ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

УДК 621.391.7

М.И. Мазурков, д-р техн. наук, проф.,
А.В. Соколов, бакалавр,
Одес. нац. политехн. ун-т

МЕТОДЫ СИНТЕЗА ДВОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СО СВОЙСТВОМ *k*-ГРАММНОГО РАСПРЕДЕЛЕНИЯ ДЛЯ ЗАДАЧ ШИФРОВАНИЯ

М.І. Мазурков, А.В. Соколов. **Методи синтезу двійкових псевдовипадкових послідовностей з властивістю *k*-грамного розподілу для задач шифрування.** Розроблено методи синтезу повного класу двійкових лінійних і нелінійних псевдовипадкових послідовностей з властивістю *k*-грамного розподілу, які дозволяють скоротити в чотири рази обсяг пам'яті апаратної реалізації підстановочних конструкцій симетричних блокових шифрів.

Ключові слова: шифрування; булеві функції; афінні коди; відстань Хеммінга; відстань нелінійності; циклічний зсув; кореляційна матриця.

М.И. Мазурков, А.В. Соколов. **Методы синтеза двоичных псевдослучайных последовательностей со свойством *k*-граммного распределения для задач шифрования.** Разработаны методы синтеза полного класса двоичных линейных и нелинейных псевдослучайных последовательностей со свойством *k*-граммного распределения, которые позволяют сократить в четіре раза объем памяти аппаратной реализации подстановочных конструкций симметричных блочных шифров.

Ключевые слова: шифрование; булевы функции; аффинные коды; расстояние Хэмминга; расстояние нелинейности; циклический сдвиг; корреляционная матрица.

M.I Mazurkov, A.V. Sokolov. **Synthesis methods of pseudo-random binary sequences with the property of the *k*-gram distribution for encryption tasks.** The synthesis methods of a full class of binary linear and nonlinear pseudo-random sequences with the property of a *k*-gram distribution are developed which allow a reduction of memory size of block codes substitution constructions hardware realization by a factor of 4.

Key words: encryption, Boolean functions, affine codes, Hamming distance, distance of nonlinearity, circular shift, correlation matrix.

Известен синтез подстановочных конструкций современных симметричных блочных шифров — *S*-блоков подстановки, и таблиц подстановок [1…3]. Определены критерии криптографической стойкости *S*-блоков подстановки: показатель случайности (непредсказуемости), свойство уравновешенности, свойство серий, свойство корреляций [4…6]. Вместе с тем, представляют практический интерес вопросы минимизации объема памяти для хранения таблиц подстановок аппаратных систем шифрования, однако такие исследования проведены недостаточно полно. Ключом к решению данной проблемы может стать использование шумоподобных сигналов — *Mg*-последовательностей, также известных как последовательности де Брейна или полные циклы [7].

Двоичная псевдослучайная *Mg*-последовательность периода $N = 2^k$, со свойством *k*-граммного распределения — последовательность, в которой каждая серия из *k* бит встречается на замкнутом цикле точно один раз [6].

Вопросы синтеза сигналов, обладающих такими практически привлекательными для задач шифрования свойствами, не нашли своего решения, и требуют дальнейших исследований.

Линейную *Mg*-последовательность можно построить на базе *M*-последовательности, порождаемой регистром сдвига с обратной связью [4], полученным в соответствии с генератор-

ным полиномом $\rho(v)$, степени $k = \deg\{\rho(v)\}$, путем добавления нуля к серии бит из $(k-1)$ нулей. Например, при $\rho(v) = v^4 + v + 1$, $k = 4$ Mg-последовательность и соответствующая ей десятичная кодирующая Q–последовательность, имеют вид

$$\begin{aligned} Mg = &\ [1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0], \\ Q = &\ [15 \quad 14 \quad 12 \quad 8 \quad 0 \quad 1 \quad 2 \quad 4 \quad 9 \quad 3 \quad 6 \quad 13 \quad 10 \quad 5 \quad 11 \quad 7]. \end{aligned} \tag{1}$$

