Таким образом, для определения позиции q неизвестного сообщения m потребуется перехватить не менее $N_1 = 2\max\limits_i \max\limits_{h\in\mathcal{H}_i}\{M(h,\alpha,\beta,(1-\Delta^2)/2)\}$ зашумлённых кодовых сообщений, где $i \in \{1,\ldots,k-l+1\}$.

Пусть $q = i$ — определённая позиция сообщения m после наблюдения N_1 зашумлённых кодовых слов. Чтобы оценить необходимый объём выборки для восстановления сообщения m, используем метод восстановления фиксированного сообщения при кодовом зашумлении; метод описан в [3]. Если гипотеза H_i верная, то для применения этого метода нужно использовать выборку (2). Пусть N_2 — необходимое число перехватов для восстановления исходного сообщения m по выборке (2). Тогда минимальное число перехватов зашумлённых кодовых слов, необходимое для восстановления исходного сообщения m, равно $\max(N_1, N_2)$.

ЛИТЕРАТУРА

1. *Wyner A. D.* The wire-tap channel // Bell Sys. Tech. J. 1975. V. 54. P. 1355–1387.
2. *Коржик В. И., Яковлев В. А.* Неасимптотические оценки эффективности кодового зашумления одного канала // Пробл. передачи информ. 1981. Т. 17. № 4 С. 11–18.
3. *Иванов В. А.* Статистические методы оценки эффективности кодового зашумления // Труды по дискретной математике. 2002. Т. 6. С. 48–63.
4. *Chabot C.* Recognition of a code in a noisy environment // Proc. IEEE ISIT, June 2007. P. 2211–2215.
5. *Yardi A. D. and Vijayakumaran S.* Detecting linear block codes in noise using the GLRT // Proc. IEEE Intern. Conf. Communications (ICC), Budapest, Hungary, June 9–13, 2013. P. 4895–4899.

УДК 519.6 DOI 10.17223/2226308X/9/23

О ТОЧНОСТИ МАТРИЧНО-ГРАФОВОГО ПОДХОДА К ОЦЕНКЕ ПЕРЕМЕШИВАЮЩИХ СВОЙСТВ ПРЕОБРАЗОВАНИЙ

С. Н. Кяжин, Ф. В. Лебедев

Приведены экспериментальные результаты оценки точности матрично-графового подхода к исследованию перемешивающих свойств нелинейных преобразований. В качестве класса преобразований, для которого проводилась оценка, взяты все преобразования множества V_n двоичных n-мерных векторов, перемешивающий граф которых есть n-вершинный граф Виландта, а также раундовые подстановки алгоритмов блочного шифрования AES, «Кузнечик» и «Магма» (ГОСТ 28147-89). Установлено, что полученные при матрично-графовом подходе оценки точны для 25 % преобразований с перемешивающим графом Виландта ($n = 9, 10, 11$), а также для раундовой подстановки алгоритмов AES и «Кузнечик». Указанные оценки не являются точными для раундовых подстановок алгоритма «Магма» и для 75 % преобразований с перемешивающим графом Виландта.

Ключевые слова: *перемешивающие свойства, матрично-графовый подход, граф Виландта, AES, «Кузнечик», «Магма».*

Введение

Для оценки перемешивающих свойств с помощью композиции преобразований используют оценочный матрично-графовый подход [1, гл. 10]. Начиная с 2010 г., в журнале «Прикладная дискретная математика» опубликован ряд теоретических и прикладных работ, развивающих данный подход (обзор результатов до 2012 г. см. в [2]).

Перемешивающим графом преобразования g множества X^n называется n-вершинный орграф $\Gamma(g)$, где пара вершин (i,j) образует дугу в $\Gamma(g)$, если и только если i является существенной переменной координатной функции g_j. Матрица $M(g)$ смежности вершин графа $\Gamma(g)$ называется перемешивающей матрицей преобразования g. Преобразование называется совершенным, если все координатные функции зависят от всех переменных.

Многие криптографические функции, например алгоритмы блочного шифрования, являются итеративными (реализуется степень некоторого преобразования g), то есть перемешивающей матрицей реализуемой функции является $M(g^i)$, $i \in \mathbb{N}$. В общем случае $(M(g))^i \geqslant M(g^i)$, $i \in \mathbb{N}$. Следовательно, если матрица $(M(g))^i$ не положительна, то преобразование g^i не совершенно, $i \in \mathbb{N}$ [1, гл. 10]. На данном утверждении основан матрично-графовый подход к исследованию перемешивающих свойств, задача которого — определить наименьшее натуральное k, при котором $(M(g))^k > 0$ (такое k называется экспонентом матрицы $M(g)$, обозначается $\exp M(g)$). Вместо матрицы $(M(g))^i$ равносильно рассматривать её носитель — матрицу, в которой все положительные элементы заменены на 1. Точность матрично-графового подхода определяется различием матриц $(M(g))^i$ и $M(g^i)$, $i \in \mathbb{N}$.

