ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ КРИПТОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

Н. М. Киселева, Е. С. Липатова, И. А. Панкратова, Е. Е. Трифонова

Национальный исследовательский Томский государственный университет, г. Томск, Россия

Представлены алгоритмы вычисления следующих криптографических характеристик векторых булевых функций: порядка корреляционной иммунности, нелинейности, компонентной алгебраической иммунности и показателя дифференциальной равномерности. Компоненты векторной булевой функции перебираются в порядке, задаваемом кодом Грея. Приводятся результаты экспериментов для случайных векторных булевых функций, подстановок и двух специальных классов $\mathcal{K}_n$ и $\mathcal{S}_{n,k}$ обратимых векторных булевых функций от n переменных, координаты которых существенно зависят от всех и заданного числа $k < n$ переменных соответственно. Доказаны некоторые свойства дифференциальной равномерности для функций из классов $\mathcal{K}_n$ и $\mathcal{S}_{n,k}$.

Ключевые слова: *векторная булева функция, корреляционная иммунность, нелинейность векторной булевой функции, компонентная алгебраическая иммунность, показатель дифференциальной равномерности.*

DOI 10.17223/20710410/46/7

ALGORITHMS FOR COMPUTING CRYPTOGRAPHIC CHARACTERISTICS OF VECTORIAL BOOLEAN FUNCTIONS

N. M. Kiseleva, E. S. Lipatova, I. A. Pankratova, E. E. Trifonova

National Research Tomsk State University, Tomsk, Russia

E-mail: kiselyov-natalya@mail.ru, katrinelipatova@gmail.com, pank@mail.tsu.ru, lizatrif@gmail.com

There are presented algorithms for calculating the cryptographic characteristics of vectorial Boolean functions, such as the order of correlation immunity, nonlinearity, component algebraic immunity, and differential uniformity order. In these algorithms, the components of a vectorial Boolean function are enumerated according to the Gray code. Experimental results are given for random vectorial Boolean functions, permutations, and two known classes $\mathcal{K}_n$ and $\mathcal{S}_{n,k}$ of invertible vectorial Boolean functions in n variables with coordinates essentially depending on all variables and on k variables, $k < n$, respectively. Some properties of differential uniformity are theoretically

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

proved for functions in $\mathcal{K}_n$ and $\mathcal{S}_{n,k}$, namely, the differential uniformity order δ_F equals 2^n for any $F \in \mathcal{S}_{n,k}$, and the inequality $2^n - 4(n-1) \leqslant \delta_F \leqslant 2^n - 4$ holds for any $F \in \mathcal{K}_n$.

Keywords: *vectorial Boolean function, nonlinearity, correlation immunity, component algebraic immunity, differential uniformity.*

Введение

Криптосистемы, стойкость которых основана на сложности решения систем нелинейных уравнений над конечным полем, являются предположительно стойкими к квантовым атакам [1]. К этому классу, в частности, относятся криптосистемы с функциональными ключами, построенные на векторных булевых функциях [2–4]. Для анализа стойкости таких криптосистем, помимо разработки специальных атак, нужно исследовать известные криптографические характеристики используемых функций. В данной работе приведены алгоритмы вычисления таких характеристик, как порядок корреляционной иммунности, нелинейность, компонентная алгебраическая иммунность и показатель дифференциальной равномерности. Алгоритмы достаточно «прямолинейны» и, скорее всего, не являются лучшими по сложности, однако их реализация позволила исследовать характеристики функций из разных классов и сформулировать ряд утверждений о свойствах функций этих классов. В п. 3 доказано несколько утверждений о дифференциальной равномерности подстановок, координатные функции которых существенно зависят от заданного числа переменных.

Приведём необходимые определения [5–7]. Пусть дана векторная булева функция $F = (f_1 \dots f_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Компонентой функции F называется булева функция $vF = v_1 f_1 \oplus \dots \oplus v_m f_m$, где $v = v_1 \dots v_m \in \mathbb{F}_2^m \setminus \{0^m\}$; 0^m — нулевой вектор длины m.

