УДК 519.17 DOI 10.17223/2226308X/10/34

СРАВНЕНИЕ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ ОРГРАФОВ РЕГИСТРОВЫХ ПРЕОБРАЗОВАНИЙ С ОДНОЙ И ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Коренева

Обозначим МАГ(n, r, k) множество модифицированных аддитивных генераторов на основе регистров сдвига длины n с k обратными связями над множеством V_r булевых r-мерных векторов, $n > k \geqslant 1$, $r > 1$. Пусть подстановка g множества V_r модифицирует обратную связь регистра из МАГ$(n, r, 1)$, подстановки g и μ множества V_r модифицируют обратные связи регистра из МАГ$(n, r, 2)$, $\Gamma(\varphi^g)$ и $\Gamma(\varphi^{g,\mu})$ — перемешивающие орграфы преобразований соответствующих регистров. Проведён сравнительный анализ, в ходе которого показано, что соотношение экспонентов орграфов $\Gamma(\varphi^{g,\mu})$ и $\Gamma(\varphi^g)$ зависит не только от числа обратных связей, но и от расположения точек съёма на регистрах. Для большого количества вариантов точек съёма величина $\zeta = \exp\Gamma(\varphi^g) - \exp\Gamma(\varphi^{g,\mu})$ положительная и ограничена сверху величиной $\exp\Gamma(\varphi^g)/2$. Описаны также те редкие случаи, когда величина ζ отрицательная. Определены наименьшие значения $\exp\Gamma(\varphi^g)$ и $\exp\Gamma(\varphi^{g,\mu})$, равные $n+1$ и $\lceil n/2 \rceil + 1$ соответственно, и условия, при которых они достигаются.

Ключевые слова: *модифицированный аддитивный генератор, перемешивающие свойства, регистр сдвига, экспонент орграфа.*

Введение

Важным свойством преобразований информации является перемешивание входных данных, оно достигается с помощью итераций преобразования, если перемешивающий орграф преобразования является примитивным. Глубина итерации, при которой каждый бит выходного значения зависит от всех битов входного вектора, характеризуется экспонентом перемешивающего орграфа. Модифицированным аддитивным генераторам (МАГ), обладающим рядом позитивных криптографических свойств, в последнее время посвящён ряд работ [1–4]. Актуальной задачей криптографического синтеза является построение на основе МАГ преобразований, перемешивающие орграфы которых имеют наименьшие или близкие к наименьшим значения экспонентов. В связи с этим в работе проводится сравнительный анализ полученных в [3, 4] оценок экспонентов перемешивающих орграфов регистровых преобразований с одной и двумя обратными связями, построенных на основе МАГ. Даны рекомендации по выбору конструктивных параметров регистров, при которых экспоненты перемешивающих орграфов близки к наименьшим значениям.

1. Конструкция МАГ

Обозначим МАГ(n, r, k) класс построенных на основе МАГ регистров сдвига длины n над множеством V_r с k обратными связями, $n > k \geqslant 1$, $r > 1$. Определим регистровые преобразования из классов МАГ$(n, r, 1)$ и МАГ$(n, r, 2)$, исследованные в [3, 4]. Обозначим: $X_0, \ldots, X_{n-1}$ — знаки начального состояния МАГ (числа кольца вычетов $\mathbb{Z}_{2^r}$); b — биекция, определяющая двоичное r-разрядное представление числа $X \in Z_{2^r}$ по правилу: если $X = 2^{r-1}x_0 + \cdots + 2x_{r-2} + x_{r-1}$, то $b(X) = \overline{X} = (x_0, \ldots, x_{r-1}) \in V_r$.

Преобразование φ^g из класса МАГ$(n, r, 1)$ имеет вид [3]

$$\varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = \left(\overline{X}_1, \ldots, \overline{X}_{n-1}, bg\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right)\right),$$

где $D = \{d_0, \ldots, d_q\} \subseteq \{0, \ldots, n-1\}$ — непустое множество точек съёма, $0 < q$, $0 = d_0 < \ldots < d_q < n$; подстановка g множества V_r модифицирует аддитивный генератор, при умножении функции применяются слева направо.

