. Наличие высокой компонентной алгебраической иммунности S-блоков способствует противостоянию алгебраическому криптоанализу поточных и блочных шифров.

ЛИТЕРАТУРА

1. *Courtois N., Meier W.* Algebraic attacks on stream ciphers with linear feedback. // Anvances in cryptology, EUROCRYPT'03, 2003, Berlin / Heidelberg: Springer Verl. (Lecture Notes in Computer Science; № 2656), pages 345-359.
2. *Matsui M.* Linear Cryptanalysis Method for DES Cipher.// EUROCRYPT '93, Lecture Notes in Computer Science, № 765, 1994, pages 386-397.
3. *Millan W., Clark A., Dawson E.* An Effective Genetic Algorithm for Finding Highly Nonlinear Boolean Functions // International Conference on Information and Communications Security, 1997, pages 149-158.
4. *Clark J., Jacob J., Stepney S., Maitra S., Millan W.* Evolving Boolean functions satisfying multiple criteria // International Conference on Cryptology in India, 2002, pages 246-259.
5. *Picek S., Jakobovic D., Miller J., Batina L., Cupic M.* Cryptographic Boolean functions: one output, many design criteria // Applied Soft Computing № 40, March 2016, pages 635-653.
6. *Behera P., Gangopadhyay S.* An improved hybrid genetic algorithm to construct balanced Boolean function with optimal cryptographic properties // Evolutionary Intelligence, 2021.
7. *Лобанов М. С.* Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций, 2008, том 15, № 6, С. 34–47.

Atutova N. D. **HYBRID APPROACH TO THE SEARCH FOR BOOLEAN FUNCTIONS WITH HIGH ALGEBRAIC IMMUNITY BASED ON HEURISTICS.** Currently, one of the most promising and developing methods for analyzing ciphers is algebraic cryptanalysis. In order to provide resilience to such type of attack, it is necessary to use Boolean functions with high algebraic immunity in constructing components of block and stream ciphers. The paper proposes a combined approach to the search for Boolean functions with high algebraic immunity based on heuristic methods, in particular, the genetic algorithm and the Hill Climbing algorithm. Computational experiments were carried out for Boolean functions of $n \leqslant 8$ variables, which demonstrated the effectiveness of the proposed approach.

Keywords: *genetic algorithm, Hill Climbing algorithm, algebraic immunity, nonlinearity, heuristics*

АТУТОВА Наталья Дмитриевна — студентка механико-математического факультета НГУ, исследователь лаборатории криптографии JetBrains Research г. Новосибирск. E-mail: **atutova.n@yandex.ru**

УДК 004.75 DOI 10.17223/2226308X/X/1

МЕТОД ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ НА ОСНОВЕ ZK-SNARK[1]

Д. О. Кондырев

В работе представлен метод обеспечения конфиденциальности данных с возможностью проверки корректности на основе протокола доказательства с нулевым разглашением zk-SNARK. Разработанный метод позволяет создавать алгоритмы на основе zk-SNARK в смарт-контрактах Ethereum, используя высокоуровневые базовые криптографические схемы.

Ключевые слова: *распределенные системы, блокчейн, доказательство с нулевым разглашением, zk-SNARK, платформа Ethereum.*

Среди технических проблем, препятствующих внедрению технологии распределенных реестров, масштабируемость и конфиденциальность являются особенно существенными. В настоящий момент ведутся активные исследования, направленные на поиск решения проблемы конфиденциальности.

Особенно остро проблема конфиденциальности встает в открытых распределенных реестрах (таких как блокчейн-системы). В таких реестрах все данные сохраняются в открытом виде и доступны всем участникам, что не всегда приемлемо при создании промышленных программных систем. Кроме того, идентификация пользователей происходит по адресу их аккаунта. Таким образом, существует возможность отслеживать действия пользователя путем анализа транзакций, в которых участвует конкретный адрес, и сопоставления адреса аккаунта и пользователя.

В работе предложен метод обеспечения конфиденциальности данных с возможностью проверки корректности. В основе метода лежит криптографический протокол неинтерактивного доказательства знания с нулевым разглашением zk-SNARK [1]. Данная работа развивает результаты, полученные ранее в [2].

В качестве базовой системы для реализации метода была выбрана платформа Ethereum – блокчейн-система общего назначения, поддерживающая смарт-контракты.

В zk-SNARK процедура проверки доказательства состоит из операций на эллиптических кривых. В частности, верификатор требует скалярного умножения и сложения на группе эллиптических кривых, а также вычислительно более сложной операции – билинейного спаривания. Ethereum предоставляет реализацию этих операций в виде предварительно скомпилированных контрактов. С их помощью есть возможность реализовать схемы на основе доказательства с нулевым разглашением в коде смарт-контрактов. Используя только встроенные инструменты, приходится оперировать низкоуровневыми примитивами, что не позволяет реализовать сложные алгоритмы.

Для возможности создавать произвольные криптографические схемы, в основе которых лежит zk-SNARK, были разработаны сторонние инструменты, такие как ZoKrates [3]. Такие решения позволяют реализовать схему в виде кода на довольно высокоуровневом языке, который затем компилируется в код смарт-контрактов. Однако, такой подход имеет ряд ограничений, которые не позволяют применять его для схем произвольного размера и сложности.

[1]Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации номер 075-15-2019-1613 и лаборатории криптографии JetBrains Research.

Для решения проблем существующих подходов предлагается добавить поддержку более высокоуровневых криптографических примитивов системы ограничений ранга 1 (R1CS - rank-1 constraint systems) непосредственно в код Ethereum-клиента. Таким образом, мы добавляем механизм задания произвольных схем непосредственно в коде смарт-контрактов. При таком подходе нет необходимости напрямую использовать операции над эллиптическими кривыми, вместо этого новые алгоритмы строятся как комбинация добавленных примитивов. Кроме того, такой подход оказывается более вычислительно эффективным за счет реализации непосредственно в Ethereum-клиенте.

В качестве базовых примитивов были добавлены схемы, реализующие логические операции (AND, OR, NOT) и операции сравнения. Их реализация выполнена на основе libsnark – криптографической библиотеки с открытым исходным кодом, которая обеспечивает эффективные реализации конструкций zk-SNARK [4].

В Ethereum-клиент добавлены соответствующие операции для возможности вызова этих методов как из кода контрактов, так и вне блокчейна. Для этого была модифицирована виртуальная машина Ethereum, куда были добавлены функции создания схемы, генерации доказательства и его верификации.

Схема, описанная разработчиком в коде смарт-контракта, транслируется в набор добавленных примитивов. Далее на их основе формируется система ограничений ранга 1 (R1CS), с которой работают алгоритмы генерации и верификации доказательства zk-SNARK.

Для каждой новой схемы необходима генерация новой пары ключей доказательства и верификации. Их генерация выполняется вне блокчейна поскольку в алгоритме генерации используется параметр безопасности, зная который можно создавать некорректные доказательства, которые будут приняты верификатором как корректные.

Таким образом, была создана система, которая позволяет разработчикам реализовывать произвольные алгоритмы на основе добавленных базовых схем непосредственно в коде смарт-контрактов. Разработанный метод позволяет сократить размер кода смарт-контрактов и кроме того, оказывается более вычислительно эффективным.

ЛИТЕРАТУРА

1. *Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M.* SNARKs for C: Verifying program executions succinctly and in zero knowledge // CRYPTO 2013, Proceedings of the 33rd Annual Cryptology Conference, Part II, volume 8043 of LNCS. Santa Barbara, CA, USA, 2013. P. 90 – 108.
2. *Кондырев Д. О.* Разработка метода сокрытия приватных данных для системы тендеров на основе технологии блокчейн // Прикладная дискретная математика, 2020, № 48, С. 63 – 81.
3. *Eberhardt J., Tai S.* ZoKrates – Scalable Privacy-Preserving Off-Chain Computations. // International Conference on Blockchain. IEEE – Halifax, Canada, 2018.
4. `https://github.com/scipr-lab/libsnark` — libsnark: a C++ library for zkSNARK proofs.

Kondyrev D. O. **ZK-SNARK-BASED DATA PRIVACY METHOD.** The paper presents a method for ensuring data confidentiality with the possibility of validation based on the zk-SNARK zero-knowledge proof protocol. This method allows the creation of zk-SNARK-based algorithms in Ethereum smart contracts code using high-level basic cryptographic schemes that implement logical operations (AND, OR, NOT) and comparison operations. Cryptographic schemes are implemented on the basis of the libsnark library as a rank-1 constraint systems (R1CS). The Ethereum virtual machine has been modified to include functions for schema creation, proof generation and verification.

Keywords: *distributed systems, blockchain, zero-knowledge proof, zk-SNARK, Ethereum platform.*

КОНДЫРЕВ Дмитрий Олегович — аспирант факультета информационных технологий Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, младший научный сотрудник Института математики им. С.Л.Соболева, г. Новосибирск. E-mail: **dkondyrev@gmail.com**

УДК 519.7 DOI 10.17223/2226308X/X/1

РАЗРАБОТКА И АНАЛИЗ ОРАКУЛА ДЛЯ ГИБРИДНОЙ АТАКИ НА КРИПТОГРАФИЧЕСКУЮ СИСТЕМУ NTRU С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА КВАНТОВОГО ПОИСКА[1]

А. О. Бахарев

В силу развития квантовых вычислений возникает необходимость в разработке и анализе криптосистем, устойчивых к атакам с использованием квантового компьютера — алгоритмов постквантовой криптографии. Стойкость многих известных постквантовых криптосистем, основанных на теории решёток, базируется на сложности решения проблемы нахождения кратчайшего вектора в решетке (SVP). Разработана и проанализирована модель квантового оракула, необходимого для реализации гибридного квантово-классического алгоритма решения задачи SVP. На примере постквантовой криптосистемы с открытым ключом NTRU, являющейся финалистом третьего раунда конкурса NIST, получены верхние оценки на число кубит и глубину схемы, требуемые для реализации данного оракула, в зависимости от параметров криптосистемы.

Ключевые слова: *криптосистема NTRU, квантовый поиск, криптография с открытым ключом, постквантовая криптография.*

Квантовые вычисления — это быстроразвивающаяся область компьютерных исследований, которая ставит под угрозу криптографическую стойкость стандартов асимметричного шифрования, используемых в настоящее время. В 2016 г. Национальный Институт Стандартов и Технологий США (NIST) объявил конкурс «Post-Quantum Cryptography Competition», по завершении которого будет принят новый — квантово-устойчивый — стандарт асимметричного шифрования. Претендентами являются подходы на основе решёток, кодов, хэш-функций, изогений и многочленов от многих переменных.

Рассмотрим подход на основе решёток.

