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.

Кватернарная функция g от n переменных называется *бент-функцией*, если $|W_g(x)| = 4^{n/2}$ для любого $x \in \mathbb{Z}_4^n$.

Целью данной работы является изучение связи свойств «быть бент» кватернарных и булевых функций. Эта задача впервые поставлена в работе [6] (см. также [7]).

Каждая кватернарная функция g от n переменных может быть представлена для любых $x, y \in \mathbb{Z}_2^n$ следующим образом:

$$g(x + 2y) = a(x, y) + 2b(x, y).$$

Здесь сложение производится по модулю 4, а функции a и b — это *компонентные* булевы функции от $2n$ переменных.

Утверждение 1. Для любой кватернарной функции $g(x+2y) = a(x, y)+2b(x, y)$ от одной переменной, где $x, y \in \mathbb{Z}_2$, справедливо, что g — кватернарная бент-функция тогда и только тогда, когда $b(x, y)$ — бент-функция и $a(x, y)$ равна $0, 1, x$ или $x \oplus 1$. Кроме того, если g — кватернарная бент-функция, то b и $a \oplus b$ — булевы бент-функции.

Компьютерные вычисления показали, что количество кватернарных бент-функций от одной переменной равно 32.

Количество кватернарных бент-функций при $n = 2$ равно 200704. Среди них 98304 таких функций, что ни одна из булевых функций a, b и $a \oplus b$ не является бент-функцией, но при этом для 3072 из них a линейная. Существуют 36864 функции, таких, что b и $a \oplus b$ — бент-функции, при этом для 33792 из них функция a нелинейная, а для 2304 и 768 a является линейной функцией или константой соответственно. Количество кватернарных функций, для которых каждая из функций a, b и $a \oplus b$ — бент-функция, равно 16384. Для оставшихся 49152 функций a является бент-функцией, b и $a \oplus b$ — нелинейные булевы функции.

Теорема 1. Пусть $g(x + 2y) = a(x, y) + 2b(x, y)$ — кватернарная бент-функция, где $x, y \in \mathbb{Z}_2^n$; a, b — булевы функции от $2n$ переменных. Тогда b и $a \oplus b$ — нелинейные функции при любом числе переменных $n \geqslant 1$.

Следующие два утверждения показывают, что между свойствами «быть бент» кватернарной функции g и её компонентных булевых функций b и $a \oplus b$ нет прямой связи.

Утверждение 2. Для любого $n \geqslant 2$ существует кватернарная бент-функция $g(x+2y) = a(x, y)+2b(x, y)$ от n переменных, где b и $a \oplus b$ не являются бент-функциями от $2n$ переменных.

Утверждение 3. Для любого n существует кватернарная функция $g(x + 2y) = a(x, y) + 2b(x, y)$ от n переменных, которая не является бент-функцией, когда b и $a \oplus b$ — булевы бент-функции от $2n$ переменных.

Представим две простые конструкции для кватернарных бент-функций от любого числа переменных.

Утверждение 4. Кватернарная функция от n переменных

$$g(x_1 + 2x_{n+1}, \ldots, x_n + 2x_{2n}) = \sum_{i=1}^{n} 2x_i x_{i+n} + cx_j,$$

где $c \in \mathbb{Z}_2$, $j \in \{1, \ldots, n\}$ и «+» — сложение по модулю 4, является бент-функцией при любом n. Заметим, что при этом

$$b(x_1, \ldots, x_{2n}) = \bigoplus_{i=1}^{n} x_i x_{i+n} \quad \text{и} \quad a(x_1, \ldots, x_{2n}) \oplus b(x_1, \ldots, x_{2n}) = \bigoplus_{i=1}^{n} x_i x_{i+n} \oplus cx_j$$

— бент-функции от $2n$ переменных.

Утверждение 5. Пусть $g(x+2y) = a(x,y)+2b(x,y)$, где $x, y \in \mathbb{Z}_2^n$ и a, b — булевы функции от $2n$ переменных, является бент-функцией. Тогда функция $g'(x+2y) = 3a(x,y)+2b(x,y)$ также является кватернарной бент-функцией от $n \geqslant 1$ переменных.

Отметим, что утверждение верно и в обратную сторону.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // Eurocrypt'1993. LNCS. 1994. V. 765. P. 386–397.
2. *Adams C.* Constructing symmetric ciphers using the CAST design procedure // Design, Codes, and Cryptography. 1997. V. 12. No. 3. P. 283–316.
3. *Hell M., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. Seattle, WA, 2006. P. 1614–1618.
4. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
5. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. 1985. V. 40. No. 1. P. 90–107.
6. *Solé P. and Tokareva N.* Connections Between Quaternary and Binary Bent Functions // Cryptology ePrint Archive, Report 2009/544. `http://eprint.iacr.org/`.
7. *Solé P. and Tokareva N.* On quaternary and binary bent functions // Прикладная дискретная математика. Приложение. 2009. № 1. С. 16–18.

UDC 519.7 DOI 10.17223/2226308X/13/11

ON A SECONDARY CONSTRUCTION OF QUADRATIC APN FUNCTIONS[1]

K. V. Kalgin, V. A. Idrisova

Almost perfect nonlinear functions possess the optimal resistance to the differential cryptanalysis and are widely studied. Most known constructions of APN functions are obtained as functions over finite fields $\mathbb{F}_{2^n}$ and very little is known about combinatorial constructions in $\mathbb{F}_2^n$. We consider how to obtain a quadratic APN function in $n+1$ variables from a given quadratic APN function in n variables using special restrictions on new terms.

Keywords: *vectorial Boolean function, APN function, quadratic function, secondary construction.*

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 a 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):

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

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

[1]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 RFBR (projects no. 18-07-01394, 20-31-70043) and Laboratory of Cryptography JetBrains Research.