ЛИТЕРАТУРА

1. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Издательство Юрайт, 2016. 209 с.
2. *Кяжин В. М., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.

УДК 519.1 DOI 10.17223/2226308X/10/39

О ХАРАКТЕРИСТИКАХ ЛОКАЛЬНО ПРИМИТИВНЫХ ОРГРАФОВ И МАТРИЦ[1]

В. М. Фомичев

Введены новые характеристики локально примитивного n-вершинного орграфа Γ (матрицы M порядка $n > 1$): матэкс, определённый как матрица $(\gamma_{i,j})$ порядка n, где $\gamma_{i,j} = (i,j)\text{-exp}\,\Gamma$, $1 \leqslant i, j \leqslant n$; k,r-экспорадиус, обозначенный $\text{exrd}_{k,r}\Gamma$ и определённый как $\min\limits_{I\times J:|I|=k,|J|=r} \gamma_{I,J}$, где $\gamma_{I,J} = \max\limits_{(i,j)\in I\times J} \gamma_{i,j}$; k,r-экспоцентр, определённый при $|I| = k$, $|J| = r$ как множество $I \times J$, такое, что $\gamma_{I,J} = \text{exrd}_{k,r}\Gamma$. С использованием введённых характеристик изложен подход к построению совершенных s-боксов размера $k \times r$ (в том числе при $k, r > 8$), используемых в конструкциях раундовых подстановок блочных шифров. Подход основан на итерациях преобразования g множества V_n двоичных n-мерных векторов, где $n > \max(k, r)$. Приведён пример построения совершенной функции $V_k \to V_r$.

Ключевые слова: *локально примитивная матрица (орграф), локальный экспонент.*

1. Новые характеристики

Обозначим: $\mathbb{N}$ — множество натуральных чисел; $n \in \mathbb{N}$; $N_n = \{1, \ldots, n\}$; V_n — множество n-мерных двоичных векторов; $I, J \subseteq N_n$, где $\varnothing \neq I = \{i_1, \ldots, i_k\}$, $\varnothing \neq J = \{j_1, \ldots, j_r\}$.

Матрица M называется $I \times J$-примитивной ((i,j)-примитивной при $I = \{i\}$, $J = \{j\}$) [1], если существует $\gamma \in \mathbb{N}$, такое, что матрица $M^t(I \times J)$, полученная из матрицы M^t удалением строк с номерами $i \neq i_1, \ldots, i_k$ и столбцов с номерами $j \neq j_1, \ldots, j_r$, положительная при любом $t \geqslant \gamma$. Наименьшее такое число γ называется $I \times J$-экспонентом матрицы M и обозначается $I \times J\text{-exp}M$ или $\gamma_{I,J}$. Элементарным экспонентом матрицы (орграфа) называется $I \times J$-экспонент при $I = \{i\}$, $J = \{j\}$, где $(i,j) \in N_n^2$, записывается как (i,j)-экспонент и обозначается $(i,j)\text{-exp}M$ или $\gamma_{i,j}$. Если матрица M не (i,j)-примитивная, то положим $(i,j)\text{-exp}M = \infty$.

В развитие математического аппарата локальной примитивности неотрицательных матриц и орграфов [1, 2], используемого для оценки перемешивающих свойств преобразований множества n-мерных векторов, введём новые характеристики: матэкс, определяющий все локальные экспоненты, k,r-экспорадиус, k,r-экспоцентр, $k, r \in N_n$. Из множества всех элементарных экспонентов матрицы M (орграфа Γ) составим квадратную матрицу $\mathfrak{M}(M) = ((i,j)\text{-exp}M)$ (матрицу $\mathfrak{M}(\Gamma) = ((i,j)\text{-exp}\,\Gamma)$) порядка n, которую назовём матрицей элементарных экспонентов, кратко матэксом, матрицы M (орграфа Γ). Любой локальный экспонент матрицы M можно вычислить по матэксу $\mathfrak{M}(M)$: $\gamma_{I,J} = I \times J\text{-exp}M = \max\limits_{(i,j)\in I\times J} (i,j)\text{-exp}M$, где $I, J \subseteq N_n$.