Определение 1. Пусть $u_1, \ldots, u_n \in \mathbb{R}^m$ — линейно независимые векторы и $n \leqslant m$. *Решёткой* называется множество

$$\mathbb{Z}u_1 \oplus \ldots \oplus \mathbb{Z}u_n = \Big\{ \sum_{i=1}^{n} b_i u_i : b_i \in \mathbb{Z} \Big\}.$$

Векторы $u_1, \ldots, u_n$ называются *базисом решётки.*

Одной из задач в теории решёток является *задача нахождения кратчайшего вектора* (SVP), которая заключается в нахождении вектора, имеющего наименьшую длину, в решётке, заданной своим базисом. В общем случае SVP является NP-трудной задачей. Стойкость систем, основанных на решётках, зависит от эффективности решения SVP, так как большинство известных атак сводятся к решению этой проблемы. Перспективными являются разработка и анализ квантовых алгоритмов, которые позволяют ускорить решение данной задачи.

В [1] представлен гибридный квантово-классический подход к поиску кратчайшего вектора решётки на основе GaussSieve [2] — одного из самых эффективных классических алгоритмов.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.

Алгоритм 1. Алгоритм GaussSieve (Micciancio, Voulgaris, 2010)

Вход: B - базис решётки
Выход: v - кратчайший вектор решётки
1: Инициализировать пустой неупорядоченный список L и пустой стек S
2: **Повторять**
3: Получить вектор v из стека (или сгенерировать новый)
4: **Пока** $w \leftarrow$ ПОИСК$\{w \in L : \|v \pm w\| \leqslant \|v\|\}$
5: Уменьшить v с помощью w $(v \leftarrow v \pm w)$
6: **Пока** $w \leftarrow$ ПОИСК$\{w \in L : \|w \pm v\| \leqslant \|w\|\}$
7: Удалить w из листа L
8: Уменьшить w с помощью v $(w \leftarrow w \pm v)$
9: Добавить w в стек S
10: **Если** v изменился **то**
11: Добавить v в стек S
12: **иначе**
13: Добавить v в лист L
14: **Пока** v не станет кратчайшим вектором
15: **Вернуть** вектор v

На вход алгоритма поступает базис решётки, на основе которого будут строиться новые векторы при условии пустого стека S. Функция «ПОИСК» перебирает векторы w в списке и проверяет их на одно из *(1) условий поиска:* $\|v \pm w\| \leqslant \|v\|$ *или* $\|w \pm v\| \leqslant \|w\|$, если такой вектор существует, то функция возвращает его, иначе функция прерывает первый цикл, в котором находится. Авторами статьи [2] предложено эвристическое условие остановки, которое основывается на количестве коллизий. Таким образом, алгоритм работает до тех пор, пока мы не получим такое число коллизий, что будем уверены, что нашли кратчайший вектор.

В рамках предложенного в [1] подхода ускорение достигается за счёт использования в функции «ПОИСК» квантового алгоритма поиска в неупорядоченном списке (алгоритма Гровера [3]). Задача, решаемая этим алгоритмом, называется *задачей поиска*. Предполагается, что есть неупорядоченный список из K элементов, в котором как минимум один элемент удовлетворяет некоторому условию. Требуется найти по крайней мере один такой элемент. Другими словами, определена булева функция f, которая по номеру элемента (его двоичному представлению) определяет, является ли элемент подходящим (в этом случае $f = 1$) или нет ($f = 0$). В такой постановке задача поиска сводится к нахождению решения(-ий) уравнения $f(x) = 1$.

В классическом варианте при условии, что решение одно, требуется $\sim K/2$ обращений к функции f для нахождения решения. Квантовый алгоритм поиск элемента в неупорядоченном списке решает данную задачу за $\sim \sqrt{K}$ обращений к *оракулу* — квантовому аналогу функции f.

Квантовый компьютер, в отличие от обычного, оперирует *кубитами* [4]. Их состояние можно представить как единичный вектор из $\mathbb{C}^2$. Произвольный вектор этого пространства может быть представлен в виде

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где $\alpha, \beta \in \mathbb{C}$ называются *амплитудами*; $|\alpha|^2$ и $|\beta|^2$ — вероятности обнаружения кубита после измерения в состояниях $|0\rangle$ и $|1\rangle$ соответственно. Говорят, что кубит находится в *суперпозиции* состояний $|0\rangle$ и $|1\rangle$.

В соответствии с постулатами квантовой механики, состояние системы из n кубит описывается *вектором состояний* из $\mathbb{C}^{2^n}$. Эволюция состояния замкнутой квантовой системы во времени описывается унитарным преобразованием.

Известно, что любая булева функция может быть реализована на квантовом компьютере, а квантовым алгоритмом, решающим задачу поиска, является *алгоритм Гровера* (рис. 1):

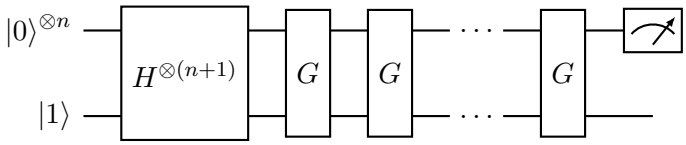


Рис. 1. Алгоритм Гровера [3]

Здесь H — вентиль Адамара, G — итерации алгоритма Гровера (рис. 2).

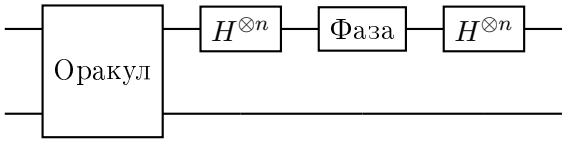


Рис. 2. Итерация Гровера

Преобразования $H^{\otimes n}$ и Фаза являются известными вентилями, в отличие от оракула, который строится под каждую задачу отдельно. В настоящей работе выполнено построение и описание оракула для квантового подхода к решению задачи поиска подходящего вектора из списка в алгоритме GaussSieve.

Оракул, представленный на рис. 3, состоит из двоичного представления номера вектора в списке, K векторов размерности d, каждая координата которых кодируется строкой длины m, переключателя, проверки на условие поиска и ответа. Его работа происходит следующим образом:

1) получение номера вектора на вход и передача его в переключатель;
2) выбор по номеру вектора из списка и копирование его;
3) проверка скопированного вектора на условие поиска(1);
4) вывод ответа: 1 — если вектор удовлетворяет условию, 0 — если нет.

Переключатель представляет собой векторную булеву функцию, которая номеру вектора сопоставляет строку: $i \to (0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на i-ом месте. Тогда, применяя вентиль CCNOT, можно удобно копировать нужный вектор номера i из списка. Для лучшего понимания того, как копируется нужный вектор, рассмотрим следующий пример (рис. 4) при $i = 2$ и $K = 2$:

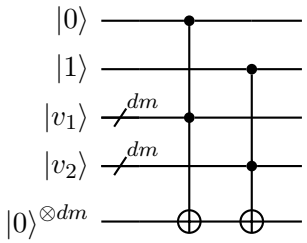


Рис. 4. Пример копирования векторов из списка

Здесь первые два кубита представляют собой строку, полученную из переключателя, v_1 и v_2 – векторы размерности d, каждая координата которых кодируется строкой длины m, а нижний регистр оставлен под место для копирования нужного вектора. Тогда в итоге работы примера вектор v_2 будет скопирован в нижний регистр.

Проверка на условие поиска(1) содержит следующие операции: сложение, вычитание, возведение в квадрат и сравнение целых чисел. Предлагается использовать дополнительный код числа для операции вычитания, таким образом, сложение и вычитание реализуются одной операцией, а сравнение чисел определяется знаком результата вычитания. Сложность реализации операций на квантовом компьютере оцениваетя количеством кубит и глубиной схемы. В табл. 1 представлены достаточные оценки для операций, реализующих переключатель и проверку на условие поиска(1). При каждом изменении вектора v или списка L в ходе работы алгоритма GaussSieve оракул строится заново.

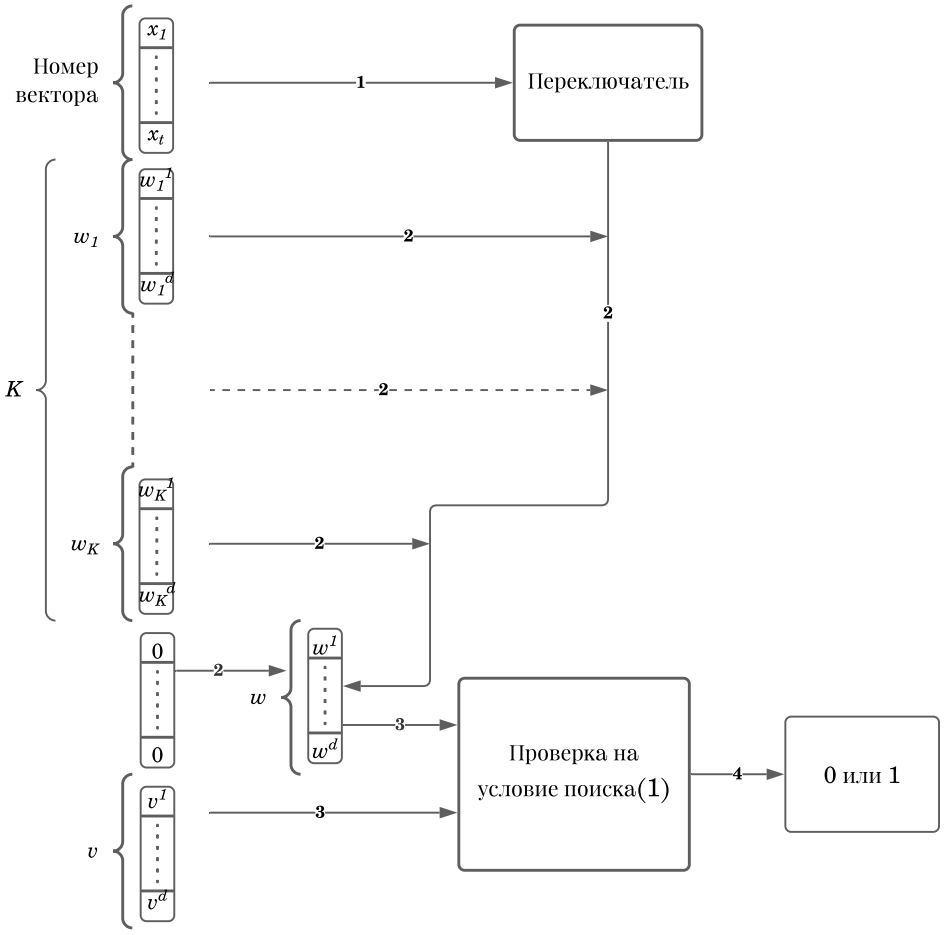


Рис. 3. Предлагаемая схема квантового оракула

Таблица 1

Количество кубит и глубина схемы, достаточные для реализации требуемых операций

Операция	Количество кубит	Глубина схемы
Сложение, вычитание целых m-битных чисел	$4m-1$	$5m-2$
Возведение целого m-битного числа в квадрат	$6m^2-5m+2$	$11m^2-15m+4$
Переключатель, где номер вектора представляется целым m-битным числом	2^m+m	3^m
Перевод целого m-битного числа в дополнительный код	$4m$	$4m+1$

Утверждение 1. Пусть имеется список длины K, состоящий из целочисленных векторов размерности d, каждая координата которых кодируется битовой строкой длины m. Тогда для реализации квантового оракула, представленного на рис. 3, потребуется не более $\lceil \log_2 K \rceil + Kdm + K + 18dm^2 - 33dm + 6d^2 + 25d + 2m + 4$ кубит. Глубина схемы не превосходит $3^{\lceil \log_2 K \rceil} + Kdm + 33dm^2 - 67dm + 15d^2 + 35d - 2m + 19$.

