5. *Szabados T.* A Simple Wide Range Approximation of Symmetric Binomial Distributions. Preprint arXiv:1612.01112 [math.PR]. 2016.
6. *Agievich S.* On the representation of bent functions by bent rectangles // Probabilistic Methods in Discrete Mathematics: Fifth Intern. Conf. (Petrozavodsk, Russia, June 1–6, 2000). Utrecht, Boston: VSP, 2002. P. 121–135.
7. *Agievich S.* Bent rectangles // Proc. NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007). Amsterdam: IOS Press, 2008. P. 3–22.

УДК 519.7 DOI 10.17223/2226308X/13/5

О МЕТРИЧЕСКИХ СВОЙСТВАХ МНОЖЕСТВА САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Приводится обзор известных метрических свойств множества самодуальных бент-функций. Бент-функция называется самодуальной, если она совпадает со своей дуальной бент-функцией, и анти-самодуальной, если совпадает с отрицанием своей дуальной. Приводится полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда. Даются результаты, касающиеся характеризации булевых функций, находящихся на максимально возможном удалении от множества самодуальных бент-функций. Описаны группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций от n переменных, автоморфизмы множества булевых функций от n переменных, которые меняют местами множества самодуальных и анти-самодуальных бент-функций, изометричные отображения, сохраняющие неизменным отношение Рэлея каждой булевой функции от n переменных. Даётся характеризация всех изометричных отображений, сохраняющих максимальную нелинейность и расстояние Хэмминга между каждой бент-функций и дуальной к ней.

Ключевые слова: *булева функция, самодуальная бент-функция, расстояние Хэмминга, изометричное отображение, метрическая регулярность, группа автоморфизмов, отношение Рэлея.*

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. *Булевой функцией* от n переменных называется отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. Множество всех булевых функций от n переменных обозначается через $\mathcal{F}_n$. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначим скалярное произведение $\bigoplus_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется число его ненулевых координат. *Расстоянием Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается $\mathrm{dist}(f, g)$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

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

[1]Работа выполнена в рамках государственного задания ИМ СО РАН (проект №0314-2019-0017) при поддержке РФФИ (проекты № 18-07-01394, 20-31-70043) и Лаборатории криптографии JetBrains Research.

Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [1]. Для множества бент-функций от n переменных используется обозначение $\mathcal{B}_n$. Для каждой $f \in \mathcal{B}_n$ однозначным образом из соотношения $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ определяется *дуальная* к ней бент-функция $\widetilde{f} \in \mathcal{B}_n$. Бент-функция f называется *самодуальной* (*анти-самодуальной*), если $f = \widetilde{f}$ (соответственно $f = \widetilde{f} \oplus 1$). Множества самодуальных и анти-самодуальных бент-функций от n переменных обозначаются через $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ соответственно [2].

Открытой проблемой является полная характеризация и описание класса самодуальных бент-функций. Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящён ряд работ (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в работе [3] приведена аффинная классификация самодуальных бент-функций от $2, 4, 6$ переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность. В [2] дана классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность, можно найти в [4]. Верхняя оценка количества самодуальных бент-функций приведена в [5]. В работах [6 – 8] представлены конструкции самодуальных бент-функций. Связь самодуальных кватернарных бент-функций и самодуальных булевых бент-функций отмечена в [9].

Согласно [10], 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 $\mathbb{F}_2$.

Далее представлены известные результаты, касающиеся метрических свойств самодуальных бент-функций, опубликованные в работах [11 – 16].

1. Самодуальные бент-функции Мэйорана — МакФарланда

Бент-функции от $2k$ переменных, представимые в виде

$$f(x, y) = \langle x, \pi(y) \rangle \oplus g(y), \quad x, y \in \mathbb{F}_2^k,$$

где π — перестановка на множестве $\mathbb{F}_2^k$ и g — булева функция от k переменных, образуют известный класс *Мэйорана — МакФарланда* [17]. Данный класс имеет мощность $2^k! \cdot 2^{2^k}$.

Через $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$) обозначим множество самодуальных (анти-самодуальных) бент-функций от n переменных из класса Мэйорана — МакФарланда. В работе [3] найдены необходимые и достаточные условия самодуальности бент-функций из класса Мэйорана — МакФарланда, а именно: бент-функция $f(x, y)$ Мэйорана — МакФарланда принадлежит множеству $\mathrm{SB}^+_{\mathcal{M}}(2k)$ тогда и только тогда, когда

$$\pi(y) = L(y \oplus c), \quad g(y) = \langle c, y \rangle \oplus d, \quad y \in \mathbb{F}_2^k,$$

где $L \in \mathcal{O}_k$; $c \in \mathbb{F}_2^k$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2^n$. Заметим, что $\left|\mathrm{SB}^+_{\mathcal{M}}(2k)\right| = 2^k \cdot |\mathcal{O}_k|$.