Порядком корреляционной иммунности $\operatorname{cor}(F)$, *нелинейностью* $N(F)$ и *компонентной алгебраической иммунностью* $\operatorname{AI}_{\text{comp}}(F)$ векторной функции F называются минимальные порядок корреляционной иммунности, нелинейность и алгебраическая иммунность её компонент соответственно:

$$\operatorname{cor}(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} \operatorname{cor}(vF), \quad N(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} N(vF), \quad \operatorname{AI}_{\text{comp}}(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} \operatorname{AI}(vF)$$

(определения соответствующих характеристик для *булевой* функции см. в [8, с. 277 и определение 2.50] и [5]).

Для функции F и векторов $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$ обозначим

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus a) = b\}|.$$

Показателем дифференциальной равномерности функции F называется

$$\delta_F = \max_{a \neq 0^n, b} \delta_F(a, b).$$

Значения $\operatorname{cor}(F)$, $N(F)$ и $\operatorname{AI}_{\text{comp}}(F)$ характеризуют стойкость криптосистемы с функцией F в качестве блока преобразования к корреляционному, линейному и алгебраическому методам криптоанализа соответственно, и они должны быть большими. Заметим, что для всех подстановок $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ имеет место $\operatorname{cor}(F) = 0$, поскольку для уравновешенных функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ верно неравенство $m \leqslant n - \operatorname{cor}(F)$ [5].

Показатель δ_F связан со способностью шифра противостоять дифференциальному криптоанализу в случаях, когда функция F используется в качестве блока замены в DES-подобном шифре [7] или (в общем случае) в произвольном итеративном блочном шифре с аддитивным раундовым ключом [9] — чем он меньше, тем лучше.

1. Алгоритмы вычисления криптографических характеристик

Для вычисления характеристик $\mathrm{cor}(F)$, $N(F)$ и $\mathrm{AI}_{\mathrm{comp}}(F)$ по определению нужно перебрать все компоненты vF функции F, $v \in \mathbb{F}_2^m \backslash \{0^m\}$. Чтобы минимизировать время вычисления компонент, будем перебирать векторы v в соответствии с *кодом Грея* — в этом случае «соседние» значения v различаются ровно в одном двоичном разряде, а значит, очередная компонента функции F получается из предыдущей прибавлением одной координатной функции (алгоритм 1).

Алгоритм 1. Перебор компонент векторной булевой функции

Вход: функция $F = (f_1 \dots f_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

1: Создать булеву функцию $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $f := \mathrm{const}\, 0$, и вектор $v_0 \in \mathbb{F}_2^m$, $v_0 := 0^m$.
2: **Для** $i = 1, \dots, 2^m - 1$:
3: $\quad v_i := i \oplus (i \gg 1)$ *// преобразование двоичного кода в код Грея;* $\gg$ *— операция сдвига вправо;* i *рассматривается и как целое число, и как булев вектор длины* m.
4: $\quad$ Положить k равным номеру (единственной) единицы в векторе $v_{i-1} \oplus v_i$;
5: $\quad f := f \oplus f_k$ *// очередная компонента.*
6: $\quad$ Обработка f.

Согласно [5], порядок корреляционной иммунности $\mathrm{cor}(F)$ функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ равен t, если и только если: 1) $W_{vF}(u) = 0$ для всех наборов $u \in \mathbb{F}_2^n$ веса от 1 до t включительно и всех компонент vF и 2) $W_{vF}(u) \neq 0$ для некоторого набора u веса $t+1$ и некоторой компоненты vF, где $W_{vF}(u) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{vF(x) \oplus ux}$ — коэффициент преобразования Уолша — Адамара функции vF. Таким образом, для вычисления $\mathrm{cor}(F)$ нужно найти ненулевой вектор u минимального веса, на котором преобразование Уолша — Адамара хотя бы одной компоненты принимает ненулевое значение. Другими словами, нам интересны такие значения u, что $W_{vF}(u) = 0$ *для всех* компонент. Поэтому, перебирая компоненты vF, будем «накапливать» в одном массиве дизъюнкцию коэффициентов $W_{vF}(u)$, $u \in \mathbb{F}_2^n$ (интерпретируя целые числа как булевы векторы) и только потом проанализируем полученный вектор (алгоритм 2).

Алгоритм 2. Вычисление $\mathrm{cor}(F)$

Вход: функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

1: Создать массив целых чисел D размера 2^n, обнулить все его элементы.
2: Перебираем компоненты vF, как в алгоритме 1.
3: **Для** каждой компоненты:
4: $\quad w := W_{vF}$; $D := D \vee w$ (поэлементно) *// шаг 6 алгоритма 1.*
5: **Для всех** $i = 1, \dots, n$:
6: $\quad$ **Для всех** векторов $u \in \mathbb{F}_2^n$ веса i:
7: $\quad\quad$ **если** $D_u \neq 0$, **то выход**, ответ: $i - 1$.
8: **Выход**, ответ: n.