Из анализа системы соответствия (1) следует, что каждая Mg-последовательность полностью определяет структуру и криптографические свойства S-блока подстановки (рис. 1), где $\mathbf{X} = \{x_0, x_1, x_2, x_3\}$, $\mathbf{Y} = \{y_0, y_1, y_2, y_3\}$ — векторы элементов, поступающих на вход и снимающихся с выходных линий S-блока, соответственно. При этом для хранения Mg-последовательности требуется в четыре раза меньший объем памяти, чем для хранения десятичной кодирующей Q-последовательности, следовательно, задача построения компактных S-блоков подстановки (рис. 1) получает принципиально новое решение, которое является особенно перспективным для криптоалгоритма стандарта [8] в виду гибкости выбора таблиц подстановки, предусмотренной последним.

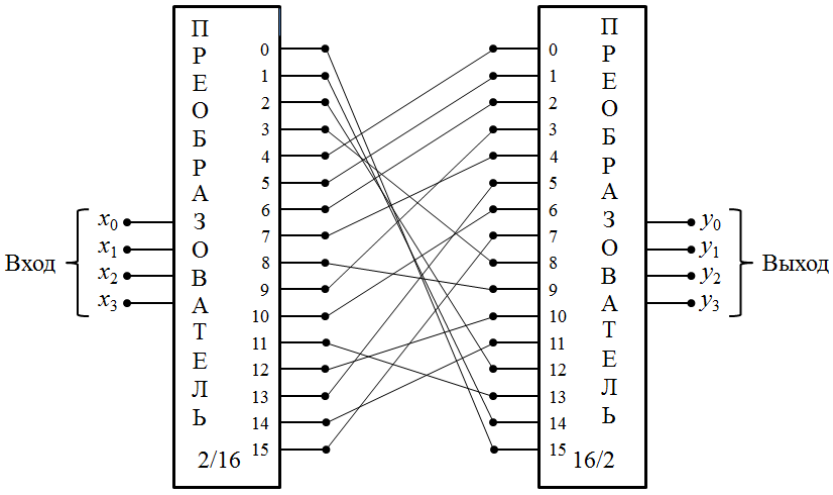


Рис. 1. Структурная схема S-блока подстановки, соответствующая Mg, Q (1)

Предлагается методология синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения на основе:

— двойного сцепления кортежей векторов (Метод 1);

— учета структурных свойств Mg–последовательностей (Метод 2);

— целочисленных функций (Метод 3).

Метод 1. Пусть $\mathbf{V}_k = \{\mathbf{A}_i\}$, $i = \overline{0, 2^k - 1}$ — линейное векторное пространство двоичных векторов размера k. Введем операции сцепления каждого вектора $\mathbf{A}_i = [\alpha_{i,k-1}, \alpha_{i,k-2}, \cdots, \alpha_{i,0}]$, где младший разряд справа.

Определение 1.1. Операции сцепления $S0$ и $S1$ произвольного вектора $\mathbf{A}_i \in \mathbf{V}_k$ — сдвиг вектора $\mathbf{A}_i$ влево на один элемент с последующей конкатенацией, соответственно, символа 0 или символа 1, и получение двоичного вектора размера k, как это показано с помощью выражений

$$\begin{array}{ll} \text{Сцепление } S0 & \text{Сцепление } S1 \\ [\alpha_{i,k-2}, \cdots, \alpha_{i,0}, 0]; & [\alpha_{i,k-2}, \cdots, \alpha_{i,0}, 1]. \end{array} \tag{2}$$

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Определение 1.2. Период ε_1 сцепления вектора $\mathbf{A}_i$ по горизонтали — это минимальное число последовательных операций сцепления $S0$, при которых вектор $\mathbf{A}_i$ переходит в нулевой, т.е. $\mathbf{A}_i \to \bar{0}$.

