УДК 519.7 DOI 10.17223/2226308X/13/9

ОЦЕНКА НЕЛИНЕЙНОСТИ СБАЛАНСИРОВАННЫХ БУЛЕВЫХ ФУНКЦИЙ, ПОРОЖДЁННЫХ ОБОБЩЁННОЙ КОНСТРУКЦИЕЙ ДОББЕРТИНА[1]

И. А. Сутормин

Предложено обобщение конструкции Доббертина для высоконелинейных сбалансированных булевых функций. Исследован спектр Уолша — Адамара и получены оценки спектрального радиуса предложенных функций. Доказана точная верхняя оценка на спектральный радиус (нижняя оценка нелинейности) и предложен способ построить сбалансированную функцию Θ от $2n$ переменных при помощи сбалансированной θ от $n-k$ переменных со спектральным радиусом $R_\Theta = 2^n + 2^k R_\theta$, где R_Θ и R_θ — спектральные радиусы Θ и θ соответственно.

Ключевые слова: *булевы функции, бент-функции, сбалансированность, нелинейность, спектральный радиус.*

В различных криптографических алгоритмах часто используются булевы функции. Нелинейность — одно из основных для них свойств, оно показывает, насколько хорошо функцию можно приблизить некоторой линейной 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.

Введём необходимые определения. *Преобразование Уолша — Адамара* булевой функции f определяется как $W_f(a) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle x,a\rangle}$, $a \in \mathbb{F}_2^n$; *спектральный радиус* $R_f = \max\limits_{a \in \mathbb{F}_2^n} |W_f(a)|$ и *нелиненость* $N_f = 2^{n-1} - R_f/2$. *Бент-функциями* называются функции от чётного числа переменных с максимальной возможной нелинейностью. Они впервые описаны в [1]. Подробную информацию об этом классе функций можно найти в [2, 3]. Булевы функции f и g от n переменных *аффинно эквивалентны*, если для всех x выполнено $g(x) = f(Ax+b)$, где A — невырожденная матрица размера $n \times n$; b — вектор длины n.

В практических целях часто требуется чтобы функция была *сбалансированной* — принимала значения 0 и 1 на одном и том же числе аргументов. Но максимальное значение нелинейности сбалансированных функций неизвестно, начиная уже с восьми переменных. Лучшие оценки получаются как следствие конкретных конструкций сбалансированных функций.

Конструкция, описанная Доббертином в [4], основана на модификации нормальных бент функций — функций от $2n$ переменных, постоянных на некотором аффинном подпространстве L размерности n. Суть конструкции заключается в замене значений бент-функции на подпространстве L значениями сбалансированной функции θ от n переменных. При этом спектральный радиус получившейся сбалансированной функции Θ равен $R_\Theta = 2^n + R_\theta$, а её нелинейность — $N_\Theta = 2^{2n-1} - 2^{n-1} - R_\theta/2$. В [4] сформулирована не опровергнутая до сих пор гипотеза о несуществовании сбалансированных функций с нелинейностью выше, чем можно получить при помощи этой конструкции.

[1]Работа выполнена в рамках государственного задания Института математики им. С. Л. Соболева СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 20-31-70043) и Лаборатории криптографии JetBrains Research.

Рассмотрим обобщение конструкции Доббертина, использующее бент-функции с близкими к нормальности свойствами, а именно бент-функции от $2n$ переменных, принимающие постоянное значение на нескольких сдвигах некоторого подпространства L размерности $n-k$, $0 \leqslant k \leqslant n-2$. Так как аффинная эквивалентность сохраняет нелинейность и сбалансированность, можно без ограничения общности рассматривать такие бент-функции в виде $f : \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{n+k} \to \mathbb{F}_2$, для которой существуют подмножества $I_0, I_1 \subset \mathbb{F}_2^{n+k}$ мощностей $|I_0| = 2^{2k-1} + 2^{k-1}$, $|I_1| = 2^{2k-1} - 2^{k-1}$, для которых справедливо

$$f(x,y) \equiv 0 \ \text{ при } y \in I_0,$$
$$f(x,y) \equiv 1 \ \text{ при } y \in I_1.$$

Такое представление прямо связано с конструкцией вида $\widetilde{f} + \mathrm{Ind}_{L^\perp}$, подробную информацию о которой можно найти в [5–7]. Здесь $\widetilde{f}$ — дуальная к f функция [3].

