5. Р 1323565.1.004-2017. Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. М.: Стандартформ, 2017.
6. Р 1323565.1.012-2017. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. М.: Стандартформ, 2017.
7. ГОС Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартформ, 2015.
8. *Kleinjung T.* Discrete logarithms in GF(p) — 768 bits. June 16, 2016. `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;a0c66b63.1606` (дата обращения: 09.01.2018)
9. Automated Validation of Internet Security Protocols and Applications. Properties (Goals). `http://www.avispa-project.org/delivs/6.1/d6-1/node3.html` (дата обращения: 28.03.2018)

УДК 519.17 DOI 10.17223/2226308X/11/20

О ПЕРЕМЕШИВАЮЩИХ И НЕЛИНЕЙНЫХ СВОЙСТВАХ МОДИФИЦИРОВАННЫХ АДДИТИВНЫХ ГЕНЕРАТОРОВ

А. М. Коренева

Исследованы локальные характеристики подстановок множества состояний модифицированных аддитивных генераторов (МАГ), построенных на основе регистров сдвига длины 8 над множеством двоичных 32-мерных векторов, для трёх вариантов множества точек съёма (обратной связи) и двух вариантов модифицирующего преобразования. К исследованным характеристикам подстановок относятся: а) локальный $(0, 256)$-экспонент перемешивающей матрицы M порядка 256, то есть наименьшее натуральное число γ_0, такое, что при любом натуральном $t \geqslant \gamma_0$ положительны все столбцы матрицы M^t с номерами $0, 1, \ldots, 31$; б) показатель 0-совершенности, то есть наименьшее число тактов работы генератора, после которых каждая координатная функция 0-го блока зависит существенно от всех битов начального состояния; в) показатель 0-сильной нелинейности, то есть наименьшее число тактов работы генератора, после которых каждая координатная функция 0-го блока является нелинейной. Вычисленные значения характеристик варьируются от 8 до 29. Полученные результаты могут быть использованы при построении криптографических алгоритмов на основе МАГ, в частности алгоритмов ключевого расписания блочных шифров, обеспечивающих сложную нелинейную взаимосвязь битов основного и раундовых ключей.

Ключевые слова: *модифицированный аддитивный генератор, нелинейные функции, перемешивающие свойства, регистр сдвига, существенная переменная.*

Введение

В основе принципа перемешивания, важного для многих криптографических алгоритмов, лежит существенная нелинейная зависимость выходных данных от элементов входа. Эти свойства важны для оценки эффективности атак на системы защиты информации, таких, например, как последовательное опробование частей секретного параметра системы. Исследованы криптографические свойства степеней преобразования модифицированного аддитивного генератора для двух модификаций аддитивного генератора и трёх вариантов множества точек съёма. С помощью матрично-графово-

го подхода [1 – 3] исследованы перемешивающие свойства преобразований генераторов, получены значения локальных экспонентов их перемешивающих матриц. Проведены вычислительные эксперименты по определению степеней преобразований МАГ, при которых каждая координатная функция определённого выходного блока является нелинейной и совершенной, т. е. существенно зависит от всех битов начального состояния генератора.

1. Конструкция МАГ

Обозначим: $m = 2^{32}$; V_{32} — множество 32-мерных двоичных векторов; $\mathbb{Z}_m$ — кольцо вычетов по модулю m; b — биективное отображение $\mathbb{Z}_m \to V_{32}$, определяющее двоичное 32-разрядное представление числа $X \in \mathbb{Z}_m$ по правилу: если $X = 2^{31}x_0 + \ldots + 2x_{30} + x_{31}$, $x_i \in \{0,1\}$, $i = 0,1,\ldots,31$, то $b(X) = \overline{X} = (x_0,\ldots,x_{31}) \in V_{32}$; $\boxplus$ — операция сложения в кольце вычетов $\mathbb{Z}_m$; МАГ-μ — аддитивный генератор, модифицированный с использованием преобразования μ множества V_{32}.

