ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/20710410/63/1

КОНСТРУКЦИЯ УРАВНОВЕШЕННЫХ ФУНКЦИЙ С ВЫСОКОЙ НЕЛИНЕЙНОСТЬЮ И ДРУГИМИ КРИПТОГРАФИЧЕСКИМИ СВОЙСТВАМИ[1]

А. С. Шапоренко

Новосибирский государственный университет, г. Новосибирск, Россия

E-mail: shaporenko.alexandr@gmail.com

Предлагается новая итеративная конструкция, которую можно применить для построения уравновешенных функций с высокой нелинейностью. Показано, как данная конструкция может быть использована для построения уравновешенных функций от чётного числа $n \geqslant 18$ переменных без линейных структур с нелинейностью $2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$. Приведены дополнительные условия, при которых функции, полученные с помощью итеративной конструкции, будут корреляционно-иммунными. Получены результаты, связанные с проблемой разложения булевых функций в сумму двух бент-функций.

Ключевые слова: *уравновешенные булевы функции, нелинейные булевы функции, бент-функции.*

CONSTRUCTION OF BALANCED FUNCTIONS WITH HIGH NONLINEARITY AND OTHER CRYPTOGRAPHIC PROPERTIES

A. S. Shaporenko

Novosibirsk State University, Novosibirsk, Russia

We present an iterative construction that can be used to construct balanced functions with high nonlinearity. Using this construction, we obtained Boolean functions in an even number $n \geqslant 18$ of variables which have no linear structures with nonlinearity $2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$. Additional conditions are given under which the functions obtained using the construction will be correlation immune. We also present results concerning "bent sum decomposition problem".

Keywords: *balanced Boolean functions, nonlinear Boolean functions, bent functions.*

Введение

Нелинейность является важным криптографическим свойством булевых функций. Шифры, которые используют функции с высокой нелинейностью в качестве своих

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2022-282.

компонент, являются более стойкими к линейному криптоанализу [1], так как их тяжелее всего приблизить аффинными функциями. Булевы функции от чётного числа переменных называются бент-функциями, если они имеют наибольшее значение нелинейности [2]. Бент-функции использовались в построении блочного шифра CAST [3], поточного шифра Grain [4] и хэш-функции HAVAL [5]. Бент-функции также связаны с некоторыми объектами теории кодирования, алгебры и комбинаторики [6, 7].

Известно, что бент-функции не обладают другим важным криптографическим свойством — они не уравновешены. Данная работа посвящена построению уравновешенных функций с высокой нелинейностью. Мы приводим итеративный способ построения уравновешенных булевых функций, которые при дополнительных условиях могут обладать такими криптографическими свойствами, как высокая нелинейность, отсутствие линейных структур и корреляционная иммунность.

Структура работы следующая: в п. 1 приведены основные определения и вспомогательные факты, которые используются при доказательстве основных результатов. Пункт 2 посвящён итеративной конструкции булевых функций, производная которых по некоторому ненулевому направлению имеет хотя бы одну линейную переменную. В п. 3 рассматривается частный случай — конструкции функций, которые имеют аффинные производные. Приводятся достаточные условия, при которых функции, полученные с помощью итеративной конструкции, обладают такими криптографическими свойствами, как уравновешенность, отсутствие линейных структур и корреляционная иммунность. В п. 4 описан способ получения уравновешенных функций от чётного числа $n \geqslant 18$ переменных без линейных структур с нелинейностью $2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$. В п. 5 приведены результаты, связанные с проблемой разложения произвольной булевой функции в сумму двух бент-функций.

1. Определения и необходимые утверждения

1.1. Булевы функции

Пусть $\mathbb{Z}_2 = \{0, 1\}$. Векторное пространство двоичных векторов длины n обозначается $\mathbb{Z}_2^n$. Пусть $\oplus$ обозначает сложение по модулю 2. Для $x, y \in \mathbb{Z}_2^n$ будем использовать следующее произведение:

$$\langle x, y \rangle = x_1 y_1 \oplus \cdots \oplus x_n y_n,$$

где x_i — i-я координата x, $i = 1, \ldots, n$.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Множество всех булевых функций от n переменных обозначим $\mathcal{F}_n$. С каждой булевой функцией f от n переменных можно связать её *носитель*:

$$\operatorname{supp}(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}.$$

Весом Хэмминга $\operatorname{wt}(f)$ функции $f \in \mathcal{F}_n$ называется количество ненулевых значений f: $|\{x \in \mathbb{Z}_2^n : f(x) = 1\}|$. Функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $\operatorname{wt}(f) = 2^{n-1}$.

Расстояние Хэмминга $\mathrm{d}(f, g)$ между двумя булевыми функциями $f, g \in \mathcal{F}_n$ вычисляется следующим образом:

$$\mathrm{d}(f, g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}|.$$

Каждую булеву функцию f от n переменных можно единственным образом представить в виде *алгебраической нормальной формы* (*АНФ*), или *полинома Жегалкина*:

$$f(x_1,\dots,x_n)=\left(\bigoplus_{k=1}^{n}\bigoplus_{i_1,\dots,i_k} a_{i_1,\dots,i_k}x_{i_1}\cdot\ldots\cdot x_{i_k}\right)\oplus a_0,$$

где при каждом k индексы $i_1,\dots,i_k$ различны и в совокупности пробегают все k-элементные подмножества $\{1,\dots,n\}$, а коэффициенты $a_{i_1,\dots,i_k}, a_0$ принимают значения 0 или 1.

Алгебраической степенью (*степенью*) $\deg(f)$ функции f называется количество переменных в самом длинном слагаемом её АНФ, при котором коэффициент не равен нулю. Функция степени не выше 1 называется *аффинной*. Аффинную функцию от n переменных можно представить в виде $\ell=\langle x,a\rangle\oplus b$, где $a\in\mathbb{Z}_2^n$ и $b\in\mathbb{Z}_2$. Множество всех аффинных функций от n переменных обозначим $\mathcal{A}_n$.

Булевы функции $f,g\in\mathcal{F}_n$ *аффинно эквивалентны*, если существуют невырожденная квадратная двоичная матрица A порядка $n\times n$ и вектор $b\in\mathbb{Z}_2^n$, такие, что $g(x)=f(Ax\oplus b)$.

Производной булевой функции $f\in\mathcal{F}_n$ называется функция $D_yf(x)=f(x)\oplus f(x\oplus y)$, где вектор $y\in\mathbb{Z}_2^n$ является *направлением*, по которому берётся производная. Легко убедиться, что $D_y\big(f\oplus g\big)=D_yf\oplus D_yg$.

Следующий факт представлен в [8] без доказательства. Для полноты приведём его с доказательством.

Лемма 1 (Н. Н. Токарева [8]). Булева функция $f\in\mathcal{F}_n$ является производной некоторой булевой функции $g\in\mathcal{F}_n$ по ненулевому направлению $y\in\mathbb{Z}_2^n$ тогда и только тогда, когда $f(x)\oplus f(x\oplus y)=0$ для всех $x\in\mathbb{Z}_2^n$.

Доказательство.

Необходимость. Пусть $D_yg(x)=f(x)$. Можно заметить, что $D_yg(x)=g(x)\oplus$ $\oplus\, g(x\oplus y)=D_yg(x\oplus y)$ для всех $x\in\mathbb{Z}_2^n$. Значит, $f(x)=f(x\oplus y)$ для всех $x\in\mathbb{Z}_2^n$.

