тельного соединения указанного регистра с полноцикловым линейным конгруэнтным генератором, использующим модуль 2^{32} и нечётный сдвиг [6, с. 156].

ЛИТЕРАТУРА

1. *Dmukh A. A., Dygin D. M., and Marshalko G. B.* A lightweight-friendly modification of GOST block cipher // Матем. вопр. криптогр. 2014. Т. 5. № 2. С. 47–55.
2. *Fomichev V. M., Avezova Ya. A., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Коренева А. М., Полеводин А. В.* Перемешивающие свойства генератора раундовых ключей алгоритма шифрования 2-ГОСТ // Информационная безопасность в банковско-финансовой сфере: Сб. научн. работ участников. М.: Прометей, 2018. С. 107–111.
4. *Дмух А., Трифонов Д., Чухно А.* О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС. Москва, РусКрипто-2018. `https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf`.
5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP) 800–22 Rev 1a. `https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic`.
6. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.

УДК 519.17 DOI 10.17223/2226308X/12/41

О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ МОДИФИЦИРОВАННЫХ МНОГОМЕРНЫХ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ

И. И. Хайруллин

Описан новый класс регистров сдвига длины n с r-битовыми ячейками, $n > 1$, $r > 1$, названных модифицированными многомерными линейными генераторами (ММЛГ). Проведено экспериментальное исследование перемешивающих свойств регистров сдвига длины 8 над V_{32} из класса ММЛГ, функция обратной связи которых построена на основе раундовой подстановки низкоресурсного блочного шифра SPECK. Для таких ММЛГ с различными множествами точек съёма $D \subseteq \{0, \ldots, 7\}$ рассчитаны локальные (0,256)-экспоненты перемешивающих матриц, то есть для каждой матрицы M определено наименьшее натуральное число γ, такое, что при любом натуральном $t \geqslant \gamma$ положительны все столбцы матрицы M^t с номерами 1,. . . ,32. Вычислены показатели 0-совершенности, то есть наименьшие значения степеней регистрового преобразования, при которых каждая координатная функция выхода существенно зависит от всех переменных входа. Для ММЛГ с точками съёма 0 и 7 значения локального экспонента и локального показателя совершенности равны 17. Полученные значения сравниваются с локальными экспонентами и локальными показателями совершенности для конструктивно схожих аналогов, построенных на основе модифицированных аддитивных генераторов. Сравнение показало, что генераторы обладают схожими перемешивающими свойствами, однако в отличие от рассмотренных схем класс ММЛГ представляет интерес для использования в условиях ограниченных ресурсов.

Ключевые слова: *модифицированный многомерный линейный генератор, пере-*

мешивающие свойства, матрично-графовый подход, перемешивающая матрица, показатель совершенности, регистр сдвига, экспонент, SPECK.

Введение

Одним из важных криптографических свойств итеративных криптографических алгоритмов является перемешивание входных данных. В основе принципа перемешивания лежит свойство существенной зависимости выходных функций от входных переменных. Для функции над двоичным конечномерным векторным пространством существенную зависимость каждого бита выхода от всех битов входа называют свойством полного перемешивания. Функции со свойством полного перемешивания называются совершенными [1].

Одним из методов оценки перемешивающих свойств преобразований является матрично-графовый подход (МГП) [2], который заключается в исследовании свойства примитивности и экспонентов для специального класса орграфов (перемешивающих орграфов) и соответствующих матриц смежности вершин этих орграфов (перемешивающих матриц). Неотрицательная матрица M называется примитивной, если M^t не содержит нулевых элементов при некотором $t \in \mathbb{N}$. Наименьшее t с таким свойством называют экспонентом матрицы M. С применением МГП в данной работе исследуется класс преобразований, построенных на основе регистров сдвига с нелинейной комбинирующей обратной связью — ММЛГ. Регистры сдвига над множеством двоичных r-мерных векторов широко используются при построении генераторов раундовых ключей итеративных блочных шифров [3 – 5].

Экспериментально определены множества точек съёма, при которых перемешивающая матрица преобразования множества состояний ММЛГ примитивна. Для различных множеств точек съёма получены значения γ локальных экспонентов перемешивающих матриц, оценивающих число тактов, после которых каждый из 32 разрядов вектора в ячейке с номером 0 может зависеть от всех битов начального заполнения регистра, иначе говоря, все столбцы с номерами 1,. . . ,32 перемешивающей матрицы в степени γ не содержат нулей. С учётом полученных значений локальных экспонентов определён показатель локальной совершенности преобразования ММЛГ, равный наименьшему числу тактов работы генератора, после которых указанная зависимость имеется.