Оценим сложность алгоритма 2:

— всего компонент $(2^m - 1)$, переход к следующей компоненте (сложение текущей с координатной функцией) — $O(2^n)$ операций, вычисление преобразования Уолша — Адамара по схеме Грина — $O(2^n n)$ [8], поэлементная дизъюнкция векторов — $O(2^n)$ операций; итого сложность шагов 2–4 составляет $O(2^{n+m}n)$ операций;

— на шагах 5–7 в худшем случае (для функции-константы) придётся перебрать $2^n - 1$ векторов.

Таким образом, сложность алгоритма 2 равна $O(2^{n+m}n)$.

Нелинейность $N(F)$ функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ тоже можно вычислить с использованием преобразования Уолша — Адамара по следующей формуле [5]:

$$N(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{u \in \mathbb{F}_2^n, \\ v \in \mathbb{F}_2^m \setminus \{0^m\}}} W_{vF}(u). \tag{1}$$

Получаем алгоритм 3 вычисления нелинейности.

Алгоритм 3. Вычисление $N(F)$

Вход: функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

1: $c := 0$.

2: Перебираем компоненты vF, как в алгоритме 1.

3: **Для** каждой компоненты:

4: $w := W_{vF}$; $d := \max\limits_{i=0,\ldots,2^n-1} |w_i|$; **если** $d > c$, **то** $c := d$.

Выход: $N(F) = 2^{n-1} - c/2$ (по формуле (1)).

Сложность алгоритма 3 равна $O(2^{n+m}n)$.

Для описания алгоритма вычисления компонентной алгебраической иммунности $\mathrm{AI}_{\mathrm{comp}}(F)$ введём следующие понятия [5]. *Аннигилятором подмножества* $A \subseteq \mathbb{F}_2^n$ называется любая булева функция от n переменных, не равная тождественно 0 и принимающая значение 0 на всех наборах из A. *Алгебраической иммунностью* множества A называется минимальная из алгебраических степеней аннигиляторов, не равных тождественно 0; обозначается $\mathrm{AI}(A)$. Для булевой функции f от n переменных обозначим $M_f^\sigma = \{x \in \mathbb{F}_2^n : f(x) = \sigma\}$, $\sigma \in \{0, 1\}$. Тогда

$$\mathrm{AI}_{\mathrm{comp}}(F) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} \mathrm{AI}(vF) = \min_{v \in \mathbb{F}_2^m \setminus \{0^m\}} \min(\mathrm{AI}(M_{vF}^0), \mathrm{AI}(M_{vF}^1)). \tag{2}$$

В соответствии с (2) получаем алгоритм 4 вычисления компонентной алгебраической иммунности.

Алгебраическую иммунность множества $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{F}_2^n$ будем искать методом неопределённых коэффициентов [10] (алгоритм 5). Для того чтобы определить, существует ли аннигилятор множества A степени не выше d, построим матрицу $B(A, d)$, столбцы которой соответствуют элементам множества A, строки — всевозможным мономам $m_1, \ldots, m_t$ от переменных $x_1, \ldots, x_n$ степеней от 0 до d, где $t = \sum\limits_{i=0}^{d} \binom{n}{i}$; на пересечении строки i и столбца j запишем значение $m_i(a_j)$. Если $\operatorname{rang} B(A, d) < t$, то существует нетривиальная нулевая линейная комбинация строк матрицы: $m_{i_1} \oplus \ldots \oplus m_{i_s} = 0^k$; тогда функция $g(x) = m_{i_1}(x) \oplus \ldots \oplus m_{i_s}(x)$ — аннигилятор множества A.

Алгоритм 4. Вычисление $\mathrm{AI}_{\mathrm{comp}}(F)$

Вход: функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

1: $c := \lceil n/2 \rceil$ // верхняя граница $\mathrm{AI}_{\mathrm{comp}}(F)$ [10].
2: Перебираем компоненты vF, как в алгоритме 1.
3: **Для** каждой компоненты:
4: $m_0 := \mathrm{AI}(M_{vF}^0)$; $m_1 := \mathrm{AI}(M_{vF}^1)$ // по алгоритму 5;
5: $c := \min(c, m_0, m_1)$.

