Определение 1. Статистики $\mathrm{fas}(\sigma) = \left\lfloor n^{-1} \sum_{i=1}^{n} \sigma_i \right\rfloor$ и $\mathrm{cas}(\sigma) = \left\lceil n^{-1} \sum_{i=1}^{n} \sigma_i \right\rceil$ задают соответственно «пол» и «потолок» средней величины символа в слове $\sigma \in \widehat{S}_n$.

Статистика fas (под именем mes) введена в [5], где с помощью рекурсивного описания установлено, что fas и des на $\widehat{S}_n$ имеют производящий многочлен $\widehat{A}_n(t, 1)$, иначе, fas и des — эйлеровы статистики на $\widehat{S}_n$. Легко показать, что $\mathrm{fas}(\sigma) + \mathrm{cas}(\mathbf{c}\sigma) = n + 1$, т. е. многочлен $t^{n+1}\widehat{A}_n(t^{-1})$ является производящим для статистики cas.

Теорема 4. Пары $(\mathrm{fas}, \mathrm{maj})$ и $(\mathrm{fas}, \mathrm{inv})$, а также пары $(\mathrm{cas}, \mathrm{maj})$ и $(\mathrm{cas}, \mathrm{inv})$ одинаково распределены на $\widehat{S}_n$.

Доказательство. Разобьём $\widehat{S}_n$ на минимальное число подмножеств, состоящих из перестановок подходящих мультимножеств символов из алфавита $\{1, \ldots, n\}$. По теореме Мак-Магона и определению 1 пары $(\mathrm{fas}, \mathrm{maj})$ и $(\mathrm{fas}, \mathrm{inv})$, а также пары $(\mathrm{cas}, \mathrm{maj})$ и $(\mathrm{cas}, \mathrm{inv})$ одинаково распределены на этих подмножествах, что и приводит к требуемому утверждению. ■

Отметим, что для пары $(\mathrm{des}, \mathrm{maj})$ на S_n неизвестна одинаково распределённая с ней пара $(\mathrm{e}, \mathrm{inv})$, где e — эйлерова статистика [1].

ЛИТЕРАТУРА

1. *Фоата А.* Распределения типа Эйлера и Мак-Магона на группе перестановок // Проблемы комбинаторного анализа. М.: Мир, 1980. С. 120–141.
2. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982. 256 с.
3. *Гульден Я., Джексон Д.* Перечислительная комбинаторика. М.: Наука, 1990. 504 с.
4. *Chow C.* A recurrence relation for the "inv" analogue of q-Eulerian polynomials // Electronic J. Combinatorics. 2010. V. 17. #N22.
5. *Бондаренко Л. Н., Шарапова М. Л.* Статистики спусков и средних на множествах слов // Проблемы теоретической кибернетики. Материалы XVII Междунар. конф. (Казань, 18–20 июня 2014 г.). Казань: Отечество, 2014. С. 63–65.

УДК 519.6 DOI 10.17223/2226308X/8/2

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ ПРЕОБРАЗОВАНИЙ РЕГИСТРОВ СДВИГА С ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Дорохова

Среди преобразований двоичных регистров сдвига с двумя обратными связями выделен класс подстановок, для которого получен критерий примитивности перемешивающих графов. Получены оценки экспонентов некоторых примитивных графов из данного класса.

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

Введение. Актуальность исследования перемешивающих свойств криптографических функций достаточно обоснована в ряде работ (см., например, [1 – 5]). Точное определение существенных переменных итеративных функций весьма трудоёмко, поэтому применяется оценочный матрично-графовый подход. Перемешивающие свойства преобразования векторного пространства V_n над полем $\mathrm{GF}(2)$ кодируются перемешиваю-

щей $0,1$-матрицей порядка n или, что равносильно, перемешивающим n-вершинным орграфом Γ, у которого матрица смежности вершин совпадает с M. Для итеративных преобразований оценка перемешивающих свойств состоит в распознавании примитивности матрицы M (графа Γ) и определении экспонента.

Примитивность и экспонент изучены для различных классов матриц и графов [2]. Перемешивающие графы подстановочных регистров сдвига с одной обратной связью изучались в [3–5]. В развитие данной тематики в работе оцениваются перемешивающие свойства одного класса подстановок регистров сдвига с двумя обратными связями.

