Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/12/13

ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА НЕКОТОРЫХ КЛАССОВ ПОДСТАНОВОК НА $\mathbb{F}_2^n$[1]

Л. А. Карпова, И. А. Панкратова

Рассматриваются два класса подстановок на $\mathbb{F}_2^n$, таких, что каждая их координатная функция существенно зависит ровно от k переменных. Приведены алгоритм вычисления матэкса перемешивающей матрицы функций из данных классов и результаты экспериментального исследования их перемешивающих свойств.

Ключевые слова: *существенная зависимость функции от переменной, перемешивающие свойства функций, элементарный экспонент, матэкс.*

Для $n \in \mathbb{N}$ обозначим через $\mathcal{F}_{n,k}$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, где $F = (f_1 \dots f_n)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, n$, существенно зависят ровно от k переменных. В [1] описаны два метода построения таких функций.

При использовании подстановок в качестве раундовых преобразований в итеративных блочных шифрах важно оценить их «перемешивающие» свойства [2], т. е. распространение существенной зависимости выходных переменных каждого раунда от входов первого раунда. В данной работе рассматриваются перемешивающие свойства функций двух подклассов класса $\mathcal{F}_{n,k}$. Под умножением матриц понимается их логическое умножение — с дизъюнкцией и конъюнкцией в качестве операций сложения и умножения соответственно.

1. Основные определения

Определение 1 [2]. *Перемешивающей матрицей* функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$, называется булева матрица $M(F) = (m_{ij})$ порядка n, где $m_{ij} = 1$, если и только если координатная функция f_j существенно зависит от переменной x_i.

Определение 2 [3]. Булева матрица M называется *положительной* ($M > 0$), если все её элементы равны 1; она называется *примитивной*, если $M^t > 0$ при некотором $t \in \mathbb{N}$; наименьшее t с таким свойством называется *экспонентом матрицы* M, обозначается $\exp M$; для непримитивной матрицы M будем считать $\exp M = \infty$.

Определение 3 [4]. Пусть M — булева матрица порядка n и $i, j \in \{1, \dots, n\}$. *Элементарным экспонентом* (*(i,j)-экспонентом*) матрицы M называется наименьшее число γ, такое, что для любого $t > \gamma$ элемент $m_{ij}^{(t)}$ матрицы M^t равен 1; обозначается $(i,j)\text{-}\exp M$. Матрица элементарных экспонентов $\mathfrak{M}(M) = \big((i,j)\text{-}\exp M\big)$ порядка n называется *матэксом матрицы* M.

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

Проясним связь степени перемешивающей матрицы функции F и существенной зависимости выходов многораундового шифра от входов первого раунда при использовании F в качестве раундового преобразования. Если $m_{ij}^{(t)} = 0$ в матрице $(M(F))^t = \left(m_{ij}^{(t)}\right)$, то j-й выход t-го раунда не зависит от переменной x_i; если $m_{ij}^{(t)} = 1$, то не обязательно такая зависимость есть. Таким образом, (i,j)-$\exp M(F)$ — это оценка снизу количества раундов, после которых j-й выход зависит от переменной x_i, так же как $\exp M(F)$ — оценка снизу количества раундов, при котором достигается полное перемешивание (существенная зависимость всех выходов от всех входных переменных).

Пример 1. Пусть $F(x_1, x_2, x_3) = (x_2 \oplus x_3, x_1 \oplus x_3, x_3)$. Тогда

$$M(F) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad (M(F))^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

$m_{31}^{(2)} = m_{32}^{(2)} = 1$, но после второго раунда имеем $F(F(x_1, x_2, x_3)) = (x_1 \oplus x_3 \oplus x_3, x_2 \oplus \oplus x_3 \oplus x_3, x_3) = (x_1, x_2, x_3)$ — зависимости первого и второго выходов от x_3 нет.

