УДК 519.17 DOI 10.17223/2226308X/12/37

ОЦЕНКА ХАРАКТЕРИСТИК НЕЛИНЕЙНОСТИ КОМПОЗИЦИЙ ФУНКЦИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ С ПОМОЩЬЮ МАТРИЧНО-ГРАФОВОГО ПОДХОДА

М. Д. Сапегина

Развивается разработанный В. М. Фомичевым матрично-графовый подход к оценке характеристик нелинейности преобразований векторных пространств с помощью троичных матриц над мультипликативной полугруппой $\{0,1,2\}$ или орграфов, дуги которых помечены числами из $\{0,1,2\}$. Орграф Γ с множеством вершин $\{1,\dots,n\}$ называется $\langle 2\rangle$-примитивным, если при некотором натуральном t для любых $i,j \in \{1,\dots,n\}$ найдётся путь из i в j длины t, проходящий через дугу с меткой «2», наименьшее такое t называется $\langle 2\rangle$-экспонентом орграфа Γ (обозначается $\langle 2\rangle$-$\exp\Gamma$). Преобразованию $g(x_1,\dots,x_n)$ множества V_n с координатными функциями $g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)$ соответствует n-вершинный орграф $\Gamma_\Theta(g)$, где дуга (i,j) помечена числом 0, 1 или 2 тогда и только тогда, когда g_j зависит от x_i соответственно фиктивно, линейно или нелинейно, $1 \leqslant i,j \leqslant n$. Преобразование g называют вполне нелинейным, если метка каждой дуги орграфа есть «2». Преобразование g называется $\langle 2\rangle$-перфективным, если при некотором натуральном t все дуги орграфа $\Gamma_\Theta(g^t)$ помечены числом «2», наименьшее такое t называется показателем полной нелинейности преобразования g (обозначается $\langle 2\rangle$-nlg). Доказано: если в помеченном примитивном орграфе Γ метка каждого простого контура содержит число «2» и $\exp\Gamma = n$, то орграф Γ является $\langle 2\rangle$-примитивным и $\langle 2\rangle$-$\exp\Gamma = \exp\Gamma$. Получена оценка $\langle 2\rangle$-экспонента матрицы нелинейности M порядка $2n$ раундовой функции блочных алгоритмов на основе сети Фейстеля с помощью $\langle 2\rangle$-экспонента матрицы нелинейности Φ порядка n функции усложнения: $\langle 2\rangle$-$\exp M \leqslant \langle 2\rangle$-$\exp\Phi + 2$. Эти результаты позволяют снизить сложность вычисления показателя полной нелинейности для некоторых преобразований g. Представлены алгоритмы распознавания полной нелинейности преобразования g и оценки показателя $\langle 2\rangle$-nlg. Для случайных преобразований средняя сложность не превышает $2\gamma(\gamma+1)\log 8n$, где $\langle 2\rangle$-$nlg = \gamma$ и элементарная операция есть вычисление любой функции на любом входном наборе. Алгоритм применён для получения точных значений $\langle 2\rangle$-nlg раундовых подстановок g алгоритмов DES и Магма, получены значения 5 и 6 соответственно.

Ключевые слова: *матрица нелинейности отображения, $\langle 2\rangle$-примитивная матрица (орграф), $\langle 2\rangle$-экспонент матрицы (орграфа), показатель полной нелинейности.*

Введение

Необходимым требованием к свойствам функций, применяемых в алгоритмах защиты данных в информационных системах, является нелинейность, иначе секретный параметр системы может быть раскрыт противником с помощью вычислительно несложного решения системы линейных уравнений [1].

Для решения актуальных задач, направленных на изучение свойства нелинейности композиций отображений векторных пространств, используется оценочный матрично-графовый подход (МГП). В работе представлены результаты, развивающие предложенный В. М. Фомичевым в [2] МГП для оценки характеристик нелинейности отображений на основе свойств троичных матриц над мультипликативной полугруппой

{0,1,2}. Этот подход обобщает МГП к исследованию примитивности и экспонентов 0,1-матриц и соответствующих орграфов.