Для анализа была выбрана криптосистема NTRU, так как она прошла в третий раунд конкурса NIST [5] и является одним из четырёх претендентов на новый постквантовый стандарт асимметрического шифрования. NTRU зависит от трёх целочисленных параметров (N, p, q), где $(p, q) = 1$. Работа осуществляется в кольце R полиномов степени не выше $N-1$ с целочисленными коэффициентами, то есть $R = \mathbb{Z}[x]/(x^N - 1)$. Элемент $F = \sum\limits_{i=0}^{N-1} F_i x^i \in R$ можно представить как вектор

$$F = [F_0, \ldots, F_{N-1}].$$

Операция умножения «$*$» в R определяется как результат циклической свёртки:

$$F * G = H,$$

$$H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i} = \sum_{i+j=k(\mathrm{mod} N)} F_i G_j.$$

Если выполняется умножение полиномов по модулю числа, то коэффициенты приводятся по этому модулю.

Секретный ключ: f, g — полиномы из R с координатами из множества $\{-1, 0, 1\}$.

Открытый ключ: N, p, q, $h = f_q * g \bmod q$, где $f_q * f = 1 \pmod q$.

Зашифрование: Пусть m — сообщение, представленное в виде полинома из R с коэффициентами из интервала $(-p/2, p/2]$. Тогда зашифрованное сообщение c вычисляется следующим образом: $c = p\varphi * h + m \bmod q$, где φ — полином из R с некоторыми ограничениями на координаты из множества $\{-1, 0, 1\}$.

Расшифрование: Определим полином $a = f * c \bmod q$. Тогда исходное сообщение восстанавливается следующим образом: $m = f_q * a \bmod p$.

Одна из самых эффективных атак [6] на NTRU сводится к решению SVP в решётке, базис которой образован строками матрицы M, построенной на основе открытого

ключа:

$$M = \begin{pmatrix} 1 & 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & 1 & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & q \end{pmatrix}$$

С большой вероятностью кратчайший вектор решётки, порождённой этим базисом, имеет вид $r = (f, g)$, а параметры оракула можно определить (оценить) следующим образом: $K \leqslant 2N$, $d = 2N$, $m = \lceil \log_2 q \rceil + 1$.

На основе оценок из табл. 1 посчитана взаимосвязь между параметрами NTRU, количеством кубит и глубиной схемы, достаточных для реализации гибридной квантово-классической атаки (табл. 2).

Таблица 2

Верхние оценки числа кубит и глубины схемы

Параметры NTRU	Количество кубит	Глубина схемы
$N = 1$, $q = 2$	105	332
$N = 2$, $q = 2$	266	428
$N = 8$, $q = 4$	3742	3498
$N = 256$, $q = 128$	4138013	2945510

Получены верхние оценки на сложность реализации квантового оракула из алгоритма Гровера для реализации гибридного квантово-классического алгоритма на основе GaussSieve, который может быть использован для атак на криптосистемы, стойкость которых зависит от решения задачи SVP. Проанализирована сложность реализации квантового оракула для атаки на постквантовую криптосистему NTRU. На сегодняшний день количество кубит, с которыми оперирует квантовый компьютер, не превосходит 76 [7]. Тогда из полученных оценок следует, что на сегодняшний день предложенная модель квантового оракула не может быть реализована на квантовом компьютере даже для самых малых параметров NTRU, так как ещё не существует квантового компьютера, оперирующего достаточным количеством кубит. В рамках дальнейшей работы предлагается оптимизировать квантовую схему оракула, получить необходимые оценки для реализации оракула данного класса, а также проанализировать другие известные классические атаки постквантовых криптосистем с целью изучения возможности их ускорения с помощью квантовых вычислений.

ЛИТЕРАТУРА

1. *Laarhoven T., Mosca M., and van de Pol J.* Finding shortest lattice vectors faster using quantum search // Des. Codes Cryptogr. 2015. V. 77. No. 2–3. P. 375–400.
2. *Micciancio D. and Voulgaris P.* Faster exponential time algorithms for the Shortest Vector roblem // 21st Ann. ACM Symp. Discrete Algorithms (SODA). 2010. P. 1468–1480.
3. *Grover L. K.* A fast quantum mechanical algorithm for database search // 28th Ann. ACM Symp. Theory Comput. (STOC). 1996. P. 212–219.
4. *Nielsen M. A. and Chuang I. L.* Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010.

5. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.
6. *Chen C., Danba O., Hoffstein J., et al.* NTRU Algorithm Specifications and Supporting Documentation. https://ntru.org/, 2019.
7. *Zhong H.-S., Wang H., Deng Y.-H., et al.* Quantum computational advantage using photons. Science, Vol. 370, Issue 6523. 2020. P. 1460-1463.

Bakharev A. O. **DEVELOPMENT AND ANALYSIS OF ORACLE FOR THE HIBRID ATTACK ON A CRYPTOGRAPHIC SYSTEM NTRU USING A QUANTUM SEARCH ALGORITHM.** Due to the development of quantum computing, there is a need for the development and analysis of cryptosystems resistant to attacks using a quantum computer (post-quantum cryptography algorithms). The security of many well-known post-quantum cryptosystems based on lattice theory depends on the complexity of solving the shortest vector problem (SVP). In the paper, a model of the quantum oracle which is required for the implementation of the hybrid quantum-classical algorithm for solving SVP is proposed and analyzed. For the public key post-quantum cryptosystem NTRU which is the finalist of the third round of the NIST competition, upper bounds for the number of qubits and the depth of the scheme are obtained. The bounds are based on the proposed model of the quantum oracle.
Keywords: *cryptosystem NTRU, quantum search, public-key cryptography, post-quantum cryptography.*

БАХАРЕВ Александр Олегович — студент Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: **sana.bakharev@gmail.com**

УДК 519.7

АФФИННЫЕ ПРОИЗВОДНЫЕ БЕНТ-ФУНКЦИЙ[1]

А. С. Шапоренко

Бент-функция может быть определена как булева функция $f(x)$ от n переменных (n четно) такая, что для любого ненулевого вектора y ее производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована – принимает значения 0 и 1 одинаково часто. Справедливо ли, что любая сбалансированная функция – производная некоторой бент-функции? В данной работе эта задача рассмотрена для частного случая сбалансированых функций $\ell_{a,b}(x) = \langle a, x\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ ненулевой и $b \in \mathbb{Z}_2$, которые называются аффинными. Было доказано, что любая неконстантная аффинная функция от $n \geqslant 4$ (четно) переменных является производной для $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ бент-функций, где $\mathcal{B}_{n-2}$ – число бент-функций от $n-2$ переменных. Получены итерационные нижние границы для числа бент-функций.

Ключевые слова: *бент-функции, булевы функции, производные бент-функций, нижние границы для числа бент-функций*

Пусть $\langle x, y\rangle$ обозначает скалярное произведение двоичных векторов по модулю 2 (обозначим $\oplus$).

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Булева функция от четного числа переменных называется бент-функцией, если она максимально нелинейна [1]. Обозначим $\mathcal{B}_n$ множество бент-функций.

Шифры, в которых используются бент-функции, более устойчивы к *линейному криптоанализу* [2], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции использовались в структуре блочного шифра *CAST* как координатные функции S–блоков [3], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре *Grain* [4]. Также бент-функции связаны с некоторыми объектами теории кодирования, например, с *кодами Рида-Маллера* [5].

Другое определение бент-функции – булева функция $f(x)$ от n переменных (n четно) такая, что для любого ненулевого вектора y ее производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована – принимает значения 0 и 1 одинаково часто [5]. Справедливо ли, что любая сбалансированная функция – производная некоторой бент-функции? В [6] было показано, что любая сбалансированная функция g от $n \leqslant 6$ переменных степени не выше $n/2 - 1$, такая, что $g(x) = g(x \oplus y)$ для всех x при некотором y, является производной некоторой бент-функции от n переменных. В данной работе эта задача рассмотрена для частного случая сбалансированых функций $\ell_{a,b}(x) = \langle a, x\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ ненулевой и $b \in \mathbb{Z}_2$, которые называются аффинными.

Теорема 1. Любая неконстантная аффинная функция $\ell_{a,b}(x)$ от $n \geqslant 4$ (четно) переменных является производной для $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ бент-функций.

Лемма 1. Для любой бент-функция и $y \neq y'$ справедливо, что $D_y g(x) \neq D_{y'} g(x)$.

Лемма 2. Пусть $D_y g(x) = l_{a,b}(x)$ для бент-фукции $g(x)$. Тогда при любом y' $D_{y'} g(x) \neq l_{a,b}(x) \oplus 1$.

Теорема 1 вместе с Леммами 1 и 2 дают следующие итерационные нижние границы для количества бент-функций от $n+2$ перемнных.

[1]Работа выполнена в рамках государственного задания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.

Теорема 2. Для любого четного $n \geqslant 4$ верно

$$|\mathcal{B}_{n+2}| \geqslant (2^{n+2} - 2)|\mathcal{B}_n|^2.$$

Данная итерационная нижняя граница хуже представленной в [7], но она вероятно может быть улучшена, если рассматривать больше одной аффинной функции или учитывать функции, которые не имеют аффинных производных. Однако задача выделения бент-функций, которые производной имеют $\ell_{a,b}$ и не имеют $\ell_{c,d}$, является непростой. Бент-функции, которые не имеют аффинных производных, рассматривались, например, в [8].

ЛИТЕРАТУРА

1. *Rothaus O. S.* On 'bent' functions //J. Combinat. Theory A, vol. 20, no. 3, pp. 300–305, 1976.
2. *Matsui M.* Linear Cryptanalysis Method for DES cipher //Advances in Cryptology – Eurocrypt 1993, Springer-Verlog, Berlin, pp. 386–397.
3. *Adams C.* Constructing symmetric ciphers using the CAST design procedure //Proc. Design, Codes, and Cryptography, vol. 12, no. 3, pp. 283–316, 1997.
4. *Hell M., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 //IEEE International Symposium on Information Theory, pp. 1614–1618, 2006.
5. *Tokareva N.* Bent functions: results and applications to cryptography //Acad. Press. Elsevier, 2015.
6. *Токарева Н. Н.* О множестве производных булевой бент-функции //ПДМ. Приложение, vol. 9, p. 35, 2016.
7. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses //Adv. Math. Commun, vol. 5, no. 4, pp. 609–621, 2011.
8. *Canteaut A, Charpin P.* Decomposing bent functions //IEEE Trans. Inform. Theory, vol. 49, no. 8, pp. 2004–2019, 2003.

