Сопоставим каждой ЛРП $u \in L_R(F)^*$ булеву функцию $f''_{u,K}(x_1, \ldots, x_m)$ по правилу $f''_{u,K}(0, \ldots, 0) = \varkappa^K_{n-1}(0) \bmod 2$,

$$f''_{u,K}(u_0(i), u_0(i+1), \ldots, u_0(i+m-1)) = \varkappa^K_{n-1}(u(i)) \bmod 2,$$

где $u_0(i) = u(i) \bmod 2$, $0 \leqslant i \leqslant 2^m - 1$. В силу выбора последовательности u вектор $(u_0(i), u_0(i+1), \ldots, u_0(i+m-1))$ принимает все возможные значения из множества $\{0,1\}^m \setminus \{(0, \ldots, 0)\}$, поэтому функция определена на всех двоичных наборах $\{0,1\}^m$. Обозначим ${B_n}''(K,F)$ множество всех булевых функций $f''_{u,K}$, соответствующих всем ЛРП u из множества $L_R(F)^*$.

Оказывается, что для функций $f''_{u,K} \in B''_n(K,F)$ справедливы такие же оценки степени нелинейности и алгебраической степени, что и для функций из класса $B'_n(K,F)$ [1].

Теорема 1. Для коэффициентов $W_f(\mathbf{a})$ Уолша — Адамара булевой функции $f = f''_{u,K}$ при всех $n \geqslant 2$ имеет место оценка

$$|W_f(\mathbf{a})| \leqslant \left(\frac{2}{\pi}\ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2}.$$

Следствие 1. При $n = 2$ и каждом чётном m класс $B''_n(K,F)$ состоит из бент-функций, а при $n = 2$ и каждом нечётном m класс $B''_n(K,F)$ состоит из платовидных функций порядка $m - 1$.

Теорема 2. Пусть $F(x) \in R[x]$ — отмеченный многочлен степени $m > |R|$ максимального периода над кольцом R, тогда для любой функции $f \in B''_n(K,F)$ справедливо соотношение $\deg f = 2^{n-1}$.

ЛИТЕРАТУРА

1. *Былков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Матем. вопр. криптогр. 2012. Т. 3. № 4. С. 25–53.
2. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. (New York). 1995. V. 76. No. 6. P. 2793–2915.

УДК 519.6

ОЦЕНКИ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ НЕКОТОРЫХ МОДИФИКАЦИЙ АДДИТИВНЫХ ГЕНЕРАТОРОВ

А. М. Дорохова

Для модификации аддитивного генератора с помощью инволютивной перестановки координат векторов исследованы условия полного перемешивания. Доказаны достаточные условия примитивности перемешивающего графа и оценки его экспонента в некоторых случаях. Полученные оценки экспонента показывают, что полное перемешивание знаков состояния генератора может быть достигнуто после числа тактов, которое существенно меньше размера состояний.

Ключевые слова: *аддитивный генератор, перемешивающий граф преобразования, экспонент графа.*

Введение

Положительным криптографическим свойством генератора гаммы $\{\gamma_1, \dots, \gamma_i, \dots\}$ является полное перемешивание входных данных, то есть зависимость знаков вырабатываемой гаммы от всех знаков начального состояния. Полное перемешивание достигается для знаков гаммы γ_i, как правило, при $i \geqslant \exp\Gamma(\varphi)$, где φ — преобразование множества внутренних состояний генератора; $\Gamma(\varphi)$ — перемешивающий граф преобразования φ; $\exp\Gamma(\varphi)$ — экспонент графа $\Gamma(\varphi)$. Если $\exp\Gamma(\varphi) = t$, то начальный отрезок гаммы $\{\gamma_1, \dots, \gamma_{t-1}\}$ часто называют «холостым ходом» и обычно не используют в ключевой последовательности. Таким образом, определение экспонентов перемешивающих графов криптографических преобразований является важной задачей анализа и синтеза криптографических систем.

Сделана оценка экспонентов перемешивающих графов преобразований, соответствующих некоторым модификациям аддитивных генераторов (аддитивные генераторы называют также запаздывающими генераторами Фибоначчи). Интерес к модификациям вызван тем, что оригинальные схемы аддитивных генераторов полного перемешивания не достигают и вообще признаны нестойкими. В то же время на основе аддитивных генераторов построен ряд алгоритмов: Fish, Pike, Mush [1].