1. Мультипликативный моноид троичных матриц (помеченных орграфов)

Пусть $G = \{0, 1, 2\}$ — мультипликативная коммутативная полугруппа с операцией, определяемой равенствами: $a0 = 0$ для любого $a \in G$; $ab = \max\{a, b\}$ для любых $a, b \neq 0$. Матрица любого размера над G называется троичной матрицей. Троичная матрица называется особенной, если она имеет нулевую строку или нулевой столбец.

Умножение троичной матрицы $A = (a_{i,j})$ размера $n \times m$ на матрицу $B = (b_{i,j})$ размера $m \times r$ задается следующим образом: $AB = C = (c_{i,j})$, где C — матрица размера $n \times r$, $c_{i,j} = \max\{a_{i,1}b_{1,j}, \ldots, a_{i,m}b_{m,j}\}$ для любых допустимых i, j, умножение элементов выполнено в полугруппе G.

Неособенная матрица называется 2-матрицей, если каждый элемент матрицы равен 2. При $n > 1$ троичной матрице $M = (m_{i,j})$ порядка n биективно соответствует помеченный n-вершинный орграф Γ, у которого дуга (i, j) имеет метку $m_{i,j}$, $0 \leqslant i, j < n$, где метка «0» равносильна отсутствию дуги в орграфе. Матрица M над полугруппой G называется матрицей меток орграфа Γ и обозначается $M(\Gamma)$.

Помеченный орграф Γ с матрицей меток $M(\Gamma) = (2)^n$, где $(2)^n$ – матрица, все элементы которой равны 2, называется полным 2-графом. Помеченный орграф Γ называется $\langle 2\rangle$-примитивным, если Γ^t является полным 2-графом при некотором $t \in \mathbb{N}$, и наименьшее t с таким свойством называется $\langle 2\rangle$-экспонентом орграфа Γ (обозначается $\langle 2\rangle$-$\exp\Gamma$).

Матрица M над G при $n = m$ называется $\langle 2\rangle$-примитивной, если M^t есть 2-матрица при некотором $t \in \mathbb{N}$. Наименьшее t с таким свойством обозначается $\langle 2\rangle$-$\exp M$ и называется $\langle 2\rangle$-экспонентом матрицы M. Если M^t есть 2-матрица при некотором $t \in \mathbb{N}$, то M^τ есть 2-матрица при любом $\tau > t$. Указанное соответствие троичных матриц и помеченных орграфов есть биекция [2], поэтому орграф Γ $\langle 2\rangle$-примитивный, если и только если $\langle 2\rangle$-примитивна матрица $M(\Gamma)$, и $\langle 2\rangle$-$\exp\Gamma = \langle 2\rangle$-$\exp M$.

2. Нелинейные свойства преобразований векторных пространств

Приведём необходимые определения [2]. Пусть P — конечное поле. Обозначим $\{f_j(x_0, \ldots, x_{n-1}) : j = 0, \ldots, m-1\}$ множество координатных функций отображения $\varphi : P^n \to P^m$. Функции φ соответствует троичная матрица $M_\Theta(\varphi) = (m_{i,j})$ над полугруппой G размера $n \times m$, называемая матрицей нелинейности функции φ, где элемент $m_{i,j}$ равен 0, 1 или 2, если и только если f_j зависит от x_i соответственно фиктивно, линейно или нелинейно, $0 \leqslant i < n$, $0 \leqslant j < m$. Равносильно можно рассматривать орграф $\Gamma_\Theta(\varphi)$ нелинейности функции φ. Заметим, что преобразование, удовлетворяющее строгому лавинному критерию, является вполне нелинейным [3].

Показателем полной нелинейности преобразования g множества P^n (обозначим $\langle 2\rangle$-nlg) называется наименьшее натуральное t (если такое существует), при котором преобразование g^t является вполне нелинейным. Известно [2], что $\langle 2\rangle$-$nlg \geqslant \langle 2\rangle$-$\exp M_\Theta(g)$.

3. Оценки $\langle 2\rangle$-экспонентов новых классов матриц нелинейности

Известно [2], что если примитивный помеченный орграф Γ имеет дугу с меткой «2», то Γ $\langle 2\rangle$-примитивный и $\langle 2\rangle$-$\exp\Gamma \leqslant \exp\Gamma + n$. Уточним эту оценку для некоторых орграфов.