Shaporenko A. S. **AFFINE DERIVATIVES OF BENT FUNCTIONS.** Bent function can be defined as a Boolean function $f(x)$ in n variables (n is even) such that for any nonzero vector y its derivative $D_y f(x) = f(x) \oplus f(x \oplus y)$ is balanced–that is, it takes values 0 and 1 equally often. Whether every balanced function is a derivative of some bent function or not is an open problem. In this paper, special case of this problem was studied. It was proven that every non-constant affine function in $n \geqslant 4$ (even) is a derivative of $(2^{n-1} - 1)|\mathcal{B}_{n-2}|^2$ bent functions, where $\mathcal{B}_{n-2}$ is the number of bent functions in $n-2$ variables. New iterative lower bounds for the number of bent functions is presented.

Keywords: *boolean functions, bent functions, derivatives of bent function, lower bounds for number of bent functions.*

Шапоренко Александр Сергеевич — м.н.с Института математики им. С. Л.Соболева СО РАН, аспирант Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, Новосибирск. E-mail: **a.shaporenko@g.nsu.ru**

УДК 519.7 DOI 10.17223/2226308X/X/1

S-БЛОКИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ ОТ МАЛОГО ЧИСЛА ПЕРЕМЕННЫХ[1]

Д. А. Зюбина, Н. Н. Токарева

Пусть π — перестановка n элементов, f — булева функция от n переменных. Рассмотрим векторную булеву функцию $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ вида $F_\pi(x) = (f(x), f(\pi(x)), \cdots, f(\pi^{n-1}(x)))$. Изучается компонентная алгебраическая иммунность функции F_π в зависимости от булевой функции f и перестановки π при $n = 3, 4, 5$. Получены полные множества булевых и частичные векторных булевых функций с максимальной алгебраической иммунностью от малого числа переменных.

Ключевые слова: *булева функция, векторная булева функция, алгебраическая иммунность, компонентная алгебраическая иммунность.*

S-блоки играют решающую роль в обеспечении стойкости блочных шифров к различным типам атак. Основная причина этого в том, что в классических и современных блочных шифрах нелинейный слой представлен именно данными блоками. S-блок является отображением множества двоичных векторов длины n в множество двоичных векторов длины m. В 2003 г. в [1] был представлен новый вид криптоанализа — алгебраический, основанный на понижении степени системы уравнений, описывающей шифр. Для противостояния такому роду атак необходимо, чтобы S-блок имел максимально возможное значение компонентной алгебраической иммунности.

В данной работе будем рассматривать S-блоки определённого вида, а именно $F_\pi(x) = (f(x), f(\pi(x)), \cdots, f(\pi^{n-1}(x)))$, где $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$; f — булева функция от n переменных; π — циклический сдвиг влево на одну позицию n элементов. Эта конструкция предложена А. Удовенко в решении олимпиадной задачи на NSUCRYPTO-2016 [2]. Он показал, что при таком построении векторной функции можно получить функцию с максимальной алгебраической иммунностью от 3, 4, ..., 10 переменных. В настоящее время остаётся открытым вопрос о существовании векторной булевой функции с максимальной компонентной иммунностью $\lceil n/2 \rceil$ от произвольного числа переменных n.

Алгебраической иммунностью $\mathrm{AI}(f)$ булевой функции f называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$ [3]. Известно, что для произвольной булевой функции f от n переменных выполнено $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции F называется минимальная алгебраическая иммунность её компонентных функций, т. е. функций $f_b(x) = \langle b, F(x) \rangle$, где $b \in \mathbb{F}_2^n$, $b \neq 0$ и $\langle a, b \rangle = a_1 b_1 \oplus \ldots \oplus a_n b_n$ — скалярное произведение векторов по модулю 2.

В данной работе для построения S-блока с максимальной компонентной алгебраической иммунностью реализован метод нахождения линейного подпространства размерности n в множестве, содержащем векторы значений нулевой функции и всех булевых функций от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. В первую очередь путём полного перебора формируется множество булевых функций

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018) при поддержке лаборатории криптографии JetBrains Research.

с максимальной алгебраической иммунностью. К этому множеству добавляется нулевой вектор. Далее из этого множества выбирается функция и на её основе строятся оставшиеся $n-1$ функций (используя перестановку π). Все эти функции также лежат в этом множестве. Затем проверяется, порождают ли все n функций линейное подпространство размерности n. Если да, то данное подпространство позволяет построить S-блок с максимальной компонентной иммунностью, выбрав в качестве координатных функций S-блока базис подпространства. Для однозначности пусть функция строится в виде $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$.

Для $n = 3$ путём полного перебора получено, что существует 56 булевых функций с максимальной алгебраической иммунностью 2. Из них на основе 12 функций (им отвечают 4 подпространства) можно построить векторную булеву функцию с максимальным значением иммунности. Все эти функции можно представить в виде АНФ общего вида.

Утверждение 1. Булевы функции f от трёх переменных с максимальной алгебраической иммунностью 2, такие, что векторные функции вида $F_\pi(x) = (f(x), f(\pi(x)), f(\pi^2(x)))$, где π — циклический сдвиг, также имеют максимальную компонентную алгебраическую иммунность 2, можно описать следующей конструкцией:

$$f(x_1, x_2, x_3) = x_i + x_j + x_i x_k + a, \quad \text{где} \quad \{i, j, k\} = \{1, 2, 3\}, \ a \in \mathbb{F}_2.$$

Для $n = 4$ путём полного перебора получено, что существует 54 952 булевых функций с максимальной алгебраической иммунностью 2. При рассмотрении всевозможных перестановок π (а не только циклического сдвига влево, как это происходило ранее) оказалось, что только при 6 перестановках существуют векторные булевы функции, которые сохраняют максимальную иммунность. Эти перестановки можно представить в векторном виде: (2, 3, 4, 1), (2, 4, 1, 3), (3, 1, 4, 2), (3, 4, 2, 1), (4, 1, 2, 3), (4, 3, 1, 2) или циклическом (1234), (1243), (1342), (1324), (1432), (1423). Для каждой перестановки существует 6144 булевых функций (или 1536 линейных подпространств), построенные на основе которых векторные булевы функции также имеют максимально возможную компонентную алгебраическую иммунность.

Утверждение 2. Пусть f — булева функция от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Если векторная булева функция $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$ имеет максимальную компонентную алгебраическую иммунность, то π является полноцикловой перестановкой.

Для $n = 5$ путём полного перебора получено, что всего существует 197 765 122 булевых функций с максимальной алгебраической иммунностью 3. Существует как минимум четыре булевых функции (им отвечает одно подпространство), на основе которых строится векторная булева функция с максимальным значением иммунности.

С учётом экспериментальных результатов сформулированы следующие гипотезы:

Гипотеза 1. Для любого $n \geqslant 2$ в множестве, состоящем из булевых функций от n переменных с максимальной алгебраической иммунностью и нулевой функции, существует линейное подпространство размерности n.

Данная гипотеза доказана для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко. Для $n = 7, 9$ пока не найдено таких подпространств.

Гипотеза 2. Пусть f — булева функция от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Тогда в её АНФ присутствует по меньшей мере по одному моному каждой степени i, где $i = 1, 2, \ldots, \lceil n/2 \rceil$.

Данная гипотеза проверена для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко.

Таким образом, возможно построение S-блока от малого числа переменных, который устойчив к алгебраическим атакам. В дальнейшем планируется анализ булевых и векторных булевых функций от большего числа переменных.

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.

Zyubina D. A., Tokareva N. N. **S-BLOCKS WITH MAXIMUM COMPONENT ALGEBRAIC IMMUNITY ON A SMALL NUMBER OF VARIABLES.** Let π be a permutation on n elements, f be a Boolean function in n variables. Define a vectorial Boolean function $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as $F_\pi(x) = (f(x), f(\pi(x)), \cdots, f(\pi^{n-1}(x)))$. In this paper, we study the component algebraic immunity of the vector Boolean function F_π as a function of the Boolean function f and the permutation π for $n = 3, 4, 5$. We obtain complete sets of Boolean and, partly, vector Boolean functions with maximum algebraic immunity on 3, 4 and 5 variables. The statement is presented that a vector Boolean function F_π can have maximum algebraic immunity only if the permutation π is full cycle.
Keywords: *Boolean function, vector Boolean function, algebraic immunity, component algebraic immunity.*

ЗЮБИНА Дарья Александровна — студентка факультета информационных технологий НГУ, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: **zyubinadarya@gmail.com**

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева СО РАН, доцент НГУ, заведующая лабораторией криптографии JetBrains Research, г. Новосибирск. E-mail: **tokareva@math.nsc.ru**

УДК 519.7 DOI 10.17223/2226308X/X/1

АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ ЛЕГКОВЕСНЫХ ШИФРОВ SIMON И SPECK[1]

А. В. Куценко, Н. Д. Атутова, Д. А. Зюбина, Е. А. Маро, С. Д. Филиппов

Представлены алгебраические атаки на шифры Simon и Speck — два семейства легковесных блочных шифров, имеющих LRX- и ARX-структуры соответственно. Они были представлены Агентством национальной безопасности США в 2013 г., а затем стандартизированы ISO как часть стандарта радиоинтерфейса RFID. Шифры алгебраически кодируются и получаемые системы булевых уравнений решаются с помощью различных SAT-решателей, а также методов, основанных на линеаризации. Впервые к этим шифрам применяются подходы, использующие разреженность систем булевых уравнений. Оценены параметры линеаризации в системах уравнений для обоих шифров. Приведено сравнение эффективности используемых методов.

Ключевые слова: *алгебраический криптоанализ, блочный шифр, легковесный шифр,* Simon, Speck.

Легковесная криптография — направление исследований, представляющее интерес в настоящее время. Это связано с тем, что влияние и использование RFID-меток, ПЛИС, смарт-карт, мобильных телефонов, сенсорных сетей и других криптографических алгоритмов для устройств с ограничениями на используемые ресурсы постоянно растёт и приобретает всё большую важность. Легковесные криптографические примитивы предназначены для обеспечения эффективности и безопасности при ограниченном объёме ресурсов. В этом случае возникает проблема поиска компромисса между безопасностью и эффективностью. В 2013 г. Агентство национальной безопасности США представило семейства Simon и Speck легковесных блочных шифров. Шифр Simon был оптимизирован для производительности на аппаратных устройствах, а Speck — для производительности в программном обеспечении. Но было подчеркнуто, что оба семейства работают исключительно хорошо как в аппаратном, так и в программном обеспечении, обеспечивая гибкость платформы, требуемую будущими приложениями. По состоянию на октябрь 2018 г. шифры Simon и Speck были стандартизированы Международной организацией по стандартизации (ISO) в рамках стандарта радиоинтерфейса RFID (радиочастотной идентификации). Эти шифры являются представителями LRX- и ARX-структур блочных шифров, основой которых является явное использование нелинейных алгебраических операций вместо S-блоков. Это обуславливает интерес к алгебраическому анализу данных шифров. Алгебраический анализ Simon проведён в [1], комбинация алгебраического и усечённого дифференциального криптоанализа шифра Simon от малого числа раундов рассмотрена в работе [2]. Алгебраические атаки представлены SAT-решателем и алгоритмом ElimLin.