Выход: $\mathrm{AI}_{\mathrm{comp}}(F) = c$.

Алгоритм 5. Вычисление алгебраической иммунности множества

Вход: множество $A \subseteq \mathbb{F}_2^n$, $|A| = k$.

1: **Если** $A = \varnothing$, **то выход**, ответ: $\mathrm{AI}(A) = 0$.
2: Построить матрицу $B = B(A, 1)$; $d := 1$; $t := n + 1$.
3: **Если** $\operatorname{rang} B < t$, **то выход**, ответ: $\mathrm{AI}(A) = d$.
4: $d := d + 1$; $t := t + \binom{n}{d}$; **если** $t > k$, **то выход**, ответ: $\mathrm{AI}(A) = d$.
5: Добавить к матрице B строки, соответствующие мономам степени d, перейти к п. 3.

Сложность алгоритма 5 при вычислении ранга методом Гаусса составляет $\mathrm{O}(k^3 d)$. Отметим, что при использовании этого алгоритма для вычисления $\mathrm{AI}_{\mathrm{comp}}(F)$ можно ввести дополнительное ограничение на шаге 4 после увеличения d: «**если** $d \geqslant \lceil n/2 \rceil$, **то выход**, ответ: $\mathrm{AI}(A) = d$». Сложность алгоритма 4 равна $\mathrm{O}(2^{m+3n} n)$.

Алгоритм 6 вычисления показателя дифференциальной равномерности получаем непосредственно из его определения.

Алгоритм 6. Вычисление показателя δ_F

Вход: функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

1: Создать вспомогательный массив целых чисел DDT размера 2^m, обнулить все его элементы.
2: $\delta := 0$.
3: **Для всех** $a \in \mathbb{F}_2^n \setminus \{0^n\}$:
4: **Для всех** $x \in \mathbb{F}_2^n$:
$b := F(x) \oplus F(x \oplus a)$; $DDT[b] := DDT[b] + 1$;
5: $d := \max\limits_{b \in \mathbb{F}_2^m} DDT[b]$; **если** $d > \delta$, **то** $\delta := d$.
6: Обнулить массив DDT.

Выход: $\delta_F = \delta$.

Сложность алгоритма 6 равна $\mathrm{O}(2^{n+\max(n,m)})$.

2. Результаты экспериментов

Все алгоритмы реализованы на языке ЛЯПАС-Т [11] и исследованы в компьютерном эксперименте на случайных функциях, подстановках и двух специальных классах обратимых функций, координаты которых зависят от заданного числа переменных. Определим эти классы [12, 13].

Для $n \in \mathbb{N}$, $n \geqslant 3$, рассмотрим класс функций $\mathcal{K}_n$, функции $F = (f_1 \dots f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ в котором получаются из тождественной подстановки G на $\mathbb{F}_2^n$ с помощью n следующих независимых транспозиций: выбираем n непересекающихся множеств $M_i = \{x^{(i)}, y^{(i)}\}$, где векторы $\{x^{(i)}, y^{(i)}\}$ соседние по i-й координате, и полагаем $F(x^{(i)}) = G(y^{(i)})$, $F(y^{(i)}) = G(x^{(i)})$, $i = 1, \dots, n$; $F(x) = G(x)$ для всех $x \notin \bigcup\limits_{i=1}^{n} M_i$. По построению, для любого $a = a_1 \dots a_n \in \mathbb{F}_2^n$ имеет место

$$f_i(a) = \begin{cases} a_i \oplus 1, & \text{если } a \in M_i, \\ a_i & \text{иначе.} \end{cases} \tag{3}$$

Доказано [12], что все координаты функций из $\mathcal{K}_n$ существенно зависят от всех n переменных и $\mathcal{K}_n \neq \varnothing$ для всех $n \geqslant 3$.