Всюду далее предполагаем, что n — чётное натуральное число. В [11] исследованы возможные расстояния Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Теорема 1 [11]. Пусть $n \geqslant 4$ и $f, g \in \mathrm{SB}^+_{\mathcal{M}}(n) \cup \mathrm{SB}^-_{\mathcal{M}}(n)$, тогда

$$\mathrm{dist}(f,g) \in \left\{ 2^{n-1}, 2^{n-1}\left(1 \pm \frac{1}{2^r}\right), r = 0, 1, \ldots, n/2-1 \right\}.$$

Более того, если $f, g \in \mathrm{SB}^+_{\mathcal{M}}(n)$ или $f, g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, то все приведённые расстояния, кроме 2^{n-1}, являются достижимыми. Для произвольной пары функций $f \in \mathrm{SB}^+_{\mathcal{M}}(n)$ и $g \in \mathrm{SB}^-_{\mathcal{M}}(n)$ справедливо $\mathrm{dist}(f,g) = 2^{n-1}$.

Анализ приведённых расстояний позволяет вычислить минимальное расстояние Хэмминга между рассматриваемыми функциями.

Следствие 1. Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между самодуальными бент-функциями от n переменных из класса Мэйорана — МакФарланда равно 2^{n-2}.

В силу того, что минимальное расстояние Хэмминга между квадратичными булевыми функциями от n переменных (кодовыми словами кода Рида — Маллера $\mathrm{RM}(2,n)$) не меньше чем 2^{n-2} [18], получаем следующее

Следствие 2. Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между квадратичными булевыми функциями достижимо на самодуальных бент-функциях от n переменных из класса Мэйорана — МакФарланда.

2. Метрическая регулярность

Известно [19], что минимальное расстояние Хэмминга между бент-функциями от n переменных равно $2^{n/2}$. В работе [12] доказано, что при $n \geqslant 4$ данное расстояние достижимо на множестве (анти-)самодуальных бент-функций.

Утверждение 1 [12]. Пусть $n \geqslant 4$, тогда минимальное расстояние Хэмминга между (анти-)самодуальными бент-функциями от n переменных равно $2^{n/2}$.

Пусть $A \subseteq \mathbb{F}_2^n$ — произвольное множество и $y \in \mathbb{F}_2^n$ — произвольный двоичный вектор. Расстояние от вектора y до множества A определяется как $\mathrm{dist}(y,A) = \min\limits_{x \in A} \mathrm{dist}(y,x)$. *Радиусом покрытия* множества A называется число $\mathrm{d}(A) = \max\limits_{y \in \mathbb{F}_2^n} \mathrm{dist}(y,A)$. Множество двоичных векторов, находящихся на расстоянии $\mathrm{d}(A)$ от множества $A \subseteq \mathbb{F}_2^n$, называется *метрическим дополнением* множества A и обозначается $\widehat{A}$ [20]. Если $\widehat{\widehat{A}} = A$, то множество A называется *метрически регулярным*.

Рассматривая данные определения применительно к векторам значений булевых функций, можно определить *радиус покрытия*, *метрическое дополнение* и *метрическую регулярность* произвольного подмножества $M \subseteq \mathcal{F}_n$ [21].

В [3] доказано, что радиус покрытия множества $\mathrm{SB}^+(n)$ равен 2^{n-1}. Следующее утверждение описывает метрическое дополнение множества самодуальных бент-функций.

Теорема 2 [12]. Пусть $n \geqslant 4$, тогда булева функция от n переменных:

— является самодуальной бент-функцией в том и только в том случае, когда она находится на расстоянии 2^{n-1} от множества всех анти-самодуальных бент-функций от n переменных, то есть является элементом множества $\widehat{\mathrm{SB}^-(n)}$;

— является анти-самодуальной бент-функцией в том и только в том случае, когда она находится на расстоянии 2^{n-1} от множества всех самодуальных бент-функций от n переменных, то есть является элементом множества $\widehat{\mathrm{SB}^+(n)}$.

В [22] доказано, что аффинными являются булевы функции, которые находятся на максимально возможном удалении от множества бент-функций, что влечёт *дуальность* в определении аффинных функций и бент-функций. Таким образом, на основании теоремы 2 можно говорить о том, что между множествами самодуальных и анти-самодуальных бент-функций от $n \geqslant 4$ переменных существует метрическая *дуальность*.

На основании теоремы 2 (случай $n = 2$ рассмотрен отдельно) показано, что

Следствие 3 [12].