Основная идея алгебраического криптоанализа состоит в составлении сложной системы булевых уравнений, описывающих преобразование шифра. Система строится на основе полностью известного алгоритма шифрования. Зашифрование на неизвестном криптоаналитику ключе некоторого количества открытых текстов позволяет провести подстановку в уравнения системы значений векторов открытых текстов и шифртек-

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research; работа первого автора выполнена при поддержке РФФИ (проект № 20-31-70043).

стов. На следующем этапе осуществляется решение системы с помощью различных методов относительно битов ключа.

Для анализа шифров было автоматизировано построение системы уравнений, описывающей преобразования раундов шифров.

Simon — семейство легковесных блочных шифров, разработанных для оптимальной производительности аппаратного обеспечения [3]. Имеет структуру классической схемы Фейстеля, на каждом раунде $2n$-битный вход раунда делится на две n-битные половины. К левой половине L применяется раундовая нелинейная небиективная функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. К выводу функции применяется операция XOR с правой половиной R и ключом k и две половины меняются местами (рис. 1).

Для шифра Simon, вводя новую переменную для каждого выхода побитовой операции $\odot$, для описания T раундов получаем $n(T-2)$ квадратичных уравнений с $n(T-2)+k$ неизвестными, где n — размер слова; T — количество раундов; k — длина ключа. При генерации ключа получается $n(T-m)$ уравнений. В результате для шифра Simon с T раундами генерируется $n(T-m)+n(T-2)$ уравнений. Количество ключей m зависит от размера входного блока $2n$ и количества раундов T.

Speck — семейство легковесных блочных шифров, обеспечивающих отличную производительность как в аппаратном, так и в программном обеспечении, но оптимизированных для работы на микроконтроллерах [3]. В каждом раунде $2n$-битных входа делятся на две n-битные половины. Каждый раунд Speck применяет операции конъюнкции, циклического сдвига влево и вправо, а также сложения по модулю 2^n. Параметры имеют следующие значения: $\alpha = 7$ и $\beta = 2$, если $n = 16$ (размер блока равен 32) и $\alpha = 8$ и $\beta = 3$ в противном случае. На рис. 2 представлена схема шифрования данного шифра. Ключевое расписание шифра Speck использует раундовую функцию для генерации раундовых ключей.

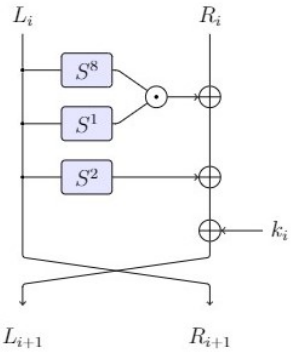


Рис. 1. Схема раундового преобразования шифра Simon [3]

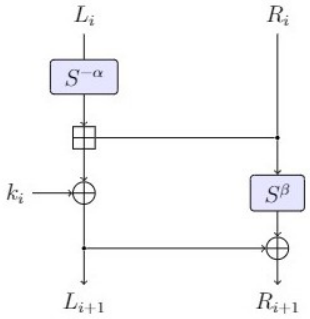


Рис. 2. Схема раундового преобразования шифра Speck [3]

В шифре Speck, вводя на каждом раунде новые переменные, получим следующие количества уравнений и неизвестных:

$$e = \begin{cases} (7n-3)(T-1) + (8n-3)(T-1) + 2n, & m = 1, \\ 2(8n-3)(T-1) + 2n, & m = 2,3,4, \end{cases}$$

$$u = \begin{cases} n(5T-4), & m = 1, \\ n(6T-5), & m = 2,3,4. \end{cases}$$

где e — число уравнений; u — число неизвестных.

1. Линеаризация

Проведение криптоанализа на небольшом количестве раундов (например, 3 и 4) с выбором стандартных характеристик нецелесообразно, так как ключи не строятся на основе исходных и между ними не будет никакой связи. Поэтому в данной работе рассматриваются шифры с $m = 1$ для $T \in \{3, 4\}$.

Рассмотрены атаки, основанные на линеаризации. Идея простой линеаризации состоит в том, чтобы присвоить каждому одночлену исходной системы новую переменную. Система после переобозначения становится линейной и решается, например, методом Гаусса. Затем для решений линейной системы проверяется, являются ли они решениями исходной нелинейной системы уравнений.

Количество различных одночленов в исходной системе определяет количество переменных n' в системе линейных уравнений, эффективность линеаризации зависит от ранга r этой системы. Множество решений не пусто, его мощность равна $2^{n'-r} \geqslant 0$, поэтому для оценки производительности необходимо проанализировать границы значений n' и r.

Рассматривая алгоритм шифрования, можем оценить количество различных мономов для каждого раунда шифра Simon. Для каждой операции вводятся новые переменные и проводится переобозначение при замене L_{i+1} и R_{i+1}; в результате получаем следующую оценку количества мономов M:

$$M \leqslant 6nT.$$

В шифре Speck основным методом сохранения степени является введение новых переменных для выходных битов нелинейных операций. В этом случае степень не будет превышать 2. На каждом раунде вводится $28n$ новых переменных. В системе уравнений, описывающей сложение по модулю 2^n, имеется всего $5(7n - 8)$ мономов. На практике оказалось, что различных мономов в системе уравнений сложения по модулю 2^n не больше $25n - 18$. Таким, образом, количество различных мономов на каждом раунде шифра Speck не больше $28n - 18$. Итоговая оценка числа различных мономов, исключая такие, которые образуются при генерации ключей (все уравнения линейны), имеет вид

$$M \leqslant (28n - 18)T.$$

XL-атака представлена в [4, 5]. На вход поступает система из m полиномиальных уравнений от n неизвестных степени d, выбирается степень $D > d$, все уравнения исходной системы умножаются на одночлены степени $D - d$ или меньше, система линеаризуется и на выходе получаем одно или несколько решений.

Для случая $d = 2$ и $D = d + 1$ анализ этой атаки [6] показывает, что единственное решение, вероятно, будет найдено, если $m \approx n^2/6$.

Алгоритм ElimLin описан в [7]. Его суть— поиск скрытых линейных уравнений, существующих в идеале, порождённом данной системой уравнений. Этот алгоритм состоит из двух последовательных шагов:

1) исключение Гаусса: в линейной оболочке исходной системы отыскиваются все линейные уравнения;
2) замена: переменные итеративно выражаются с помощью найденных линейных уравнений, получаемые выражения подставляются в исходную систему.

В табл. 1 и 2 приведены результаты для простой линеаризации, XL-метода и ElimLin. Полученные данные позволяют сравнить эффективность этих методов для

Simon и Speck. Для XL-метода $D = 3$. Сложность полного перебора составляет 2^{16} (при $n = 16$, $m = 1$). Как видно из табл. 1, метод линеаризации начиная с 4–5 раундов даёт худшие результаты, чем атака полным перебором. Использование метода простой линеаризации для $T \geqslant 4$ и XL-метода для пяти раундов (шифра Simon) не улучшает поиск решения по сравнению с полным перебором.

Таблица 1

Результаты применения атак, основанных на линеаризации

Шифр, параметры	Метод	Кол-во уравнений	Кол-во переменных	Кол-во мономов	Кол-во решений
Simon, $T = 3$, $m = 1$	Линеаризация	48	32	48	4, только одно явл. ключом
	XL-метод	1584	32	992	1
Simon, $T = 4$, $m = 1$	Линеаризация	64	48	80	65536
	XL-метод	3136	48	2616	256, только одно явл. ключом
Simon, $T = 5$, $m = 1$	Линеаризация	80	64	112	2^{32}
	XL-метод	5200	64	5008	2^{336}
Speck, $T = 3$, $m = 1$	Линеаризация	500	176	1236	—
	XL-метод	88500	176	185216	—

Таблица 2

Результаты применения метода ElimLin

Шифр, параметры	(Кол-во уравнений, кол-во лин. уравнений)	(Кол-во уравнений, кол-во лин. уравнений) после ElimLin
Simon, $T = 3$, $m = 1$	(48, 32)	(48, 32)
Simon, $T = 5$, $m = 1$	(80, 32)	(80, 48)
Speck, $T = 3$, $m = 1$	(500, 132)	(307, 137)
Speck, $T = 5$, $m = 2$	(1032, 296)	(654, 297)

2. SAT-решатели

Задача булевой выполнимости (SAT) — это задача принятия решения, в которой для произвольной булевой формулы возникает вопрос, существует ли такое значение переменных, что формула имеет значение `true`. Эта задача является NP-трудной.

Криптоанализ на основе SAT предполагает два этапа: на первом этапе обеспечивается кодирование SAT, например перевод данной системы из алгебраической нормальной формы (АНФ) в конъюнктивную нормальную форму. Мы используем конвертер anf2cnf [8] из библиотеки PolyBoRi, интегрированной в Sage. На втором этапе полученный экземпляр SAT-задачи решается с помощью SAT-решателя. Для криптографических систем часто применяются SAT-решатели CryptoMiniSat [9] и Lingering (с его параллельными версиями Plingeling и Treengeling) [10]. Мы применяем SAT-решатели CryptoMiniSat (в Sage ver. 6.10) и Lingeling, Plingeling, Treengeling на ПК со следующими параметрами: Core i5-4690 CPU 3,5 ГГц (x4), 12 Гбайт оперативной памяти. Экспериментальные результаты шифров Simon и Speck представлены в табл. 3. Рассмотрены два генератора систем уравнений в форме АНФ для шифра Simon: в одном все раундовые ключи являются независимыми переменными, в другом все раундовые ключи представлены алгоритмом ключевого расписания.