Достаточность. Пусть i — первая ненулевая координата y и $g(x)=x_if(x)$ для всех $x\in\mathbb{Z}_2^n$. Тогда

$$D_yg(x)=x_if(x)\oplus(x_i\oplus1)f(x\oplus y)=f(x)\text{ для всех }x\in\mathbb{Z}_2^n.$$

Следовательно, f — производная g по направлению y. ■

Для каждого $y\in\mathbb{Z}_2^n$ *коэффициентом Уолша — Адамара* $W_f(y)$ булевой функции $f\in\mathcal{F}_n$ называется величина, определяемая равенством

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

Нам также понадобятся следующие хорошо известные факты:

Лемма 2. Булева функция $f\in\mathcal{F}_n$ является уравновешенной тогда и только тогда, когда $W_f(0)=0$.

Лемма 3. Пусть $f\in\mathcal{F}_n$, $\ell\in\mathcal{A}_n$ и $\ell(x)=\langle a,x\rangle\oplus b$, где $a\in\mathbb{Z}_2^n, b\in\mathbb{Z}_2$. Тогда для любого $c\in\mathbb{Z}_2^n$ справедливо $W_{f\oplus\ell}(c)=(-1)^b\,W_f(a\oplus c)$.

1.2. Бент-функции

Нелинейностью N_f булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от данной функции до множества всех аффинных функций:

$$N_f = \mathrm{d}(f, \mathcal{A}_n) = \min_{a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2} \mathrm{d}(f, \ell_{a,b}),$$

где $\ell_{a,b}(x) = \langle a, x \rangle \oplus b$.

Лемма 4 (О. Ротхаус [2]). Пусть $f \in \mathcal{F}_n$. Тогда

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^n} |W_f(a)|.$$

Булева функция от чётного числа переменных n называется *бент-функцией*, если её нелинейность достигает наибольшего возможного значения $2^{n-1} - 2^{n/2-1}$. Обозначим через $\mathcal{B}_n$ множество всех бент-функций от n переменных.

Бент-функции были определены О. Ротхаусом в 60-х годах прошлого века, хотя его работа [2] была опубликована только в 1976 г. Однако известно, что с конца 1950-х годов в Советском Союзе исследовались булевы функции с аналогичными свойствами, которые называли «минимальными функциями». В 1961 г. математики В. А. Елисеев и О. П. Степченков описали класс функций, который является аналогом класса Мэйорана — МакФарланда, представленного в 1973 г. Бент-функции также связаны с другими математическими объектами. Так, например, Р. Л. МакФарланд [9] и Дж. Диллон [10] исследовали бент-функции в терминах разностных множеств.

Нам понадобятся следующие хорошо известные факты:

Лемма 5. Пусть $f \in \mathcal{B}_n$ и $n \geqslant 4$. Тогда $\deg(f) \leqslant n/2$.

Лемма 6. Пусть $f \in \mathcal{B}_n$. Тогда $\mathrm{wt}(f) = 2^{n-1} \pm 2^{n/2-1}$.

Следовательно, бент-функции никогда не являются уравновешенными.

Лемма 7 (О. Ротхаус [2]). Булева функция $f \in \mathcal{F}_n$ является бент-функцией тогда и только тогда, когда $W_f(y) = \pm 2^{n/2}$ для любого $y \in \mathbb{Z}_2^n$.

Лемма 8 (О. Ротхаус [2]). Пусть $f \in \mathcal{B}_n$. Тогда:

1) любая булева функция, аффинно эквивалентная f, является бент-функцией;
2) функция $f \oplus \ell$ является бент-функцией от n переменных для любой аффинной функции ℓ.

Для бент-функции f от n переменных *дуальная функция* $\tilde{f}$ определяется с помощью равенств $W_f(y) = 2^{n/2}(-1)^{\tilde{f}(y)}$ для всех $y \in \mathbb{Z}_2^n$. Отметим, что $\tilde{f}$ также является бент-функцией [7].

Лемма 9 (О. Ротхаус [2]). Булева функция $f \in \mathcal{F}_n$ является бент-функцией тогда и только тогда, когда для любого ненулевого направления y её производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ является уравновешенной.

Приведём один из самых известных классов бент-функций — класс Мэйорана — МакФарланда, который был впервые определён в [10] и основан на работах Дж. А. Майорана и Р. Л. МакФарланда 1971–1973 гг.

Лемма 10 (Дж. Диллон [10]). Пусть $x, y \in \mathbb{Z}_2^n$, π — взаимно однозначное отображение на $\mathbb{Z}_2^n$, $g \in \mathcal{F}_n$ — произвольная функция. Тогда функция

$$f(x, y) = \langle \pi(x), y \rangle \oplus g(x)$$

— бент-функция от $2n$ переменных.

1.3. Линейные структуры и корреляционная иммунность

Переменная булевой функции называется *линейной*, если она входит в АНФ функции линейно. Если переменная не входит в АНФ булевой функции, то эта переменная называется *фиктивной*. Булева функция f *имеет линейную структуру*, если существует ненулевое направление $y \in \mathbb{Z}_2^n$, такое, что $D_y f(x) \equiv \mathrm{const}$. Следующий факт показывает, что функции, которые имеют линейные структуры, эквивалентны функциям с простым строением.

Лемма 11 (О. А. Логачев и др. [11]). Пусть $f \in \mathcal{F}_n$ имеет линейную структуру. Тогда существует функция $g \in \mathcal{F}_n$, которая аффинно эквивалентна f и имеет линейную или фиктивную переменную.

Булева функция $f \in \mathcal{F}_n$ называется *корреляционно-иммунной порядка* r, $1 \leqslant r \leqslant n$, если для любой её подфункции $g = f^{a_1,\ldots,a_r}_{i_1,\ldots,i_r}$, полученной из f подстановкой констант $a_1, \ldots, a_r$ вместо переменных $x_{i_1}, \ldots, x_{i_r}$, выполняется $\mathrm{wt}(g) = \mathrm{wt}(f)/2^r$. Требование корреляционной иммунности функции связано с противостоянием корреляционной атаке [12].

Лемма 12 (Т. Зигенталер [12]). Функция $f \in \mathcal{F}_n$ является корреляционно-иммунной порядка r, если и только если $W_f(a) = 0$ для всех векторов $a \in \mathbb{Z}_2^n$, таких, что $1 \leqslant \mathrm{wt}(a) \leqslant r$.

1.4. Уравновешенные функции с высокой нелинейностью

Как уже отмечалось, бент-функции не являются уравновешенными, что вызывает статистическую корреляцию между открытым и зашифрованным текстами.

Максимальная нелинейность уравновешенных функций неизвестна для $n > 7$. В работе [13] приведена следующая верхняя оценка нелинейности уравновешенных функций от чётного числа переменных.

Утверждение 1 (Дж. Себерри и др. [13]). Пусть $n \geqslant 4$ — чётное число и f — уравновешенная булева функция от n переменных. Тогда $N_f \leqslant 2^{n-1} - 2^{n/2-1} - 2$.

Одним из способов построения уравновешенных функций с высокой нелинейностью является преобразование бент-функций с целью получения уравновешенных булевых функций, которые сохраняют высокие значения нелинейности [14, 15]. Уравновешенным функциям с высокой нелинейностью посвящены также работы [13, 16–18].

2. Конструкция булевых функций, производные которых имеют линейную переменную

Опишем конструкцию булевых функций, производная которых по некоторому ненулевому направлению имеет хотя бы одну линейную переменную. Данная конструкция имеет управляемую производную и позволяет строить все булевы функции, имеющие в качестве своей производной по некоторому ненулевому направлению функцию хотя бы с одной линейной переменной. Для $n = 4$ и 6 покажем, что множество функций, которые можно построить с помощью данной конструкции, содержит уравновешенные функции с высокой нелинейностью.