Для $k, n \in \mathbb{N}$, $3 \leqslant k \leqslant n$, построим функцию $F = (f_1 \dots f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ так. Пусть $H = (h_1 \dots h_k)$ — некоторая функция из $\mathcal{K}_k$. Положим $f_i(x_1, \dots, x_n) = h_i(x_1, \dots, x_k)$, $i = 1, \dots, k$ (переменные $x_{k+1}, \dots, x_n$ у функций $f_1, \dots, f_k$ фиктивные), и $f_i = x_i \oplus$ $\oplus\, \varphi_i(x_1, \dots, x_{i-1})$ для $i = k+1, \dots, n$, где $\varphi_{k+1}, \dots, \varphi_n$ — произвольные функции, существенно зависящие ровно от $(k-1)$ из своих переменных. Обозначим класс функций, построенных таким образом, через $\mathcal{S}_{n,k}$. В [13, утверждение 3] доказано, что функции из $\mathcal{S}_{n,k}$ являются подстановками на $\mathbb{F}_2^n$; все их координаты существенно зависят ровно от k переменных. Необходимость ограничивать количество существенных переменных у координат векторных булевых функций может возникнуть, в частности, при построении криптосистем, где такие функции являются ключами [2–4], а значит, нужно уметь их эффективно задавать и быстро вычислять.

Эксперименты на функциях $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ дали следующие результаты.

1) Порядок корреляционной иммунности случайной функции, как правило, равен 0, редко — 1.
2) Для нелинейности:
   - при фиксированном n с ростом m значение $N(F)$ убывает; например, при $n = 5$ среднее значение $N_{\text{ср}}(F) = 6{,}6$ при $m = 5$ и $N_{\text{ср}}(F) \leqslant 2$ при $m \geqslant 18$;
   - если $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — подстановка, то её нелинейность растёт с ростом n, приближаясь к теоретической верхней границе $N_{\max} = 2^{n-1} - 2^{n/2-1}$: от 47 % при $n = 5$ до 93 % при $n = 12$;
   - если $F \in \mathcal{K}_n$, то $N(F) = 2$ (доказано в [14]); отсюда следует, что $N(F) \leqslant 2^{n-k+1}$ для $F \in \mathcal{S}_{n,k}$, поскольку первые k координат такой функции F получаются добавлением $(n-k)$ фиктивных переменных, каждая из которых увеличивает нелинейность функции в два раза. В экспериментах для функций $F \in \mathcal{S}_{n,k}$ всегда выполняется $N(F) = 2^{n-k+1}$, кроме случаев $k = 3$ (всегда получаем 0) и $k = 4$ (получаем 0 или 2^{n-3}).
3) Для алгебраической иммунности:
   - для случайных подстановок F почти всегда $\text{AI}_{\text{comp}}(F) = n/2$ (максимально возможное) при чётном n и $\text{AI}_{\text{comp}}(F) = (n-1)/2$ (на 1 меньше максимально возможного) при нечётном n; это согласуется с результатами [15] для уравновешенных булевых функций f: для чётного n вероятность того, что минимальная среди степеней аннигиляторов множества M_f^1 равна $n/2$, близка к 1; для нечётного n эта степень с бóльшей вероятностью (0,711 против 0,289) равна $(n-1)/2$, чем $(n+1)/2$ (максимально возможной);

— если $F \in \mathcal{K}_n$, то $\mathrm{AI}_{\mathrm{comp}}(F) = 2$ (доказано в [14]); отсюда следует, что $\mathrm{AI}_{\mathrm{comp}}(F) \leqslant 2$ для $F \in \mathcal{S}_{n,k}$, поскольку добавление фиктивных переменных не влияет на алгебраическую иммунность функции. В экспериментах получено: $\mathrm{AI}_{\mathrm{comp}}(F) = 1$ для функций $F \in \mathcal{S}_{n,k}$ всегда при $k = 3$ и иногда при $k \geqslant 4$; последнее — чем больше n и k, тем реже (почти всегда $\mathrm{AI}_{\mathrm{comp}}(F) = 2$).

4) Для показателя дифференциальной равномерности:
   — при $n \geqslant m$, как правило, $\delta_F = 2^n$;
   — при фиксированном n с ростом m значение δ_F убывает;
   — если $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — подстановка, то её дифференциальная равномерность в среднем много меньше, чем дифференциальная равномерность случайной такой функции (без условия обратимости).

Эксперименты на функциях из класса $\mathcal{K}_n$ позволили сформулировать некоторые утверждения об их дифференциальной равномерности.

3. Свойство дифференциальной равномерности функций из классов $\mathcal{K}_n$ и $\mathcal{S}_{n,k}$

Для $j \in \{1, \ldots, n\}$ обозначим e_j булев вектор длины n с единственной 1 в j-й координате.

