5. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
6. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4. С. 14–30.
7. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
8. Словарь криптографических терминов. М.: МЦНМО, 2016. 94 с.
9. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
10. *Панков К. Н.* Уточнённые асимптотические оценки для числа $(n, m, k)$-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
11. *Панков К. Н.* Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. № 11. С. 49–52.
12. *Canfield E. R., Gao Z., Greenhill C., et al.* Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.
13. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
14. *Панков К. Н.* Улучшенные асимптотические оценки для числа корреляционно-иммунных и $k$-эластичных двоичных вектор-функций // Дискретная математика. 2018. № 2. С. 73–98.
15. *Денисов О. В.* Асимптотическая формула для числа корреляционно-иммунных порядка $k$ булевых функций // Дискретная математика. 1991. № 2. С. 25–46.

УДК 519.7 DOI 10.17223/2226308X/12/20

# О КОМПОНЕНТАХ НЕКОТОРЫХ КЛАССОВ ОБРАТИМЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

И. А. Панкратова

В классе обратимых векторных булевых функций от $n$ переменных, координатные функции которых существенно зависят от всех переменных, рассматриваются подклассы $\mathcal{K}_n$ и $\mathcal{K}'_n$, функции в которых получены с помощью $n$ независимых транспозиций из тождественной подстановки и из подстановки, каждая координатная функция которой существенно зависит от одной переменной, соответственно. Приводятся некоторые свойства компонент функций из этих классов.

**Ключевые слова:** *векторная булева функция, обратимые функции, нелинейность векторной булевой функции, компонентная алгебраическая иммунность.*

Для $n \in \mathbb{N}$ рассмотрим обратимые векторные булевы функции $F = (f_1 \dots f_n)$ на $\mathbb{F}_2^n$, такие, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят от всех $n$ переменных. В [1] предложен алгоритм 1 построения некоторой такой функции, который состоит в следующем: стартуя с тождественной подстановки $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, на $i$-м шаге, $i = 1, \dots, n$, выбираем два соседних по $i$-й координате и не выбранных на предыдущих шагах вектора $a, b \in \mathbb{F}_2^n$ и меняем местами значения $G(a)$ и $G(b)$.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Обозначим класс функций, которые можно получить алгоритмом 1, через $\mathcal{K}_n$. В [1] доказано, что $\mathcal{K}_n \neq \varnothing$ для всех $n > 2$; в [2] описаны некоторые свойства координат функций из $\mathcal{K}_n$.

В [1] предложена модификация алгоритма 1 построения функций из класса $\mathcal{K}_n$, состоящая в том, что отправной точкой алгоритма является не обязательно тождественная подстановка $G$, а такая, что каждая координатная функция существенно зависит ровно от одной переменной, т. е. $G = (g_1 \dots g_n)$, $g_i = x_{j_i}^{\sigma_i}$, где $\{j_1, \dots, j_n\} = \{1, \dots, n\}$, $\sigma_i \in \{0, 1\}$ и $x_i^0 = \overline{x_i}$, $x_i^1 = x_i$, $i = 1, \dots, n$. Будем называть эту модификацию алгоритмом $1'$, а класс функций, которые можно таким образом получить, обозначим $\mathcal{K}'_n$.

**Утверждение 1.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}_n$. Тогда для всех $i = 1, \dots, n$ функция $f_i$ имеет единственную линейную переменную $x_i$.

Пусть $v = (v_1 \dots v_n) \in (\mathbb{F}_2^n)^* = \mathbb{F}_2^n \setminus \{00 \dots 0\}$. *Компонентой функции* $F = (f_1 \dots f_n)$ называется скалярное произведение $vF : \mathbb{F}_2^n \to \mathbb{F}_2$, $vF(x) = \bigoplus\limits_{i=1}^{n} v_i f_i(x) = \bigoplus\limits_{v_i=1} f_i(x)$. Через $\mathrm{w}(v)$ обозначим вес вектора $v$ (количество единиц в нём).

**Утверждение 2.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$ и $F$ получена алгоритмом $1'$ из начальной подстановки $G = (x_{j_1}^{\sigma_1} \dots x_{j_n}^{\sigma_n})$. Тогда $f_i$ имеет единственную линейную переменную $x_{j_i}$, $i = 1, \dots, n$.

**Утверждение 3.** Пусть $F = (f_1 \dots f_n) \in \mathcal{K}'_n$. Тогда для всех $v = v_1 \dots v_n \in \mathbb{F}_2^n$, таких, что $\mathrm{w}(v) > 2$, компонентная функция $vF$ не имеет фиктивных и линейных переменных.