Теорема 1. Пусть $n \geqslant 2$ — чётное число, $g_1, g_2, h_1 \in \mathcal{F}_n$, $(y, 1, y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $h(x, x_{n+1}, x_{n+2}) = (D_y h_1(x) \oplus y_{n+2}) x_{n+1} \oplus h_1(x) \oplus x_{n+2}$. Тогда функция $f \in \mathcal{F}_{n+2}$, построенная следующим образом:

$$\begin{aligned} f(x, x_{n+1}, x_{n+2}) = \big((D_y g_1(x) \oplus 1) h(x, x_{n+1}, x_{n+2}) \oplus D_y g_2(x)\big) x_{n+1} \oplus \\ \oplus g_1(x) h(x, x_{n+1}, x_{n+2}) \oplus g_2(x), \end{aligned} \tag{1}$$

имеет h своей производной по направлению $(y, 1, y_{n+2})$. При этом для вектора $(a, a_{n+1}, a_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $c = \langle a, y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2}$ справедливо

$$W_f(a, a_{n+1}, a_{n+2}) = (-1)^{c\cdot a_{n+2}} \cdot 2 \cdot W_{cg_1(x)\oplus g_2(x)\oplus a_{n+2}h_1(x)}(a).$$

Доказательство. Заметим, что $D_{(y,1,y_{n+2})}h(x, x_{n+1}, x_{n+2}) = 0$ для любого $(x, x_{n+1}, x_{n+2}) \in \mathbb{Z}_2^{n+2}$. Из леммы 1 следует, что h является производной булевой функции по направлению $(y, 1, y_{n+2})$. Для любой функции $f \in \mathcal{F}_{n+2}$, которая имеет h своей производной по направлению $(y, 1, y_{n+2})$, справедливо

$$f(x, x_{n+1}, x_{n+2}) \oplus f(x \oplus y, x_{n+1} \oplus 1, x_{n+2} \oplus y_{n+2}) = h(x, x_{n+1}, x_{n+2}). \tag{2}$$

Поскольку $h(x, x_{n+1}, x_{n+2}) = h(x \oplus y, x_{n+1} \oplus 1, x_{n+2} \oplus y_{n+2})$, получаем, что

$$h(x, x_{n+1}, x_{n+2}) = 1 \iff h(x \oplus y, x_{n+1} \oplus 1, x_{n+2} \oplus y_{n+2}) = 1. \tag{3}$$

Если $h(x, x_{n+1}, x_{n+2}) = 1$, то, поскольку h зависит линейно от переменной x_{n+2}, имеем $h(x, x_{n+1}, x_{n+2} \oplus 1) = 0$. Таким образом, справедливо, что

$$\{x : \exists x_{n+2} \in \mathbb{Z}_2\,(h(x, 0, x_{n+2}) = 1)\} = \{x : \exists x_{n+2} \in \mathbb{Z}_2\,(h(x, 0, x_{n+2}) = 0)\} = \mathbb{Z}_2^n. \tag{4}$$

Из (2)–(4) следует, что любая булева функция f от $(n + 2)$ переменных, для которой $D_{(y,1,y_{n+2})}f(x, x_{n+1}, x_{n+2}) = h(x, x_{n+1}, x_{n+2})$, имеет следующее представление:

$$\begin{cases} f(x, 0, x_{n+2}) = f_1(x), & \text{если } h(x, 0, x_{n+2}) = 1, \\ f(x \oplus y, 1, x_{n+2} \oplus y_{n+2}) = f_1(x) \oplus 1, & \text{если } h(x \oplus y, 1, x_{n+2} \oplus y_{n+2}) = 1, \\ f(x, 0, x_{n+2}) = f_2(x), & \text{если } h(x, 0, x_{n+2}) = 0, \\ f(x \oplus y, 1, x_{n+2} \oplus y_{n+2}) = f_2(x), & \text{если } h(x \oplus y, 1, x_{n+2} \oplus y_{n+2}) = 0, \end{cases} \tag{5}$$

где f_1 и f_2 — произвольные функции от n переменных. Следовательно, перебирая все возможные f_1 и f_2, мы получим все булевы функции от $(n + 2)$ переменных, которые имеют $h(x, x_{n+1}, x_{n+2})$ своими производными по направлению $(y, 1, y_{n+2})$.

Положим, что $g_1 = f_1 \oplus f_2$ и $g_2 = f_2$. Тогда формула (1) для функции f следует из представления (5).

Отметим, что для $(x, x_{n+1}, x_{n+2}) \in \mathbb{Z}_2^{n+2}$ выполняется

$$x_{n+2} = h(x, x_{n+1}, x_{n+2}) \oplus (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x). \tag{6}$$

Теперь проверим, чему равны коэффициенты Уолша — Адамара функции f для каждого $(a, a_{n+1}, a_{n+2}) \in \mathbb{Z}_2^{n+2}$. Заметим, что

$$\langle (x, x_{n+1}, x_{n+2}), (a, a_{n+1}, a_{n+2})\rangle = \langle a, x\rangle \oplus a_{n+1}x_{n+1} \oplus a_{n+2}x_{n+2}.$$

Тогда из (2) следует, что

$$\begin{aligned} W_f(a, a_{n+1}, a_{n+2}) &= \sum_{(x,x_{n+1},x_{n+2})\in\mathbb{Z}_2^{n+2}} (-1)^{f(x,x_{n+1},x_{n+2})\oplus\langle(x,x_{n+1},x_{n+2}),(a,a_{n+1},a_{n+2})\rangle} = \\ &= \sum_{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} + \\ &+ (-1)^{f(x\oplus y,1,x_{n+2}\oplus y_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}}\Big) = \end{aligned}$$

$$= \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} + $$

$$+(-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}\oplus 1}\Big) +$$

$$+ \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} \Big((-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}} + (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}\oplus\langle a,y\rangle\oplus a_{n+1}\oplus a_{n+2}y_{n+2}}\Big).$$

Допустим, что $\langle a,y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2} = 0$. Тогда

$$W_f(a,a_{n+1},a_{n+2}) = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}}.$$

Из (4) и (5) следует, что если $a_{n+2} = 0$, то

$$W_f(a,a_{n+1},0) = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle} = 2\sum_{x\in\mathbb{Z}_2^n} (-1)^{f_2(x)\oplus\langle a,x\rangle} = 2W_{f_2}(a) = 2W_{g_2}(a).$$

Если $a_{n+2} = 1$, то из (5) и (6) следует, что

$$W_f(a,a_{n+1},1) = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle\oplus x_{n+2}} = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=0}} (-1)^{f_2(x)\oplus\langle a,x\rangle\oplus h_1(x)}.$$

Тогда, согласно (4), справедливо

$$W_f(a,a_{n+1},1) = 2\sum_{x\in\mathbb{Z}_2^n} (-1)^{f_2(x)\oplus h_1(x)\oplus\langle a,x\rangle} = 2\,W_{f_2\oplus h_1}(a) = 2\,W_{g_2\oplus h_1}(a).$$

Теперь пусть $\langle a,y\rangle \oplus a_{n+1} \oplus a_{n+2}y_{n+2} = 1$. Тогда

$$W_f(a,a_{n+1},a_{n+2}) = \sum_{(x,x_{n+1},x_{n+2})\in\mathbb{Z}_2^{n+2}} (-1)^{f(x,x_{n+1},x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+1}x_{n+1}\oplus a_{n+2}x_{n+2}} =$$

$$= 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f(x,0,x_{n+2})\oplus\langle a,x\rangle\oplus a_{n+2}x_{n+2}}.$$

Из (4) и (5) следует, что если $a_{n+2} = 0$, то

$$W_f(a,a_{n+1},0) = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus\langle a,x\rangle} = 2\sum_{x\in\mathbb{Z}_2^n} (-1)^{f_1(x)\oplus\langle a,x\rangle} = 2\,W_{f_1}(a) = 2\,W_{g_1\oplus g_2}(a).$$