При $0 < m < n-2$ преобразование $\varphi^{g,\mu}$ из класса МАГ$(n, r, 2)$ имеет вид [4]

$$\varphi^{g,\mu}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, f_m, \ldots, \overline{X}_{n-1}, f_{n-1}),$$

где функции обратных связей f_{n-1} и f_m определены равенствами

$$f_{n-1} = bg\left(\left(\sum_{k\in D} X_k\right) \bmod 2^r\right), \quad f_m = b\mu\left(\left(\sum_{k\in \Delta} X_k\right) \bmod 2^r\right);$$

$D, \Delta \subseteq \{0, \ldots, n-1\}$, $\Delta = \{\delta_0, \ldots, \delta_p\}$, $p > 0$, $0 < \delta_1 < \ldots < \delta_p < n$, причём $\delta_0 = m+1$ (условие биективности преобразования $\varphi^{g,\mu}$); μ — подстановка множества V_r.

2. Оценки экспонентов перемешивающих орграфов МАГ$(n, r, 1)$ и МАГ$(n, r, 2)$

Орграф Γ примитивный, если некоторая его степень является полным орграфом, наименьшая из таких степеней называется экспонентом орграфа Γ. Обозначим: $\exp\Gamma$ — экспонент орграфа Γ; $\Gamma(\varphi)$ — перемешивающий орграф преобразования φ. В [3, 4] описаны множества дуг, путей и контуров орграфов $\Gamma(\varphi^g)$ и $\Gamma(\varphi^{g,\mu})$, получены критерии их примитивности и верхние оценки экспонентов.

Оценка $\exp\Gamma(\varphi^g)$ имеет вид [3, теорема 5]

$$\exp\Gamma(\varphi^g) \leqslant \Phi(\Lambda) + \rho(D) + 2n - d_q, \tag{1}$$

где $\Phi(\Lambda)$ — число Фробениуса; $\Lambda = \{l_1, l_2, \ldots, l_s\}$, $s \geqslant 1$, — множество взаимно простых длин контуров в $\Gamma(\varphi^g)$, все вершины которых принадлежат множеству $V(r-1) = \{r-1+rk : k = 0, \ldots, n-1\}$; $\rho(D) = \max\{n-d_q, d_q-d_{q-1}, \ldots, d_1-d_0\}$.

Для оценки $\exp\Gamma(\varphi^{g,\mu})$ [4] использованы величины, характеризующие разброс точек съёма МАГ и некоторые другие:

- $\rho(D) = \max\{n-d_q, d_q-d_{q-1}, \ldots, d_1-d_0\}$ при $d_q > m$;
- $\rho(\Delta, D) = \max\{\max\{n-\delta_p, \delta_p-\delta_{p-1}, \ldots, \delta_{\tau+2}-\delta_0\} + m - d_q + 1, \max\{m-d_q+1, d_q-d_{q-1}, \ldots, d_1-d_0\}\}$ при $d_q \leqslant m$;
- $\rho(\Delta) = \max\{\delta_1 + n - \delta_p, \delta_p - \delta_{p-1}, \ldots, \delta_0 - \delta_\tau, \ldots, \delta_2 - \delta_1\}$ при $\delta_1 \leqslant m$;
- $\varepsilon = \max\{2n - m - 2 - d_q, n + m - \max\{\delta_0, \delta_p\}\}$;
- $\varepsilon' = \max\{2m + 1 - \delta_\tau, n - 1 - d_t\}$;
- d_t и δ_τ — ближайшие к m точки съёма из D и Δ соответственно.

Оценка $\exp\Gamma(\varphi^{g,\mu})$ имеет следующий вид [4, теорема 6]:

$$\text{а)}\ \exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda_1) + 1 + \rho(d_q) + \varepsilon, \tag{2}$$

где $\rho(d_q) = \rho(D)$ при $d_q > m$, $\rho(d_q) = \rho(\Delta, D)$ при $d_q \leqslant m$ и Λ_1 — множество взаимно простых длин контуров в $\Gamma(\varphi^{g,\mu})$, проходящих через вершину $nr-1$, все вершины которых принадлежат $V(r-1)$;

$$\text{б)}\ \exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda_2) + 1 + \rho(\Delta) + \varepsilon', \tag{3}$$

где Λ_2 — множество взаимно простых длин контуров в $\Gamma(\varphi^{g,\mu})$, не проходящих через $nr-1$, все вершины которых принадлежат $V(r-1)$;

$$\text{в)}\ \exp\Gamma(\varphi^{g,\mu}) \leqslant \Phi(\Lambda_3) + 1 + \rho(d_q) + n - \max\{\delta_0, \delta_p\} + \varepsilon', \tag{4}$$

где Λ_3 — множество взаимно простых длин контуров в $\Gamma(\varphi^{g,\mu})$, все вершины которых принадлежат $V(r-1)$, причём контуры длин $l_1, l_2, \ldots, l_h$, $1 \leqslant h < s$, проходят через $nr-1$, а контуры длин $l_{h+1}, \ldots, l_s$ проходят через $r-1+rm$ и не проходят через $nr-1$.