Таблица 3

Результаты SAT-решателя для шифров Speck и Speck

Параметры	Кол-во ур-ий	Кол-во неизв.	Параметры SAT	SAT	Время, с	RAM, Мбайт
Шифр Simon						
$T = 8$, $m = 2$ (с раунд. ключом)	224	224	384 лит., 2528 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— 69811,9 4775,5 12702,81	— 120,5 260,3 182
$T = 8$, $m = 2$ (ключ. расписание)	128	128	368 лит., 4448 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— 845,4 1188,8 4426,12	— 26,6 169,2 95
$T = 9$, $m = 2$ (ключ. расписание)	144	144	480 лит., 6448 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— >260174,3 47799,2 24547,91	— >180,7 620,3 172
$T = 10$, $m = 2$ (ключ. расписание)	160	160	560 лит., 8096 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— — 17554,9 60776,91	— — 458,8 234
Шифр Speck						
$T = 3$, $m = 1$	500	176	1460 лит., 11020 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	0,56 0,9 0,97 0,2	 9,6 4 1,9
$T = 4$, $m = 2$	782	320	2492 лит., 17380 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	21,4 3,0 8,25 61,4	 17,3 15 14,8
$T = 5$, $m = 2$	1032	416	3312 лит., 23184 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— — 14448,17 —	— — 278 —
$T = 6$, $m = 2$	1282	512	4132 лит., 28988 клоз	CryptoMiniSat Plingeling Treengeling Lingeling	— — 123353,82 —	— — 546 —

Прочерки в табл. 3 означают, что SAT решателю не удалось найти решение системы. Для шифра Speck CryptoMiniSat при $T = 3, 4$ не выдал размер файла.

3. Метод Раддума — Семаева

Данный подход к решению разреженных полиномиальных систем уравнений над полем $\mathbb{F}_2$ был представлен Г. Раддумом и И. Семаевым в работе [11]. Анализ и некоторые свойства можно найти в [12].

По исходной системе уравнений строится граф. Вершины соответствуют каждому уравнению (верхний набор вершин), также присутствуют вершины, образуемые пересечением наборов переменных соответствующих уравнений (нижний набор вершин). Каждой вершине приписан список возможных означиваний соответствующих переменных. Обработка и поиск решения осуществляется с помощью так называемой процедуры Agreeing-Gluing (согласования-склейки). Процедура согласования берет две соседние вершины и обновляет их списки, удаляя векторы, которые имеют разные под-

векторы для общих переменных. Процедура склеивания заменяет две вершины новой вершиной с обновлённым списком означиваний.

В качестве результатов использования этого алгоритма для атаки на Simon и Speck мы приводим только максимальное количество раундов, для которых алгоритм завершился за допустимое время. Стоит отметить, что временная сложность сильно зависит от эвристики, используемой для запуска процесса согласования, будь то (частичное) разделение или склейка.

Для шифра Simon максимальное число переменных в уравнении зависит от количества раундов и ключей. Для 6 переменных количество уравнений будет соответствовать $n(T-2)+n(T-m)$.

Благодаря введению новых переменных в каждый раунд шифра Speck количество переменных на каждом раунде не зависит от количества раундов T и ключей m. Максимальное количество переменных в одном уравнении равно 6; количество уравнений и переменных представлено в табл. 4 для $m=1$ и табл. 5 для $m=2,3,4$.

Таблица 4

Количество переменных каждого уравнения шифра Speck, $m=1$

Кол-во переменных	Кол-во уравнений
6	$2(T-1)(2n-4)$
5	$2(T-1)n$
4	$6(T-1)n+(T-2)n$
3	$2(n+1)(T-1)$
2	$3n$

Таблица 5

Количество переменных каждого уравнения шифра Speck, $m=2,3,4$

Кол-во переменных	Кол-во уравнений
6	$2(T-1)(2n-4)$
5	$2(T-1)n$
4	$6(T-1)n+(T-2)n$
3	$2(n+1)(T-1)$
2	$(T-1)n+3n$

Алгоритм Agreeing-Gluing был запущен для Simon до 9 раундов, для Speck — до 6 (табл. 6).

Таблица 6

Параметры алгоритма Раддума — Семаева для шифров Simon и Speck

Параметры	Количество уравнений	Количество неизвестных	Верхний набор	Нижний набор
Шифр Simon				
$T = 7$, $m = 2$	112	112	112	800
$T = 8$, $m = 2$	128	128	128	1072
$T = 9$, $m = 2$	144	144	144	1600
Шифр Speck				
$T = 3$, $m = 1$	500	176	500	558
$T = 4$, $m = 2$	782	320	782	749
$T = 5$, $m = 2$	1032	416	1032	1005
$T = 6$, $m = 2$	1282	512	1282	1229

4. Анализ полученных результатов и заключение

В работе предпринята попытка оценить устойчивость шифра Speck к алгебраическому криптоанализу с помощью различных методов. Экспериментальные результаты показывают, что методы алгебраического анализа являются перспективным способом анализа надёжности современных шифров (в частности, легковесных). Применительно к шифрам Simon и Speck показано, что методы, основанные на линеаризации, неэффективны уже при малом количестве раундов. С использованием SAT-решателя для шифра Simon решение найдено до 10 раундов включительно, для шифра Speck — до 6 раундов. Применение алгоритма Раддума — Семаева даёт результат для шифра Simon до 9 раундов, Speck — до 6. Результаты алгебраического анализа показывают, что включение дополнительных нелинейных операций (например, операции сложения по модулю 2^n) значительно увеличивает время атаки и объём используемой памяти. Поэтому рассмотренные методы более эффективны для криптоанализа шифра Simon, чем для Speck. В то же время разреженность систем уравнений, описывающих шифры Simon и Speck, достаточно высока, что приводит к мысли о целесообразности использования метода Раддума-Семаева, разработанного специально для таких систем.

В дальнейшем планируется провести теоретическую оценку сложности алгебраического анализа для полнораундовых шифров Simon и Speck, а также оценить эффективность использования алгоритма Бухбергера.

ЛИТЕРАТУРА

1. *Raddum H.* Algebraic analysis of the Simon block cipher family // LNCS. 2015. V. 9230. P. 157–169.
2. *Courtois N., Mourouzis T., Song G., et al.* Combined algebraic and truncated differential cryptanalysis on reduced-round Simon // 11th Intern. Conf. Security Cryptogr. 2014. P. 399–404
3. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.
4. *Courtois N., Shamir A., Patarin J., and Klimov A.* Efficient algorithms for solving overdefined systems of multivariate polynomial equations // LNCS. 2000. V. 1807. P. 293–407.
5. *Courtois N.* The Security of Cryptographic Primitives based on Multivariate Algebraic Problems. Ph.D. Thesis, Paris, 2001.
6. *Bard G.* Algebraic Cryptanalysis. Springer, 2009. 356 p.

7. *Courtois N. and Bard G. V.* Algebraic cryptanalysis of the data encryption standard // LNCS. 2007. V. 4887. P. 152–169.
8. *Albrecht M., Brickenstein M., and Soos M.* An ANF to CNF Converter using a Dense/Sparse Strategy. `https://doc.sagemath.org/html/en/reference/sat/sage/sat/converters/polybori.html`.
9. *Soos M.* The CryptoMiniSat 5 set of solvers at SAT competition 2016 // Proc. SAT Competition. Helsinki, 2016. P. 28.
10. *Biere A.* CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT entering the SAT Competition 2017 // Proc. SAT Competition. Helsinki, 2017. P. 14–15.
11. *Raddum H. and Semaev I.* New Technique for Solving Sparse Equation Systems. IACR Cryptology ePrint Archive, 2006/475, 2006.
12. *Biere A.* New technique for solving sparse equation systems // Des. Codes Cryptogr. 2008. V. 49. No. 1–3. P. 47–60.

Kutsenko A. V., Atutova N. D., Zyubina D. A., Maro E. A., Filippov S. D. **ALGEBRAIC CRYPTANALYSIS OF ROUND-REDUCED LIGHTWEIGHT CIPHERS SIMON AND SPECK.** This paper presents algebraic attacks on Simon and Speck, two families of lightweight block ciphers having LRX- and ARX-structures respectively. They were presented by the U.S. National Security Agency in 2013 and later standardized by ISO as a part of the RFID air interface standard. The ciphers are algebraically encoded, and the resulting systems of Boolean equations are solved with different SAT solvers as well as methods based on the linearization. For the first time, the approaches that use the sparsity of systems of Boolean equations are applied to these ciphers. The linearization parameters in systems of equations for both of the ciphers are estimated. A comparison of the efficiency of the used methods is provided.The results of the algebraic analysis show that the inclusion of additional nonlinear operations significantly increases the attack time and the amount of memory used. Therefore, the methods considered are more effective for cryptanalysis of the Simon cipher than Speck.
Keywords: *algebraic cryptanalysis, block cipher, lightweight cryptography,* Simon, Speck.

КУЦЕНКО Александр Владимирович — аспирант механико-математического факультета Новосибирского государственного университета, м.н.с. Института математики СО РАН им. С.Л. Соболева, г. Новосибирск. E-mail: **alexandrkutsenko@bk.ru**

АТУТОВА Наталья Дмитриевна — студентка механико-математического факультета Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: **atutova.n@yandex.ru**

ЗЮБИНА Дарья Александровна — студентка факультета информационных технологий Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: **zyubinadarya@gmail.com**

МАРО Екатерина Александровна — кандидат технических наук, доцент кафедры безопасности информационных технологий Южного федерального университета, г. Таганрог. E-mail: **marokat@gmail.com**

ФИЛИППОВ Степан Дмитриевич — студент Санкт-Петербургского государственного университета, г. Санкт-Петербург. E-mail: **filippowstepan@yandex.ru**

минимум четыре булевых функции (им отвечает одно подпространство), на основе которых строится векторная булева функция с максимальным значением иммунности.

С учётом экспериментальных результатов сформулированы следующие гипотезы:

Гипотеза 1. Для любого $n \geqslant 2$ в множестве, состоящем из булевых функций от n переменных с максимальной алгебраической иммунностью и нулевой функции, существует линейное подпространство размерности n.

Данная гипотеза доказана для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко. Для $n = 7, 9$ пока не найдено таких подпространств.

Гипотеза 2. Пусть f — булева функция от n переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Тогда в её АНФ присутствует по меньшей мере по одному моному каждой степени i, где $i = 1, 2, \ldots, \lceil n/2 \rceil$.

Данная гипотеза проверена для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко.

Таким образом, возможно построение S-блока от малого числа переменных, который устойчив к алгебраическим атакам. В дальнейшем планируется анализ булевых и векторных булевых функций от большего числа переменных.

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.

УДК 519.7 DOI 10.17223/2226308X/14/6

О НЕКОТОРЫХ СВОЙСТВАХ САМОДУАЛЬНЫХ ОБОБЩЁННЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Бент-функции вида $\mathbb{F}_2^n \to \mathbb{Z}_q$, где $q \geqslant 2$ — натуральное число, называются обобщёнными бент-функциями. Обобщённые бент-функции, для которых можно определить дуальную бент-функцию, называются регулярными. Регулярная обобщённая бент-функция называется самодуальной, если она совпадает со своей дуальной. Получены необходимые и достаточные условия самодуальности обобщённых бент-функций из класса Елисеева — Мэйорана — МакФарланда. Представлен полный спектр расстояний Ли между данными функциями. Доказано несуществование аффинных самодуальных обобщённых бент-функций. Приведён класс изометричных отображений, сохраняющих самодуальность обобщённой бент-функции. С помощью данных отображений получена уточнённая классификация самодуальных бент-функций вида $\mathbb{F}_2^4 \to \mathbb{Z}_4$.