Пусть $(X_0,\ldots,X_7)$ — начальное состояние МАГ-μ, где $X_0,\ldots,X_7 \in \mathbb{Z}_m$. При $i \geqslant 0$ закон рекурсии состояний МАГ-μ имеет вид (в записи $b\mu b^{-1}$ отображения применяются слева направо)

$$X_{i+7} = b\mu b^{-1}\left(\left(\sum_{k\in D} X_{i+k}\right) \mod 2^{32}\right),$$

где $D = d_0,\ldots,d_q$ — множество точек съёма функции обратной связи, $D \subseteq \{0,\ldots,7\}$, $0 < q$, $0 = d_0 < \ldots < d_q$. Обозначим через φ^μ преобразование множества V_{256}, реализуемое МАГ-μ:

$$\varphi^\mu(\overline{X}_0,\ldots,\overline{X}_7) = (\overline{X}_1,\ldots,\overline{X}_6, f^\mu(\overline{X}_0,\ldots,\overline{X}_7)). \tag{1}$$

Схема генератора МАГ-μ с множеством точек съёма $\{0,1,3,5,7\}$ приведена на рис. 1, его выходная последовательность есть X_i, $i \geqslant 0$.

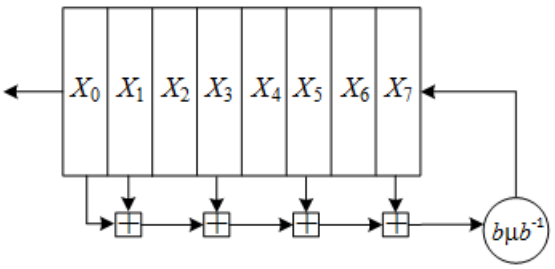

Рис. 1. Схема генератора МАГ-μ

2. Оценки перемешивающих свойств МАГ

Перемешивающие свойства МАГ-μ близки к наилучшим, если перемешивающий орграф $\Gamma(\varphi^\mu)$ преобразования φ^μ является примитивным. Необходимое условие этого [2, с. 225] — достижимость вершины 31 из вершины 0 в перемешивающем орграфе $\Gamma(\mu)$ преобразования μ (множество вершин $\Gamma(\varphi^\mu)$ есть $\{0,1,\ldots,31\}$).

В качестве модификации μ исследованы:

1) подстановка τ циклического сдвига на 1 шаг: $\tau(y_0,\ldots,y_{30},y_{31}) = (y_1,\ldots,y_{31},y_0)$;
2) преобразование θ множества V_{32} следующего вида:

$$\theta(y_0,\ldots,y_{30},y_{31}) = ((y_4,\ldots,y_7) \oplus S(y_0,y_1,y_2,y_3), (y_8,\ldots,y_{11}) \oplus S(y_0,y_1,y_2,y_3),\ldots,$$
$$(y_{28},\ldots,y_{31}) \oplus S(y_0,y_1,y_2,y_3), S(y_0,y_1,y_2,y_3)),$$

где S — функция одного из s-боксов алгоритма ГОСТ 28147-89, определённых в [4].

Обозначим: $\varphi^{\mu}_{u+32k}(\overline{X}_0,\ldots,\overline{X}_7)$ — координатные булевы функции преобразования φ^{μ}; f^{μ}_{u} — координатные булевы функции обратной связи регистра МАГ-μ; $\mu_u(y_0,\ldots,y_{31})$ — координатные булевы функции преобразования μ, $u=0,\ldots,31$, $E(f)$ — множество номеров существенных переменных булевой функции f.

Для обеих модификаций при различных множествах точек съёма $D_1=\{0,7\}$, $D_2=\{0,1,3,5,7\}$, $D_3=\{0,1,\ldots,7\}$ построены перемешивающий орграф $\Gamma(\varphi^{\mu})$ с множеством вершин $\{0,1,\ldots,255\}$ и перемешивающая матрица $M(\varphi^{\mu})$ размера 256×256. При $u=0,\ldots,31$ и $k=0,1,\ldots,6$ выполнено $E(\varphi^{\mu}_{u+32k})=\{u+32(k+1)\}$. При $k=7$ множества $E(\varphi^{\mu}_{u+32k})$ и $E(f^{\mu}_{u}(\overline{X}_0,\ldots,\overline{X}_7))$ равны, из формулы (1) следует, что $f^{\mu}_{u}(\overline{X}_0,\ldots,\overline{X}_7)=\mu_u\left(b\left(\sum\limits_{k\in D}X_k\right)\bmod 2^{32}\right)$. Множество $E(\varphi^{\mu}_{u+224})$ описывается теоремой [2, с. 220]: для функции φ^{μ}_{u+224}, $u=0,\ldots,31$, переменная x_{v+32k} существенная при $v=\theta,\ldots,31$, если и только если $k\in D$ и переменная y_θ существенная для μ_u, $0\leqslant\theta\leqslant31$.