[1]Работа выполнена в соответствии с грантом РФФИ № 16-01-00226.

Если $M \geqslant M'$, то (i,j)-exp$M \leqslant (i,j)$-expM' для любой пары $(i,j) \in N_n^2$ и $\mathfrak{M}(M) \leqslant \leqslant \mathfrak{M}(M')$.

Определим в Γ характеристики, связанные с локальными экспонентами. Назовём k,r-экспорадиусом орграфа Γ величину, обозначаемую $\mathrm{exrd}_{k,r}\Gamma$: $\mathrm{exrd}_{k,r}\Gamma = \min\limits_{I\times J:|I|=k,|J|=r} \gamma_{I,J}$.

При $|I| = k$, $|J| = r$ множество $I \times J$ назовем k,r-экспоцентром графа Γ, если $\gamma_{I,J} = \mathrm{exrd}_{k,r}\Gamma$. При любых фиксированных k,r в примитивном орграфе Γ существует k,r-экспоцентр, в общем случае не единственный. Если орграф Γ локально примитивный, то k,r-экспоцентр существует, если орграф Γ имеет конечный k,r-экспорадиус.

2. К задаче построения s-боксов

Покажем прикладное значение введённых характеристик, приведём пример расчёта. Важным элементом блочных алгоритмов шифрования являются нелинейные отображения $V_k \to V_r$, называемые s-боксами размера $k \times r$ и используемые при построении раундовых подстановок блочных шифров (в DES, ГОСТ 28147-89 и «Кузнечике» s-боксы имеют размеры 6×4, 4×4 и 8×8 соответственно). При разработке к свойствам s-боксов предъявляется ряд требований: биективность (при $k = r$), совершенность (то есть существенная зависимость каждой координатной булевой функции от всех входных переменных), простота программной и/или аппаратной реализации и др. При небольших размерах ($r \leqslant 8$) s-боксы обычно реализуют с помощью таблиц. Однако чем больше r, тем более ресурсоёмкой является табличная реализация как по размеру памяти, так и по времени. Значит, актуальна разработка быстрых алгоритмов реализации s-бокса. Изложим идею одного подхода.

Совершенные s-боксы размера $k \times r$, в том числе при больших k и r, можно реализовать на основе итераций преобразования g множества V_n, где $n > \max(k,r)$.

Обозначим $X = \{x_1,\ldots,x_n\}$; $\{g_1(X),\ldots,g_n(X)\}$ — система координатных функций преобразования g; $G^t = \{g_1^t(X),\ldots,g_n^t(X)\}$ — система координатных функций преобразования g^t, $t = 1,2,\ldots$; Γ — перемешивающий орграф преобразования g; M — матрица смежности вершин орграфа Γ; G_J^t — бесповторная упорядоченная выборка размера r из множества G^t, такая, что $g_j^t(X) \in G_J^t \Leftrightarrow j \in J$; X_I — бесповторная упорядоченная выборка размера k из множества X, такая, что $x_i \in X_I \Leftrightarrow i \in I$. Выборкам X_I и G_J^t при любой фиксации $\bar\alpha$ переменных из $X\backslash X_I$ соответствует система координатных функций отображения $s_t(\bar\alpha) : V_k \to V_r$, $t = 1,2,\ldots$

Определим, при каких множествах I,J и каком наименьшем натуральном t отображение $s_t(\bar\alpha)$ является совершенным. Для быстроты реализации $s_t(\bar\alpha)$ важно, чтобы некоторые локальные экспоненты перемешивающей матрицы были относительно невелики.