1. Конструкция ММЛГ

Рассмотрим многомерный линейный генератор – генератор, построенный на основе регистра сдвига длины n над кольцом вычетов по модулю 2^r, $r > 1$. При $i \geqslant n$ знак гаммы X_i образуется в соответствии с законом рекурсии

$$X_i = b^{-1}\left(\bigoplus_{j=0}^{n-1} b(a_j X_{j+i-n})\right),$$

где $a_1, \ldots, a_{n-1} \in \{0, 1\}$; $a_0 = 1$; b — биекция $\mathbb{Z}_{2^r} \leftrightarrow V_r$, определяющая двоичное r-разрядное представление числа $X \in \mathbb{Z}_{2^r}$ по правилу: если $X = 2^{r-1}x_0 + \ldots + 2x_{r-2} + x_{r-1}$, то $b(X) = \bar{X} = x_0 \ldots x_{n-1}$, $\bar{X} \in V_r$; b^{-1} — обратная к b функция.

Модифицируем многомерный линейный генератор с помощью преобразования $g : V_r \to V_r$, назовём такой генератор ММЛГ, закон рекурсии для выходного знака X_i имеет вид

$$X_i = b^{-1}\left(g\left(\bigoplus_{j=0}^{n-1} b(a_j X_{j+i-n})\right)\right).$$

Обозначим через $\varphi^g : V_{nr} \to V_{nr}$ преобразование множества состояний ММЛГ

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

где $f^g(\bar{X}_0, \ldots, \bar{X}_{n-1}) = g(f(\bar{X}_0, \ldots, \bar{X}_{n-1})) = g\left(\bigoplus\limits_{k \in D} b(X_k)\right)$ — функция обратной связи $f^g : V_{nr} \to V_r$ ММЛГ; $D = \{d_0, \ldots, d_q\} \subseteq \{0, \ldots, n-1\}$ — множество точек съёма (номеров существенных переменных функции f).

Схема ММЛГ приведена на рис. 1, через Q обозначен выход генератора.

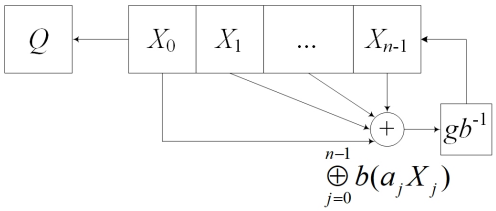

Рис. 1. Схема функционирования ММЛГ

Рассмотрим класс ММЛГ, построенных на основе регистров сдвига длины 8 над V_{32}. В качестве модифицирующего преобразования используем раундовую подстановку низкоресурсного блочного алгоритма шифрования SPECK с блоком длины 32 бита и соответствующими для данного размера блока параметрами алгоритма, описанными в [6]. Обозначим такое модифицирующее преобразование через $\hat{S}_{32}$. Оно обладает рядом позитивных свойств:

— экспонент перемешивающей матрицы преобразования $\hat{S}_{32}$ равен 4, что сравнимо со значениями экспонентов других современных низкоресурсных алгоритмов блочного шифрования;
— имеет малые показатели ресурсоёмкости в сравнении с другими современными низкоресурсными алгоритмами блочного шифрования, в частности по площади аппаратной реализации. Это свойство особенно полезно с учётом современных тенденций, направленных на построение низкоресурсных алгоритмов.

2. Экспериментальное исследование перемешивающих свойств

В ходе эксперимента исследованы ММЛГ, построенные на основе регистров сдвига длины 8 над V_{32} с модифицирующим преобразованием $\hat{S}_{32}$ и различными множествами точек съёма $D \subseteq \{0, \ldots, 7\}$. Для каждого регистрового преобразования построена перемешивающая матрица M и определено значение локального (0,256)-экспонента, то есть наименьшее натуральное число γ, такое, что при любом натуральном $t \geqslant \gamma$ положительны все столбцы матрицы M^t с номерами {1,. . . ,32}. Проведён вычислительный эксперимент по определению показателя 0-совершенности, то есть наименьшего числа тактов работы ММЛГ, после которого каждая координатная функция нулевого блока существенно зависит от всех знаков начального состояния.

В табл. 1 представлены значения локальных характеристик перемешивания для некоторых представителей $\hat{S}_{32}$-модификации ММЛГ с различными множествами точек съёма.

Исходя из соображений экономичности аппаратной реализации, рассмотрим $\hat{S}_{32}$-модификацию ММЛГ с множеством точек съёма $D = \{0, 7\}$. Сравним полученные значения локальных экспонентов и локальных показателей совершенности с аналогичными характеристиками для конструктивно схожих аналогов генератора. Рассмотрим

Таблица 1

Значения локальных характеристик перемешивания для $\hat{S}_{32}$-модификаций

Мощность множества точек съёма	Множество точек съёма	Показатель 0-совершенности	Локальный (0,256)-экспонент
2	{0,7}	17	17
3	{0,3,7}	14	14
4	{0,1,4,7}	13	13
5	{0,1,3,5,7}	12	12

схемы МАГ-μ_1 и МАГ-μ_2 [6], а также МАГ-$\hat{S}_{32}$ — преобразование аддитивного генератора, модифицированного с использованием SPECK. Сравнение перемешивающих характеристик приведено в табл. 2.