Обзор результатов по экспонентам графов, полученных до 2012 г., дан в [2]. Для перемешивающих графов биективных регистров сдвига над множеством двоичных векторов, к которым относятся, в частности, аддитивные генераторы и рассматриваемые модификации, общие оценки уточнены в [3, 4]. В работе эти оценки получают дальнейшее уточнение за счёт особенностей аддитивных генераторов и их модификаций.

1. Аддитивные генераторы

Генераторы построены на основе принципа, использованного в линейных регистрах сдвига, но оперируют с числами в кольце вычетов $\mathbb{Z}/2^r$, где $r > 1$. Обозначим n длину регистра, ячейки регистра сдвига занумеруем числами $0,\dots,n-1$. Обозначим $X_0, X_1, \dots, X_{n-1}$ числа из $\mathbb{Z}/2^r$, образующие начальное состояние генератора. При $i \geqslant n$ знак гаммы X_i образуется по формуле

$$X_i = \sum_{j=0}^{n} a_j X_{j+i-n} \bmod 2^r, \tag{1}$$

где $a_0, \dots, a_{n-1} \in \{0, 1\}$. Следовательно, аддитивный генератор есть регистр сдвига длины n с функцией обратной связи $f(y_0, \dots, y_{n-1}) = \sum_{j=0}^{n-1} a_j y_j \bmod 2^r$. Так как $a_0 = 1$ (в противном случае длина регистра меньше n), $f(y_1, \dots, y_n)$ биективна по переменной y_0, то есть регистр реализует подстановку множества состояний [5, теорема 5.5]. Для изучения перемешивающих свойств подстановки генератора используем двоичное представление $\delta(X_i)$ числа X_i, $i \geqslant 0$, являющееся r-мерным вектором пространства V_r (младшим битом является r-й бит), состояние генератора является rn-мерным вектором пространства V_{rn}.

2. Перемешивающие свойства модифицированного генератора.

Критерий полного перемешивания — примитивность перемешивающего орграфа подстановки; необходимым условием является сильная связность орграфа. Заметим, что для регистра сдвига, определяемого законом рекурсии (1), перемешивающий граф не сильносвязный. Для достижения сильной связности модифицируем аддитивный

генератор с помощью инволюции I множества V_r: $I(x_1,\dots,x_r)=(x_r,\dots,x_1)$. Тогда при $i \geqslant n$

$$\delta(X_i) = I\left(\delta\left(\left(X_{i-n} + \sum_{j=1}^{n-1} a_j X_{j+i-n}\right) \bmod 2^r\right)\right). \qquad (2)$$

Используем обозначения и результаты работ [3, 4]. Пусть φ — подстановка регистра сдвига. Состояние регистра в текущий момент времени задано двоичной матрицей размера $r \times n$, где k-й столбец матрицы, обозначаемый $y_{k+1} = (x_{1+rk},\dots,x_{r+rk})^{\mathrm{T}}$ (T — транспонирование), записан в k-й ячейке регистра сдвига, $k = 0, 1, \dots, n-1$. Подстановка φ задается системой rn булевых координатных функций $\{\varphi_1(x_1,\dots,x_{rn}),\dots,\varphi_{rn}(x_1,\dots,x_{rn})\}$, где функция $\varphi_{v+rk}(x_1,\dots,x_{rn})$ вычисляет v-й бит x_{v+rk} вектора y_{k+1}, $v = 1,\dots,r$, $k = 0, 1, \dots, n-1$.

Обозначим $S(\varphi_j)$ множество номеров существенных булевых переменных функции $\varphi_j(x_1,\dots,x_{rn})$, $j = 1,\dots,rn$. Перемешивающий граф $\Gamma(\varphi)$ подстановки φ есть rn-вершинный орграф, в котором есть дуга (i,j), если и только если $i \in S(\varphi_j)$, $i,j \in \{1,\dots,rn\}$.

Обозначим θ функцию отождествления вершин орграфа $\Gamma(\varphi)$: для $v = 1,\dots,r$ положим $\theta(v+rk) = v$, $k = 0, 1, \dots, n-1$. Функция θ индуцирует отображение орграфа $\Gamma(\varphi)$ в r-вершинный орграф $\Gamma(\psi)$, где (v,u) есть дуга орграфа $\Gamma(\psi)$, если и только если функция $\varphi_{u+r(n-1)}$ зависит существенно хотя бы от одной из переменных множества $\{x_v, x_{v+r},\dots,x_{v+r(n-1)}\}$, $v,u \in \{1,\dots,r\}$. Орграф $\Gamma(\varphi)$ сильносвязный, если и только если $\Gamma(\psi)$ сильносвязный [3, теорема 2].

