УДК 519.1 DOI 10.17223/2226308X/10/4

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩИХ ПОДСТАНОВОК РЕГИСТРОВ СДВИГА[1]

В. С. Григорьев, В. М. Фомичев

Исследованы некоторые вопросы примитивности перемешивающих орграфов композиций регистровых подстановок и связь экспонентов прямой и обратной подстановок. Пусть $G(g)$ — перемешивающий орграф подстановки g регистра левого сдвига длины n и $\{i_1, \ldots, i_m\}$ — множество номеров существенных переменных функции обратной связи. Установлено, что орграф $G(g)$ примитивный тогда и только тогда, когда примитивен орграф $G(g^{-1})$. При этом $\exp G(g) = \exp G(g^{-1})$, если $i_k + i_{m+2-k} = n + 2$ для всех $k = 2, \ldots, m$. Для подстановки g регистра правого сдвига длины n с обратной связью $x_n \oplus \psi(x_1, \ldots, x_{n-1})$ и подстановки h регистра левого сдвига длины n с обратной связью $x_1 \oplus \phi(x_2, \ldots, x_n)$ показано, что 1) множество дуг перемешивающего орграфа $G(gh)$ состоит из n петель (по одной в каждой вершине) и дуг вида (i, n), где $i \in \{1, \ldots, n-1\}$, таких, что x_i — существенная переменная функции $\psi(x_1, \ldots, x_{n-1}) \oplus \phi(x_1, \ldots, x_{n-1})$; 2) множество дуг перемешивающего орграфа $G(hg)$ состоит из n петель (по одной в каждой вершине) и дуг вида $(i, 1)$, где $i \in \{2, \ldots, n\}$, таких, что x_i — существенная переменная функции $\psi(x_2, \ldots, x_n) \oplus \phi(x_2, \ldots, x_n)$. Для преобразования g регистра правого сдвига длины n с обратной связью $f(x_1, \ldots, x_n)$ и треугольной подстановки h множества $\{0,1\}^n$ показано, что если орграф $G(g)$ примитивный, то примитивными являются орграфы $G(g) \cdot G(h)$ и $G(h) \cdot G(g)$ и экспонент каждого из этих орграфов не превосходит $\exp G(g)$.

Ключевые слова: *перемешивающий граф преобразования, примитивный граф, экспонент графа, регистр сдвига, треугольное преобразование.*

Введение

Одним из положительных криптографических свойств преобразований векторных пространств является хорошее перемешивание, то есть зависимость каждого бита выходного вектора от всех входных битов. При исследовании различных классов преобразований используется матрично-графовый подход, существо которого состоит в изучении свойства примитивности перемешивающей матрицы (орграфа) преобразования и определении экспонента или локальных экспонентов матрицы (орграфа). Обзор известных на сегодняшний день результатов содержится в [1].

Вместе с тем имеются мало изученные области, связанные с определением экспонентов или локальных экспонентов матриц (орграфов). В некоторых задачах важно определить экспонент как прямой, так и обратной подстановки (например, при оценке эффективности применения метода согласования к анализу симметричных блочных шифров).

Работа посвящена вопросам примитивности перемешивающих орграфов композиций регистровых подстановок, а также связи экспонентов прямой и обратной подстановок.

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

1. Регистр сдвига с одной обратной связью

Обозначим $g(x_1, \ldots, x_n)$ обратимое преобразование двоичного регистра левого сдвига длины n с обратной связью $x_1 \oplus \psi(x_2, \ldots, x_n)$:

$$g(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1 \oplus \psi(x_2, \ldots, x_n)) = (y_1, \ldots, y_n). \quad (1)$$

Преобразование $g^{-1}(y_1, \ldots, y_n)$ реализуется двоичным регистром правого сдвига длины n с обратной связью $y_n \oplus \phi(y_1, \ldots, y_{n-1})$:

$$g^{-1}(y_1, \ldots, y_n) = (y_n \oplus \phi(y_1, \ldots, y_{n-1}),\ y_1, \ldots, y_{n-1}) = (x_1, \ldots, x_n). \quad (2)$$

Пусть регистр сдвига имеет m ячеек съёма с номерами $i_1, \ldots, i_m$, где $1 = i_1 < \ldots < i_m \leqslant n$, то есть функция обратной связи $x_1 \oplus \psi(x_2, \ldots, x_n)$ имеет m существенных переменных. Тогда в соответствии с (1) n-вершинный перемешивающий орграф $G(g)$ состоит из гамильтонова контура $(n, \ldots, 2, 1)$ и дуг $(i_2, n), \ldots, (i_m, n)$. Следовательно, орграф $G(g)$ содержит m простых контуров длин n, $n - i_2 + 1$, $\ldots$, $n - i_m + 1$.

В соответствии с (2) n-вершинный перемешивающий орграф $G(g^{-1})$ состоит из гамильтонова контура $(1, 2, \ldots, n)$ и дуг $(i_2 - 1, n), \ldots, (i_m - 1, n)$. Следовательно, орграф $G(g^{-1})$ содержит m простых контуров длин n, $i_2 - 1$, $\ldots$, $i_m - 1$.

В соответствии с универсальным критерием орграф $G(g)$ примитивный, если и только если он сильносвязный и имеет $m \geqslant 1$ простых контуров с длинами $l_1, \ldots, l_m$, где $(l_1, \ldots, l_m) = 1$ [2, с. 103].

