

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  $n \geq 2$  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  $i = 1, 2, \dots, \lceil n/2 \rceil$ .

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<sup>1</sup>

А. В. Куценко

Бент-функции вида  $\mathbb{F}_2^n \rightarrow \mathbb{Z}_q$ , где  $q \geq 2$  — 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  $\mathbb{F}_2^4 \rightarrow \mathbb{Z}_4$ .

**Ключевые слова:** самодуальная бент-функция, обобщённая бент-функция, класс Елисеева — Мэйорана — МакФарланда, расстояние Ли.

<sup>1</sup>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  $\mathbb{F}_2^n \rightarrow \mathbb{Z}_q$ . 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  $\bigoplus_{i=1}^n x_i y_i$ . *Весом Хэмминга*  $\text{wt}(x)$  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  $\text{dist}(f, g)$ . Согласно [1], назовём ортогональной группой порядка  $n$  над полем  $\mathbb{F}_2$  группу

$$\mathcal{O}_n = \{L \in \text{GL}(n, \mathbb{F}_2) : LL^T = I_n\},$$

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  $H_f : \mathbb{F}_2^n \rightarrow \mathbb{C}$ , 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  $\text{wt}_L(x) = \min\{x, q - x\}$ . *Расстояние Ли*  $\text{dist}_L(f, g)$  между функциями  $f, g \in \mathcal{GF}_n^q$  определяется как

$$\text{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \text{wt}_L(\delta(x)),$$

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  $\tilde{f} \in \mathcal{GF}_n^q$ , такая, что  $H_f(y) = \omega^{\tilde{f}(y)} 2^{n/2}$ , то бент-функция  $f$  называется *регулярной*, а функция  $\tilde{f}$  — дуальной к  $f$ . Дуальная функция также является регулярной обобщённой бент-функцией. Если  $f = \tilde{f}$ , то  $f$  называется *самодуальной* обобщённой бент-функцией. Если  $f = \tilde{f} + q/2$ , то  $f$  называется *антисамодуальной* обобщённой бент-функцией. Всюду далее считается, что  $q$  — чётное натуральное число.

Открытой проблемой является полная характеристика и описание класса булевых самодуальных бент-функций ( $q = 2$ ). Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящено большое количество работ (С. 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  $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$ , где  $p$  простое. Получен ряд результатов, в частности представлена полная классификация квадратичных самодуальных бент-функций. Связь самодуальных обобщённых бент-функций вида  $\mathbb{F}_2^n \rightarrow \mathbb{Z}_4$  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  $\mathbb{F}_2^n \rightarrow \mathbb{Z}_q$ , 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  $\pi$  — 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

$$f(x, y) = \frac{q}{2} \langle x, \pi(y) \rangle + g(y), \quad x, y \in \mathbb{F}_2^{n/2},$$

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  $L \in \mathcal{O}_{n/2}$ ;  $b \in \mathbb{F}_2^{n/2}$ ;  $\text{wt}(b)$  — 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  $\text{Sp}_L$ .

**Теорема 1.** Справедливо

$$\text{Sp}_L = \{q \cdot 2^{n-2}\} \cup \bigcup_{w=0}^{q/2} \bigcup_{r=0}^{n/2-1} \left\{ q \cdot 2^{n-2} \left( 1 \pm \frac{1}{2^r} \right) \mp w \cdot 2^{n-r} \right\}.$$

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  $\lambda_0, \lambda_1, \dots, \lambda_n \in \mathbb{Z}_q$ .

Далее представлен класс отображений, сохраняющих (анти)самодуальность обобщённой бент-функции.

**Теорема 3.** Отображения множества всех обобщённых булевых функций от  $n$  переменных в себя, имеющие вид

$$f(x) \longrightarrow f(L(x \oplus c)) + \frac{q}{2}\langle c, x \rangle + d, \quad x \in \mathbb{F}_2^n,$$

где  $L \in \mathcal{O}_n$ ,  $c \in \mathbb{F}_2^n$ ,  $\text{wt}(c)$  — 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. *Çeşmelioglu 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.