3. *Mcdonald C., Charnes C., and Pieprzyk J.* Attacking Bivium with MiniSat. Technical Report 2007/040. ECRYPT Stream Cipher Project, 2007.
4. *Eibach T., Pilz E., and Volkel G.* Attacking Bivium using SAT solvers // LNCS. 2008. V. 4996. P. 63–76.
5. *Soos M., Nohl K., and Castelluccia C.* Extending SAT solvers to cryptographic problems // LNCS. 2009. V. 5584. P. 244–257.
6. *Заикин О. С., Семенов А. А.* Применение метода Монте-Карло к прогнозированию времени параллельного решения проблемы булевой выполнимости // Вычислительные методы и программирование: новые вычислительные технологии. 2014. Т. 15. № 1. С. 22–35.
7. *Semenov A. A. and Zaikin O. S.* Using Monte Carlo method for searching partitionings of hard variants of Boolean satisfiability problem // LNCS. 2015. V. 9251. P. 222–230.
8. *Lechtaler A. C., Cipriano M., Garcia E., et al.* Model design for a reduced variant of a Trivium type stream cipher // J. Computer Science & Technology. 2014. V. 14. No. 1. P. 55–58.
9. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
10. *Otpuschennikov I. V., Semenov A. A., and Kochemazov S. E.* Transalg: a tool for translating procedural descriptions of discrete functions to SAT // Proc. 5th Intern. Workshop on Computer Science and Engineering: Information Processing and Control Engineering (WCSE 2015-IPCE). 2015. P. 289–294.
11. *Bard G. V.* Algebraic Cryptanalysis. Springer, 2009.

УДК 519.1 DOI 10.17223/2226308X/9/20

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ЭКСПОНЕНТОВ РАУНДОВЫХ ПЕРЕМЕШИВАЮЩИХ МАТРИЦ ОБОБЩЁННЫХ СЕТЕЙ ФЕЙСТЕЛЯ

А. М. Коренева, В. Н. Мартышин

Исследованы перемешивающие свойства раундовых функций обобщённых сетей Фейстеля, построенных на основе регистров сдвига длины 4 над множеством двоичных 32-мерных векторов. Рассмотрены регистровые функции с различным числом обратных связей регистра. Приведены результаты экспериментального исследования, направленного на выбор параметров регистровых функций, при которых реализуется наиболее быстрое перемешивание входных данных.

Ключевые слова: *обобщённая сеть Фейстеля, раунд шифрования, перемешивающая матрица, экспонент матрицы.*

Введение

Обозначим через $R(n, r, k)$ класс регистров сдвига длины n над множеством V_r двоичных r-мерных векторов с k обратными связями, $n, r > 1$, $k \geqslant 1$. Класс $R(n, r, k)$ обобщает класс $R(2, r, 1)$, относящийся к оригинальным сетям Фейстеля.

Увеличение длины базового регистра способствует увеличению производительности шифрования и вместе с тем числа раундов, достаточного для перемешивания входных данных. Свойства обобщённых сетей Фейстеля (ОСФ) исследовались как в зарубежных [1 – 4], так и в отечественных работах [5 – 7]. На основе ОСФ построены алгоритмы CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT и др. В [3] исследованы классы сетей $R(n, r, n/2)$, n — чётное (эти сети названы обобщёнными сетями Фейстеля 2-го типа). Отмечено, что вычислительная реализация таких сетей допускает распараллеливание и количество раундов, необходимых для перемешивания входных

данных, оценивается снизу величиной порядка n. С целью улучшения перемешивающих свойств сетей из класса $R(n, r, n/2)$ в [3] предложено заменить циклический сдвиг подблоков перестановками, что позволило понизить оценку числа раундов полного перемешивания подблоков до $2\log_2 n$.

В [4] исследованы классы сетей $R(n, r, 1)$, $R(n, r, n/2)$, $R(n, r, n-1)$ (ОСФ 1-го, 2-го и 3-го типа соответственно). С помощью орграфа перемешивания подблоков получены оценки числа раундов перемешивания входных подблоков: $(n-1)^2+1$ для $R(n, r, 1)$; n для двух других.

Отметим, что перемешивание входных подблоков не обеспечивает перемешивания битов (зависимости каждого бита выходного блока от всех входных битов), что сохраняет возможность применения некоторых криптоаналитических атак. Следовательно, исследование битового перемешивания для ОСФ является актуальным.

Работа посвящена перемешивающим свойствам раундовых функций ОСФ, построенных на основе классов регистров сдвига $R(4, 32, k)$, $k = 1, 2, 3$, т. е. ОСФ 1-го, 2-го и 3-го типа соответственно. Для исследования перемешивающих свойств используется оценочный матрично-графовый подход, который заключается в построении перемешивающей матрицы M для раундовой функции и экспериментальном определении значения её экспонента ($\exp M$). Значение $\exp M$ оценивает снизу число итераций, необходимое для полного перемешивания входных данных, то есть для обеспечения существенной зависимости каждой координатной булевой функции от всех входных переменных. Приведены результаты экспериментального исследования, направленного на выбор параметров регистровых функций, при которых реализуется наиболее быстрое полное перемешивание входных данных.