Утверждение 1. Пусть $F \in \mathcal{K}_n$, $a = \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2} \oplus \ldots \oplus \mathrm{e}_{i_k}$, $j \in \{i_1, \ldots, i_k\}$. Тогда

$$\sum_{b=(b_1 \ldots b_n) \in \mathbb{F}_2^n : b_j = 0} \delta_F(a, b) = \begin{cases} 4, & k > 1, \\ 0, & k = 1. \end{cases}$$

Доказательство. Запишем:

$$\sum_{b=(b_1 \ldots b_n) \in \mathbb{F}_2^n : b_j = 0} \delta_F(a, b) = \sum_{b=(b_1 \ldots b_n) \in \mathbb{F}_2^n : b_j = 0} |\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus a) = b\}| =$$
$$= |\{x \in \mathbb{F}_2^n : f_j(x) = f_j(x \oplus a)\}|.$$

Заметим, что x и $x \oplus a$ различаются в j-й координате. Тогда из формулы (3) следует, что $f_j(x) = f_j(x \oplus a)$, если и только если ровно один из векторов x и $x \oplus a$ принадлежит M_j, где $M_j = \{c, c \oplus \mathrm{e}_j\}$ для некоторого $c \in \mathbb{F}_2^n$. Если $k = 1$ и, следовательно, $a = \mathrm{e}_j$, то x и $x \oplus a$ одновременно либо принадлежат, либо не принадлежат M_j. При $k > 1$ условие выполняется для $x \in X = \{c, c \oplus \mathrm{e}_j, c \oplus a, c \oplus \mathrm{e}_j \oplus a\}$; ввиду того, что вес вектора a больше 1, все векторы в X различны. ■

Утверждение 2. Пусть $F \in \mathcal{K}_n$, $a = \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2} \oplus \ldots \oplus \mathrm{e}_{i_k}$, $j \notin \{i_1, \ldots, i_k\}$. Тогда

$$\sum_{b=(b_1 \ldots b_n) \in \mathbb{F}_2^n : b_j = 1} \delta_F(a, b) = 4.$$

Доказательство. Аналогично доказательству утверждения 1 получим

$$\sum_{b=(b_1 \ldots b_n) \in \mathbb{F}_2^n : b_j = 1} \delta_F(a, b) = |\{x \in \mathbb{F}_2^n : f_j(x) \neq f_j(x \oplus a)\}|.$$

Поскольку j-е координаты x и $x \oplus a$ совпадают, из формулы (3) следует, что $f_j(x) \neq$ $\neq f_j(x \oplus a)$, если и только если ровно один из векторов x и $x \oplus a$ принадлежит $M_j =$ $= \{c, c \oplus \mathrm{e}_j\}$. Это условие выполняется для $x \in X = \{c, c \oplus \mathrm{e}_j, c \oplus a, c \oplus \mathrm{e}_j \oplus a\}$; ввиду того, что $a \neq \mathrm{e}_j$, все векторы в X различны. ■

Из утверждений 1 и 2 следует, что $\delta_F(a,b) \leqslant 4$ для всех $F \in \mathcal{K}_n$ и $a \neq b$; ввиду чётности значений $\delta_F(a,b)$ это означает, что $\delta_F(a,b) \in \{0,2,4\}$.

Утверждение 3. Пусть $F \in \mathcal{K}_n$, $a = \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2} \oplus \ldots \oplus \mathrm{e}_{i_k}$, $b = (b_1 \ldots b_n) \in \mathbb{F}_2^n$ и $b_j = 0$ для всех $j \in \{i_1, \ldots, i_k\}$. Тогда $\delta_F(a,b) = 0$.

Доказательство. Обозначим $X = \{x \in \mathbb{F}_2^n : \forall\, j \in \{i_1, \ldots, i_k\}(f_j(x) = f_j(x \oplus a))\}$. Тогда для a и b в условии утверждения $\delta_F(a,b) = |X|$ и для $x \in X$ должно выполняться условие: ровно один из векторов x и $x \oplus a$ принадлежит M_j, $j = i_1, \ldots, i_k$. Поскольку множества M_j не пересекаются, это условие не может выполняться при $k > 2$; случай $k = 1$ рассмотрен в утверждении 1. Осталось рассмотреть случай $k = 2$.