Через $\Phi(l_1, \ldots, l_m)$ обозначим число Фробениуса для натуральных аргументов $l_1, \ldots, l_m$. Тогда экспонент примитивного перемешивающего орграфа $G(g)$ регистра сдвига равен

$$\exp G(g) = \max_{1 \leqslant i,j \leqslant n} \rho(i, j) + \Phi(n, n - i_2 + 1, \ldots, n - i_m + 1) + 1,$$

где $\rho(i, j)$ — длина кратчайшего пути в $G(g)$ из вершины i в вершину j, проходящего через вершину n (общую вершину всех m контуров) [3]. В нашем случае

$$\max_{1 \leqslant i,j \leqslant n} \rho(i, j) = \rho(g) + n - 1,$$

где $\rho(g) = \max\{i_2 - i_1, \ldots, i_m - i_{m-1}, n - i_m\}$ — наибольший «разброс» m точек съёма на регистре длины n.

Экспонент примитивного перемешивающего орграфа $G(g^{-1})$ регистра сдвига равен $\exp G(g^{-1}) = \max\limits_{1 \leqslant i,j \leqslant n} \rho(i, j) + \Phi(n, i_2 - 1, \ldots, i_m - 1) + 1$. Следовательно, $\exp G(g) = \exp G(g^{-1})$, если $\{i_2 - 1, \ldots,\ i_m - 1\} = \{n - i_2 + 1, \ldots, n - i_m + 1\}$.

Теорема 1. Орграф $G(g)$ примитивен тогда и только тогда, когда примитивен орграф $G(g^{-1})$. При этом $\exp G(g) = \exp G(g^{-1})$, если $i_k + i_{m+2-k} = n + 2$ для всех $k = 2, \ldots, m$.

Исследованы перемешивающие орграфы композиции двух регистровых подстановок с разнонаправленными сдвигами. Композиции различных преобразований исследованы в [4].

Теорема 2. Пусть g — подстановка регистра правого сдвига длины n с обратной связью $x_n \oplus \psi(x_1, \ldots, x_{n-1})$, h — подстановка регистра левого сдвига длины n с обратной связью $x_1 \oplus \phi(x_2, \ldots, x_n)$. Тогда:

1) множество дуг перемешивающего орграфа $G(gh)$ подстановки gh состоит из n петель (по одной в каждой вершине) и дуг вида (i, n), где $i \in \{1, \dots n-1\}$, таких, что x_i — существенная переменная функции $\psi(x_1, \dots, x_{n-1}) \oplus \phi(x_1, \dots, x_{n-1})$;
2) множество дуг перемешивающего орграфа $G(hg)$ подстановки hg состоит из n петель (по одной в каждой вершине) и дуг вида $(i, 1)$, где $i \in \{2, \dots, n\}$, таких, что x_i — существенная переменная функции $\psi(x_2, \dots, x_n) \oplus \phi(x_2, \dots, x_n)$.

Следствие 1. Орграф $G(gh)$ является (i, n)-примитивным при $i \in \{1, \dots, n-1\}$, если и только если x_i — существенная переменная функции $\psi(x_1, \dots, x_{n-1}) \oplus \phi(x_1, \dots, x_{n-1})$, в этом случае (i, n)-$\exp G(gh) = 1$.

Следствие 2. Орграф $G(hg)$ является $(i, 1)$-примитивным при $i \in \{2, \dots, n\}$, если и только если x_i — существенная переменная функции $\psi(x_2, \dots, x_n) \oplus \phi(x_2, \dots, x_n)$, в этом случае $(i, 1)$-$\exp G(hg) = 1$.

2. Композиция треугольного и регистрового преобразований

Пусть треугольное преобразование $h(x_1, \dots, x_n)$ множества X^n задано координатными функциями

$$h(x_1, \dots, x_n) = (t_1(x_1), t_2(x_1, x_2), \dots, t_n(x_1, \dots, x_n)) = (y_1, \dots, y_n).$$

Обратное преобразование также есть треугольная подстановка множества X^n:

$$h^{-1}(y_1, \dots, y_n) = (\psi_1(y_1), \psi_2(y_1, y_2), \dots, \psi_n(y_1, \dots, y_n)) = (x_1, \dots, x_n).$$

Преобразование $h(x_1, \dots, x_n)$ множества X^n биективно тогда и только тогда, когда функция $t_i(x_1, \dots, x_i)$ биективна по переменной x_i, $i = 1, \dots, n$ [1, с. 129]. Матрица смежности перемешивающего орграфа $G(h)$ (и $G(h^{-1})$) является верхнетреугольной; перемешивающие орграфы имеют петли в каждой вершине.

Теорема 3. Пусть g — преобразование двоичного регистра правого сдвига длины n с обратной связью $f(x_1, \dots, x_n)$, h — треугольная подстановка множества $\{0, 1\}^n$. Пусть задана бинарная операция. Если орграф $G(g)$ примитивный, то примитивными являются орграфы $G(g) \cdot G(h)$ и $G(h) \cdot G(g)$, где $(\cdot)$ – операция произведения графов; экспонент каждого из этих орграфов не превосходит $\exp G(g)$.

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. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
3. *Фомичев В. М.* Об оценках экспонентов орграфов с использованием чисел Фробениуса // Прикладная дискретная математика. Приложение. 2014. № 7. С. 137–140.
4. *Авезова Я. Э., Фомичев В. М.* Условия примитивности системы двух графов // Прикладная дискретная математика. Приложение. 2015. № 8. С. 113–114.