Отображение $s_t(\bar\alpha)$ имеет наилучшие перемешивающие свойства, если орграф Γ является $I \times J$-примитивным и при фиксированных I,J наименьшее t с таким свойством равно $I \times J$-exp$\,\Gamma$. Если $\mathrm{exrd}_{k,r}\Gamma = \theta$, то минимизация значения t выполняется с помощью выбора множеств I и J порядка k и r соответственно таким образом, чтобы $I \times J$-exp$\,\Gamma = \theta$. Следовательно, наилучший (в смысле времени реализации) выбор множеств I и J для построения совершенного отображения выполняется тогда, когда $I \times J$ есть k,r-экспоцентр графа Γ.

Существование среди $s_\theta(\bar\alpha)$ совершенного отображения $V_k \to V_r$ зависит от преобразования g. Отметим, что примеры успешной реализации описанного подхода к построению совершенных подстановок имеются [3].

Пример 1. Пусть g — преобразование регистра левого сдвига с функцией обратной связи $f(x_1,\dots,x_8)=x_1\oplus x_3x_4\oplus x_8$, длина регистра равна 8. Построим отображения $V_4\to V_4$ вида $s_\theta(\bar\alpha)$.

Перемешивающий 8-вершинный орграф Γ преобразования g примитивный (рис. 1), так как сильносвязный и имеет петлю. Составим матэкс $\mathfrak{M}(\Gamma)$ орграфа Γ, где (i,j)-$\exp\Gamma$ равен длине кратчайшего пути из i в j, проходящего через вершину с петлей:

$$\mathfrak{M}(\Gamma)=\begin{pmatrix}8&7&6&5&4&3&2&1\\9&8&7&6&5&4&3&2\\8&7&6&5&4&3&2&1\\8&7&6&5&4&3&2&1\\9&8&7&6&5&4&3&2\\10&9&8&7&6&5&4&3\\11&10&9&8&7&6&5&4\\7&6&5&4&3&2&1&1\end{pmatrix}.$$

По матэксу $\mathfrak{M}(\Gamma)$ определяем $\exp\Gamma=11$; $4,4$-экспорадиус равен 4.

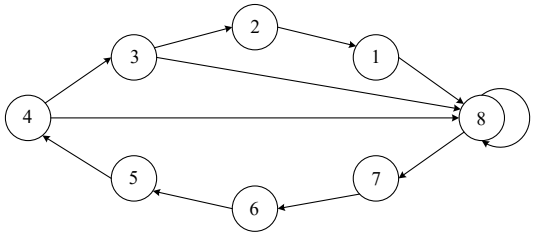

Рис. 1. Перемешивающий орграф Γ

Выпишем системы координатных функций для преобразований g, g^2, g^3, g^4:

t	g_1^t	g_2^t	g_3^t	g_4^t	g_5^t	g_6^t	g_7^t	g_8^t
1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	f_1
2	x_3	x_4	x_5	x_6	x_7	x_8	f_1	f_2
3	x_4	x_5	x_6	x_7	x_8	f_1	f_2	f_3
4	x_5	x_6	x_7	x_8	f_1	f_2	f_3	f_4

Здесь $f_1(x_1,\dots,x_8)=x_1\oplus x_3x_4\oplus x_8$, $f_2(x_1,\dots,x_8)=x_2\oplus x_4x_5\oplus f_1(x_1,\dots,x_8)$, $f_3(x_1,\dots,x_8)=x_3\oplus x_5x_6\oplus f_2(x_1,\dots,x_8)$, $f_4(x_1,\dots,x_8)=x_4\oplus x_6x_7\oplus f_3(x_1,\dots,x_8)$.

В Γ имеется один $4,4$-экспоцентр $\{1,3,4,8\}\times\{5,6,7,8\}$, которому соответствует класс отображений $V_4\to V_4$ (при различных фиксациях переменных x_2,x_5,x_6,x_7 координатных функций f_1, f_2, f_3, f_4). Например, при фиксации $x_6=x_7=0$ и $x_2=x_5=1$ имеем совершенное отображение $V_4\to V_4$, заданное системой координатных функций

$$\{x_1\oplus x_3x_4\oplus x_8,\ x_1\oplus x_3x_4\oplus x_8\oplus x_4\oplus 1,\ x_1\oplus x_3x_4\oplus x_8\oplus x_3\oplus x_4\oplus 1,\ x_1\oplus x_3x_4\oplus x_8\oplus x_3\oplus 1\}.$$

Заметим, что данное отображение не является примером «хорошего» s-бокса, так как оно не биективно ($f_1(x_1,\dots,x_8)\oplus f_2(x_1,\dots,x_8)\oplus f_3(x_1,\dots,x_8)\oplus f_4(x_1,\dots,x_8)=1$).