1) Множество $\mathrm{SB}^+(n)$ всех самодуальных бент-функций от n переменных является метрически регулярным.
2) Множество $\mathrm{SB}^-(n)$ всех анти-самодуальных бент-функций от n переменных является метрически регулярным.

3. Группа автоморфизмов

Отображение всех булевых функций от n переменных в себя называется *изометричным*, если оно сохраняет расстояние Хэмминга между каждой парой булевых функций от n переменных. Множество изометричных отображений множества всех булевых функций от n переменных в себя будем обозначать через $\mathcal{I}_n$. Известно, что каждое такое отображение однозначно представляется в виде

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где π — перестановка на множестве $\mathbb{F}_2^n$; g — булева функция от n переменных [23]. Отображение такого вида обозначим через $\varphi_{\pi,g} \in \mathcal{I}_n$. Известно, что каждое изометричное отображение множества всех булевых функций от чётного числа переменных n в себя, оставляющее множество $\mathcal{B}_n$ на месте, представимо в виде композиции аффинного преобразования координат и прибавления аффинной функции от n переменных [24].

Группой автоморфизмов фиксированного подмножества $M \subseteq \mathcal{F}_n$ называется группа элементов множества $\mathcal{I}_n$, оставляющая множество M на месте; она обозначается $\mathrm{Aut}\,(M)$.

В [4] (см. также [3]) доказано, что отображение всех булевых функций от n переменных в себя, имеющее вид

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$, сохраняет самодуальность бент-функции. Нетрудно видеть, что все отображения данного вида являются элементами множества $\mathcal{I}_n$. Группа таких преобразований называется *расширенной ортогональной группой* и обозначается $\overline{\mathcal{O}}_n$ [4, 25]. Известно, что $\overline{\mathcal{O}}_n$ является подгруппой группы $\mathrm{GL}\,(n+2, \mathbb{F}_2)$ [4].

В [2] отмечено, что отображение всех булевых функций от n переменных в себя, имеющее вид

$$f(x) \longrightarrow f\left(x \oplus c\right) \oplus \langle c, x\rangle\,,$$

где $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число, определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$. Очевидно, что такое отображение сохраняет расстояние Хэмминга. Частный случай отображения данного вида — при $c = (1, 0, 0, \ldots, 0) \in \mathbb{F}_2^n$ — ранее был расмотрен в [3], на основании чего был сделан вывод о том, что между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ существует взаимно однозначное соответствие.

В [13] получено обобщение данных результатов в рамках класса изометричных отображений: доказано, что группы автоморфизмов множеств $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ совпадают.

Теорема 3 [13]. При $n \geqslant 4$ справедливо $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right)$.

Получен следующий критерий сохранения самодуальности.

Теорема 4 [13]. Пусть $n \geqslant 4$, тогда изометричное отображение $\varphi_{\pi,g}$ является элементом грппы $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$ в том и только в том случае, когда для любых $x, y \in \mathbb{F}_2^n$ справедливо

$$\langle \pi(x), y\rangle \oplus g(x) = \left\langle x, \pi^{-1}(y)\right\rangle \oplus g\left(\pi^{-1}(y)\right).$$

С использованием этого критерия и теоремы 3 получено описание группы автоморфизмов множества (анти-)самодуальных бент-функций от n переменных.

Теорема 5 [13]. При $n \geqslant 4$ справедливо

$$\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right) = \overline{\mathcal{O}}_n.$$

Из этих результатов следует, что более общего подхода к классификации самодуальных бент-функций на основе изометричных отображений, чем предложенный в [3, 4], не существует.

Применительно к биекциям между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ получен следующий критерий.

Теорема 6 [13]. Пусть $n \geqslant 4$, тогда изометричное отображение $\varphi_{\pi,g}$ определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ в том и только в том случае, когда для любых $x, y \in \mathbb{F}_2^n$ справедливо

$$\langle \pi(x), y\rangle \oplus g(x) = \left\langle x, \pi^{-1}(y)\right\rangle \oplus g\left(\pi^{-1}(y)\right) \oplus 1.$$

С использованием данного критерия получена общая форма изметричных отображений, определяющих биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$.

Теорема 7 [13]. При $n \geqslant 4$ изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$, если и только если

$$\pi(x) = L\left(x \oplus c\right),\ g(x) = \langle c, x\rangle \oplus d,\ x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

Из теорем 5 и 7 следует, что чётность веса Хэмминга вектора $c \in \mathbb{F}_2^n$, фигурирующего в описании расширенной ортогональной группы, является «переключателем» между изометричным отображением, сохраняющим (анти-)самодуальность, и изометричным отображением, меняющим местами самодуальные и анти-самодуальные бент-функции.