**Утверждение 4.** $|\mathcal{K}'_n| = 2^n\, n! |\mathcal{K}_n|$.

Приведём определения некоторых криптографических характеристик векторных булевых функций [3]. *Нелинейность* $N_F$ функции $F$ — минимальная нелинейность её компонент. *Степень* $\deg F$ функции $F$ — максимальная степень её компонент (совпадает с максимальной степенью координатных функций). *Компонентная алгебраическая иммунность* $\mathrm{AI}_{\mathrm{comp}}(F)$ функции $F$ — минимальная алгебраическая иммунность её компонент.

**Утверждение 5.** Для функции $F \in \mathcal{K}'_n$ выполняются следующие свойства:

1) $N_F = 2$;
2) $\deg F = n - 1$;
3) $\mathrm{AI}_{\mathrm{comp}}(F) = 2$;
4) если $v \in \mathbb{F}_2^n$ и $\mathrm{w}(v) \leqslant 2^{n-3}$, то нелинейность компонентной функции $vF$ равна $N_{vF} = 2\mathrm{w}(v)$.

Подробное изложение представленных результатов и доказательства утверждений можно найти в [4].

## ЛИТЕРАТУРА

1. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
2. *Карпова Л. А., Панкратова И. А.* Свойства координатных функций одного класса подстановок на $\mathbb{F}_2^n$ // Прикладная дискретная математика. Приложение. 2017. № 10. С. 38–40.

3. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
4. *Панкратова И. А.* Свойства компонент некоторых классов векторных булевых функций // Прикладная дискретная математика. 2019. № 44. С. 5–11.

УДК 519.713.2+519.714.5 DOI 10.17223/2226308X/12/21

# ЛИНЕЙНОЕ РАЗЛОЖЕНИЕ ДИСКРЕТНЫХ ФУНКЦИЙ В ТЕРМИНАХ ОПЕРАЦИИ СДВИГ-КОМПОЗИЦИИ

И. В. Чередник

Исследуется операция сдвиг-композиции дискретных функций, возникающая при гомоморфизмах конечных регистров сдвига. Для произвольной функции над конечным полем описаны все возможные представления в виде сдвиг-композиции двух функций, правая из которых линейная. Кроме того, изучена возможность представления произвольной функции над конечным полем сдвиг-композицией трёх функций, в которой обе крайние функции линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.

**Ключевые слова:** *дискретные функции, конечные поля, регистр сдвига, сдвиг-композиция.*

## Введение

Пусть $\Omega_q$ — конечное множество из $q$ элементов. В данной работе будем использовать множество переменных $\{x_0, x_1, x_2, \ldots\}$, а множество всех функций $q$-значной логики от переменных $x_0, x_1, x_2, \ldots$ будем обозначать через $F_q$. Произвольную функцию $f \in F_q$ всегда можно рассматривать как функцию от соответствующего допустимого набора переменных $x_0, x_1, \ldots, x_n$. В работах отечественных криптографов К. Г. Таболова, В. А. Башева, А. Я. Прососова, В. И. Солодовникова и др. была введена и исследована (преимущественно в терминах гомоморфизмов регистров сдвига) операция сдвиг-композиции на множестве всех функций $F_q$:

$$f(x_0, \ldots, x_n) \lhd g(x_0, \ldots, x_m) = f(g(x_0, \ldots, x_m), \ldots, g(x_n, \ldots, x_{n+m})).$$

В работах перечисленных авторов в разной степени общности и направленности достаточно подробно исследована связь между представлением функции $f$ в виде сдвиг-композиции $f = g \lhd h$ и существованием гомоморфизма регистра сдвига, соответствующего функции $f$, на меньший регистр сдвига, соответствующий функции $g$ (все основные результаты по данной тематике единым образом изложены в [1]). Так, например, в [2] описаны все возможные представления функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = l \lhd g$, где $l$ — линейная, что позволило указать все возможные гомоморфизмы регистра сдвига с обратной связью $f$ на линейные регистры сдвига.

В настоящей работе предлагается описание всех возможных представлений произвольной функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = g \lhd l$, где $l$ — линейная. Кроме того, изучена возможность представления произвольной функции $f$ над конечным полем $\mathbb{F}_q$ в виде $f = l_1 \lhd g \lhd l_2$, где $l_1, l_2$ — линейные. Доказано, что в случае простого поля для линейных функций, а также для квадратичных функций, линейных по крайней переменной, понятия приводимости и линейной приводимости совпадают.