1. Биективные регистры сдвига с двумя обратными связями. Преобразование $\varphi(x_1,\ldots,x_{n+m})$ множества V_{n+m} автономного регистра левого сдвига длины $n+m$ с двумя обратными связями задаётся координатными булевыми функциями:

$$\varphi(x_1,\ldots,x_{n+m})=(x_2,\ldots,x_n,\varphi_n(x_1,\ldots,x_{n+m}),x_{n+2},\ldots,x_{n+m},\varphi_{n+m}(x_1,\ldots,x_{n+m})). \quad (1)$$

Рассмотрим класс указанных преобразований регистров сдвига (обозначим его $R(g,h)$), где

$$\varphi_n(x_1,\ldots,x_{n+m}) = x_{n+1}\oplus h(x_{n+2},\ldots,x_{n+m}); \quad (2)$$

$$\varphi_{n+m}(x_1,\ldots,x_{n+m}) = x_1\oplus g(x_1,\ldots,x_n). \quad (3)$$

Регистр из класса $R(g,h)$ изображён на рис. 1.

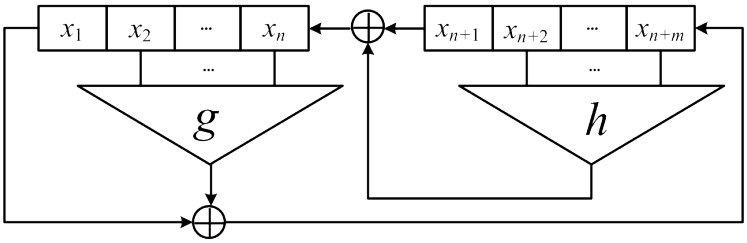

Рис. 1. Регистр сдвига с двумя обратными связями

Система функций $\Phi=\{f_1(x_1,\ldots,x_{n+m}),f_2(x_1,\ldots,x_{n+m})\}$ называется биективной по множеству переменных $\{x_i,x_j\}$, если она реализует биективное преобразование множества $\{0,1\}^2$ при любой фиксации переменных $\{x_1,\ldots,x_{n+m}\}\setminus\{x_i,x_j\}$ [6]. В силу соотношений (2), (3) система функций $\{\varphi_n,\varphi_{n+m}\}$ биективна по множеству переменных $\{x_{n+1},x_1\}$ и класс $R(g,h)$ состоит из подстановок в соответствии с теоремой 1 из [6].

2. Свойства перемешивающего графа. Обозначим через φ регистровую подстановку с двумя обратными связями, координатные функции которой заданы формулами (2) и (3) соответственно; через Δ и D — множества номеров существенных переменных соответственно функций φ_{n+m} и φ_n: $\Delta=\{\delta_1,\ldots,\delta_k\}$, $D=\{d_1,\ldots,d_q\}$, где $1=\delta_1<\ldots<\delta_k\leqslant n$, $n+1=d_1<\ldots<d_q\leqslant n+m$.

Исследуем примитивность $(n+m)$-вершинного перемешивающего орграфа $\Gamma(\varphi)$ подстановки φ. Необходимым условием примитивности орграфа $\Gamma(\varphi)$ является сильная связность.

Обозначим через Γ_0 граф $\Gamma(\varphi)$ при $h(x_{n+2},\ldots,x_{n+m})=g(x_2,\ldots,x_n)\equiv 0$. Из равенств (1)–(3) следует, что орграф Γ_0 представляет собой гамильтонов контур длины $n+m$. Так как Γ_0 — часть орграфа $\Gamma(\varphi)$ при любых функциях $h(x_{n+2},\ldots,x_{n+m})$ и $g(x_2,\ldots,x_n)$, то орграф $\Gamma(\varphi)$ сильносвязный.

Опишем контуры орграфа $\Gamma(\varphi)$. Для последовательности $w_0, w_1, \ldots, w_l$ путей в орграфе $\Gamma(\varphi)$ определим операцию конкатенации (обозначается символом $\cdot$). Если конечная вершина предыдущего пути совпадает с начальной вершиной следующего, то результатом операции является путь $w = w_0 \cdot w_1 \cdot \ldots \cdot w_l$. Обозначим $[i, j]$ путь w из вершины i в вершину j в орграфе $\Gamma(\varphi)$, $L(w)$ — длина пути w в орграфе $\Gamma(\varphi)$.

Числа множеств D и Δ определяют в $\Gamma(\varphi)$ простые контуры

$$C_{i,j} = [n, \delta_i] \cdot \mu \cdot [n + m, d_j] \cdot \nu,$$

где $\mu = (\delta_i, n + m)$ и $\nu = (d_j, n)$ — дуги орграфа $\Gamma(\varphi)$, длина контура $C_{i,j}$ определена равенством $L(C_{i,j}) = 2n + m + 2 - \delta_i - d_j$, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant k$. Орграф $\Gamma(\varphi)$ изображён на рис. 2.

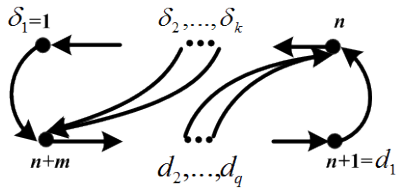

Рис. 2. Перемешивающий орграф $\Gamma(\varphi)$

Множество $\{a_1, \ldots, a_p\}$ натуральных чисел называется примитивным, если $(a_1, \ldots, a_p) = 1$. Обозначим $S = \{2n + m + 2 - \delta_i - d_j : i = 1, \ldots, q,\ j = 1, \ldots, k\}$. Справедлив следующий критерий примитивности.