Если $a_{n+2} = 1$, то из (5) и (6) следует, что

$$W_f(a,a_{n+1},1) = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus\langle a,x\rangle\oplus x_{n+2}} = 2 \sum_{\substack{(x,0,x_{n+2})\in\mathbb{Z}_2^{n+2}\\ h(x,0,x_{n+2})=1}} (-1)^{f_1(x)\oplus h_1(x)\oplus\langle a,x\rangle\oplus 1}.$$

Тогда, согласно (4), справедливо

$$W_f(a,a_{n+1},1) = 2\sum_{x\in\mathbb{Z}_2^n} (-1)^{f_1(x)\oplus h_1(x)\oplus\langle a,x\rangle\oplus 1} = -2\,W_{f_1\oplus h_1}(a) = -2\,W_{g_1\oplus g_2\oplus h_1}(a).$$

Теорема 1 доказана. ■

Отметим, что произвольная функция $h \in \mathcal{F}_{n+2}$, которая имеет хотя бы одну линейную переменную, может быть представлена следующим образом: $h(x, x_{n+1}, x_{n+2}) = h_2(x)x_{n+1} \oplus h_1(x) \oplus x_{n+2}$, где $h_1, h_2 \in \mathcal{F}_n$ и $x \in \mathbb{Z}_2^n$. Тогда по лемме 1 функция h является производной некоторой функции по направлению $(y, 1, y_{n+2})$ тогда и только тогда, когда $D_{(y,1,y_{n+2})}h(x, x_{n+1}, x_{n+2}) = 0$. Отсюда нетрудно получить, что $h_2(x) = D_y h_1(x) \oplus y_{n+2}$. Таким образом, теорема 1 позволяет построить все функции от n переменных, производная которых по некоторому ненулевому направлению имеют хотя бы одну линейную переменную.

Полным перебором проверено, что для $n = 4$ множество всех функций, производная которых по некоторому ненулевому направлению имеет хотя бы одну линейную переменную, состоит из 28 896 функций. Это множество содержит все 896 бент-функций от четырёх переменных. Кроме того, все 10 920 уравновешенных функций от четырёх переменных, которые имеют нелинейность 4 (максимально возможную для уравновешенных функций), имеют производную по некоторому ненулевому направлению хотя бы с одной линейной переменной. Более того, все уравновешенные функции, производная которых по некоторому ненулевому направлению имеет хотя бы одну линейную переменную, имеют нелинейность 4.

Булева функция от шести переменных

$$x_3x_4x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_2x_5x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4$$

является уравновешенной и имеет нелинейность 24, тогда как верхняя оценка нелинейности для уравновешенных функций от чётного числа переменных (утверждение 1) даёт 26. Её производная по направлению $(1, 0, \ldots, 0)$ является аффинной. Отметим, что оценка 26 нелинейности уравновешенных функций от 6 переменных достижима [13].

Таким образом, для $n = 6$ существует уравновешенная функция, производная которой по некоторому ненулевому направлению имеет хотя бы одну линейную переменную, с нелинейностью $2^{n-1} - 2^{n/2-1} - 4$. Более того, доказана следующая

Теорема 2. Пусть $f \in \mathcal{F}_{n+2}$ — уравновешенная функция от чётного $n \geqslant 6$ числа переменных, производная которой по некоторому ненулевому направлению имеет хотя бы одну линейную переменную. Тогда $N_f \leqslant 2^{n+1} - 2^{n/2} - 4$.

Доказательство. Из теоремы 1 известно, что f имеет форму (1), при этом g_2 из (1) является уравновешенной функцией от n переменных. Тогда из утверждения 1 верна следующая оценка: $N_{g_2} \leqslant 2^{n-1} - 2^{n/2-1} - 2$. Таким образом, из леммы 4 следует $\max\limits_{a \in \mathbb{Z}_2^n} |W_{g_2}| \geqslant 2^{n/2} + 4$. Тогда из теоремы 1 заключаем, что $N_f = 2^{n+1} - \max\limits_{a \in \mathbb{Z}_2^n, g \in M} |W_g(a)|$, где $M = \{g_2, g_1 \oplus g_2, g_2 \oplus h_1, g_1 \oplus g_2 \oplus h_1\}$, и, следовательно, $N_f \leqslant 2^{n+1} - 2^{n/2} - 4$. ■

3. Криптографические свойства булевых функций, которые имеют аффинные производные

Рассмотрим частный случай конструкции из теоремы 1 — итеративную конструкцию функций, которые имеют аффинные производные, и приведём достаточные условия, при которых функции, полученные с помощью этой конструкции, обладают такими криптографическими свойствами, как уравновешенность, отсутствие линейных структур и корреляционная иммунность.

Утверждение 2. Пусть $n \geqslant 2$ — чётное число, $g_1, g_2 \in \mathcal{F}_n$, $(y, 1, y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $b \in \mathbb{Z}_2^n$ такие, что $\langle b, y \rangle = y_{n+2}$, и

$$h(x, x_{n+1}, x_{n+2}) = \langle b, x \rangle \oplus c \oplus x_{n+2}, \text{ где } c \in \mathbb{Z}_2.$$

Тогда $f \in \mathcal{F}_{n+2}$ из (1) является уравновешенной функцией от $n+2$ переменных, если и только если g_2 — уравновешенная функция от n переменных. При этом

$$N_f = 2^{n+1} - \max_{a \in \mathbb{Z}_2^n, g \in \{g_2, g_1 \oplus g_2\}} |W_g(a)|.$$

Доказательство. Пусть $\ell_1(x) = \langle b, x \rangle \oplus c$, где $x \in \mathbb{Z}_2^n$. Можно убедиться, что $D_y \ell_1(x) = y_{n+2}$ для любого $x \in \mathbb{Z}_2^n$ и

$$h(x, x_{n+1}, x_{n+2}) = (D_y \ell_1(x) \oplus y_{n+2}) x_{n+1} \oplus \ell_1(x) \oplus x_{n+2}.$$

Из теоремы 1 и леммы 3 для $f \in \mathcal{F}_{n+2}$ из (1) следует, что

$$|W_f(a, a_{n+1}, a_{n+2})| = \begin{cases} 2\,|W_{g_2}(a)|, & \text{если } \langle a, y \rangle = a_{n+1} \text{ и } a_{n+2} = 0, \\ 2\,|W_{g_2}(a \oplus b)|, & \text{если } \langle a, y \rangle = a_{n+1} \oplus y_{n+2} \text{ и } a_{n+2} = 1, \\ 2\,|W_{g_1 \oplus g_2}(a)|, & \text{если } \langle a, y \rangle = a_{n+1} \oplus 1 \text{ и } a_{n+2} = 0, \\ 2\,|W_{g_1 \oplus g_2}(a \oplus b)|, & \text{если } \langle a, y \rangle = a_{n+1} \oplus y_{n+2} \oplus 1 \text{ и } a_{n+2} = 1. \end{cases}$$

Тогда $W_f(\mathbf{0}) = W_{g_2}(0)$ и первое утверждение следует из леммы 2. Второе утверждение следует из леммы 4. ■

3.1. Функции без линейных структур

Приведём достаточные условия того, что функции из утверждения 2 не имеют линейных структур.

Теорема 3. Пусть $n \geqslant 2$ — чётное число, g_1, g_2 — булевы функции от n переменных, $(y, 1, y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $\ell_1 \in \mathcal{A}_n$ такие, что $D_y \ell_1(x) = y_{n+2}$ и $h(x) = \ell_1(x) \oplus x_{n+2}$. Тогда если g_2 и $g_1 \oplus g_2$ являются уравновешенной функцией и бент-функцией от n переменных соответственно, то булева функция $f \in \mathcal{F}_{n+2}$ из (1) является уравновешенной и не имеет линейных структур.