Определение 1.3. Период ε_2 сцепления вектора $\mathbf{A}_i$ по вертикали — это минимальное число последовательных операций сцепления $S1$, при которых вектор $\mathbf{A}_i$ переходит в единичный, т.е. $\mathbf{A}_i \to \bar{1}$.

На основе принятых определений установлены свойства операторов $S0$ и $S1$:

Свойство 1.1. Все четные векторы $\mathbf{A}_\gamma$, $\gamma = 2i$ имеют максимальный период сцепления по вертикали $\varepsilon_2 = k+1$, и, следовательно, образуют вертикальный кортеж $\mathbf{C} = \left[\mathbf{A}_\gamma^{S0_{\varepsilon_2}}, \mathbf{A}_\gamma^{S0_{\varepsilon_2-1}}, ..., \mathbf{A}_\gamma^{S0_1}\right]^T$, где $\mathbf{A}_\gamma^{S0_\iota}$ — ι последовательных операций сцепления $S0$ вектора $\mathbf{A}_\gamma$, T — оператор транспонирования. Каждый вектор полученного кортежа $\mathbf{C}$ с помощью оператора $S0$ образует свой горизонтальный кортеж $\mathbf{D}_u = \left[\mathbf{C}_u^{S1_1}, ..., \mathbf{C}_u^{S1_{\varepsilon_1-1}}, \mathbf{C}_u^{S1_{\varepsilon_1}}\right]$, где $\mathbf{C}_u^{S1_\iota}$ — ι последовательных операций сцепления $S1$ вектора $\mathbf{C}_u$, $u = \overline{1, \varepsilon_2}$. Пусть множество всех построенных таким образом кортежей $\mathbf{C}$ и $\mathbf{D}_u$ образует хранилище кортежей вектора $\mathbf{A}_i$. Пару четных векторов $\{\mathbf{A}_\gamma, \mathbf{A}_{\gamma+2^{k-1}}\}$, $i = \overline{0, 2^{k-2}-1}$ назовем образующей. Ясно, что число таких пар