Определим характеристики перемешивающего графа $\Gamma(\varphi)$ модифицированного генератора. Из (2) следует, что $S(\psi_u) = \{r, r-1,\dots,r-u+1\}$, $u = 1,\dots,r$. Сильная связность орграфов $\Gamma(\varphi)$ и $\Gamma(\psi)$ (она достигается сочетанием инволюции I с суммированием по модулю 2^r) вытекает, в частности, из наличия в $\Gamma(\psi)$ дуг $(r,1)$, $(r,2)$, $(r,3)$, $(r-1,2)$, $(r-1,3)$, $(r-2,3)$, …, (r,r), $(r-1,r)$, …, $(3,r)$, $(2,r)$, $(1,r)$. Графы $\Gamma(\psi)$ при $r \in \{3,4\}$ изображены на рис. 1.

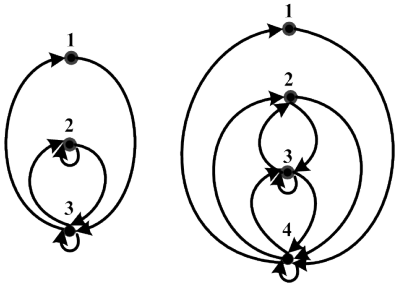

Рис. 1. Графы $\Gamma(\psi)$ при $r = 3$ и $r = 4$

Определим условия примитивности орграфа $\Gamma(\varphi)$ на основе универсального критерия [2, с. 10]. Из (2) следует, что в графе $\Gamma(\varphi)$ имеются простые циклы длины $2n$ вида

$$B_u = (u+r(n-1), u+r(n-2),\dots,u+r,u,r-u+1+r(n-1),r-u+1+r(n-2),\dots,r-u+1),\quad u=1,\dots,\lfloor r/2\rfloor,$$
$$E_u = (u+r(n-1), u+r(n-2),\dots,u+r,u,r-z+1+r(n-1),r-z+1+r(n-2),\dots,r-z+1),\quad u=\lceil (r+1)/2\rceil,\dots,r-1,\ z=1,\dots,u-1,$$

и простые циклы длины n вида

$$H_u = (u + r(n-1), u + r(n-2), \ldots, u + r, u), \quad u = \lceil (r+1)/2 \rceil, \ldots, r.$$

Остальные циклы графа $\Gamma(\varphi)$ определяются точками съёма с регистра (то есть номерами существенных переменных функции обратной связи).

Теорема 1 (достаточное условие примитивности перемешивающего графа $\Gamma(\varphi)$). Пусть обратная связь модифицированного регистра использует множество точек съёма $D = \{m - d_0, m - d_1, \ldots, m - d_k\}$, где $0 = d_0 < d_1 < \cdots < d_k = m < n$. Тогда

1) $S(\varphi_{u+r(n-1)}) = \{x_{v+rt} : v = r, r-1, \ldots, r-u+1, t \in D\}$, $u = 1, \ldots, r$;

2) граф $\Gamma(\varphi)$ примитивен, если $(n, d_1, \ldots, d_k) = 1$.

Следствие. Орграф $\Gamma(\varphi)$ примитивный, если

1) $d_i - d_{i-1} = 1$ при некотором $i \in \{1, \ldots, k\}$;

2) $(n, m) = 1$, в этом случае $\exp \Gamma(\varphi) \leqslant n^2 + (2r - 3 - m)n + 2m$, если $m \leqslant n - 2$;

3) при $m = n - 1$ выполнена оценка $\exp \Gamma(\varphi) \leqslant 2n - 2$.

Пример. Пусть обратная связь модифицированного регистра использует две точки съёма $D = \{m, 0\}$ и $r = 3$. Граф $\Gamma(\varphi)$ изображён на рис. 2, список циклов дан в таблице.