2. Класс функций $S_{n,k}$

В [1, 5] предложен следующий метод построения функций $F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \in \mathcal{F}_{n,k}$:

1) строим функцию $G(x_1, \ldots, x_k) = (g_1(x_1, \ldots, x_k), \ldots, g_k(x_1, \ldots, x_k)) \in \mathcal{F}_{k,k}$ (например, способом, описанным в [6]);
2) для $i = 1, \ldots, k$ полагаем $f_i(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_k)$, переменные $x_{k+1}, \ldots, x_n$ фиктивны для f_i;
3) для $i = k+1, \ldots, n$ полагаем $f_i(x_1, \ldots, x_n) = x_i \oplus h_i(x_1, \ldots, x_{i-1})$, где h_i — любая функция, существенно зависящая от любых $(k-1)$ переменных из $x_1, \ldots, x_{i-1}$.

В [5] доказано, что полученная функция F является подстановкой на $\mathbb{F}_2^n$.

Обозначим $S_{n,k}$ класс функций, которые можно построить таким способом. По построению, каждая координатная функция f_i функции $F \in S_{n,k}$ существенно зависит ровно от k переменных; таким образом, $S_{n,k} \subseteq \mathcal{F}_{n,k}$.

Перемешивающая матрица функции $F \in S_{n,k}$ имеет следующий вид:

$$M(F) = \begin{pmatrix} \overbrace{1\,1\,\ldots\,1}^{k} & 0\,0\,\ldots\,0 \\ 1\,1\,\ldots\,1 & 0\,0\,\ldots\,0 \\ \ldots & \ldots \\ 1\,1\,\ldots\,1 & 0\,0\,\ldots\,0 \\ *\;*\;\ldots\;* & 1\,0\,\ldots\,0 \\ *\;*\;\ldots\;* & *\,1\,\ldots\,0 \\ \ldots & \ldots \\ *\;*\;\ldots\;* & *\;*\;\ldots\,1 \end{pmatrix}.$$

Здесь $m_{ij} = 1$ для всех $i, j \leqslant k$; $m_{ij} = 0$ для всех $i \leqslant k$, $j > k$; $m_{ii} = 1$ для всех $i = 1, \ldots, n$; в позициях, отмеченных «$*$», могут быть как нули, так и единицы (по k единиц в каждой строке). Таким образом, при всех $t \in \mathbb{N}$ для матрицы $(M(F))^t = \left(m_{ij}^{(t)}\right)$ выполняется $m_{ij}^{(t)} = 0$ для всех $i \leqslant k$, $j > k$, поэтому матрица $M(F)$ непримитивная и $\exp M(F) = \infty$.

Оценим элементарные экспоненты матрицы $M(F)$. Из [7] (утверждение $1, a$ при $I = \{i\}$, $J = \{j\}$) следует, что если $a_{ii} = 1$ или $a_{jj} = 1$ в матрице $A = (a_{ij})$ и $a_{ij}^{(\gamma)} = 1$ в матрице $A^\gamma = \left(a_{ij}^{(\gamma)}\right)$, причём γ — минимальное с таким условием, то (i, j)-$\exp A = \gamma$. В матрице $M(F)$ все диагональные элементы единичные, поэтому при возведении матрицы в степень единицы в ней ведут себя «монотонно»: если $m_{ij}^{(k)} = 1$ в матрице $(M(F))^k$, то $m_{ij}^{(t)} = 1$ в матрице $(M(F))^t$ для всех $t \geqslant k$. Получаем алгоритм 1 вычисления матэкса матрицы $M(F)$, который состоит в возведении матрицы в степень до тех пор, пока в ней не перестанут появляться новые единицы.

Алгоритм 1. Вычисление матэкса матрицы с единичной диагональю

Вход: $M = (m_{ij})$ — булева матрица порядка n; $m_{ii} = 1$ для всех $i = 1, \ldots, n$.
Выход: $\mathfrak{M}(M) = (r_{ij})$.

1: **Для** $i = 1, \ldots, n$
2: **Для** $j = 1, \ldots, n$

$$r_{ij} := \begin{cases} 1, & m_{ij} = 1, \\ \infty & \text{иначе.} \end{cases}$$

3: $C := M$.
4: **Для** $k = 2, 3, \ldots$
5: $B := C$; $C := BM$; $D := B \oplus C$ (поэлементно), пусть $D = (d_{ij})$.
6: **Если** D — нулевая матрица, **то**
выход.
7: **Для** $i = 1, \ldots, n$
8: **Для** $j = 1, \ldots, n$
9: **Если** $d_{ij} = 1$, **то**
$r_{ij} := k$.