$$p = 2^{k-2}, k = 3,4,5,\cdots \tag{3}$$

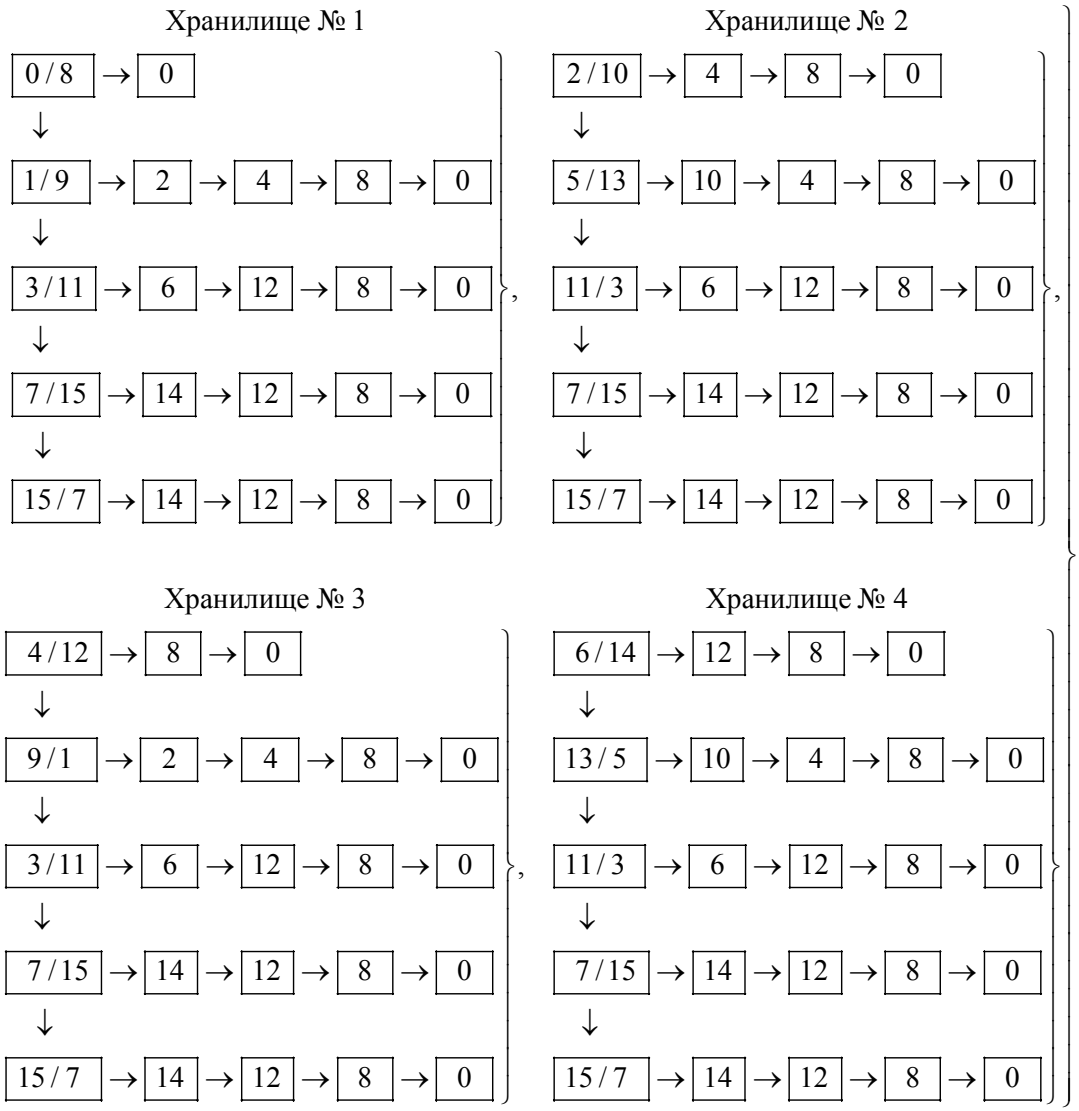
определяет число хранилищ для данного значения размерности k.

Свойство 1.2. Каждый образующий вектор из данной образующей пары формирует на основе операций сцепления $S0$ и $S1$ тождественно равные множества кортежей $\mathbf{C}$ и $\mathbf{D}_u$, т.е. тождественно равные хранилища кортежей, соответственно.

Построение ансамблей линейных и нелинейных *Mg*-последовательностей максимального периода $N = 2^k$ сводится к реализации метода двойного сцепления: сцепления между векторами (для формирования всех кортежей векторов в рамках каждого хранилища) и между хранилищами (для сцепления подходящих кортежей), при этом в каждое хранилище следует входить только один раз. Выбранный на данной итерации кортеж векторов назовем подходящим, если он заканчивается одним из образующих векторов другого хранилища.

Для сокращения записи и большей наглядности изложения каждый вектор $\mathbf{A}_i$ представляется своим номером i. Технические детали конструктивного правила построения *Mg*-последовательностей, со свойством k-граммного распределения, представим в виде шагов с конкретными примерами:

Шаг 1.1. Для заданного значения k построить $p = 2^{k-2}$ хранилищ кортежей векторов. Например, для $k = 4$ соответствующие множества кортежей и хранилища представлены в виде сформированной на основе операторов $S0$ и $S1$ алгебраической конструкции



(4)

Шаг 1.2. В качестве первого хранилища для построения кортежей максимального периода N фиксируется Хранилище № 1. Перебирая всевозможные структуры кортежей и учитывая их связи между хранилищами, можно найти множество опорных кодирующих последовательностей Q_i, каждая максимального периода $N = 16$ (табл. 1).