Теорема 1. Если в примитивном помеченном орграфе Γ любой простой контур проходит через дугу с меткой «2» и $\exp\Gamma \geqslant n$, то Γ является $\langle 2\rangle$-примитивным и $\langle 2\rangle\text{-}\exp\Gamma = \exp\Gamma$.

Теорема 2. Если блоковая запись матрицы нелинейности M, в которой каждый элемент есть подматрица размера $n \times n$, имеет вид

$$M = \begin{pmatrix} 0 & E \\ E & \Phi \end{pmatrix},$$

где 0 — нулевая подматрица; E — единичная подматрица; Φ — $\langle 2\rangle$-примитивная матрица и $\langle 2\rangle\text{-}\exp\Phi = t$, то $\langle 2\rangle\text{-}\exp M \leqslant t + 2$.

Данная теорема может применяться для оценки $\langle 2\rangle$-экспонента матрицы нелинейности раундовой функции алгоритмов, построенных на основе сети Фейстеля, с помощью $\langle 2\rangle$-экспонента матрицы нелинейности функции усложнения. Это существенно сокращает расчёты, поскольку для оценки вычисляется $\langle 2\rangle$-экспонент матрицы нелинейности функции усложнения, порядок которой меньше порядка матрицы нелинейности раундовой функции в 2 раза.

Обозначим: V_n — множество двоичных n-мерных векторов; $g(x_1, \ldots, x_n)$ — преобразование множества V_n; $g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)$ — координатные булевы функции преобразования g; $I(x)$ — множество номеров единичных координат вектора $x \in V_n$; $e_i \in V_n$, где $I(e_i) = \{i\}$, $i = 1, \ldots, n$.

Приведём алгоритмы распознавания полной нелинейности преобразования g и оценки показателя $\langle 2\rangle$-nlg.

Лемма 1. Пусть для тройки векторов $a, b, e_i \in V_n$ выполнено $g(a \oplus e_i) \oplus g(a) \oplus \oplus g(b \oplus e_i) \oplus g(b) = \varepsilon_i$, тогда координатная функция $g_j(x_1, \ldots, x_n)$ преобразования g зависит нелинейно от переменной x_i для любого $j \in I(\varepsilon_i)$, $i = 1, \ldots, n$.

Обозначим $\vee(\varepsilon_1, \ldots, \varepsilon_t)$ покоординатную дизъюнкцию векторов $\varepsilon_1, \ldots, \varepsilon_t \in V_n$.

Следствие 1. Пусть имеется множество троек векторов (a_s, b_s, e_i), $s = 1, \ldots, t(i)$, такое, что $g(a_s \oplus e_i) \oplus g(a_s) \oplus g(b_s \oplus e_i) \oplus g(b_s) = \varepsilon_{i,s}$ и $I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t(i)})) = \{1, \ldots, n\}$, $i = 1, \ldots, n$. Тогда преобразование $g(x_1, \ldots, x_n)$ является вполне нелинейным.

Лемма 2. Если преобразование $g(x_1, \ldots, x_n)$ случайное, то для всех $i = 1, \ldots, n$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, n\}] = (1 - 2^{-t})^n$, $t = 1, 2, \ldots$

Следствие 2. Для случайного преобразования $g(x_1, \ldots, x_n)$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = = \{1, \ldots, n\}] > 1 - n2^{-t}$.

Лемма 3. При $n > 3$ среди всех преобразований множества V_n доля вполне нелинейных преобразований не меньше $1 - n^2 2^{-2^{n-1}+1}$.