Оценка экспонента примитивного орграфа Γ наименьшая, если в Γ есть петля (в этом случае $\Phi(1) = \Phi(1, l_2, \ldots, l_s) = -1$ при любых $l_2, \ldots, l_s$). Оценка $\exp\Gamma(\varphi^g)$ в случае петель в $\Gamma(\varphi^g)$ (т. е. когда $(n-1) \in D$) имеет вид

$$\exp\Gamma(\varphi^g) \leqslant \rho(D) + n, \tag{5}$$

а оценка $\exp\Gamma(\varphi^{g,\mu})$ в случае петель в $\Gamma(\varphi^{g,\mu})$ (т. е. когда $(n-1) \in D$, $m \in \Delta$)

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \min\{\rho(D) + \varepsilon, \rho(\Delta) + \varepsilon'\}. \tag{6}$$

3. Сравнение оценок экспонентов

Сравним оценки $\exp\Gamma(\varphi^{g,\mu})$ и $\exp\Gamma(\varphi^g)$ при различных значениях параметров регистров.

Если множества D одинаковы для регистров φ^g и $\varphi^{g,\mu}$, то оценки (2)–(4) ниже по сравнению с (1) и оценка (5) ниже по сравнению с (6) в следующих случаях:

1) при любом множестве точек съёма Δ и любом значении параметра m второй обратной связи оценка (2) ниже (1):
   - на величину $m+1$, если $2m - \max\{\delta_0, \delta_p\} < n - d_q - 2$;
   - на величину $n + \max\{\delta_0, \delta_p\} - d_q - m - 1$ в противном случае;
2) при $\Phi(\Lambda_2) + 1 + \rho(\Delta) \leqslant \Phi(\Lambda) + \rho(D)$ и любом m оценка (3) ниже (1):
   - на величину $2(n-m-1) + \delta_\tau - d_q$, если $2m - \delta_\tau < n - d_q - 2$;
   - на величину $n + d_t - d_q$ в противном случае;
3) при $\Phi(\Lambda_3) \leqslant \Phi(\Lambda)$ оценка (4) ниже (1):
   - на величину $n + \max\{\delta_0, \delta_p\} + \delta_\tau - 2m - 2 - d_q$, если $m + \delta_\tau < n - d_q - 1$ и $2m - \delta_\tau < n - d_q - 2$;
   - на величину $\max\{\delta_0, \delta_p\} + d_t - d_q$, если $m + d_t > d_q - 1$ и $2m - \delta_\tau \geqslant n - d_q - 2$;
4) при любых Δ и m оценка (6) ниже (5) на величину

$$\rho(D) + n - \min\{\rho(D) + \varepsilon, \rho(\Delta) + \varepsilon'\}.$$

При $m = \lceil n/2 \rceil - 1$, $m \in D$ и $(n-1) \in \Delta$ справедлива оценка

$$\exp\Gamma(\varphi^{g,\mu}) \leqslant \min\{\rho(D), \rho(\Delta)\} + \lceil n/2 \rceil,$$

при этом абсолютный минимум оценки (6) достигается при $\min\{\rho(D), \rho(\Delta)\} = 1$ и равен $\lceil n/2 \rceil + 1$. Заметим, что абсолютный минимум оценки (5) достигается при $\rho(D) = 1$ и равен $n+1$.

Если множества D различны для регистров φ^g и $\varphi^{g,\mu}$, то есть D_1 и Δ — множества точек съёма регистра $\varphi^{g,\mu}$, а D_2 — множество точек съёма регистра φ^g, то оценки $\exp\Gamma(\varphi^{g,\mu})$ хуже оценок $\exp\Gamma(\varphi^g)$ в следующих случаях:

1) при D_1, таком, что $\Phi(\Lambda_1) = O(n^2)$, и при $D_2 \supset D_1$, таком что $\Phi(\Lambda) < n$, оценка (2) хуже (1);
2) при $\Phi(\Lambda_2) + 1 + \rho(\Delta) > \Phi(\Lambda) + \rho(D)$ оценка (3) хуже (1);
3) при $\Phi(\Lambda_3) > \Phi(\Lambda)$, $m + \delta_\tau > n - d_q - 1$ и $m + d_t > d_q - 1$ оценка (4) хуже (1);
4) при $m = \lceil n/2 \rceil - 1$ и $\rho(\Delta) \geqslant \rho(D_1) + 1$ оценка (6) хуже оценки (5).