1. ОСФ на основе класса регистров сдвига $R(4,32,k)$

Сети классов регистров сдвига $R(4, 32, 1), R(4, 32, 2), R(4, 32, 3)$ реализуют преобразования $g^{(1)}, g^{(2)}, g^{(3)}$ соответственно:

$$g^{(1)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, X_3, X_4, X_1); \tag{1}$$

$$g^{(2)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, X_3, F_w(X_3) \oplus X_4, X_1); \tag{2}$$

$$g^{(3)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, F_w(X_2) \oplus X_3, F_v(X_3) \oplus X_4, X_1), \tag{3}$$

где $q, w, v, X_1, X_2, X_3, X_4 \in V_{32}$; (X_1, X_2, X_3, X_4) — открытый текст; q, w, v — раундовые ключи (подключи в случае схем типа 2 и 3); $F_a : V_{32} \to V_{32}$ — функция усложнения, реализуемая при раундовом ключе (подключе) $a \in \{q, w, v\}$. Схемы раунда шифрования для ОСФ 1-го, 2-го и 3-го типа представлены на рис. 1, выходные подблоки Y_1, Y_2, Y_3, Y_4 определены в соответствии с формулами (1)–(3).

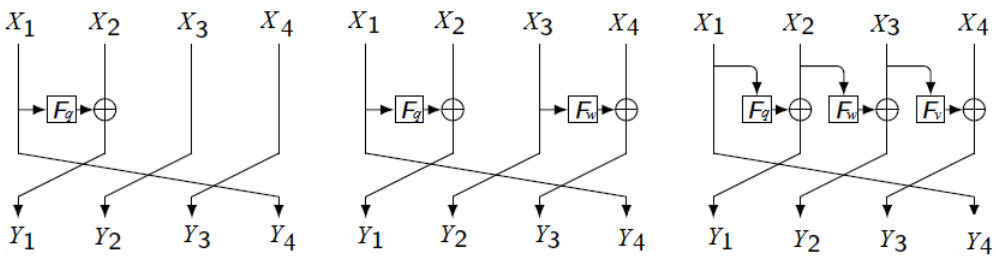

Рис. 1. Схемы раунда шифрования для ОСФ 1-го, 2-го и 3-го типов

2. Экспериментальное исследование перемешивающих свойств ОСФ при некоторых вариантах функции усложнения

Раундовые функции алгоритмов шифрования на основе ОСФ 2-го и 3-го типа могут использовать идентичные функции усложнения, что позволяет применить распараллеливание при вычислении раундовой функции. В эксперименте в качестве функции F_a, $a \in \{q, w, v\}$, использована функция усложнения отечественного алгоритма блочного шифрования ГОСТ 28147-89 (с различными вариантами подмешивания раундовых ключей), свойства которой хорошо изучены. Определим функцию усложнения F_a:

$$F_a(X_i) = T_{\text{left}}(S_{8,4}(X_i * a)),$$

где $a, X_i \in V_{32}$, $i = 1, 2, 3$; $*$ означает или XOR-суммирование двоичных векторов (обозначаемое $\oplus$), или сложение по модулю 2^{32} (обозначаемое $+$); $S_{8,4} = (S_1, \ldots, S_8)$; $S_1, \ldots, S_8$ — преобразования множества V_4 (s-боксы алгоритма ГОСТ 28147-89); T_{left} — циклический сдвиг векторов из V_{32} на 11 битов влево. Используя (1), (2) и (3), построим перемешивающие матрицы $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$. В матрицах $M(g^{(i)})$, $i = 1, 2, 3$, обозначим подматрицы размера 32×32: 0 — нулевая (состоящая из нулей) подматрица; E — единичная подматрица; $\Psi = \psi(i, j)$, где $\psi(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i, j \in \{1, \ldots, 32\}$; $\Phi = \phi(i, j)$, где $\phi(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i \in \{65, \ldots, 96\}$, $j \in \{65, \ldots, 96\}$; $\Lambda = \lambda(i, j)$, где $\lambda(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i \in \{33, \ldots, 64\}$, $j \in \{33, \ldots, 64\}$. Таким образом, матрицы $M(g^{(i)})$, $i = 1, 2, 3$, имеют следующий вид:

$$M(g^{(1)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \end{pmatrix}, M(g^{(2)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & 0 & 0 & 0 \\ 0 & E & \Phi & 0 \\ 0 & 0 & E & 0 \end{pmatrix}, M(g^{(3)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & \Lambda & 0 & 0 \\ 0 & E & \Phi & 0 \\ 0 & 0 & E & 0 \end{pmatrix}.$$

В таблице приведены результаты вычислительного эксперимента по определению значений экспонентов перемешивающих матриц $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$ в зависимости от способов построения функций F_a.

Значения экспонентов перемешивающих матриц $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$

Функция F_a	$\exp M(g^{(1)})$	$\exp M(g^{(2)})$	$\exp M(g^{(3)})$
$T_{\text{left}}(S_{8,4}(X_i \oplus a))$	14	12	12
$T_{\text{left}}(S_{8,4}(X_i + a))$	9	7	7

В результате экспериментальных исследований получены некоторые рекомендации по выбору параметров функций обратной связи регистров сдвига, при которых реализуется наиболее быстрое полное перемешивание входных данных. В частности, к улучшению перемешивающих свойств приводит:

1) Замена циклического левого сдвига на 11 бит инволюцией координат вектора ($T_{\text{inv}}(x_1, \ldots, x_{32}) = (x_{32}, \ldots, x_1)$). При таком изменении $\exp M(g^{(1)}) = 8$, $\exp M(g^{(2)}) = 6$, $\exp M(g^{(3)}) = 6$.
2) Укрупнение s-боксов (использование преобразований $S_1, \ldots, S_4$ множества V_8). В этом случае $\exp M(g^{(1)}) = 8$, $\exp M(g^{(2)}) = 6$, $\exp M(g^{(3)}) = 6$.
3) Использование инволютивной перестановки битов в начальных подблоках, являющихся аргументами функции усложнения (для схемы 2-го типа это подблоки 2 и 4). В этом случае $\exp M(g^{(2)}) = 5$.

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.*