При помощи бент-функции такого вида и набора θ_y, $y \in I_0 \cup I_1$, сбалансированных функций от $n-k$ переменных строится обобщающая конструкцию Доббертина функция Θ:

$$\Theta(x,y) = \begin{cases} \theta_y(x) & \text{при } y \in I_0 \cup I_1, \\ f(x,y) & \text{иначе.} \end{cases} \tag{1}$$

При $k = 0$ описанная конструкция полностью совпадает с конструкцией Доббертина, при $k = 1$ она также эквивалентна конструкции Доббертина.

Теорема 1. Функция Θ вида (1) является сбалансированной функцией и её коэффициенты Уолша — Адамара вычисляются по формуле

$$W_\Theta(a,b) = \begin{cases} W_f(a,b) + \sum\limits_{y \in I_0 \cup I_1} (-1)^{\langle b,y \rangle} W_{\theta_y}(a), & \text{если } a \neq 0, \\ 0 & \text{иначе.} \end{cases}$$

Следствие 1. Спектральный радиус Θ не превосходит $2^n + \sum\limits_{y \in I_0 \cup I_1} R_{\theta_y}$, причём всегда можно выбрать θ_y, при которых оценка достигается.

Теорема 2. Пусть θ — сбалансированная функция $n-k$ переменных, $\theta_y = \theta$ при $y \in I_0$ и $\theta_y = \theta \oplus 1$ при $y \in I_1$. Тогда

$$R_\Theta = 2^n + 2^k R_\theta.$$

Получившееся R_Θ зависит от R_θ, k и n. Несмотря на то, что θ является функцией от $n-k$ переменных, наилучший результат достигается при $k = 0$, то есть в случае, описанном Доббертином.

ЛИТЕРАТУРА

1. *Rothaus O.* On "bent" functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *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.
3. *Tokareva N. N.* Bent Functions. Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
4. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // LNCS. 1994. V. 1008. P. 61–74.

5. *Kolomeec N.* On properties of a bent function secondary construction // Proc. BFA'2020. https://boolean.w.uib.no/bfa-2020.
6. *Коломеец Н. А.* О некоторых свойствах конструкции бент-функций с помощью подпространств произвольной размерности // Прикладная дискретная математика. Приложение. 2018. № 11. С. 41–43.
7. *Carlet C.* Two new classes of bent functions // LNCS. 1994. V. 765. P. 77–101.

УДК 519.7 DOI 10.17223/2226308X/13/10

СВЯЗЬ МЕЖДУ КВАТЕРНАРНЫМИ И КОМПОНЕНТНЫМИ БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. С. Шапоренко

Исследуются кватернарные бент-функции. Функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется кватернарной функцией от n переменных. Доказано, что свойство кватернарной функции $g(x + 2y) = a(x, y) + 2b(x, y)$ быть бент напрямую не зависит от того, являются ли функции b и $a \oplus b$ булевыми бент-функциями. Получено количество кватернарных бент-функций от одной и двух переменных с описанием свойств булевых функций b и $a \oplus b$. Представлены простые конструкции кватернарных бент-функций от любого числа переменных.

Ключевые слова: *кватернарные функции, булевы функции, бент-функции.*

Пусть $\langle x, y\rangle$ обозначает скалярное произведение двоичных векторов x и y по модулю 2, а $x.y$ — их скалярное произведение по модулю 4.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. *Преобразованием Уолша — Адамара булевой функции* f от n переменных называется целочисленная функция $W_f(x)$, заданная на множестве $\mathbb{Z}_2^n$ равенством

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

Булева функция f от чётного числа n переменных называется *бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$.

Шифры, в которых используются бент-функции, более устойчивы к *линейному криптоанализу* [1], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции используются в блочном шифре CAST как координатные функции S-блоков [2], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре Grain [3]. Бент-функции связаны также с некоторыми объектами теории кодирования, например с кодами Рида — Маллера [4].

Функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *кватернарной функцией* от n переменных [5]. *Преобразование Уолша — Адамара кватернарной функции* g определяется следующим образом:

$$W_g(x) = \sum_{y \in \mathbb{Z}_4^n} i^{x.y+g(y)},$$

где «+» означает сложение по модулю 4.

[1]Работа выполнена в рамках государственного задания Института математики им. С. Л. Соболева СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 18-07-01394) и Лаборатории криптографии JetBrains Research.