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 $*J$-$\exp\Gamma$ 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 задано системой булевых функций $g = \{g_1(x_1, \ldots, x_{n+m+p}), \ldots, g_{n+m+p}(x_1, \ldots, x_{n+m+p})\}$, где

$$\begin{gathered} S(g_n) = S(f_1) \cup \{n\} \cup S(u), S(g_i) = \{i, i+1\} \cup S(u),\ i = 1, \ldots, n-1, \\ S(g_{n+m}) = S(f_2) \cup \{n+m\} \cup S(u), \\ S(g_i) = \{i, i+1\} \cup S(u), i = n+1, \ldots, n+m-1, \\ S(g_{n+m+p}) = S(f_3) \cup \{n+m+p\} \cup S(u), \\ S(g_i) = \{i, i+1\} \cup S(u),\ i = n+m+1, \ldots, n+m+p-1. \end{gathered} \tag{1}$$

Из равенств (1) следует, что в Γ в каждой вершине имеется петля. Соответствующие ЛРС подграфы графа Γ являются сильносвязными, и имеются дуги (t, s), (τ, s) и (θ, s) при любом $s = 1, \ldots, n{+}m{+}p$. Следовательно, орграф Γ сильносвязный, примитивный.

Определим $\exp\Gamma$ и локальный экспонент $*J$-$\exp\Gamma$ [2] при $J = \{1, n+1, n+m+1\}$. Так как Γ содержит $n+m+p$ петель и дуги (t, s), (τ, s) и (θ, s), $s = 1, \ldots, n+m+p$, то в соответствии с теоремой 2 [3]

$$\exp\Gamma = 1 + \max\{\max_{i=1,\ldots,n} \rho(i, t), \max_{i=n+1,\ldots,n+m} \rho(i, \tau), \max_{i=n+m+1,\ldots,n+m+p} \rho(i, \theta)\}, \tag{2}$$

где $\rho(i, a)$ — длина кратчайшего пути в Γ от i до a, при этом $\rho(i, i) = 0$.

Пусть $A \subseteq \{1, \ldots, n+m+p\}$, обозначим $\rho(i, A) = \min\limits_{a \in A} \rho(i, a)$, где $\rho(i, A) = 0$, если $i \in A$. Тогда

$$\rho(i, t) = \rho(i, S(f_1)) + 1 + n - t \text{ при } i < t, \rho(i, t) = i - t \text{ при } i > t; \tag{3}$$

$$\rho(i, \tau) = \rho(i, S(f_2)) + 1 + n + m - \tau \text{ при } i < \tau, \rho(i, \tau) = i - \tau \text{ при } i > \tau; \tag{4}$$

$$\rho(i, \theta) = \rho(i, S(f_3)) + 1 + n + m + p - \theta \text{ при } i < \theta, \rho(i, \theta) = i - \theta \text{ при } i > \theta. \tag{5}$$

Из равенств (2)–(5) следует

$$\begin{gathered} \exp\Gamma = 2 + \max\{n - t + \max_{i=1,\ldots,t-1} \rho(i, S(f_1)), \\ n + m - \tau + \max_{i=n+1,\ldots,\tau-1} \rho(i, S(f_2)), n + m + p - \theta + \max_{i=n+m+1,\ldots,\theta-1} \rho(i, S(f_3))\}. \end{gathered} \tag{6}$$

Из (6) в данных условиях получаем:

1) $\exp\Gamma$ принимает наименьшее значение, равное $1 + \max\{\lceil n/\nu \rceil, \lceil m/\mu \rceil, \lceil p/\pi \rceil\}$, если $t = n$, $\tau = n+m$, $\theta = n+m+p$ и множества $S(f_1)$, $S(f_2)$ и $S(f_3)$ разделяют приблизительно на равные отрезки соответственно числовые множества $\{1, \ldots, n\}$, $\{n+1, \ldots, n+m\}$ и $\{n+m+1, \ldots, n+m+p\}$;
2) $\exp\Gamma$ принимает наибольшее значение, равное $\max\{n, m, p\}$, если $t = 1$, $\tau = n{+}1$, $\theta = n+m+1$.