Таблица 1

Множество кодирующих Q -последовательностей

Q_i	Элементы кодирующей Q_i -последовательностей, $N = 16$															
Q_1	0	1	2	4	9	3	6	13	10	5	11	7	15	14	12	8
Q_2	0	1	2	4	9	3	7	15	14	13	10	5	11	6	12	8
Q_3	0	1	2	5	10	4	9	3	6	13	11	7	15	14	12	8
Q_4	0	1	2	5	10	4	9	3	7	15	14	13	11	6	12	8
Q_5	0	1	2	5	11	6	12	9	3	7	15	14	13	10	4	8
Q_6	0	1	2	5	11	6	13	10	4	9	3	7	15	14	12	8
Q_7	0	1	2	5	11	7	15	14	12	9	3	6	13	10	4	8

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Q_i	Элементы кодирующей Q_i-последовательностей, $N=16$															
Q_8	0	1	2	5	11	7	15	14	13	10	4	9	3	6	12	8
Q_9	0	1	3	6	12	9	2	5	11	7	15	14	13	10	4	8
Q_{10}	0	1	3	6	13	10	4	9	2	5	11	7	15	14	12	8
Q_{11}	0	1	3	6	13	10	5	11	7	15	14	12	9	2	4	8
Q_{12}	0	1	3	6	13	11	7	15	14	12	9	2	5	10	4	8
Q_{13}	0	1	3	7	15	14	12	9	2	5	11	6	13	10	4	8
Q_{14}	0	1	3	7	15	14	13	10	4	9	2	5	11	6	12	8
Q_{15}	0	1	3	7	15	14	13	10	5	11	6	12	9	2	4	8
Q_{16}	0	1	3	7	15	14	13	11	6	12	9	2	5	10	4	8

Другие кодирующие последовательности получим путем всех циклических сдвигов каждой образующей Q_i-последовательности.

Шаг 1.3. В соответствии с системой (1) строится полное множество Mg_j-последовательностей, $j=\overline{1,256}$, линейных и нелинейных. Например, на основе данных таблицы 1 строится в порядке возрастания множество всех образующих Mg_g-последовательностей, $g=\overline{1,16}$, каждая со свойством k-граммного распределения, рядом с ней проставлен десятичный эквивалент $(Mg_g)_{10}$.

$$G=\begin{bmatrix}
Mg_1 = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_1)_{10}=\mathbf{2479}\\
Mg_2 = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1], & (Mg_2)_{10}=2539\\
Mg_3 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_3)_{10}=2671\\
Mg_4 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1], & (Mg_4)_{10}=2683\\
Mg_5 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1], & (Mg_5)_{10}=2877\\
Mg_6 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1], & (Mg_6)_{10}=2927\\
Mg_7 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1], & (Mg_7)_{10}=3031\\
Mg_8 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1], & (Mg_8)_{10}=3027\\
Mg_9 = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1], & (Mg_9)_{10}=3261\\
Mg_{10} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_{10})_{10}=3375\\
Mg_{11} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1], & (Mg_{11})_{10}=3449\\
Mg_{12} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1], & (Mg_{12})_{10}=3557\\
Mg_{13} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1], & (Mg_{13})_{10}=\mathbf{3885}\\
Mg_{14} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1], & (Mg_{14})_{10}=3915\\
Mg_{15} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1], & (Mg_{15})_{10}=3929\\
Mg_{16} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1], & (Mg_{16})_{10}=3941
\end{bmatrix}. \qquad (5)$$

Линейные Mg_1 и Mg_{13}-последовательности, которые могут быть построены на базе M-последовательностей, отмечены жирным шрифтом своих десятичных эквивалентов. Уже при $k>4$ Метод 1 довольно трудоемкий, поскольку, по сути, сводится к перебору всех воз-

можных комбинаций кортежей в хранилищах. Расчет Mg-последовательностей длины 32 бита на эталонном компьютере проводился более 10-ти часов.

Для сокращения объема вычислений предлагается метод синтеза Mg-последовательностей, учитывающий их структурные свойства.