На основе леммы 1 реализован алгоритм распознавания полной нелинейности различных степеней преобразования g. Для этого для всех $i = 1, \ldots, n$ фиксируем вектор e_i и генерируем пары случайных векторов (a_s, b_s), $s = 1, \ldots, t(i)$, и при $h = 1, 2, 3, \ldots$ вычисляем $\varepsilon^h_{i,s} = g^h(a_s \oplus e_i) \oplus g^h(a_s) \oplus g^h(b_s \oplus e_i) \oplus g^h(b_s)$. Если при некоторых $s \leqslant t(i)$ и $h \in \mathbb{N}$ (из вероятностных соображений по отношению к случайным функциям взято $t(i) = \log 4n$, т. е. $s = 1, \ldots, \log 4n$, так как при $t = \log 4n$ $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, n\}] > 0{,}75$) выполнено $I(\vee(\varepsilon^h_{i,1}, \ldots, \varepsilon^h_{i,t(i)})) = \{1, \ldots, n\}$ для всех $i = 1, \ldots, n$, то преобразование g^h вполне нелинейное и $\langle 2\rangle$-$nlg \leqslant h$. Данный алгоритм позволяет оценить сверху показатель полной нелинейности преобразования g.

Оценим вычислительную сложность алгоритма. Элементарной операцией будем считать вычисление значения любой функции на любом входном наборе.

Теорема 3. Пусть g есть $\langle 2\rangle$-перфективное преобразование множества V_n и $\langle 2\rangle$-$nlg = \gamma$. Если при случайном независимом и равновероятном выборе из $V_n \times V_n$ пар векторов (a_s, b_s) величины $\varepsilon^h_{i,s}$, $s = 1, \ldots, t$, независимы и распределены равномерно, $h = 1, 2, \ldots$, где $\varepsilon^h_{i,s} = g^h(a_s \oplus e_i) \oplus g^h(a_s) \oplus g^h(b_s \oplus e_i) \oplus g^h(b_s)$, то средняя сложность алгоритма с параметром $t = \log 4n$ не превышает $2\gamma(\gamma + 1) \log 8n$.

С помощью разработанного алгоритма с параметром $t = 100$ (поскольку тогда $\mathsf{P}[I(\vee(\varepsilon_{i,1}, \ldots, \varepsilon_{i,t})) = \{1, \ldots, 64\}] \to 1$) определены верхние оценки показателей полной нелинейности раундовых подстановок алгоритмов DES и Магма. Для алгоритма DES она равна 5, для алгоритма Магма — 6.

В [5] с помощью МГП на основе свойств троичных матриц получены нижние оценки показателей полной нелинейности для раундовых подстановок алгоритмов DES и Магма. Они совпадают с полученными верхними оценками показателей полной нелинейности. Таким образом, для алгоритма DES наименьшая степень, в которой раундовая подстановка является вполне нелинейной, равно 5, для алгоритма Магма — 6.

Выводы

Разработан и реализован алгоритм для вычисления верхней оценки показателя полной нелинейности отображений со сложностью, не превышающей $2\gamma(\gamma + 1) \log 8n$, где показатель полной нелинейности исследуемого преобразования $\langle 2\rangle$-$nlg = \gamma$ и элементарная операция есть вычисление любой функции на любом входном наборе. Получены точные значения показателей полной нелинейности раундовых подстановок алгоритмов DES и Магма, они равны 5 и 6 соответственно. Доказано достаточное условие равенства $\langle 2\rangle$-$\exp \Gamma = \exp \Gamma$. Получена оценка $\langle 2\rangle$-экспонента матрицы нелинейности M порядка $2n$ раундовой функции блочных алгоритмов на основе сети Фейстеля с помощью $\langle 2\rangle$-экспонента матрицы нелинейности Φ порядка n функции усложнения, а именно: $\langle 2\rangle$-$\exp M \leqslant \langle 2\rangle$-$\exp \Phi + 2$. Эта оценка позволяет снизить сложность вычисления показателя полной нелинейности.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Фомичев В. М.* О производительности некоторых итеративных алгоритмов блочного шифрования из класса WBC // New Trends in Coding Systems and Techniques. LDN: Intech Publishing, 2019. С. 14.
3. *Фомичев В. М.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: ЮРАЙТ, 2016.
4. *Сапегина М. Д.* Оценка характеристик нелинейности раундовых подстановок алгоритмов «DES» и «Магма» // Информационная безопасность в банковско-финансовой сфере. Сб. науч. работ участников Междунар. молодежной науч.-практич. конф. в рамках V Междунар. форума «Как попасть в пятерку?». М.: Прометей, 2018. С. 6.