В силу наличия в Γ дуг (t, s), (τ, s) и (θ, s) при любом $s = 1, \ldots, n+m+p$ оценка локального экспонента $*J$-$\exp\Gamma$ не зависит от J и совпадает с оценкой экспонента Γ.

В схеме генератора A5/1 $n = 19$, $m = 22$, $p = 23$, $\nu = 4$, $\mu = 2$, $\pi = 4$. Расчёты показали, что $*J$-$\exp\Gamma = 21$, где $J = \{1, 20, 42\}$.

Длина холостого хода генератора A5/1 (количество начальных тактов, при которых знаки гаммы игнорируются) равна 100, то есть более чем в 4 раза превышает значение экспонента. Это, по-видимому, надёжно обеспечивает зависимость каждого знака гаммы от всех знаков начального состояния генератора и делает конструктивно обоснованным выбор длины холостого хода.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. № 1(7). С. 118–124.

УДК 519.7 DOI 10.17223/2226308X/8/4

О НЕКОТОРЫХ МЕТРИЧЕСКИХ СВОЙСТВАХ ЛИНЕЙНЫХ ПОДПРОСТРАНСТВ БУЛЕВА КУБА[1]

А. К. Облаухов

Исследуются метрические дополнения подмножеств булева куба. Дана общая характеризация метрических дополнений линейных подпространств. Доказано, что полностью регулярные коды являются метрически регулярными.

Ключевые слова: *подпространство, метрически регулярное множество, метрическое дополнение, полностью регулярный код.*

Через $\mathbb{F}_2^n$ в работе обозначается множество всех двоичных векторов длины n. *Расстоянием Хэмминга* от вектора $y \in \mathbb{F}_2^n$ до множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(y, X) = \min\limits_{x \in X} \mathrm{wt}(y \oplus x)$, $\mathrm{wt}(\cdot)$ — двоичный вес (число единиц в векторе). *Максимальным расстоянием* от множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(X) = \max\limits_{z \in \mathbb{F}_2^n} \mathrm{d}(z, X)$. Вектор y называется *максимально удалённым* от множества X, если $\mathrm{d}(y, X) = \mathrm{d}(X)$. Через $|X|$ обозначается мощность множества X, через $\mathrm{supp}(y)$ — носитель вектора y — множество $\{i : y_i = 1\}$. *Сдвигом* множества X на вектор $a \in \mathbb{F}_2^n$ называется множество $a \oplus X = \{a \oplus x : x \in X\}$.

Множество $Y \subseteq \mathbb{F}_2^n$, состоящее из всех максимально удалённых от множества X векторов, назовём *метрическим дополнением* множества X и обозначим $Y = \widehat{X}$. Множество $X \subseteq \mathbb{F}_2^n$ называется *метрически регулярным*, если $X = \widehat{\widehat{X}}$.

В [1] была поставлена задача классификации метрически регулярных множеств. Известно [2], что множество всех аффинных функций метрически регулярно.

Исследуются свойства метрических дополнений линейных подпространств. Множество $L \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых векторов $x, y \in L$ их сумма $x \oplus y$ лежит в L. Следующие два утверждения характеризуют метрические дополнения линейных подпространств.

Утверждение 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда множество $\widehat{L}$ — это объединение сдвигов подпространства L. Пусть $a \in \mathbb{F}_2^n$ — произвольный вектор. Тогда расстояние от L до любого вектора из сдвига $a \oplus L$ совпадает с расстоянием от L до вектора a.

Теорема 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда

$$\mathrm{d}(L) \leqslant n - k.$$

У каждого линейного подпространства L существует единственный базис специального вида, который назовём *каноническим базисом*. Матрица из векторов этого базиса имеет вид

[1]Исследование выполнено при финансовой поддержке РФФИ (проект № 15-31-20635).