Доказательство. Рассмотрим производную функции f из (1) по направлению (z, z_{n+1}, z_{n+2}), где $z \in \mathbb{Z}_2^n$ и $z_{n+1}, z_{n+2} \in \mathbb{Z}_2$:

$$\begin{gathered} D_{(z, z_{n+1}, z_{n+2})} f(x, x_{n+1}, x_{n+2}) = \big((D_y g_1(x) \oplus 1)(\ell_1(x) \oplus x_{n+2}) \oplus D_y g_2(x)\big) x_{n+1} \oplus \\ \oplus g_1(x)(\ell_1(x) \oplus x_{n+2}) \oplus g_2(x) \oplus \\ \oplus \big((D_y g_1(x \oplus z) \oplus 1)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus D_y g_2(x \oplus z)\big) x_{n+1} \oplus \\ \oplus \big((D_y g_1(x \oplus z) \oplus 1)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus D_y g_2(x \oplus z)\big) z_{n+1} \oplus \\ \oplus g_1(x \oplus z)(\ell_1(x \oplus z) \oplus x_{n+2} \oplus z_{n+2}) \oplus g_2(x \oplus z). \end{gathered}$$

Пусть $\ell_1(x \oplus z) = \ell_1(x) \oplus d$, где $d \in \mathbb{Z}_2$. Заметим, что если $z = \mathbf{0}$, то $d = 0$. Тогда

$$\begin{gathered} D_{(z, z_{n+1}, z_{n+2})} f(x, x_{n+1}, x_{n+2}) = x_{n+1} x_{n+2} \big(D_z D_y g_1(x)\big) \oplus \\ \oplus x_{n+1} \big(\ell_1(x) D_z D_y g_1(x) \oplus (z_{n+2} \oplus d) D_y g_1(x \oplus z) \oplus D_z D_y g_2(x) \oplus z_{n+2} \oplus d\big) \oplus \\ \oplus x_{n+2} \big(D_z g_1(x) \oplus z_{n+1}(D_y g_1(x \oplus z) \oplus 1)\big) \oplus \ell_1(x) D_z g_1(x) \oplus \\ \oplus z_{n+1}(D_y g_1(x \oplus z) \oplus 1) \ell_1(x) \oplus z_{n+1} d (D_y g_1(x \oplus z) \oplus 1) \oplus \\ \oplus z_{n+1} D_y g_2(x \oplus z) \oplus z_{n+1} z_{n+2}(D_y g_1(x \oplus z) \oplus 1) \oplus (z_{n+2} \oplus d) g_1(x \oplus z) \oplus D_z g_2(x). \end{gathered}$$

Докажем, что для любого ненулевого направления (z, z_{n+1}, z_{n+2}) функция $D_{(z, z_{n+1}, z_{n+2})} f$ не является константой. Предположим обратное. Пусть $D_{(z, z_{n+1}, z_{n+2})} f \equiv \text{const}$ для $(z, z_{n+1}, z_{n+2}) \neq (0, \ldots, 0)$.

Пусть $z_{n+1} = 0$. Тогда $D_z g_1(x) = 0$. Если $z_{n+2} = d$, то $z \neq \mathbf{0}$ и $D_{(z,0,d)}f$ имеет слагаемое $D_z g_2(x) = D_z\big(g_1(x) \oplus g_2(x)\big)$, которое не является константой, согласно лемме 9.

Если $z_{n+2} = d \oplus 1$, то $D_{(z,0,d\oplus 1)}f$ имеет слагаемое $g_1(x \oplus z) \oplus g_2(x \oplus z) \oplus g_2(x)$, которое для любого z не является константой, поскольку $g_2(x)$ уравновешенная, а $g_1(x \oplus z) \oplus g_2(x \oplus z)$ является бент-функцией, согласно лемме 8.

Пусть $z_{n+1} = 1$. Тогда

$$D_z g_1(x) = D_y g_1(x \oplus z) \oplus 1.$$

Заметим, что если $y = z$, то равенство не выполняется.

Если $z_{n+2} = d$, то $D_{(z,1,d)}f$ имеет слагаемое

$$\begin{aligned} D_y g_2(x \oplus z) \oplus D_z g_2(x) &= D_y\big(g_1(x \oplus z) \oplus g_2(x \oplus z)\big) \oplus D_z\big(g_1(x) \oplus g_2(x)\big) \oplus 1 = \\ &= D_{y\oplus z}\big(g_1(x) \oplus g_2(x)\big) \oplus 1, \end{aligned}$$

которое для $y \neq z$ не является константой, согласно лемме 9.

Если $z_{n+2} = d \oplus 1$, то $D_{(z,1,d\oplus 1)}f$ имеет слагаемое

$$g_1(x \oplus y \oplus z) \oplus D_y g_2(x \oplus z) \oplus D_z g_2(x) \oplus 1 = g_1(x \oplus y \oplus z) \oplus g_2(x \oplus y \oplus z) \oplus g_2(x) \oplus 1,$$

которое для любого z не является константой, поскольку $g_2(x)$ и $g_2(x) \oplus 1$ являются уравновешенными, а $g_1(x \oplus y \oplus z) \oplus g_2(x \oplus y \oplus z)$ — бент-функция, согласно лемме 8. Таким образом, $D_{(z,z_{n+1},z_{n+2})}f \not\equiv \mathrm{const}$ для любого $(z, z_{n+1}, z_{n+2}) \neq (0, \ldots, 0)$.

Пусть $\ell_1(x) = \langle b, x\rangle \oplus c$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$. Так как $D_y\ell_1(x) = y_{n+2}$, то $\langle b, y\rangle = y_{n+2}$. Из утверждения 2 следует, что f уравновешенная. ■

3.2. Корреляционно-иммунные функции

Приведём достаточные условия того, что функции из утверждения 2 являются корреляционно-иммунными.

Утверждение 3. Пусть $n \geqslant 2$ — чётное число, $g_1, g_2 \in \mathcal{F}_n$, $(y, 1, y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $b \in \mathbb{Z}_2^n$ такие, что $\langle b, y\rangle = y_{n+2}$ и $h(x, x_{n+1}, x_{n+2}) = \langle b, x\rangle \oplus c \oplus x_{n+2}$ для $c \in \mathbb{Z}_2$. Тогда если функции g_2 и $g_1 \oplus g_2$ являются корреляционно-иммунными порядка r, то функция $f \in \mathcal{F}_{n+2}$ из (1) корреляционно-иммунна порядка r. Если при этом g_2 уравновешенная, то f также уравновешенная.

Доказательство. Пусть $\ell_1(x) = \langle b, x\rangle \oplus c$, где $x \in \mathbb{Z}_2^n$. Можно убедиться, что $D_y\ell_1(x) = y_{n+2}$ для любого $x \in \mathbb{Z}_2^n$ и

$$h(x, x_{n+1}, x_{n+2}) = (D_y\ell_1(x) \oplus y_{n+2})x_{n+1} \oplus \ell_1(x) \oplus x_{n+2}.$$

Из теоремы 1 и леммы 3 для $f \in \mathcal{F}_{n+2}$ из (1) следует, что

$$|W_f(a, a_{n+1}, a_{n+2})| = \begin{cases} 2\,|W_{g_2}(a)|, & \text{если } \langle a, y\rangle = a_{n+1} \text{ и } a_{n+2} = 0, \\ 2\,|W_{g_2}(a \oplus b)|, & \text{если } \langle a, y\rangle = a_{n+1} \oplus y_{n+2} \text{ и } a_{n+2} = 1, \\ 2\,|W_{g_1\oplus g_2}(a)|, & \text{если } \langle a, y\rangle = a_{n+1} \oplus 1 \text{ и } a_{n+2} = 0, \\ 2\,|W_{g_1\oplus g_2}(a \oplus b)|, & \text{если } \langle a, y\rangle = a_{n+1} \oplus y_{n+2} \oplus 1 \text{ и } a_{n+2} = 1. \end{cases}$$

Тогда первое утверждение следует из леммы 12, а второе — из утверждения 2. ■

4. Построение уравновешенных функций с высокой нелинейностью

Используем итеративную конструкцию из теоремы 3 и уравновешенную функцию от 16 переменных с высокой нелинейностью, представленную в [18], для построения уравновешенных функций от чётного числа переменных $n \geqslant 18$ без линейных структур с нелинейностью

$$2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7}).$$

Сравним полученные значения нелинейности уравновешенных функций с верхней оценкой нелинейности из утверждения 1, а также со значениями нелинейности уравновешенных функций, полученных в других работах.