Ключевые слова: *самодуальная бент-функция, обобщённая бент-функция, класс Елисеева — Мэйорана — МакФарланда, расстояние Ли.*

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 20-31-70043) и лаборатории криптографии JetBrains Research.

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. Пусть q — натуральное число; *обобщённой булевой функцией* от n переменных называется отображение вида $\mathbb{F}_2^n \to \mathbb{Z}_q$. Множество всех обобщённых булевых функций от n переменных обозначим $\mathcal{GF}_n^q$. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначается значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется число его ненулевых координат. *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения; обозначается $\mathrm{dist}(f, g)$. Согласно [1], назовём ортогональной группой порядка n над полем $\mathbb{F}_2$ группу

$$\mathcal{O}_n = \left\{L \in \mathrm{GL}\,(n, \mathbb{F}_2) : LL^{\mathrm{T}} = I_n\right\},$$

где L^{T} — транспонирование L; I_n — единичная матрица порядка n над полем $\mathbb{F}_2$.

Обобщённым преобразованием Уолша — Адамара функции $f \in \mathcal{GF}_n^q$ называется функция $H_f : \mathbb{F}_2^n \to \mathbb{C}$, заданная равенством

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}, \quad y \in \mathbb{F}_2^n,$$

где $\omega = e^{2\pi i/q}$. Функция $f \in \mathcal{GF}_n^q$ называется *обобщённой бент-функцией*, если $|H_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [2]. Обзор различных обобщений бент-функций представлен в работе [3]. Множество обобщённых бент-функций обозначается через $\mathcal{GB}_n^q$. *Весом Ли* вектора $x \in \mathbb{Z}_q$ называется число $\mathrm{wt}_L(x) = \min\{x, q - x\}$. *Расстояние Ли* $\mathrm{dist}_L(f, g)$ между функиями $f, g \in \mathcal{GF}_n^q$ определяется как

$$\mathrm{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L\left(\delta(x)\right),$$

где $\delta \in \mathcal{GF}_n^q$ и $\delta(x) = f(x) + (q-1)g(x)$ для любого $x \in \mathbb{F}_2^n$.

Пусть $f \in \mathcal{GB}_n^q$, тогда если существует функция $\widetilde{f} \in \mathcal{GF}_n^q$, такая, что $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$, то бент-функция f называется *регулярной*, а функция $\widetilde{f}$ — дуальной к f. Дуальная функция также является регулярной обобщённой бент-функцией. Если $f = \widetilde{f}$, то f называется *самодуальной* обобщённой бент-функцией. Если $f = \widetilde{f} + q/2$, то f называется *антисамодуальной* обобщённой бент-функцией. Всюду далее считается, что q — чётное натуральное число.

Открытой проблемой является полная характеризация и описание класса булевых самодуальных бент-функций ($q = 2$). Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящёно большое количество работ (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). Подробную информацию о бент-функциях и их приложениях можно найти в книге [4]. В ряде работ исследованы свойства самодуальных бент-функций в рамках различных обобщений бент-функций: так, в [5, 6] рассматривается обобщение вида $\mathbb{F}_p^n \to \mathbb{F}_p$, где p простое. Получен ряд результатов, в частности представлена полная классификация квадратичных самодуальных бент-функций. Связь самодуальных обобщённых бент-функций вида $\mathbb{F}_2^n \to \mathbb{Z}_4$ и самодуальных булевых бент-функций исследована в работе [7]. На основе обнаруженной взаимосвязи сделан вывод о несуществовании самодуальных обобщённых бент-функций указанного вида в случае нечётного числа переменных.

В настоящей работе исследуются свойства самодуальных обобщённых бент-функций $\mathbb{F}_2^n \to \mathbb{Z}_q$, где q — чётное натуральное число.

Булевы бент-функции от чётного числа переменных n, представимые в виде

$$f(x,y) = \langle x, \pi(y)\rangle \oplus g(y), \quad x,y \in \mathbb{F}_2^{n/2},$$

где π — перестановка на множестве $\mathbb{F}_2^{n/2}$ и g — булева функция от $n/2$ переменных, формируют хорошо известный класс *Елисеева — Мэйорана — МакФарланда*. Обобщённые бент-функции вида

$$f(x,y) = \frac{q}{2}\langle x, \pi(y)\rangle + g(y), \quad x,y \in \mathbb{F}_2^{n/2},$$

образуют класс *обобщённых бент-функций Елисеева — Мэйорана — МакФарланда*.

Утверждение 1. Обобщённая бент-функция Елисеева — Мэйорана — МакФарланда

$$f(x,y) = \frac{q}{2}\,\langle x, \pi(y)\rangle + g(y),\ x,y \in \mathbb{F}_2^{n/2},$$

является (анти)самодуальной тогда и только тогда, когда

$$\pi(y) = L\,(y \oplus b)\,, \quad g(y) = \frac{q}{2}\,\langle b, y\rangle + d, \quad y \in \mathbb{F}_2^{n/2},$$

где $L \in \mathcal{O}_{n/2}$; $b \in \mathbb{F}_2^{n/2}$; $\mathrm{wt}\,(b)$ — чётное (нечётное) число; $d \in \mathbb{Z}_q$.

Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Елисеева — Мэйорана — МакФарланда получен в работе [8]. Далее представлен спектр расстояний Ли между (анти)самодуальными обобщёнными бент-функциями из класса Елисеева — Мэйорана — МакФарланда. Для данного спектра используется обозначение Sp_L.

Теорема 1. Справедливо

$$\mathrm{Sp}_L = \left\{q \cdot 2^{n-2}\right\} \cup \bigcup_{w=0}^{q/2} \bigcup_{r=0}^{n/2-1} \left\{q \cdot 2^{n-2}\left(1 \pm \frac{1}{2^r}\right) \mp w \cdot 2^{n-r}\right\}.$$

Более того, все приведённые расстояния достижимы.

На основе данного результата можно сделать вывод о минимальном расстоянии Ли между рассматриваемыми функциями.

Утверждение 2. Минимальное расстояние Ли между (анти)самодуальными обобщёнными бент-функциями из класса Елисеева — Мэйорана — МакФарланда от n переменных равно $q \cdot 2^{n-3}$.

Хорошо известно, что булева бент-функция и, как следствие, самодуальная булева бент-функция не может быть аффинной. Тем не менее в работе [9] показано, что для обобщённых бент-функций данный вопрос нетривиален, в частности, для случая, когда q кратно 4, существуют аффинные обобщённые бент-функции. Следующий результат показывает отсутствие аффинных самодуальных обобщённых бент-функций для произвольного чётного q.

Теорема 2. Для любого положительного чётного q и произвольного натурального n не существует самодуальных обобщённых бент-функций вида

$$f(x) = \sum_{i=1}^{n} \lambda_i x_i + \lambda_0,$$

где $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$.

Далее представлен класс отображений, сохраняющих (анти)самодуальность обобщенной бент-функции.

Теорема 3. Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) + \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — чётное число, $d \in \mathbb{Z}_q$, сохраняют (анти)самодуальность обобщённой бент-функции.

Заметим, что каждое такое отображение сохраняет расстояние Хэмминга и расстояние Ли между обобщёнными бент-функциями, то есть является изометричным. С помощью отображений данного вида получена уточнённая классификация кватернарных самодуальных бент-функций от четырёх переменных (таблица).

Классификация самодуальных обобщённых бент-функций от четырёх переменных для $q = 4$

Вектор значений представителя класса эквивалентности	Размер класса
0220202022000000	24
2022220222020200	64
0330313133110110	48
0330302132010110	120
1321213122010100	96
0220213023100000	48
Число функций	400

ЛИТЕРАТУРА

1. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. V. 13. No. 3. P. 450–491.
2. *Schmidt K.-U.* Quaternary constant-amplitude codes for multicode CDMA // IEEE Trans. Inform. Theory. 2009. V. 55. No. 4. P. 1824–1832.
3. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискрет. анализ исслед. опер. 2010. Т. 17. № 1. С. 33–62.
4. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
5. *Çeşmelioğlu A., Meidl W., and Pott A.* On the dual of (non)-weakly regular bent functions and self-dual bent functions // Adv. Math. Commun. 2013. V. 7. No. 4. P. 425–440.
6. *Hou X.-D.* Classification of p-ary self dual quadratic bent functions, p odd // J. Algebra. 2013. V. 391. P. 62–81.
7. *Sok L., Shi M., and Solé P.* Classification and construction of quaternary self-dual bent functions // Cryptogr. Commun. 2018. V. 10. No. 2. P. 277–289.
8. *Kutsenko A. V.* The Hamming distance spectrum between self-dual Maiorana — McFarland bent functions // J. Appl. Industr. Math. 2018. V. 12. No. 1. P. 112–125.
9. *Singh B. K.* On cross-correlation spectrum of generalized bent functions in generalized Maiorana — McFarland class // Inform. Sci. Lett. 2013. V. 2. No. 3. P. 139–145.

УДК 519.7

Применение эвристических методов для поиска булевых функций с высокой алгебраической иммунностью

Н.Д. Атутова
Новосибирский государственный университет
Лаборатория криптографии JetBrains Research

Развивающийся интерес к криптоанализу повышает потребность в улучшении стойкости шифров. Для защиты от статистических и аналитических видов криптонализа в качестве компонент шифра необходимо использовать булевы функции, обладающие хорошими криптографическими характеристиками. Целью работы является построение булевых функций с высокой алгебраической иммунностью - характеристикой, повышающей стойкость шифра к алгебраическим атакам.

Алгебраическая иммунность булевой функции f - минимальное число d такое, что существует булева функция g степени d не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f + 1)g = 0$ [1].

Выделяют три способа получения булевой функции с хорошими криптографическими свойствами: полный перебор, алгебраическое конструирование и эвристики. При росте числа переменных n множество булевых функций растет дважды экспоненциально, что ухудшает эффективность полного перебора. Алгебраическое построение заведомо сужает множество решений. Перспективным является подход, использующий эвристические методы, в основе которых лежит структурированный перебор с параметрами для достижения желаемого результата.

В работе предложен и реализован на языке программирования c++ комбинированный подход на основе генетического алгоритма и локального поиска (в частности, поиск восхождением к вершине) для построения булевых функций с высокой алгебраической иммунностью. Для небольшого числа переменных ($n \leqslant 5$) были проведены вычислительные эксперименты, продемонстрировавшие эффективность предлагаемого подхода.

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

[1] Токарева Н. Н. Симметричная криптография. Краткий курс: учебное пособие // Новосиб. гос. ун-т. Новосибирск, 2012.

Научный руководитель – канд. физ.-мат. наук Н.Н.Токарева, А.В. Куценко.