В работе приведены результаты экспериментального исследования точности матрично-графового подхода для преобразований с перемешивающим графом Виландта (класс графов Виландта введён в [3]) и для раундовых подстановок ряда блочных шифров.

1. Точность матрично-графового подхода к оценке перемешивающих свойств нелинейных преобразований с перемешивающим графом Виландта

Обозначим через $G_W(n)$ множество всех нелинейных преобразований множества V_n вида $g = g' \oplus \alpha$ с перемешивающим графом Виландта, где $\alpha \in V_n$ и преобразование $g' : V_n \to V_n$ задано системой координатных функций:

$$g' = \{g_1(x_n), g_2(x_1), g_3(x_2), \ldots, g_{n-1}(x_{n-2}), g_n(x_{n-2}, x_{n-1})\}.$$

По результатам вычислительного эксперимента множество $G_W(10)$ разбивается на равномощные классы G_1, G_2, G_3, G_4. Каждому классу однозначно соответствует последовательность значений $d_{\mathrm{H}}((M(g))^i, M(g^i))$, $i = 2, \ldots, 100$, где $d_{\mathrm{H}}(M_1, M_2)$ — расстояние Хэмминга между матрицами M_1, M_2, определяемое как количество различных элементов. В табл. 1 приведены условия распределения преобразований по классам.

Таблица 1

$g_{10} = x_8x_9$ или $g_{10} = x_8x_9 \oplus x_8 \oplus x_9$	$g_{10} = x_8x_9 \oplus x_9$	$g_{10} = x_8x_9 \oplus x_8$	Условия принадлежности классам
G_1	G_3	G_2	$\|\alpha\|$ нечётный, $\alpha_9 = 0$
G_2	G_4	G_1	$\|\alpha\|$ чётный, $\alpha_9 = 1$
G_3	G_1	G_4	$\|\alpha\|$ нечётный, $\alpha_9 = 1$
G_4	G_2	G_3	$\|\alpha\|$ чётный, $\alpha_9 = 0$

Для преобразований $g \in \{G_1, G_2, G_3\}$ выполнено $(M(g))^k \neq M(g^k)$, начиная с некоторого $k \in \mathbb{N}$. Для преобразования $g \in G_4$ для любого $i \in \mathbb{N}$ выполнено равенство $(M(g))^i = M(g^i)$. При $n = 9, 11$ наблюдается аналогичное разбиение, что позволяет выдвинуть гипотезу о подобном разбиении данного множества преобразований на классы при любом $n > 2$.

Для преобразований $g \in G_W(n)$ выполнены свойства, связанные с перемешиванием.

Утверждение 1. Пусть полугрупповое преобразование $g \in G_W(n)$ имеет тип (d, m), $\gamma = \exp M(g)$. Если $d + m < \gamma$, то существует такое $i \in \mathbb{N}$, что $(M(g))^i > M(g^i)$.

Утверждение 2. Для любого $g \in G_W(n)$ найдётся такой вектор $\alpha \in V_n$, что для любого $i \in \mathbb{N}$ преобразование $(g \oplus \alpha)^i$ не является совершенным.

2. Точность матрично-графового подхода к оценке перемешивающих свойств раундовых подстановок шифров AES, «Кузнечик» и «Магма»

Пусть g_1, g_2 — раундовые подстановки алгоритмов блочного шифрования AES [4] и «Кузнечик» [5] соответственно, построенных на основе SP-сетей. Для $g \in \{g_1, g_2\}$ экспериментально определено, что $M(g^k) = (M(g))^k$ для $k = 2, \ldots, h$, где h — число раундов шифрования алгоритма ($h \in \{10, 12, 14\}$ при $g = g_1$, $h = 9$ при $g = g_2$).

Для алгоритма «Магма» [5], построенного на основе сети Фейстеля, матрично-графовый подход не является точным. В табл. 2 для раундовой подстановки g показана зависимость границы k, при которой $d_{\mathrm{H}}(M(g^i), (M(g))^i) = 0$ для $i \geqslant k$, от числа нулевых младших битов раундового ключа при условии, что все раундовые ключи равны.

Таблица 2

Число нулевых младших битов ключа	$\exp M(g)$	Значения k
0, …, 16	3	6
17, …, 20	3	7
21, …, 32	4	8

Выводы

Результаты оценочного матрично-графового подхода к исследованию перемешивающих свойств преобразований для некоторых преобразований абсолютно точны (для 25 % преобразований из множества $G_W(n)$, $n = 9, 10, 11$). Для многих других преобразований оценки не точны, но могут считаться практически приемлемыми.

Направление дальнейших исследований перемешивающих свойств преобразований следует увязать с глубоким изучением их алгебраических и комбинаторных свойств.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. FIPS PUB 197. Advanced Encryption Standard. NIST, 2001. 47 p.
5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015. 25 с.