Для $\mathfrak{M}(M(F)) = (r_{ij})$ обозначим $\gamma_F = \max\limits_{i,j}\{r_{ij} : r_{ij} \neq \infty\}$ — максимальный конечный элементарный экспонент перемешивающей матрицы функции F. Содержательный смысл этой величины следующий: при использовании F в качестве раундового преобразования в итеративном блочном шифре для количества раундов γ_F достигается максимально возможная «степень перемешивания» — зависимость выходов последнего раунда от входов первого раунда, которая не изменится при увеличении числа раундов.

Алгоритм 1 вычисления матэкса и алгоритм генерации случайной функции класса $S_{n,k}$ реализованы программно. Эксперименты показали, что γ_F принимает значения от 2 до 5 для функций $F \in S_{n,k}$ при $n = 4, \ldots, 26$; как и ожидалось, γ_F возрастает с ростом разности $n - k$, т. е. с увеличением числа нулей в перемешивающей матрице функции F.

3. Класс функций $P_{n,k}$

Если $k|n$, то можно предложить следующий способ построения функций $F = (f_1, \ldots, f_n) \in \mathcal{F}_{n,k}$. Пусть $s = n/k$, построим s функций $G_1, \ldots, G_s \in \mathcal{F}_{k,k}$, $G_i = \left(g_1^{(i)}, \ldots, g_k^{(i)}\right)$, $i = 1, \ldots, s$, и положим $f_{tk+i}(x_1, \ldots, x_n) = g_i^{(t+1)}(x_{tk+1}, \ldots, x_{(t+1)k})$, $t = 0, \ldots, s-1$, $i = 1, \ldots, k$. Класс функций, полученных таким способом, будем обозначать $P_{n,k}$. Схема построения функции F приведена на рис. 1, её перемешивающая матрица — на рис. 2.

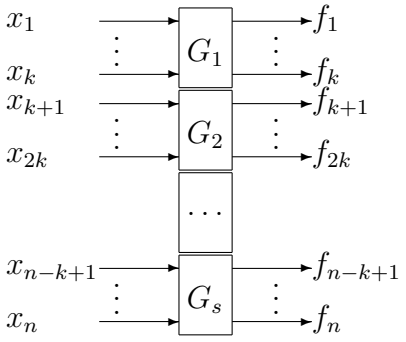

Рис. 1

$$M(F) = \begin{pmatrix} \overbrace{11\dots1}^{k} & 00\dots0 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 11\dots1 & 00\dots0 & \dots & 00\dots0 \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \end{pmatrix}.$$

Рис. 2

Видно, что $(M(F))^t = M(F)$ для всех $t \in \mathbb{N}$, поэтому

$$(i,j)\text{-}\exp M(F) = \begin{cases} 1, & \text{если } m_{ij} = 1, \\ \infty & \text{иначе,} \end{cases}$$

где $M(F) = (m_{ij})$. Для достижения перемешивающих свойств функции класса $P_{n,k}$ можно применять в качестве преобразований замены только в SP-сетях [2, с. 290], чередуя их с преобразованиями перестановки.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. *Фомичев В. М.* О характеристиках локально примитивных орграфов и матриц // Прикладная дискретная математика. Приложение. 2017. № 10. С. 96–99.
5. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
6. *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.
7. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3. С. 68–80.

УДК 519.7 DOI 10.17223/2226308X/12/14

О СВОЙСТВАХ БЕНТ-ФУНКЦИЙ, ПОСТРОЕННЫХ ПО НЕКОТОРОЙ БЕНТ-ФУНКЦИИ С ПОМОЩЬЮ ПОДПРОСТРАНСТВ

Н. А. Коломеец

Рассматриваются свойства конструкции $f \oplus \mathrm{Ind}_L$, где f — бент-функция от $2k$ переменных, а L — аффинное подпространство, при определённых условиях порождающей бент-функции. Доказано, что с помощью подпространств размерности $k+1$ конструкция порождает одинаковое число функций и по f, и по её дуальной