4. Расстояние Хэмминга между бент-функций и дуальной к ней

Согласно [3, 25], *отношением Рэлея* (the Rayleigh quotient) S_f булевой функции f от n переменных называется число

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

Известно [3], что абсолютное значение S_f не превосходит $2^{3n/2}$, при этом в случае, когда n — чётное число, данная оценка достигается только на самодуальных бент-функциях $\left(+2^{3n/2}\right)$ и анти-самодуальных бент-функциях $\left(-2^{3n/2}\right)$.

В [13] исследованы вопросы сохранения и смены знака отношения Рэлея каждой булевой функции от n переменых при изометричных преобразованиях.

Теорема 8 [13]. Пусть $n \geqslant 4$, тогда изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ сохраняет отношение Рэлея каждой булевой функции от n переменных в том и только в том случае, когда $\varphi_{\pi,g} \in \mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$.

Теорема 9 [13]. Пусть $n \geqslant 4$, тогда изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ меняет знак отношения Рэлея каждой булевой функции от n переменных в том и только в том случае, когда оно определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$.

Пусть $f \in \mathcal{B}_n$. Из соотношения

$$\mathrm{dist}(f, \widetilde{f}) = 2^{n-1} - \frac{S_f}{2^{n/2+1}}$$

следует, что отношение Рэлея полностью характеризует расстояние Хэмминга между бент-функцией $f \in \mathcal{B}_n$ и дуальной к ней функцией $\widetilde{f} \in \mathcal{B}_n$. Таким образом, на основе теорем 5 и 8 можно получить следующий результат.

Теорема 10 [13]. При $n \geqslant 4$ изометричное отображение $\varphi_{\pi,g} \in \mathcal{I}_n$ оставляет множество бент-функций от n переменных на месте и сохраняет расстояние Хэмминга между бент-функцией и дуальной к ней тогда и только тогда, когда

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d, \quad x \in \mathbb{F}_2^n,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Hou X.-D.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 2. P. 183–198.
3. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. V. 1. P. 384–399.
4. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
5. *Hyun J. Y., Lee H., and Lee Y.* MacWilliams duality and Gleason-type theorem on self-dual bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 3. P. 295–304.
6. *Luo G., Cao X., and Mesnager S.* Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. 2019. V. 11. No. 6. P. 1261–1273.
7. *Mesnager S.* Several new infinite families of bent functions and their duals // IEEE Trans. Inf. Theory. 2014. V. 60. No. 7. P. 4397–4407.
8. *Rifà J. and Zinoviev V. A.* On binary quadratic symmetric bent and almost bent functions. arXiv:1211.5257v3, 2019.
9. *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.
10. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. V. 13. No. 3. P. 450–491.
11. *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.

12. *Kutsenko A.* Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.
13. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions // Cryptogr. Commun. 2020.
14. *Куценко А. В.* О множестве расстояний Хэмминга между самодуальными бент-функциями // Прикладная дискретная математика. Приложение. 2016. № 9. С. 29–30.
15. *Куценко А. В.* О некоторых свойствах самодуальных бент-функций // Прикладная дискретная математика. Приложение. 2018. № 11. С. 44–46.
16. *Куценко А. В.* Изометричные отображения множества всех булевых функций в себя, сохраняющие самодуальность и отношение Рэлея // Прикладная дискретная математика. Приложение. 2019. № 12. С. 55–58.
17. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
18. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam, New York, Oxford, North-Holland, 1983. 782 p.
19. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
20. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Вып. 23. № 3. С. 93–106
21. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
22. *Tokareva N.* Duality between bent functions and affine functions // Discrete Math. 2012. V. 312. No. 3. P. 666–670.
23. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
24. *Tokareva N. N.* The group of automorphisms of the set of bent functions // Discrete Math. Appl. 2010. V. 20. No. 5. P. 655–664.
25. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.

УДК 519.7 DOI 10.17223/2226308X/13/6

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕКОТОРЫХ КОМПОЗИЦИЙ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

Е. С. Липатова

Рассматриваются три класса обратимых векторных булевых функций, таких, что каждая их координатная функция существенно зависит от заданного числа переменных. Приведены результаты экспериментального исследования криптографических свойств композиций функций из этих классов.

Ключевые слова: *векторная булева функция, нелинейность, алгебраическая иммунность, дифференциальная равномерность.*

Обозначим через $\mathcal{F}_n$ множество всех подстановок на $\mathbb{F}_2^n$ и будем рассматривать следующие подклассы функций из $\mathcal{F}_n$:

1) $\mathcal{K}_n$ — функции, полученные из тождественной подстановки с помощью n независимых транспозиций [1];