УДК 519.7

S-блоки с высокой компонентной алгебраической иммунностью

Д. А. Зюбина
Новосибирский государственный университет
Лаборатория криптографии JetBrains Research

Одной из основных разновидностей блочных шифров является подстановочно-перестановочная сеть, которая является комбинацией подстановок (S-блоков) и перестановок. *S-блок* представляет собой векторную булеву функцию, построенную на основе n булевых функций от n переменных. Для того, чтобы шифр был достаточно устойчив к алгебраическим атакам, необходимо чтобы компонентная алгебраическая иммунность S-блока принимала максимально возможное значение.

Алгебраической иммунностью $AI(f)$ булевой функции f называется минимальное число d такое, что существует булева функция g степени d, не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$ [1]. Для функции f от n переменных максимально возможное $AI(f) = \left\lceil \frac{n}{2} \right\rceil$. *Компонентной алгебраической иммунностью* $AI_{comp}(F)$ векторной булевой функции называется минимальная алгебраическая иммунность ее компонентных функций, т.е. функций $f_b(x) = \langle b, F(x) \rangle$, где $b \in \mathbb{Z}_2^n, b \neq 0$ и $\langle a, b \rangle = a_1 b_1 \oplus \ldots \oplus a_n b_n$ – скалярное произведение векторов по модулю 2.

В данной работе для построения S-блока с максимальной компонентной алгебраической иммунностью был реализован метод нахождения линейного подпространства размерности n в множестве булевых функций от n переменных с максимальной алгебраической иммунностью.

Гипотеза. В множестве, состоящем из булевых функций от n переменных с максимальной алгебраической иммунностью и нулевой функции, существует линейное подпространство размерности n.

В частности, было получено, что существует в точности 1888 таких линейных подпространств размерности 3 для булевых функций от 3 переменных. В результате на полученных данных возможно построение S-блока, устойчивого к алгебраическим атакам.

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

---

1. Meier W., Pasalic E., and Carlet C. Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.

Научный руководитель – к.ф.-м.н. Н.Н.Токарева

УДК 004.056.55

Разработка автоматизированного анализа шифров на алгебраическую криптоустойчивость

Н. Д. Атутова[1,2], Д. А. Зюбина[1,2], С. Д. Филиппов[3]
[1]Новосибирский государственный университет
[2]Лаборатория криптографии JetBrains Research
[3]Санкт-Петербургский государственный университет

В настоящее время защита информации обеспечивается с помощью шифрования данных. Для достаточной надежности необходима высокая стойкость к статистическим и аналитическим методам криптоанализа шифра. Основная идея алгебраического криптоанализа состоит в составлении сложной системы булевых уравнений, описывающих преобразование шифра, и нахождении решений данной системы, соответствующих секретному ключу.

Целью работы является реализация автоматического построения систем уравнений для анализа, и получение оценок стойкости шифров к алгебраическим атакам. В рамках данной работы булевы уравнения представляются в форме АНФ: полиномы, в которых используются только операции сложения и умножения по модулю 2, а также константы 0 и 1 [1].

Рассмотрены Simon и Speck - шифры, имеющие структуры LRX- и ARX- шифров, представленные АНБ США в 2013 году. Реализованы алгоритмы построения систем уравнений в форме АНФ для рассматриваемых шифров. Полученные уравнения использованы для реализации методов решений систем и получения оценок стойкости: SAT-решатель, XL-метод, ElimLin, алгоритм Бухбергера. В результате было выяснено, что наибольшую эффективность показали атаки с помощью SAT-решателя.

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

---

1. Токарева Н. Н. Симметричная криптография. Краткий курс: учебное пособие // Новосиб. гос. ун-т. Новосибирск, 2012.

Научный руководитель – к.ф.-м.н. Н.Н.Токарева, А.В. Куценко.

УДК 519.7

Построение функций обратной связи в нелинейном регистре сдвига

М. А. Панферов

Новосибирский государственный университет
Лаборатория криптографии JetBrains Research

В настоящеее время активно используют регистры сдвига с нелинейной обратной связью для построения генераторов в поточных шифрах. Рассмотрим фильтрующий генератор, состоящий из регистра сдвига с нелинейной обратной связью. Пусть регистр имеет длину n и использует функцию обратной связи $f(x_1, \ldots, x_n)$. В случае линейной обратной связи известны многие свойства функции f, тогда как нелинейные функции активно изучаются. Подробнее о нелинейных регистрах сдвига см. [1].

В данной работе исследовались нелинейные функции обратной связи $f(x_1, \ldots, x_n)$ от n переменных, с помощью которых генератор может порождать псевдослучайную последовательность максимальной длины 2^n. А именно, была написана программа, которая позволяет построить функции $f(x)$ при малых $n < 6$ для дальнейшего их изучения и классификации.

Для $n = 3$ найдено 2 функции, для $n = 4$ найдено 16 функций, а для $n = 5$ найдено 2048 функций.

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

[1] A. Menezes, P. C. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press,pp. 191–222, 1996.

Научный руководитель – канд. физ.-мат. наук, доц. Н. Н. Токарева

УДК 519.7

Свойства функции в регистре сдвига с нелинейной обратной связью

Т. А. Бонич
Новосибирский государственный университет
Лаборатория криптографии JetBrains Research

Регистры сдвига с обратной связью часто используются для построения поточных шифров. Особым интересом пользуются регистры сдвига с нелинейными обратными связями (NFSR). Такие регистры состоят из двух частей: бинарный вектор $x = (x_1, \dots x_n)$ длины n и определенная на нем функция обратной связи $f : (x_1, \dots, x_n) \to \{0, 1\}$, где $f -$ нелинейная булева функция от n переменных. Работа нелинейного регистра сдвига представлена, например, в [1]. В случае с регистром сдвига с линейной обратной связью известно, какие функции использовать, чтобы получить псевдослучайную последовательность максимального периода. А для нелинейного случая известно мало.

В данной работе изучены функции обратной связи, которые позволяют генератору производить псевдослучайную последовательность максимального периода, 2^n. А именно, на основе нескольких частных случаев, выявлены некоторые особенности данных функций.

Предложение 1. *Все нелинейные булевы функции от n переменных, которые позволяют генератору производить псевдослучайную последовательность максимального периода, 2^n, будут содержать в своей АНФ следующие мономы:* 1, x_1, $x_2x_3...x_n$.

Предложение 2. *Для каждого $n \leq 12$ нелинейная булева функция от n переменных вида $1 \oplus x_i \oplus x_1 \oplus x_2x_3...x_n$, где $i = 2, \dots, n$, позволяет генератору производить псевдослучайную последовательность максимального периода, 2^n.*

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

[1] A. Menezes, P. C. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press,pp. 191–222, 1996.

Научный руководитель – канд. физ.-мат. наук, доц. Н.Н.Токарева

УДК 519.7

Реализация и анализ гибридной атаки на криптографическую систему NTRU при малых значениях параметров с использованием алгоритма квантового поиска

А. О. Бахарев
Новосибирский государственный университет
Лаборатория криптографии JetBrains Research

Квантовые вычисления – это быстроразвивающаяся область компьютерных исследований, которая ставит под угрозу криптографическую стойкость стандартов асимметричного шифрования, используемых в настоящее время. В 2016 году National Institute of Standards and Technology (NIST) объявил конкурс «Post-Quantum Cryptography Competition» (PQCC), по завершении которого будет принят новый – квантово-устойчивый – стандарт асимметричного шифрования. Претендентами являются подходы на основе решёток, кодов, хэш-функций, изогений и многочленов от многих переменных.

Одним из финалистов третьего раунда конкурса PQCC является криптографическая система с открытым ключом NTRU, основанная на решётках. Основной метод криптоанализа системы NTRU сводится к решению задачи поиска кратчайшего вектора решётки (SVP), в общем случае являющейся NP-трудной. Перспективными являются разработка и анализ квантовых алгоритмов, которые позволяют ускорить решение данной задачи. В статье [1] был представлен гибридный подход к поиску кратчайшего вектора решётки, в рамках которого используется квантовый алгоритм поиска (Quantum search). Целью настоящей работы является анализ эффективности указанного выше подхода для атаки на криптосистему NTRU.

Получена реализация гибридного алгоритма поиска кратчайшего вектора решётки с использованием симулятора квантовых вычислений IBM Quantum Experience. Сделан вывод о параметрах системы NTRU, против которой можно эффективно применять гибридную атаку с использованием существующих квантовых симуляторов.

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

1. Laarhoven, T., Mosca, M. & van de Pol, J. Finding shortest lattice vectors faster using quantum search. *Des. Codes Cryptogr.* 77, 375–400 (2015).

Научные руководители – канд. физ.-мат. наук Н.Н. Токарева, А.В. Куценко.

УДК 519.7

Рекуррентные формулы для разностной характеристики XOR относительно сложения по модулю 2^n

И. А. Сутормин
Новосибирский государственный университет

В компонентах шифров ARX архитектуры используются три операции: сложение по модулю 2^n ($\boxplus$), циклический сдвиг и покомпонентное сложение по модулю 2 ($\oplus$, XOR). Дифференциальный криптоанализ **??** основан на изучении преобразования разностей открытых текстов в разности шифртекстов. Сложность его проведения является недостатком ARX шифров. Выбирая в качестве разности разность по модулю 2^n, эффективность дифференциального криптоанализа зависит от величин $\mathrm{adp}^{\oplus}$ своих компонент

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{P}[x, y \in \mathbb{Z}_2^n |\ (x \boxplus \alpha) \oplus (y \boxplus \beta) = (x \oplus y) \boxplus \gamma\,].$$

Теорема 1. *Пусть $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, $\alpha = (\alpha_n, \dots \alpha_1)$. За $\alpha 1$ обозначается вектор $(\alpha_n, \dots \alpha_1, 1) \in \mathbb{Z}_2^{n+1}$, за $\overline{\alpha}$ - вектор α с инвертированными битами. Тогда для $\mathrm{adp}^{\oplus}$ выполняются следующие равенства:*

$$\begin{aligned}
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) &= \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 0) &= \frac{1}{4}(\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \mathrm{adp}^{\oplus}(\overline{\alpha}, \overline{\beta} \to \gamma) \\
&\quad + \mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma) + \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma)) \\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 1) &= \frac{1}{4}(\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \overline{\gamma}) \\
&\quad + \mathrm{adp}^{\oplus}(\overline{\alpha}, \beta \to \gamma) + \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma})) \\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) &= \frac{1}{4}(\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}) \\
&\quad + \mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}) + \mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma)) \\
\mathrm{adp}^{\oplus}(\alpha 1, \beta 0 \to \gamma 0) &= \mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 0) = 0 \\
\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 1) &= \mathrm{adp}^{\oplus}(\alpha 1, \beta 1 \to \gamma 1) = 0
\end{aligned}$$

Работа выполнена при поддержке лаборатории криптографии JetBrains Research.

[1] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1):3–72, January 1991.

Научные руководители – к.ф.-м.н. Н.А. Коломеец, к.ф.-м.н. А.А. Городилова