Локальный $(0,256)$-экспонент матрицы M размера 256×256 есть наименьшее натуральное число γ_0, такое, что при любом натуральном $t\geqslant\gamma_0$ у матрицы M^t все столбцы с номерами из $0,1,\ldots,31$ положительны. Величины локальных $(0,256)$-экспонентов, приведённые далее в таблице, оценивают снизу число тактов работы генераторов, при которых возможно полное перемешивание знаков начального состояния.

3. Экспериментальные исследования криптографических свойств МАГ

Показателем 0-совершенности назовём наименьшее число γ тактов работы генератора, после которых каждая координатная функция 0-го блока существенно зависит от всех битов начального состояния. Показателем 0-сильной нелинейности назовём наименьшее число ξ тактов работы генератора, после которых каждая координатная функция 0-го блока является нелинейной.

Проведён вычислительный эксперимент по определению значения γ, в ходе которого для каждого из рассмотренных типов МАГ опробовано порядка 2^{24} пар двоичных векторов длины 256, соседних по каждой из координат. Проверено, что в каждом случае совершенная зависимость сохраняется как минимум до 500 такта работы генератора. Для каждого варианта МАГ вычислены значения γ и ξ (таблица).

Значения γ_0,γ и ξ для рассмотренных типов МАГ

γ_0 / γ / ξ	D_1	D_2	D_3
μ_1	15 / 29 / 9	10 / 18 / 9	9 / 16 / 9
μ_2	14 / 16 / 8	9 / 11 / 8	8 / 10 / 8

Выводы

Исследованы показатели 0-совершенности и 0-сильной нелинейности подстановок множества состояний для шести вариантов МАГ. Эти характеристики определяют важные криптографические свойства выходных последовательностей МАГ. Результаты экспериментального исследования показали, что показатель 0-совершенности не превышает удвоенного значения локального экспонента, а совершенная зависимость носит устойчивый характер (имеется на протяжении 500 тактов работы МАГ). Полученные результаты могут быть использованы при построении криптографических алгоритмов на основе МАГ, в частности при построении ключевого расписания

блочных шифров, обеспечивающего сложную нелинейную зависимость битов раундовых ключей от битов основного ключа.

ЛИТЕРАТУРА

1. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: Юрайт, 2016. 209 с.
2. *Fomichev V. M. and Koreneva, A. M.* Mixing properties of Modified Additive Generators // J. Appl. Indust. Math. 2017. V. 11. No. 2. P. 215–226.
3. *Фомичёв В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.
4. МР 26.2.003-2013 «Информационная технология. Криптографическая защита информации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89». М.: ТК 26, 2013.

УДК 519.1 DOI 10.17223/2226308X/11/21

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СВОЙСТВ НЕКОТОРЫХ «ЛЕГКОВЕСНЫХ» АЛГОРИТМОВ

К. В. Максимов, И. И. Хайруллин

Систематизированы подходы к построению блочных алгоритмов «легковесной» криптографии, изучены некоторые «легковесные» алгоритмы на основе сетей Фейстеля и SP-сетей и оценены их перемешивающие и нелинейные свойства. Определены понятия показателя сильной нелинейности (наименьшее число раундов, при котором каждая координатная функция выходного блока является нелинейной) и показателя совершенности (наименьшее число раундов, при котором каждый бит выходного блока существенно зависит от всех битов входного блока). Для алгоритмов PRESENT, MIDORI, SKINNY, CLEFIA и LILLIPUT получены точные значения экспонентов матриц существенной зависимости, построенных для раундовых функций (соответственно 3, 3, 6, 5, 5), оценки показателей совершенности (4, 3, 6, 5, 5) и показателей сильной нелинейности (1, 1, 1, 2, 2). Экспериментально установлено, что на протяжении 500 раундов каждая координатная функция выходного блока является нелинейной.

Ключевые слова: *«легковесная» криптография, сеть Фейстеля, SP-сеть, матрица существенной зависимости, экспонент матрицы, показатель сильной нелинейности, показатель совершенности.*

Введение

Основные направления развития криптографии во многом связаны с развитием средств связи, информационных технологий и вычислительной техники. Именно прогресс в этих областях сделал возможным повсеместное использование компактных устройств с малой вычислительной мощностью, имеющих доступ к сети Интернет и реализующих концепцию «Интернета вещей». Примерами таких устройств могут служить радиочастотные метки (RFID), средства автоматизированных систем управления технологическими процессами (SCADA), беспроводные сенсоры, электронные средства идентификации личности [1].