Метод 2. Применение метода перебора всего множества неприемлемо из-за объема исследуемого множества даже при сравнительно небольших значениях k. Для сокращения объема вычислений вводится тестирование текущей перебираемой последовательности T_i на соответствие структурным свойствам Mg-последовательностей. Последовательность T_i представляется в виде десятичного числа — ее номера $(T_i)_{10}$, и в виде N-разрядного двоичного вектора $(\mathbf{T}_i)_2 = \left\{t_{2^k}, t_{2^k-1}, ..., t_0\right\}$, т.е.

$$T_i = (T_i)_{10} = (\boldsymbol{T}_i)_2, \quad i = \overline{0, 2^{k-1}-1}, \tag{6}$$

где $i = \overline{0, 2^{2^k}}$ — переменная цикла поиска. Причем вторая половина последовательностей из полного множества T_i инверсна первой и, следовательно, перебор можно сократить в два раза, приняв $i = \overline{0, \left(2^N/2\right)}$.

Полученные на основе Метода 1 результаты синтеза Mg-последовательностей позволяют сформулировать ряд общих свойств.

Свойство 2.1. Свойство сбалансированности. Для каждой Mg-последовательности выполняется свойство сбалансированности $K^{(1)} = K^{(0)} = N/2$, где $K^{(1)}$ и $K^{(0)}$ соответственно число символов “1” и число символов "0" на максимальном периоде N Mg-последовательности. Следовательно, тестированию должны подвергаться только последовательности T_i, удовлетворяющие свойству 2.1.

Свойство 2.2. Свойство k-граммного распределения. В тестируемой последовательности T_i содержатся блоки из одних нулей или из одних единиц размера $k \le \log_2 N$, иначе она не рассматривается.

Свойство 2.3. Все образующие Mg-последовательности имеют нечетный десятичный эквивалент, вида

$$(Mg_{\text{образующая}})_{10} = 2\lambda + 1, \ \ \lambda \in \mathbb{Z}, \tag{7}$$

следовательно, переменную цикла поиска i можно изменять с шагом $step = 2$, что также сокращает перебор в два раза.

Свойство 2.4. Десятичный эквивалент первой Mg–последовательности должен быть выше минимального значения ее номера

$$\left(T_{\min}\right)_{10} = 2^{N-k-1} + 2^{N-2k} + 1, \ N = 2^k, \tag{8}$$

т.е. следует начинать перебор с минимального значения номера $\left(T_i\right)_{10} \ge \left(T_{\min}\right)_{10}$ тестируемой последовательности T_i. Этот результат следует из утверждений Метода 1.

Свойство 2.5. Десятичный эквивалент последней тестируемой Mg–последовательности должен быть ниже максимального значения номера

$$\left(T_{\max}\right)_{10} \le \left(T_{\min}\right)_{10} + 2^{N-k-1}, \tag{9}$$

поскольку все Mg_i-последовательности, расположенные после данного десятичного эквивалента, будут совпадать с ранее найденными с точностью до циклического сдвига.

Структурные свойства двоичной (эквивалентной бинарной) последовательности часто описывают с помощью количества входящих в нее блоков, где блок — последовательность одинаковых символов [11].

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Свойство 2.6. Каждая *Mg* -последовательность содержит оптимальное количество блоков символов, которым в соответствии с гипотезой Л.Е. Варакина [11] обладают только последовательности с незначительными пиками автокорреляционных функций,

$$\mu_{opt} = N / 2 . \quad (10)$$

На основании свойств 2.1…2.5 разработан метод, эффективный для поиска полного множества образующих *Mg* -последовательностей со свойством *k* -граммного распределения, что позволило существенно сократить время вычислений. Например, время поиска полного класса *Mg* –последовательностей длины $N = 32$ сократилось до трех минут, вместо 10 часов, как в Методе 1.