В [18] показано, как построить уравновешенную функцию от 16 переменных с нелинейностью 32 598. Мы использовали её в качестве уравновешенной функции g_2 из теоремы 3, чтобы получить уравновешенную булеву функцию от 18 переменных с высокой нелинейностью.

Пусть $\sigma_{2,16}$ — булева функция от 16 переменных, которая содержит все квадратичные слагаемые и только их, и $f_{16} = \sigma_{2,16} \oplus \bigoplus\limits_{i=1}^{n/2} x_i$. Тогда g_2 можно задать с помощью её носителя: $\operatorname{supp}(g_2) = \operatorname{supp}(f_{16}) \cup S$, где

$$S = \{8256, 2080, 4112, 2049, 36912, 5264, 34840, 10264, 49169, 38400, 1632, 3075, 2570, 16800, 16908, 1569, 24612, 12417, 29504, 17825, 37413, 18965, 41410, 16613, 5028, 35122, 21656, 61968, 42122, 8000, 24873, 9546, 21541, 10763, 35881, 57372, 45256, 42033, 37524, 19529, 7237, 16446, 17888, 20881, 26817, 49539, 14964, 54452, 51612, 22981, 20723, 989, 46868, 50830, 11884, 1518, 5363, 36553, 43729, 39321, 50459, 55401, 37771, 52359, 5965, 8511, 18551, 58538, 14987, 53799, 44090, 10156, 29283, 27057, 58443, 61497, 35782, 44047, 22940, 7540, 19865, 43961, 15221, 62179, 43927, 57240, 59741, 61867, 14190, 62511, 44665, 3067, 8107, 61937, 51161, 42937, 31835, 44725, 30435, 14324, 30381, 31964, 56506, 54652, 59951, 61206, 43993, 14310, 58959, 32494, 24443, 32381, 62451, 60915, 60381, 44990, 62845, 36351, 32508, 61147, 56309, 32351, 48503, 57215, 32751, 63483, 64510, 65535\}$$

и каждому числу из S ставится в соответствие вектор его двоичного представления длины 16.

В качестве $g_1 \oplus g_2$ мы взяли бент-функцию $\bigoplus\limits_{i=1}^{8} x_i x_{i+8} \oplus \prod\limits_{i=1}^{8} x_i$, которая, согласно лемме 10, принадлежит классу Мэйорана — МакФарланда. Пусть $\ell(x) = \bigoplus\limits_{i=2}^{18} x_i$ и $y = (1, 0, 0, \ldots, 0)$.

Итоговая уравновешенная булева функция f от 18 переменных, которая получается с помощью конструкции из теоремы 3, имеет степень 16, нелинейность $N_f = 130\,732$ и не имеет линейных структур. Стоит отметить, что конструкция из теоремы 3 позволяет получить больше одной функции от 18 переменных с указанной нелинейностью. Достаточно рассмотреть другие направления y, число которых равно $2^{17} - 1$ [19]. Эти направления — ненулевые векторы y, такие, что $\langle (0, 1, \ldots, 1), y \rangle = 0$. В качестве функции $g_1 \oplus g_2$ можно взять бент-функцию, полученную с помощью других известных конструкций бент-функций.

В свою очередь, полученную функцию f от 18 переменных можно использовать, чтобы построить уравновешенную функцию от 20 переменных с нелинейностью

523 608, так как из леммы 4 следует, что $\max\limits_{a\in\mathbb{Z}_2^{18}} W_f(a) = 680 = 2^{18/2} + 2^{18/2-2} + 2^{18/2-4} + + 2^{18/2-6}$. Кроме того, если в качестве $g_1 \oplus g_2$ снова взять бент-функцию, например, из класса Мэйорана — МакФарланда, то по теореме 3 полученная функция не будет иметь линейных структур.

Таким образом, итеративная конструкция из теоремы 3 позволяет строить уравновешенные функции f от чётного числа переменных $n \geqslant 18$ без линейных структур с нелинейностью

$$N_f = 2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7}), \tag{7}$$

поскольку $\max\limits_{a\in\mathbb{Z}_2^{n-2}} W_{g_2}(a) = 2^{(n-2)/2} + 2^{(n-2)/2-2} + 2^{(n-2)/2-4} + 2^{(n-2)/2-6}$.

В табл. 1 приведены значения нелинейности функций, которые можно получить с помощью теоремы 3, и значения нелинейности уравновешенных функций, полученных в работах К. Ху и др. [16] и К. Карле и др. [17]. Отметим, что в [16] рассматриваются значения $n \leqslant 28$, а нелинейность (7) имеют уравновешенные функции от чётного числа $n \geqslant 18$ переменных.

Таблица 1

n	$2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$	N_f [16]	N_f [17]
18	130 732	130 504	130 688
20	523 608	523 154	Не приводится
22	2 095 792	2 094 980	Не приводится
24	8 385 888	8 384 490	Не приводится
26	33 548 992	33 545 992	Не приводится
28	134 206 848	134 201 460	Не приводится

Из табл. 1 видно, что значения нелинейности уравновешенных функций, которые могут быть получены с помощью теоремы 3, превосходят значения из работ [16, 17].

В табл. 2 приводятся значения нелинейности функций, которые можно получить с помощью теоремы 3, и верхние оценки нелинейности уравновешенных функций из утверждения 1 для $18 \leqslant n \leqslant 28$.

Таблица 2

n	$2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$	$2^{n-1} - 2^{n/2-1} - 2$
18	130 732	130 814
20	523 608	523 774
22	2 095 792	2 096 126
24	8 385 888	8 386 558
26	33 548 992	33 550 334
28	134 206 848	134 209 534

5. Проблема разложения булевых функций в сумму двух бент-функций

Докажем верхнюю оценку степени функции $(f_1 \oplus f_2)h$, где h — булева функция от n переменных, f_1 и f_2 — бент-функции от n переменных, причём $h \oplus f_1$ и $h \oplus f_2$ также являются бент-функциями.

Вопрос о разложении булевых функций в сумму двух бент-функций поставлен Н. Н. Токаревой в работе [20].

Гипотеза 1 (Н. Н. Токарева [20]). Пусть n — чётное число. Тогда любая булева функция от n переменных степени не больше $n/2$ может быть разложена в сумму двух бент-функций от n переменных.

В [20] гипотеза 1 проверена с помощью полного перебора для $n \leqslant 6$. Согласно [20], если гипотеза 1 верна, то справедлива следующая нижняя оценка для числа бент-функций от n переменных:

$$|\mathcal{B}_n| \geqslant 2^{2^{n-2}+\binom{n}{n/2}/4}.$$

В [19] показана связь этой гипотезы со следующей проблемой о производных бент-функций: любая сбалансированная функция f от чётного числа переменных n степени не больше $n/2-1$, такая, что $f(x) = f(x \oplus y)$ для любого $x \in \mathbb{Z}_2^n$ и некоторого ненулевого $y \in \mathbb{Z}_2^n$, является производной бент-функции от n переменных. Эта связь также следует из теоремы 1.

