4) Замена циклического сдвига подблоков другой перестановкой. Например, в схеме 3-го типа можно заменить перестановку подблоков $\pi = \{4, 1, 2, 3\}$ на $\pi = \{4, 1, 3, 2\}$. В этом случае $\exp M(g^{(3)}) = 5$.

Выводы

Экспериментально получены значения экспонентов раундовых перемешивающих матриц ОСФ, построенных на основе регистров сдвига длины 4. Это позволяет сформулировать обоснованные рекомендации по выбору числа итераций раундового преобразования, при котором обеспечивается существенная зависимость каждой координатной функции выхода от всех переменных входа. Даны рекомендации по выбору параметров функций обратной связи регистров сдвига, при которых реализуется наиболее быстрое перемешивание входных данных.

ЛИТЕРАТУРА

1. *Nyberg K.* Generalized Feistel networks // ASIACRYPT'96. LNCS. 2005. V. 1163. P. 91–104.
2. *Hoang V. T. and Rogaway P.* On generalized Feistel networks // CRYPTO'2010. LNCS. 2010. V. 6223. P. 613–630.
3. *Suzaki T. and Minematsu K.* Improving the generalized Feistel // FSE'2010. LNCS. 2010. V. 6147. P. 19–39.
4. *Berger T P., Minier M., and Thomas G.* Extended generalized Feistel networks using matrix representation // LNSC. 2014. V. 8282. P. 289–305.
5. *Пудовкина М. А., Токтарев А. В.* Об оценке числа раундов с невозможными разностями в обобщённых алгоритмах шифрования Фейстеля // Прикладная дискретная математика. 2015. № 1. С. 37–51.
6. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
7. *Коренева А. М.* О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями // Прикладная дискретная математика. 2013. № 6. С. 39–41.

УДК 519.1 DOI 10.17223/2226308X/9/21

О СУЩЕСТВЕННЫХ ПЕРЕМЕННЫХ ФУНКЦИИ ПЕРЕХОДОВ МОДИФИЦИРОВАННОГО АДДИТИВНОГО ГЕНЕРАТОРА

А. М. Коренева, В. М. Фомичёв

Исследован класс биективных регистров сдвига длины n над множеством V_r двоичных r-мерных векторов, $n, r > 1$, построенных на основе аддитивных генераторов по модулю 2^r, модифицированных с использованием подстановки множества V_r. Функция обратной связи таких регистров является композицией функции обратной связи аддитивного генератора и преобразования множества V_r. Задача точного определения существенных переменных для композиции нелинейных функций, как правило, сложна, однако использование комбинаторных свойств биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$ позволило полностью описать множество существенных переменных функции обратной связи исследуемых регистров.

Ключевые слова: *аддитивный генератор, существенная переменная, перемешивающие свойства.*

Введение

Работа посвящена исследованию подстановок регистров сдвига длины n над множеством V_r двоичных r-мерных векторов при $n, r > 1$. Данный класс подстановок (обозначим его $R(n, r)$) обобщает как класс $R(2, r)$, лежащий в основе сетей Фейстеля, так и подстановки множества состояний аддитивных генераторов (обозначим $R_{\mathrm{ad}}(n, r)$ этот подкласс класса $R(n, r)$).

Аддитивные генераторы исследуются с середины XX века. В [1] дан краткий обзор аддитивных генераторов чисел по модулю m, указаны их преимущества и недостатки. Один из первых аддитивных генераторов построен Дж. Ж. Митчелом и Д. Ф. Муром в 1958 г.: последовательность, генерируемая в соответствии с законом рекурсии $X_n = (X_{n-24} + X_{n-55}) \bmod m$, $n \geqslant 55$, где m — чётное число; $X_0, \ldots, X_{54}$ — произвольные целые не все чётные числа. Выбор чисел 24 и 55 обеспечивает длину периода $2^{55} - 1$ последовательности, составленной из младших двоичных разрядов чисел X_n. Позднее на основе аддитивных генераторов были построены криптографические алгоритмы Fish, Pike, Mush [2].

Известно, что аддитивные генераторы по модулю 2^r плохо перемешивают входные данные. В связи с этим представляет интерес изучение перемешивающих свойств модификаций аддитивных генераторов по модулю 2^r с помощью подстановки, применяемой к функции обратной связи. Заметим, что перемешивающие свойства регистров из $R(n, r)$ исследованы в [3, 4]. В [5] получены условия полного перемешивания для модификации аддитивного генератора с помощью инволютивной перестановки координат векторов из V_r. В настоящей работе с целью исследования перемешивающих свойств широкого класса модификаций описано множество существенных переменных функции, являющейся композицией функции обратной связи регистра из $R_{\mathrm{ad}}(n, r)$ и произвольной подстановки множества V_r.