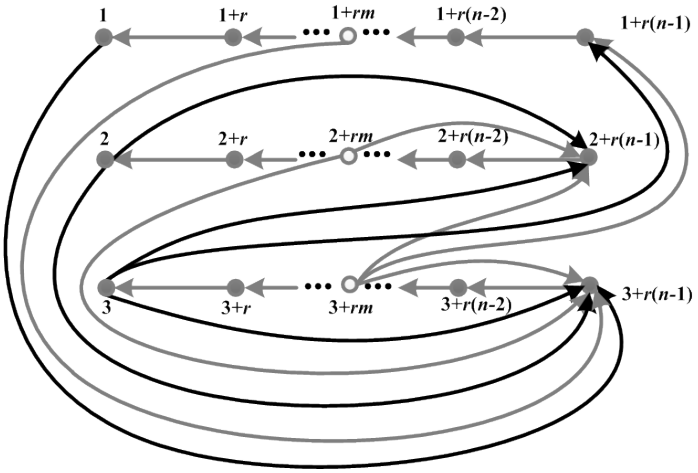

Рис. 2. Граф $\Gamma(\varphi)$ при $r = 3$

Циклы графа $\Gamma(\varphi)$ при $r = 3$

Цикл	Длина	Количество
$u + r(n-1), \ldots, u + r, u, r - u + 1 + r(n-1), \ldots, r - u + 1$	$2n$	1 $(u = 1)$
$u + r(n-1), \ldots, u + rm, r - u + 1 + r(n-1), \ldots, r - u + 1$	$2n - m$	1 $(u = 1)$
$u + r(n-1), \ldots, u + rm, r - u + 1 + r(n-1), \ldots, r - u + 1 + rm$	$2n - 2m$	1 $(u = 1)$
$u + r(n-1), \ldots, u + r, u, r + r(n-1), \ldots, r$	$2n - 2m$	1 $(u = 2)$
$u + r(n-1), \ldots, u + rm, r + r(n-1), \ldots, r$	$2n - m$	1 $(u = 2)$
$u + r(n-1), \ldots, u + rm, r + r(n-1), \ldots, r + rm$	$2n - 2m$	1 $(u = 2)$
$u + r(n-1), \ldots, u + r, u$	n	2 $(u = 2, 3)$
$u + r(n-1), \ldots, u + rm$	$n - m$	2 $(u = 2, 3)$

Данный граф $\Gamma(\varphi)$ примитивный при $(n, m) = 1$. При $r = 3$ в зависимости от m получаем оценки в соответствии со следствием теоремы:

1) при $d_1 - d_0 = 1$ $(m = 1)$ имеет место $\exp \Gamma(\varphi) \leqslant n^2 + 2n + 2$;

2) при $(n, m) = 1$, $2 \leqslant m \leqslant n-2$ верна оценка $\exp\Gamma(\varphi) \leqslant n^2 + (3-m)n + 2m$ (взяты длины циклов $n - m$ и n);

3) при $m = n - 1$ выполняется $\exp\Gamma(\varphi) \leqslant 2n - 2$.

Вывод: выбор параметров модифицированного аддитивного генератора позволяет достичь полного перемешивания за число тактов работы, которое существенно меньше размера (в битах) состояний генератора.

ЛИТЕРАТУРА

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
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.* Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1 (23). С. 77–83.
5. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
6. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.
7. *Фомичев В. М.* Свойства путей в графах и в мультиграфах // Прикладная дискретная математика. 2010. № 1 (7). С. 118–124.

УДК 512.62

АЛГОРИТМ ПОСТРОЕНИЯ СИСТЕМЫ ПРЕДСТАВИТЕЛЕЙ ЦИКЛОВ МАКСИМАЛЬНОЙ ДЛИНЫ ПОЛИНОМИАЛЬНЫХ ПОДСТАНОВОК НАД КОЛЬЦОМ ГАЛУА

Д. М. Ермилов

В отличие от полей и колец вычетов, над кольцами Галуа не существует транзитивных полиномов, то есть биективных полиномов, которые реализуют полноцикловую подстановку. Максимальная длина цикла полиномиального преобразования над кольцом Галуа равна $q(q-1)p^{n-2}$, где q^n — мощность кольца, а p^n — его характеристика. Предлагается алгоритм построения системы представителей всех циклов полиномиальных преобразований колец Галуа, имеющих максимальную длину. Сложность построенного алгоритма, выраженная в количестве операций умножения в кольце Галуа, равна $\mathrm{O}(lq^{n-1})$ при n, стремящемся к бесконечности, где l — степень многочлена полиномиального преобразования.

Ключевые слова: *кольца Галуа, нелинейные рекуррентные последовательности.*

Рассмотрим кольцо Галуа $R = \mathrm{GR}(q^n, p^n)$ мощности q^n и характеристики p^n, где $q = p^m$. Пусть $f(x) \in R[x]$ — биективный полином над кольцом Галуа R. Граф преобразования, задаваемого полиномом $f(x)$ над кольцом R, обозначим через $G_{f,R}$. Напомним, что цикловая структура графа — это таблица $[l_1^{k_1}, \ldots, l_t^{k_t}]$, указывающая, что граф состоит из k_1 циклов длины l_1, …, k_t циклов длины l_t. В работе [1] показано, что граф $G_{f,R}$ не может содержать цикл, длина которого больше $q(q-1)p^{n-2}$.