Пример. Для перемешивающего орграфа $\Gamma(\varphi^g)$ регистра сдвига с одной обратной связью при $n = 8$, $r = 32$, $D = D_2 = \{0, 3, 4, 6, 7\}$ из формулы (5) следует оценка $\exp\Gamma(\varphi^g) \leqslant 11$ (здесь $\rho(D) = 3$).

а) Оценим $\exp\Gamma(\varphi^{g,\mu})$ перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ регистра с двумя обратными связями при тех же значениях n, r, D. Пусть $m = 3$. Тогда при любом Δ из (6) следует оценка $\exp\Gamma(\varphi^{g,\mu}) \leqslant 7$. Минимум оценки (6) достигается при $\rho(\Delta) = 1$: $\exp\Gamma(\varphi^{g,\mu}) \leqslant 5$.

б) Оценим $\exp\Gamma(\varphi^{g,\mu})$ при тех же значениях n, r, m и при $D_1 = \{0, 6, 7\}$, $\Delta = \{3, 4\}$. В этом случае $\rho(D_1) = 6$, $\rho(\Delta) = 7$ (т. е. $\rho(\Delta) \geqslant \rho(D_1) + 1$) и $\varepsilon = \varepsilon' = 7$. Из (6) следует оценка $\exp\Gamma(\varphi^{g,\mu}) \leqslant 13$, а из (5) — оценка $\exp\Gamma(\varphi^g) \leqslant 11$.

Выводы

Проведено сравнение верхних оценок экспонентов перемешивающих орграфов $\Gamma(\varphi^g)$ и $\Gamma(\varphi^{g,\mu})$ преобразований регистров сдвига φ^g и $\varphi^{g,\mu}$ с одной и двумя обратными связями, построенных на основе МАГ. Получены условия, при которых оценка $\exp\Gamma(\varphi^{g,\mu})$ ниже оценки $\exp\Gamma(\varphi^g)$. Добавление второй обратной связи улучшает перемешивающие свойства регистра $\varphi^{g,\mu}$. При одинаковых множествах точек съёма D у регистров φ^g и $\varphi^{g,\mu}$ перемешивающие свойства лучше у регистра с двумя обратными связями. Экспоненты перемешивающих орграфов $\Gamma(\varphi^{g,\mu})$ близки к наименьшим значениям при $m = \lceil n/2 \rceil - 1$, $\{m, n-1\} \in D \cap \Delta$. Если величина $\min\{\rho(D), \rho(\Delta)\}$ близка к 1, то оценка $\exp\Gamma(\varphi^{g,\mu})$ улучшается до 50 %.

ЛИТЕРАТУРА

1. *Дорохова* (*Коренева*) *А. М.* Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 60–64.
2. *Коренева А. М., Фомичёв В. М.* О существенных переменных функции переходов модифицированного аддитивного генератора // Прикладная дискретная математика. Приложение. 2016. № 9. С. 51–54.
3. *Коренева А. М., Фомичёв В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискретный анализ и исследование операций. 2017. № 2. С. 47–67.
4. *Коренева А. М.* О примитивности перемешивающих орграфов биективных регистров сдвига с двумя обратными связями // Прикладная дискретная математика. 2017 (в печати).

УДК 519.17 DOI 10.17223/2226308X/10/35

СТРОЕНИЕ ЛОКАЛЬНО ПРИМИТИВНЫХ ОРГРАФОВ

С. Н. Кяжин

Исследованы свойства строения $i \times j$-примитивного орграфа, используемые при расчёте $i \times j$-экспонента орграфа. Показано, что $i \times j$-примитивный орграф есть или компонента сильной связности (ксс), или множество ксс, соединённых определённым образом простыми путями, все вершины которых, за исключением, быть может, начальной и конечной, являются ациклическими. Множество ксс разбивается на $k + 1$ ярусов в соответствии с удалённостью от вершины i. Описано строение перемешивающего графа преобразования множества состояний генератора последовательностей с перемежающимся шагом, построенного на основе регистров сдвига длин m, n, r. Показано, что $i \times (m+n)$- и $i \times (m+n+r)$-примитивный перемешивающий граф преобразования множества V_{m+n+r} состояний генератора