Пусть $a = \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2}$, $M_{i_1} = \{c, c \oplus \mathrm{e}_{i_1}\}$, $M_{i_2} = \{d, d \oplus \mathrm{e}_{i_2}\}$ и без ограничения общности $x \in M_{i_1}$, $x \oplus a \in M_{i_2}$. Если $x = c$, то $x \oplus a = x \oplus \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2}$; при $x \oplus a = d$ получаем $d \oplus \mathrm{e}_{i_2} = c \oplus \mathrm{e}_{i_1} \in M_{i_1}$, а если $x \oplus a = d \oplus \mathrm{e}_{i_2}$, то $d = c \oplus \mathrm{e}_{i_1} \in M_{i_1}$; оба вывода противоречат тому, что $M_{i_1} \cap M_{i_2} = \varnothing$. Случай $x = c \oplus \mathrm{e}_{i_1}$ рассматривается аналогично. ■

Утверждение 4. Пусть $F \in \mathcal{K}_n$, $a \in \mathbb{F}_2^n$. Тогда $\delta_F(a,a) \geqslant 2^n - 4n$, если вес a больше 1, и $\delta_F(a,a) \geqslant 2^n - 4(n-1)$ иначе.

Доказательство. Из того, что $\sum\limits_{b \in \mathbb{F}_2^n} \delta_F(a,b) = 2^n$, следует

$$\delta_F(a,a) = 2^n - \sum_{b \neq a} \delta_F(a,b). \tag{4}$$

Пусть $a = \mathrm{e}_{i_1} \oplus \mathrm{e}_{i_2} \oplus \ldots \oplus \mathrm{e}_{i_k}$. Запишем:

$$\sum_{b \neq a} \delta_F(a,b) \leqslant \sum_{j=1}^{n} \sum_{a, b \in \mathbb{F}_2^n : b_j \neq a_j} \delta_F(a,b) = \underbrace{\sum_{j \in \{i_1, \ldots, i_k\}} \sum_{b \in \mathbb{F}_2^n : b_j = 0} \delta_F(a,b)}_{S_1} + \underbrace{\sum_{j \notin \{i_1, \ldots, i_k\}} \sum_{b \in \mathbb{F}_2^n : b_j = 1} \delta_F(a,b)}_{S_2}.$$

Из утверждения 1 следует, что

$$S_1 = \begin{cases} 4k, & \text{если } k > 1, \\ 0, & \text{если } k = 1, \end{cases}$$

из утверждения 2 получаем $S_2 = 4(n-k)$. Тогда

$$\sum_{b \neq a} \delta_F(a,b) \leqslant \begin{cases} 4n, & \text{если } k > 1, \\ 4(n-1), & \text{если } k = 1. \end{cases} \tag{5}$$

Из (4) и (5) следует справедливость утверждения 4. ■

Утверждение 5. Для любой функции $F \in \mathcal{K}_n$ имеет место

$$2^n - 4(n-1) \leqslant \delta_F \leqslant 2^n - 4.$$

Доказательство. Нижняя граница следует непосредственно из утверждения 4. Из утверждений 1 и 2 получаем, что $\sum\limits_{b \neq a} \delta_F(a,b) \geqslant 4$ для любого ненулевого $a \in \mathbb{F}_2^n$, а значит, $\delta_F(a,a) \leqslant 2^n - 4$. Тогда из того, что $\delta_F(a,b) \leqslant 4$ для любых $a \neq b$ и неравенства $4 \leqslant 2^n - 4$, верного при всех $n \geqslant 3$, следует $\delta_F \leqslant 2^n - 4$. ■

Утверждение 6. Пусть $G = (g_1 \ldots g_n) \in \mathcal{S}_{n,k}$ и $k < n$. Тогда $\delta_G = 2^n$.