Утверждение 4. Пусть $n \geqslant 2$ — чётное число, $g_1, g_2, h_1 \in \mathcal{F}_n$, вектор $(y, 1, y_{n+2}) \in \in \mathbb{Z}_2^{n+2}$ такой, что

$$h(x, x_{n+1}, x_{n+2}) = (D_y h_1(x) \oplus y_2)x_{n+1} \oplus h_1(x) \oplus x_{n+2}.$$

Тогда $f \in \mathcal{F}_{n+2}$ из (1) имеет функцию h своей производной по направлению $(y, 1, y_{n+2})$ и является бент-функцией от $n+2$ переменных тогда и только тогда, когда g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$, $g_1 \oplus g_2 \oplus h_1$ являются бент-функциями от n переменных.

Доказательство. Из леммы 4 и теоремы 1 следует, что

$$N_f = 2^{n+1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^{n+2}} |W_f(a)| = 2^{n+1} - 2^{n/2}$$

тогда и только тогда, когда для любого $b \in \mathbb{Z}_2^n$ справедливо

$$|W_{g_1 \oplus g_2}(b)| = |W_{g_2}(b)| = |W_{g_1 \oplus g_2 \oplus h_1}(b)| = |W_{g_2 \oplus h_1}(b)| = 2^{n/2}.$$

Из леммы 7 следует, что g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$, $g_1 \oplus g_2 \oplus h_1$ являются бент-функциями от n переменных. ■

Приведём два вспомогательных утверждения.

Утверждение 5 (Н. Н. Токарева [20]). Пусть f_1, f_2, f_3 — бент-функции от n переменных. Тогда функция f, определённая следующим образом:

$$\begin{aligned} f(0,0,x) &= f_1(x), & f(0,1,x) &= f_2(x), \\ f(1,0,x) &= f_3(x), & f(1,1,x) &= f_4(x), \end{aligned}$$

является бент-функцией от $n+2$ переменных тогда и только тогда, когда f_4 — бент-функция от n переменных и $\tilde{f}_1 \oplus \tilde{f}_2 \oplus \tilde{f}_3 \oplus \tilde{f}_4 = 1$.

Утверждение 5 является упрощённой версией результата из работы А. Канто и П. Шарпин 2003 г. [21]. В [21] доказано также

Утверждение 6 (А. Канто и П. Шарпин [21]). Пусть $f_1, f_2, f_3, f_4 \in \mathcal{F}_n$ и функция f, определённая следующим образом:

$$\begin{aligned} f(0,0,x) &= f_1(x), & f(0,1,x) &= f_2(x), \\ f(1,0,x) &= f_3(x), & f(1,1,x) &= f_4(x), \end{aligned}$$

является бент-функцией от $n+2$ переменных. Тогда f_1 — бент-функция, если и только если f_2, f_3, f_4 — бент-функции от n переменных.

Теорема 4. Пусть $n \geqslant 2$ — чётное число, $h \in \mathcal{F}_n$ и $f_1, f_2, h \oplus f_1, h \oplus f_2 \in \mathcal{B}_n$. Тогда:

1) $\deg((f_1 \oplus f_2)h) \leqslant (n+2)/2$;
2) следующие утверждения эквивалентны:
   а) $\varphi_1(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_1(x) \in \mathcal{B}_n$;
   б) $\varphi_2(x) = \big(f_1(x) \oplus f_2(x)\big)h(x) \oplus f_2(x) \in \mathcal{B}_n$;
   в) $\varphi_3(x) = \big(f_1(x \oplus y) \oplus f_2(x \oplus y)\big)h(x \oplus y) \oplus f_2(x \oplus y) \oplus h(x \oplus y) \in \mathcal{B}_n$, где $y \in \mathbb{Z}_2^n$;
   г) $\varphi_4(x) = \big(f_1(x \oplus y) \oplus f_2(x \oplus y)\big)h(x \oplus y) \oplus f_1(x \oplus y) \oplus h(x \oplus y) \in \mathcal{B}_n$, где $y \in \mathbb{Z}_2^n$;
   д) $\widetilde{\varphi_1} \oplus \widetilde{\varphi_2} \oplus \widetilde{\varphi_3} \oplus \widetilde{\varphi_4} \equiv 0$.

Доказательство. Пусть $y \in \mathbb{Z}_2^n$. Тогда $g \in \mathcal{F}_{n+2}$, такая, что

$$g(x, x_{n+1}, x_{n+2}) = \big(h(x) \oplus h(x \oplus y)\big)x_{n+1} \oplus h(x) \oplus x_{n+2},$$

удовлетворяет условию утверждения 4 для направления $(y, 1, 0)$. Следовательно, булева функция от $n+2$ переменных

$$f(x, x_{n+1}, x_{n+2}) = \big((D_y g_1(x) \oplus 1)g(x, x_{n+1}, x_{n+2}) \oplus D_y g_2(x)\big)x_{n+1} \oplus \\ \oplus g_1(x)g(x, x_{n+1}, x_{n+2}) \oplus g_2(x),$$

где $g_1 = f_1 \oplus f_2$ и $g_2 = f_2$, является бент-функцией от $n+2$ переменных. Из леммы 5 следует, что $\deg(f) \leqslant (n+2)/2$ и $\deg(g_1 h) = \deg((f_1 \oplus f_2)h) \leqslant (n+2)/2$.

Легко убедиться в том, что

$$f(x, 0, 0) = g_1(x)h(x) \oplus g_2(x) = \varphi_2(x),$$
$$f(x, 0, 1) = g_1(x)h(x) \oplus g_1(x) \oplus g_2(x) = \varphi_1(x),$$
$$f(x, 1, 0) = g_1(x \oplus y)h(x \oplus y) \oplus g_2(x \oplus y) \oplus h(x \oplus y) = \varphi_3(x),$$
$$f(x, 1, 1) = g_1(x \oplus y)h(x \oplus y) \oplus g_1(x \oplus y) \oplus g_2(x \oplus y) \oplus h(x \oplus y) \oplus 1 = \varphi_4(x) \oplus 1.$$

Тогда из утверждений 5 и 6 следует второе утверждение теоремы. ■

Следствие 1. Пусть $h, g \in \mathcal{F}_n$ и $\deg(hg) > (n+2)/2$. Тогда если $f_1, f_2 \in \mathcal{B}_n$ и $h \equiv f_1 \oplus f_2$, то хотя бы одна из функций $g \oplus f_1$ или $g \oplus f_2$ не является бент-функцией.

Следствие 2. Пусть $h \in \mathcal{F}_n$ и $f_1, f_2, h \oplus f_1, h \oplus f_2 \in \mathcal{B}_n$. Тогда если $(f_1 \oplus f_2)h \equiv 0$ или $(f_1 \oplus f_2)h \equiv h$, при этом $f_3(x) = h(x \oplus y) \oplus f_1(x \oplus y)$ и $f_4(x) = h(x \oplus y) \oplus f_2(x \oplus y)$, где $y \in \mathbb{Z}_2^n$, то справедливо, что $\widetilde{f_1} \oplus \widetilde{f_2} \equiv \widetilde{f_3} \oplus \widetilde{f_4}$.

В обозначениях теоремы 4 приведём пример того, как верхняя оценка степени функции $(f_1 \oplus f_2)h$ может быть использована для описания бент-функций f_1 и f_2.