Метод 3. В основе метода лежит эвристический подход к синтезу образующих *Mg* -последовательностей на основе свойств специальных целочисленных функций. В теории клеточных автоматов часто используется функция целочисленного аргумента вида $\xi(n) = \mathrm{XOR}\{n, 2n\}$ [10], которая вычисляется как поэлементная сумма по модулю двух двух чисел: n и $2n$, представленных своими двоичными векторами. Поскольку десятичный эквивалент каждой образующей *Mg* -последовательности — число нечетное, то проводится модификация функции $\xi(n)$ так, чтобы она генерировала множество нечетных чисел, т.е. построится целочисленная функция

$$\psi(h) = \mathrm{XOR}\{2h+1, 2(2h+1)\}, \; h = \overline{1, 2^k - 1} . \quad (11)$$

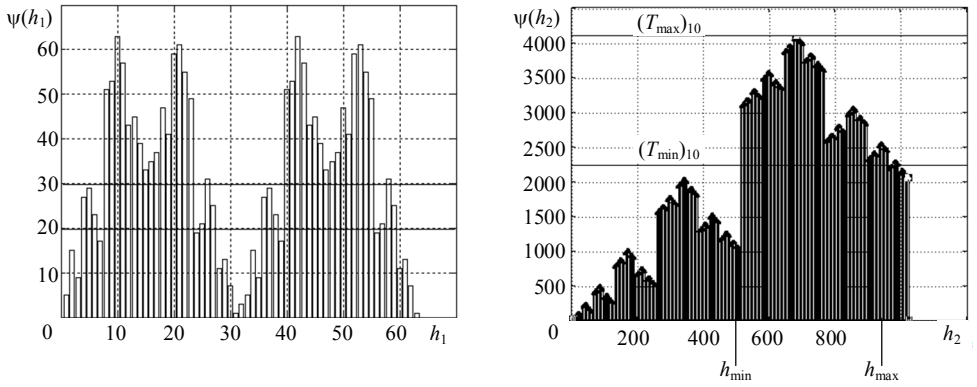
Проведенные исследования позволили установить ряд свойств этой функции.

Свойство 3.1. Целочисленная функция $\psi(h)$ является симметрической относительно аргумента $h = 2^{k-1}$, т.е.

$$\psi(h) = f(h + 2^{k-1}), \quad h = \overline{1, 2^k - 1} . \quad (12)$$

Свойство 3.2. Область поиска десятичных эквивалентов на основе целочисленной функции сокращается в два раза, по сравнению с Методом 2, при этом в области поиска всегда сохраняются все десятичные эквиваленты образующих *Mg* -последовательностей.

В качестве иллюстрации этих свойств приведены столбцовые диаграммы целочисленной функции $\psi(h)$ (рис. 2).



а *б*

Рис. 2. Столбцовые диаграммы целочисленной функции: $\psi(h_1) \bmod 2^6, \; h_1 = \overline{0, 64}$ *(а);*
$\psi(h_2) \bmod 2^{16}, \; h_2 = \overline{0, 1024}$ *(б)*

Алгоритм поиска *Mg* -последовательностей на основе целочисленной функции (12) по методу 3 состоит из двух шагов:

— для поиска всех образующих Mg-последовательностей по Методу 2 по известным минимальному и максимальному значениям номера $(T_{\min})_{10}$, $(T_{\max})_{10}$, необходимому и достаточному числу итераций $\Delta_2 = [(i_{\max})_{10} - (i_{\min})_{10}]/2$, найти границы изменения $h_{\min}$ и $h_{\max}$ переменной целочисленной функции (11) и число итераций для поиска этих же образующих Mg-последовательностей по Методу 3, из уравнений

$$i_{\min} = \psi(h_{\min}), \quad i_{\max} = \psi(h_{\max}), \quad \Delta_3 = h_{\max} - h_{\min}; \tag{13}$$

— построить множество значений целочисленной функции $\psi(h)$ в диапазоне Δ_3, и отобрать методом проб значения, которые соответствуют десятичным эквивалентам Mg-последовательностей.