1. Определяющие функции аддитивных генераторов и модификаций

Рассмотрим аддитивный генератор по модулю 2^r (регистр сдвига длины n над кольцом вычетов $\mathbb{Z}_{2^r}$), $r > 1$. Для $i \geqslant n$ знак X_i образуется в соответствии с законом рекурсии

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

где $a_1, \ldots, a_{n-1} \in \{0, 1\}$ и $a_0 = 1$. Из закона рекурсии (1) следует, что i-е разряды двоичного представления каждого из чисел $X_0, X_1, \ldots, X_{n-1}$ текущего состояния зависят только от r-го, …, i-го разрядов чисел предыдущего состояния, $i = 1, \ldots, r$, что исключает хорошие перемешивающие свойства преобразования множества состояний аддитивного генератора. Модифицируем аддитивный генератор с помощью преобразования g множества V_r, такой генератор назовем g-модификацией аддитивного генератора.

Обозначим через b биекцию $\mathbb{Z}_{2^r} \leftrightarrow V_r$, сопоставляющую числу $X_i \in \mathbb{Z}_{2^r}$ его двоичное представление (b^{-1} — обратная к b функция). Для g-модификации аддитивного генератора закон рекурсии имеет вид

$$X_i = b^{-1}(g(b((\sum_{j=0}^{n-1} a_j X_{j+i-n}) \bmod 2^r))), \quad i \geqslant n. \tag{2}$$

Обозначим через φ^g преобразование множества V_{nr}, которое реализуется g-модификацией

$$\varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, \overline{X}_{n-1}, f^g(\overline{X}_0, \ldots, \overline{X}_{n-1})). \tag{3}$$

Следовательно, φ^g есть преобразование регистра сдвига с обратной связью $f^g : V_{nr} \to V_r$, где

$$f^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = g(f(\overline{X}_0, \ldots, \overline{X}_{n-1})) = g(b((\sum_{j=0}^{n-1} a_j X_j) \bmod 2^r)). \qquad (4)$$

Функция обратной связи g-модификации является композицией функции f обратной связи аддитивного генератора и преобразования g множества V_r. Определим модифицированный аддитивный генератор как автономный автомат $A = (V_{nr}, V_r, h, \psi)$, где V_{nr} — множество состояний; V_r — выходной алфавит; $h = \varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — функция переходов; $\psi = f^g(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — функция выходов. Исследуем множество существенных переменных функции переходов этого генератора.

2. Свойства биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$

Функцию f, определённую на множестве X, назовем постоянной на подмножестве $Q \subseteq X$, если ограничение f на Q есть константа. При $\tau = 1, \ldots, r-1$ выполнены следующие разбиения:

1) r-мерный куб V_r разбивается на $2^{r-\tau}$ подкубов $Q(c_{\tau+1}, \ldots, c_r)$ размерности τ вида
$$Q(c_{\tau+1}, \ldots, c_r) = \{(y_1, \ldots, y_\tau, c_{\tau+1}, \ldots, c_r) : y_1, \ldots, y_\tau \in \{0, 1\}\},$$
где $(c_{\tau+1}, \ldots, c_r) \in V_{r-\tau}$;
2) аддитивная группа $\mathbb{Z}_{2^r}$ разбивается на $2^{r-\tau}$ смежных классов вида $2^{r-\tau}\mathbb{Z}_{2^r} + a$ по подгруппе $2^{r-\tau}\mathbb{Z}_{2^r}$, где $a \in \mathbb{Z}_{2^{r-\tau}}$.

Такие системы подкубов и смежных классов обозначим соответственно Q_r^τ и $\mathbb{Z}_{2^r}^\tau$. С преобразованием g связано преобразование $\hat{g}$ группы $\mathbb{Z}_{2^r}$:

$$\hat{g}(Y) = b^{-1}(g(b(Y))).$$

Из формул (2)–(4) непосредственно следуют леммы 1 и 2.

Лемма 1. Биекция $b : \mathbb{Z}_{2^r} \leftrightarrow V_r$ индуцирует биекцию $\xi : Q_r^\tau \leftrightarrow \mathbb{Z}_{2^r}^\tau$ со свойством $\xi(Q(c_{\tau+1}, \ldots, c_r)) = 2^{r-\tau}\mathbb{Z}_{2^r} + b^{-1}(0, \ldots, 0, c_{\tau+1}, \ldots, c_r)$.