В рамках описанного подхода проблема построения s-боксов размера $k\times r$ при заданных k,r сводится к поиску при некоторых $n>\max(k,r)$ преобразований g множества V_n, таких, что, используя их степени, можно построить отображения $V_k\to V_r$ с заданным набором свойств.

ЛИТЕРАТУРА

1. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
2. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 1. С. 97–119.
3. *Фомичев В. М., Задорожный Д. И., Коренева А. М., Лолич Д. М., Юзбашев А. В.* Об алгоритмической реализации s-боксов // Проблемы информационной безопасности. Компьютерные системы. 2017 (в печати).

УДК 519.1 DOI 10.17223/2226308X/10/40

О СВОЙСТВАХ ТРЁХКАСКАДНОГО ГЕНЕРАТОРА С ПЕРЕМЕЖАЮЩИМСЯ ШАГОМ, ПОСТРОЕННОГО НА ОСНОВЕ СХЕМЫ ДВИЖЕНИЯ «СТОП-ВПЕРЁД»[1]

В. М. Фомичев, Д. М. Колесова

Посчитан ряд характеристик трёхкаскадного генератора гаммы с перемежающимся шагом (схема движения «стоп-вперед»), где первый управляющий каскад построен на основе регистра сдвига с линейной обратной связью (ЛРС) длины n, второй управляющий каскад — на основе двух ЛРС длин m и μ, третий генерирующий каскад — на основе двух ЛРС длин r и ρ. Если все ЛРС имеют примитивные характеристические многочлены и числа n, m, μ, r, ρ попарно взаимно простые, то длина периода t гаммы генератора равна $(2^n-1)(2^m-1)(2^\mu-1)(2^r-1)(2^\rho-1)$. Циклическая группа генератора порядка t порождается подстановкой множества состояний, реализуемой за один такт, и содержит линейную подгруппу порядка $(2^r-1)(2^\rho-1)$. Получены значения локальных $i,(p+1)$-экспонентов перемешивающего орграфа генератора, $i=1,\dots,p$, где $p=n+m+\mu+r+\rho$, из которых следует, что длину «холостого хода» генератора целесообразно определить не меньше, чем $\max\{n+2, \max(m,\mu)+1, \max(r,\rho)\}$.

Ключевые слова: *генератор гаммы, регистр сдвига с линейной обратной связью, длина периода гаммы, перемешивающие свойства, локальная примитивность орграфа.*

Введение

Генераторы гаммы с неравномерным движением, активно исследуемые как в России, так и за рубежом [1, гл. 18], относительно просто реализуются и обладают рядом положительных криптографических свойств: большая длина периода, высокая линейная сложность и др. К этому классу относятся двухкаскадные генераторы с перемежающимся шагом, построенные на основе двух генераторов «стоп-вперед». Для их обобщения — трёхкаскадных генераторов с перемежающимся шагом — получен ряд свойств.

1. Функционирование трёхкаскадного генератора с перемежающимся шагом

Первый управляющий каскад есть фильтрующий генератор на базе ЛРС-x длины n и фильтрующей функции $f(x_1,\dots,x_n)$, генерирующий управляющую гамму $\{\gamma_{i,x} : i=1,2,\dots\}$. Второй управляющий каскад состоит из ЛРС-y и ЛРС-z соответственно длины m (номера ячеек $n+1,\dots,n+m$) и μ (номера ячеек $n+m+1,\dots,$

[1]Работа первого автора выполнена в соответствии с грантом РФФИ № 16-01-00226.