Теорема 1. Перемешивающий орграф $\Gamma(\varphi)$ примитивный, если и только если множество S примитивное.

3. Оценки экспонента. Верны оценки экспонента для некоторых примитивных орграфов $\Gamma(\varphi)$.

Утверждение 1. Если $(n + 1, m - 1) = 1$ и $n + m \in D$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant n^2 + nm + 2m - 2$.

Оценка экспонента следует из теоремы 1 [7] при $l = n + m$, $\lambda = h = n + 1$.

Утверждение 2. Если $(m + 1, n - 1) = 1$ и $n \in \Delta$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant m^2 + mn + 2n - 2$.

Оценка экспонента следует из теоремы 1 [7] при $l = n + m$, $\lambda = h = m + 1$.

Утверждение 3. Если в D (или в Δ) имеются числа a, b, такие, что $a - b = 1$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) = \lambda^2 + 2b - 1$, где $\lambda = n + m - b$.

Оценка экспонента следует из теоремы 1 [7] при $l = \lambda + 1$, $h = \lambda$.

Обозначим через $\mu(n, m)$ чётное число из пары чисел n и m разной чётности.

Утверждение 4. Если числа n и m разной чётности, $n \in \Delta$, $n + m \in D$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant \mu(n, m) + 2(n + m) - 3$.

Оценка экспонента следует из теоремы 1 [7] при $l = \mu(n, m) + 1$, $\lambda = h = 2$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
4. *Дорохова А. М., Фомичев В. М.* Уточненные оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1(23). С. 77–83.
5. *Дорохова А. М.* Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 60–64.
6. *Коренева А. М.* О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями // Прикладная дискретная математика. Приложение. 2013. № 6. С. 39–41.
7. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.

УДК 519.6 DOI 10.17223/2226308X/8/3

О ЛОКАЛЬНЫХ ЭКСПОНЕНТАХ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ АЛГОРИТМАМИ ТИПА A5/1

С. Н. Кяжин, В. М. Фомичев

Для реализуемых алгоритмами типа A5/1 преобразований, построенных на основе линейных регистров сдвига длин n, m и p с характеристическими многочленами веса ν, μ и π соответственно, показана примитивность перемешивающих графов. Получены верхняя и нижняя оценки экспонента и локального экспонента перемешивающего графа Γ, зависящие от указанных параметров: $1+\max\{\lceil n/\nu\rceil, \lceil m/\mu\rceil, \lceil p/\pi\rceil\} \leqslant \exp\Gamma \leqslant \max\{n, m, p\}$. Для перемешивающего графа Γ преобразования генератора A5/1 получено значение экспонента $\exp\Gamma$ и локального экспонента $*J\text{-}\exp\Gamma$ при $J = \{1, 20, 42\}$, равное 21, что согласуется с длиной холостого хода генератора.

Ключевые слова: *генератор A5/1, примитивный граф, экспонент, локальный экспонент.*

Алгоритм A5/1 [1, с. 389] — поточный шифр гаммирования, построенный на основе трёх линейных регистров сдвига (ЛРС) над GF(2) длин 19, 22 и 23. Сумма битов, снимаемых с крайних ячеек ЛРС, образует гамму. Нелинейность преобразования состояний генератора достигается за счёт самоуправляемой схемы неравномерного движения регистров (каждый такт 2 или 3 регистра сдвигаются на 1 шаг).

Опишем перемешивающий граф Γ для обобщения генератора A5/1. Обозначим $(x_1, \ldots, x_{n+m+p})$ начальное состояние генератора, $S(f)$ — множество номеров существенных переменных функции f. Пусть генератор состоит из трёх регистров длин n, m и p с функциями обратной связи f_1, f_2 и f_3, чьи множества точек съёма суть $S(f_1) = \{b_1, \ldots, b_\nu\}$, $S(f_2) = \{c_1, \ldots, c_\mu\}$ и $S(f_3) = \{d_1, \ldots, d_\pi\}$ соответственно. Движение ЛРС на 0–1 шагов определено булевой функцией $u(x_t, x_\tau, x_\theta)$ от трёх существенных переменных, где $S(u) = \{t, \tau, \theta\}$; $1 \leqslant t \leqslant n$; $t \notin S(f_1)$; $n+1 \leqslant \tau \leqslant n+m$; $\tau \notin S(f_2)$; $n+m+1 \leqslant \theta \leqslant n+m+p$; $\theta \notin S(f_3)$. Тогда преобразование g состояний генератора за-