Обозначим $g_u(y_1, \ldots, y_r)$ координатные булевы функции преобразования g, u=$1, \ldots, r$.

Лемма 2. Функция $g_u(y_1, \ldots, y_r)$ постоянна на любом подкубе из системы Q_r^τ, если и только если $y_1, \ldots, y_\tau$ — фиктивные переменные координатной функции g_u, $u = 1, \ldots, r$.

3. Существенные переменные функции переходов

Обозначим: $\varphi^g_{u+rk}(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — координатные булевы функции преобразования φ^g, $u = 1, \ldots, r$, $k = 0, 1, \ldots, n-1$; $D = \{d_0, \ldots, d_q\}$ — множество точек съёма регистра φ^g (то есть множество номеров существенных переменных функции обратной связи регистра φ^g), где $0 < q$, $0 = d_0 < \cdots < d_q < n$ и $j \in D \Leftrightarrow a_j = 1$; $E(\varphi^g_j)$ — множество номеров существенных переменных координатной функции φ^g_j, $j = 1, \ldots, nr$.

Из (3) следует, что $E(\varphi^g_{u+rk}) = \{u + r(k+1)\}$ при $u = 1, \ldots, r$ и $k = 0, 1, \ldots, n-2$. Осталось описать существенные переменные координатных функций при $k = n-1$. Из (4) следует $\varphi^g_{u+r(n-1)}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = g_u(b((\sum_{j=0}^{n-1} a_j X_j) \bmod 2^r))$.

Теорема 1. Для множества переменных функции $\varphi^g_{u+r(n-1)}$, $u = 1, \ldots, r$, верно:

а) x_{v+rk} фиктивная при любом $k \notin D$, $v = 1, \ldots, r$;

б) x_{v+rk} фиктивная при любом $k \in D$, $v = 1, \ldots, \tau$, если переменные $y_1, \ldots, y_\tau$ фиктивные для функции g_u, $\tau \geqslant 1$;

в) x_{v+rk} существенная при $v = \theta, \ldots, r$ и при любом $k \in D$, если переменная y_θ существенная для функции g_u, $\theta \geqslant 1$.

Пример 1. Пусть g-модифицированный аддитивный генератор построен на основе регистра сдвига длины n над V_4, $D = \{0, i, n-1\}$, где $0 < i < n-1$. На рис. 1 изображена схема g-модификации аддитивного генератора, знаком «+» обозначено сложение по модулю 2^{32}.

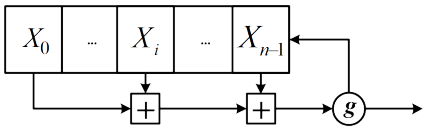

Рис. 1. Схема g-модификации аддитивного генератора

Пусть номера существенных переменных координатных функций преобразования g определены множествами $E(g_1) = \{2, 4\}$, $E(g_2) = \{3\}$, $E(g_3) = \{1\}$, $E(g_4) = \{4\}$. Тогда в соответствии с (3) и с теоремой 1, в получаем полное описание существенных переменных функции обратной связи g-модификации (таблица).

Номера существенных переменных функции переходов g-модификации

$k = 0, 1, \ldots, n-2$		$k = n-1$		
u	$E(\varphi^g_{u+rk})$	u	$E(g_u)$	$E(\varphi^g_{u+r(n-1)})$
1	$\{1 + r(k+1)\}$	1	$\{2, 4\}$	$\{2, 3, 4, 2 + ri, 3 + ri, 4 + ri, 2 + r(n-1), 3 + r(n-1), 4 + r(n-1)\}$
2	$\{2 + r(k+1)\}$	2	$\{4\}$	$\{4, 4 + ri, 4 + r(n-1)\}$
3	$\{3 + r(k+1)\}$	3	$\{1\}$	$\{1, 2, 3, 4, 1 + ri, 2 + ri, 3 + ri, 4 + ri, 1 + r(n-1), 2 + r(n-1), 3 + r(n-1), 4 + r(n-1)\}$
4	$\{4 + r(k+1)\}$	4	$\{3\}$	$\{3, 4, 3 + ri, 4 + ri, 3 + r(n-1), 4 + r(n-1)\}$

Выводы

С использованием комбинаторных свойств биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$ полностью описаны существенные переменные функции переходов модифицированного аддитивного генератора. Это позволяет изучать свойства перемешивающей матрицы (графа) преобразования множества состояний модифицированного аддитивного генератора.

ЛИТЕРАТУРА

1. *Кнут Д. Э.* Искусство программирования. Т. 2. Получисленные алгоритмы, 3-е изд. М.: Издательский дом «Вильямс», 2003.

2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.

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.