Пусть $h(x) = x_1 x_2$ — булева функция от четырёх переменных, $x \in \mathbb{Z}_2^4$, и $f_1, f_2 \in \mathcal{B}_4$ такие, что $h \oplus f_1$ и $h \oplus f_2$ являются бент-функциями. Положим, что АНФ функции f_1 содержит моном $x_3 x_4$, а АНФ функции f_2 его не содержит. Тогда $\deg((f_1 \oplus f_2)h) = 4 > 3 = (n+2)/2$. Таким образом, либо каждая бент-функция из разложения функции $h(x)$ в сумму двух бент-функций имеет моном $x_3 x_4$ в своей АНФ, либо каждая из них его не имеет. Пример достижения оценки можно получить для следующих функций от четырёх переменных: $h(x) = x_3$, $f_1(x) = x_1 x_2 \oplus x_3 x_4$ и $f_2(x) = x_1 x_3 \oplus x_2 x_4$.

Заключение

Работа посвящена вопросу построения уравновешенных булевых функций с высокими значениями нелинейности. Приведена итеративная конструкция уравновешенных функций от чётного числа переменных, с помощью которой получена булева функция от 18 переменных со значением нелинейности 130 732. Эта функция может быть

использована для итеративного построения уравновешенных функций от чётного числа $n \geqslant 20$ переменных с нелинейностью $2^{n-1} - (2^{n/2-1} + 2^{n/2-3} + 2^{n/2-5} + 2^{n/2-7})$.

Приведены достаточные условия того, что функции, полученные с помощью конструкции, обладают такими свойствами, как отсутствие линейных структур и корреляционная иммунность. Интерес представляет также изучение дополнительных условий, при которых получаемые функции будут, например, удовлетворять строгому лавинному критерию (SAC) или критерию распространения $\mathrm{PC}(k)$ порядка k.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
2. *Rothaus O. S.* On bent functions // J. Comb. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
3. *Adams C. M.* Constructing symmetric ciphers using the CAST design procedure // Des. Codes Cryptogr. 1997. V. 12. No. 3. P. 283–316.
4. *Hell C., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. Seattle, WA, USA, 2006. P. 1614–1618.
5. *Zheng Y., Pieprzyk J., and Seberry J.* Haval — a one-way hashing algorithm with variable length of output (extended abstract) // LNCS. 1993. V. 718. P. 83–104.
6. *Helleseth T. and Kholosha A.* Bent functions and their connections to combinatorics / S. R. Blackburn, S. Gerke, and M. Wildon (eds.). Surveys in Combinatorics. London Math. Soc. Lecture Note Ser. 2013. V. 409. Cambridge: Cambridge University Press, 2013. P. 91–126.
7. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. London: Acad. Press, 2015.
8. *Токарева Н. Н.* О множестве производных булевой бент-функции // Прикладная дискретная математика. Приложение. 2016. № 9. С. 327–350.
9. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.
10. *Dillon J. F.* Elementary Hadamard Difference Sets. PhD. Thesis. Univ. of Maryland, 1974.
11. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
12. *Siegentaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. 30. No. 5. P. 776–780.
13. *Seberry J., Zhang X-M., and Zheng Y.* Nonlinearly balanced Boolean functions and their propagation characteristics // LNCS. 1994. V. 773. P. 49–60.
14. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // LNCS. 1994. V. 1008. P. 61–74.
15. *Dobbertin H. and Leander G.* Cryptographer's Toolkit for Construction of 8-bit Bent Functions. Cryptology ePrint Archive. Report 2005/089. 2005.
16. *Hu X., Yang B., and Huang M.* A construction of highly nonlinear Boolean functions with optimal algebraic immunity and low hardware implementation cost // Discr. Appl. Math. 2020. V. 285. P. 407–422.
17. *Carlet C., Djurasevic M., Jakobovic D., et al.* Evolving Constructions for Balanced, Highly Nonlinear Boolean Functions. `https://arxiv.org/abs/2202.08743`. 2022.
18. *Gini A. and Meaux P.* Weightwise perfectly balanced functions and nonlinearity // LNCS. 2023. V. 13874. P. 386–397.
19. *Shaporenko A.* Derivatives of bent functions in connection with the bent sum decomposition problem // Des. Codes Cryptogr. 2023. V. 91. P. 1607–1625.
20. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609–621.

21. *Canteaut A. and Charpin P.* Decomposing bent functions // IEEE Trans. Inform. Theory. 2003. V. 49. No. 8. P. 2004–2019.

REFERENCES

1. *Matsui M.* Linear cryptanalysis method for DES cipher. LNCS, 1994, vol. 765, pp. 386–397.
2. *Rothaus O. S.* On bent functions. J. Comb. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.
3. *Adams C. M.* Constructing symmetric ciphers using the CAST design procedure. Des. Codes Cryptogr., 1997, vol. 12, no. 3, pp. 283–316.
4. *Hell C., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128. IEEE Intern. Symp. Inform. Theory, Seattle, WA, USA, 2006, pp. 1614–1618.
5. *Zheng Y., Pieprzyk J., and Seberry J.* Haval — a one-way hashing algorithm with variable length of output (extended abstract). LNCS, 1993, vol. 718, pp. 83–104.
6. *Helleseth T. and Kholosha A.* Bent functions and their connections to combinatorics. S. R. Blackburn, S. Gerke, and M. Wildon (eds.). Surveys in Combinatorics. London Math. Soc. Lecture Note Ser., 2013, vol. 409, Cambridge, Cambridge University Press, 2013, pp. 91–126.
7. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. London, Acad. Press, 2015.
8. *Tokareva N. N.* O mnozhestve proizvodnykh bulevoy bent-funktsii [On the set of derivatives of a Boolean bent function]. Prikladnaya diskretnaya matematika. Prilozhenie, 2016, no. 9, pp. 327–350. (in Russian)
9. *McFarland R. L.* A family of difference sets in non-cyclic groups. J. Combin. Theory, Ser. A, 1973, vol. 15, pp. 1–10.
10. *Dillon J. F.* Elementary Hadamard Difference Sets. PhD. Thesis, Univ. of Maryland, 1974.
11. *Logachev O. A., Salnikov A. A., and Yashchenko V. V.* Boolean Functions in Coding Theory and Cryptography. AMS, 2012. 334 p.
12. *Siegentaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, 1984, vol. 30, no. 5. pp. 776–780.
13. *Seberry J., Zhang X-M., and Zheng Y.* Nonlinearly balanced boolean functions and their propagation characteristics. LNCS, 1994, vol. 773, pp. 49–60.
14. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity. LNCS, 1994, vol. 1008, pp. 61–74.
15. *Dobbertin H. and Leander G.* Cryptographer's Toolkit for Construction of 8-bit Bent Functions. Cryptology ePrint Archive, report 2005/089, 2005.
16. *Hu X., Yang B., and Huang M.* A construction of highly nonlinear Boolean functions with optimal algebraic immunity and low hardware implementation cost. Discrete Appl. Math., 2020, vol. 285, pp. 407–422.
17. *Carlet C., Djurasevic M., Jakobovic D., et al.* Evolving Constructions for Balanced, Highly Nonlinear Boolean Functions. `https://arxiv.org/abs/2202.08743`. 2022.
18. *Gini A. and Meaux P.* Weightwise perfectly balanced functions and nonlinearity. LNCS, 2023, vol. 13874, pp. 386–397.
19. *Shaporenko A.* Derivatives of bent functions in connection with the bent sum decomposition problem. Des. Codes Cryptogr., 2023, vol. 91, pp. 1607–1625.
20. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses. Adv. Math. Commun., 2011, vol. 5, no. 4, pp. 609–621.
21. *Canteaut A. and Charpin P.* Decomposing bent functions. IEEE Trans. Inform. Theory, 2003, vol. 49, no. 8, pp. 2004–2019.