Доказательство. По построению, переменная x_n является линейной для функции g_n и фиктивной для остальных координат. Тогда $G(x) \oplus G(x \oplus \mathrm{e}_n) = \mathrm{e}_n$ для всех $x \in \mathbb{F}_2^n$, т. е. $\delta_G(\mathrm{e}_n, \mathrm{e}_n) = 2^n$, следовательно, $\delta_G = 2^n$. ■

Заключение

Исследования показали, что функции из классов $\mathcal{K}_n$ и $\mathcal{S}_{n,k}$ являются криптографически слабыми: их нелинейность и компонентная алгебраическая иммунность малы, а показатель дифференциальной равномерности близок (или равен — для класса $\mathcal{S}_{n,k}$) к максимальному (т. е. худшему) значению 2^n. К достоинствам таких функций можно отнести возможность управлять количеством существенных переменных у их координат; для функций класса $\mathcal{K}_n$ дополнительно — отсутствие линейных и фиктивных переменных у компонент, не равных координатам, и высокая степень $(n-1)$ — максимально возможная для подстановок. Направления дальнейших исследований:

1) изучение применимости атак, эксплуатирующих отмеченные слабости функций, к криптосистемам [2 – 4], как следствие — оценка стойкости этих криптосистем;
2) изучение композиций функций из классов $\mathcal{K}_n$ и $\mathcal{S}_{n,k}$ между собой и с другими функциями с целью нивелирования их недостатков при сохранении положительных свойств;
3) разработка новых алгоритмов генерации обратимых векторных булевых функций с «хорошими» криптографическими характеристиками.

Авторы благодарят Г. П. Агибалова за внимание к работе и ценные замечания.

ЛИТЕРАТУРА

1. *Ding J. and Yang B. Y.* Multivariate public key cryptography // Post-Quantum Cryptography / eds. D. J. Bernstein, J. Buchmann, and E. Dahmen. Berlin; Heidelberg: Springer, 2009. P. 193–241.
2. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
3. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
4. *Agibalov G. P.* ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57–65.
5. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
6. *Canteaut A.* Lecture Notes on Cryptographic Boolean Functions. Paris: Inria, 2016. 48 p.
7. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
8. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.
9. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1 (1). С. 34–42.
10. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474–491.
11. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для русского языка программирования // Прикладная дискретная математика. 2013. № 3(21). С. 93–104.
12. *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.

13. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
14. *Панкратова И. А.* Свойства компонент некоторых классов векторных булевых функций // Прикладная дискретная математика. 2019. № 44. С. 5–11.
15. *Canteaut A.* Open problems related to algebraic attacks on stream ciphers // Proc. WCC'2005, Bergen, Norway, March 14–18, 2005. P. 120–134.

REFERENCES

1. *Ding J. and Yang B. Y.* Multivariate public key cryptography. Post-Quantum Cryptography (eds. D. J. Bernstein, J. Buchmann, and E. Dahmen). Berlin; Heidelberg, Springer, 2009, pp. 193–241.
2. *Agibalov G. P.* Substitution block ciphers with functional keys. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 57–65.
3. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 23–33.
4. *Agibalov G. P.* ElGamal cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 42, pp. 57–65.
5. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
6. *Canteaut A.* Lecture Notes on Cryptographic Boolean Functions. Paris, Inria, 2016. 48 p.
7. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 55–64.
8. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2004, 472 p. (in Russian)
9. *Agibalov G. P.* Elementy teorii differentsial'nogo kriptoanaliza iterativnykh blochnykh shifrov s additivnym raundovym klyuchom [Some theoretical aspects of differential cryptanalysis of the iterated block ciphers with additive round key]. Prikladnaya Diskretnaya Matematika, 2008, no. 1 (1), pp. 34–42. (in Russian)
10. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions. LNCS, 2004, vol. 3027, pp. 474–491.
11. *Agibalov G. P., Lipskiy V. B., and Pankratova I. A.* O kriptograficheskom rasshirenii i ego realizatsii dlya russkogo yazyka programmirovaniya [Cryptographic extension and its implementation for Russian programming language]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 93–104. (in Russian)
12. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables. Proc. CSIST'16, Minsk, BSU Publ., 2016, pp. 519–521.
13. *Pankratova I. A.* Ob obratimosti vektornykh bulevykh funktsiy [On the invertibility of vector Boolean functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2015, no. 8, pp. 35–37. (in Russian)
14. *Pankratova I. A.* Svoystva komponent nekotorykh klassov vektornykh bulevykh funktsiy [Properties of components for some classes of vectorial Boolean functions]. Prikladnaya Diskretnaya Matematika, 2019, no. 44, pp. 5–11. (in Russian)
15. *Canteaut A.* Open problems related to algebraic attacks on stream ciphers. Proc. WCC'2005, Bergen, Norway, March 14–18, 2005, pp. 120–134.