Таблица 2

Сравнение перемешивающих характеристик

Схема регистра сдвига	МАГ-μ_1	МАГ-μ_2	МАГ-$\hat{S}_{32}$	ММЛГ-$\hat{S}_{32}$
(0,256)-экспонент	15	14	15	17
Показатель 0-совершенности	29	16	16	17

Выводы

С помощью матрично-графового подхода исследованы перемешивающие свойства нового класса регистровых преобразований — многомерных линейных генераторов, модифицированных с использованием преобразования SPECK. По результатам исследования предложена схема на основе регистра сдвига с двумя точками обратной связи, которая обеспечивает паритет по качеству перемешивающих свойств и площади аппаратной реализации. Значения перемешивающих характеристик для предложенной схемы близки к аналогичным характеристикам для конструктивно схожих схем генераторов, однако, в отличие от рассмотренных схем, ММЛГ представляет интерес для использования в условиях ограниченных ресурсов.

Автор выражает благодарность д.ф.-м.н. профессору В. М. Фомичеву и к.ф.-м.н. А. М. Кореневой за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты. М.: Юрайт, 2017.
2. *Fomichev V. M., Avezova Ya. A., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Fomichev V. M. and Koreneva A. M.* On Efficiency of Block Encryption by Improved Key Schedule. Ярославль, CTCrypt-2016. `https://ctcrypt.ru/files/files/2016/12fomichev.pdf`.
4. *Фомичев В. М., Задорожный Д. И., Коренева А. М., Тулебаев А. И.* О ключевом расписании на основе модифицированного аддитивного генератора. Москва, РусКрипто-2018. `https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Koreneva.pdf`.
5. *Дмух А., Трифонов Д., Чухно А.* О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС.

Москва, РусКрипто-2018. https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf.

6. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK families of lightweight block ciphers. https://eprint.iacr.org/2013/404.pdf.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/42

A METHOD FOR CONSTRUCTING PERMUTATIONS, INVOLUTIONS AND ORTHOMORPHISMS WITH STRONG CRYPTOGRAPHIC PROPERTIES

R. A. de la Cruz Jiménez

S-Boxes are crucial components in the design of many symmetric ciphers. To construct permutations having strong cryptographic properties is not a trivial task. In this work, we propose a new scheme based on the well-known Lai-Massey structure for generating permutations of dimension $n = 2k$, $k \geqslant 2$. The main cores of our constructions are: the inversion in $\mathrm{GF}(2^k)$, an arbitrary k-bit non-bijective function (which has no pre-image for 0) and any k-bit permutation. Combining these components with the finite field multiplication, we provide new 8-bit permutations without fixed points possessing a very good combination for nonlinearity, differential uniformity and minimum degree — (104; 6; 7) which can be described by a system of polynomial equations with degree 3. Also, we show that our approach can be used for constructing involutions and orthomorphisms with strong cryptographic properties.

Keywords: *S-Box, permutation, Boolean functions.*

Let V_n be n-dimensional vector space over the field $\mathrm{GF}(2)$, by $S(V_n)$ we denote the symmetric group on set of 2^n elements. The finite field of size 2^n is denoted by $\mathrm{GF}(2^n)$, where $\mathrm{GF}(2^n) = \mathrm{GF}(2)[\xi]/g(\xi)$, for some irreducible polynomial $g(\xi)$ of degree n. We use the notation $\mathbb{Z}/2^n$ for the ring of the integers modulo 2^n. There are bijective mappings between $\mathbb{Z}/2^n$, V_n, and $\mathrm{GF}(2^n)$ defined by the correspondences:

$$\left[a_{n-1} \cdot 2^{n-1} + \ldots + a_0\right] \quad \leftrightarrow \quad (a_{n-1}, \ldots, a_0) \quad \leftrightarrow \quad \left[a_{n-1} \cdot \xi^{n-1} + \ldots + a_0\right].$$

Using these mapping in what follows, we make no difference between vectors of V_n and the corresponding elements in $\mathbb{Z}/2^n$ and $\mathrm{GF}(2^n)$.

Throughout the article, we shall use the following operations and notations:

$a \| b$ — concatenation of the vectors a, b of V_l, i.e. a vector from V_{2l};
0 — the null vector of V_l;
$\oplus$ — bitwise eXclusive-OR — addition in $\mathrm{GF}(2^l)$;
$\langle a, b \rangle$ — the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of V_l, $\langle a, b \rangle = a_{l-1}b_{l-1} \oplus \ldots \oplus a_0 b_0$;
$\mathrm{w}_H(a)$ — the Hamming weight of a binary vector $a \in V_l$;
$\otimes$ — finite field multiplication;
$\Lambda \circ \Psi$ — a composition of mappings, where Ψ is the first to operate;
Ψ^{-1} — the inverse transformation to some bijective mapping Ψ.

Now, we introduce some basic concepts needed to describe and analyze S-Boxes with respect to linear, differential, and algebraic attacks. For this purpose, we consider an n-bit S-Box Φ as a vector of Boolean functions:

$$\Phi = (f_{n-1}, \ldots, f_0), \ \ f_i : V_n \to V_1, \ \ i = 0, 1, \ldots n-1.$$