Проиллюстрируем приведенный метод синтеза конкретным примером, осуществив поиск образующих Mg–последовательностей длины $N = 16$ бит. По Методу 1 проведена оценка верхней и нижней границ области поиска Mg–последовательностей

$$\begin{cases} Mg_1 > \{00001001\ \ 00000001\}_2 = 2305_{10} = i_{\min}; \\ Mg_{16} < \{00001111\ \ 11111111\}_2 = 4095_{10} = i_{\max}. \end{cases} \tag{14}$$

Из соотношения (13) и данных рисунка 2 определяется $\Delta_3 = 959 - 512 = 450$ итераций. Получены значения аргументов h и целочисленной функции $\psi(h)$, соответствующие всему классу образующих Mg–последовательностей длины 16 бит (табл. 2).

Таблица 2

Соответствие значений целочисленной функции $\psi(h)$ классу Mg –последовательностей

Значения аргумента	h	565	593	619	626	653	657	667	668
Значения целочисленной функции	$\psi(h)$	3261	3557	3449	3375	3885	3941	3929	3915
Образующая Mg-последовательность	Mg_i	Mg_9	Mg_{12}	Mg_{11}	Mg_{10}	Mg_{13}	Mg_{16}	Mg_{15}	Mg_{14}
Значения аргумента	h	768	788	856	861	866	885	940	946
Значения целочисленной функции	$\psi(h)$	2671	2683	3027	3021	2895	2877	2539	2479
Образующая Mg-последовательность	Mg_i	Mg_3	Mg_4	Mg_8	Mg_7	Mg_6	Mg_5	Mg_2	Mg_1

Одной из важнейших криптографических характеристик S-блока подстановки является его расстояние нелинейности d_S, определяемое как минимальное расстояние (dist) Хэмминга между каждой компонентной булевой функцией $f_i(X)$, представленной в алгебраически нормальной форме, и всеми кодовыми словами аффинного $A(N,k)$–кода [3,5,9]

$$d_S = \min\left\{\text{dist}(f_i, \varphi_j)\right\},\ i = \overline{1,k},\ j = \overline{1,2^k}, \tag{15}$$

где f_i — булева функция,

φ_j — кодовые слова аффинного $A(N,k)$-кода.

Другой весьма распространенный критерий качества S-блока подстановки — каждый бит выходного вектора y_j является статистически независимым от каждого бита входного вектора x_i. Количественно степень линейной статистической (корреляционной) связи между выходны-

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

ми и входными битами описывают с помощью корреляционной матрицы $\mathbf{R} = \left\| r_{i,j} \right\|$, $i, j = \overline{0, k-1}$, где коэффициенты корреляции

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j})}{N/2},\ i, j = \overline{0, k-1}. \qquad (16)$$

Минимаксное по модулю значение коэффициента $\left| r_{\min\max} \right| \le 0,25$, или отсутствие корреляции между битами выхода и входа $(r_{i,j} = 0)$, считается хорошим качеством шифра [3, 5]. Результаты проведенных исследований позволили выявить экономичные S–блоки подстановки с (наилучшими) минимаксными показателями (15) и (16) (табл. 3).

Таблица 3

Криптографические свойства экономичных S-блоков

Период $N = 2^k$	Объем класса $W = 2^{N/2}$	Минимаксные параметры		Количество J минимаксных S-блоков
		d_S	$\left| r_{\min\max} \right|$	
16	256	4,6	0,25	195
32	65536	12	0,125	379

Например, последовательность вида $Mg = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1]$ является минимаксной и обеспечивает построение S–блока подстановки с минимаксной корреляционной матрицей

$$\mathbf{R} = \begin{bmatrix} 0{,}2500 & 0{,}2500 & 0 & -0{,}2500 \\ 0{,}2500 & -0{,}2500 & -0{,}2500 & 0 \\ 0 & 0{,}2500 & 0 & -0{,}2500 \\ 0{,}2500 & -0{,}2500 & 0{,}2500 & -0{,}2500 \end{bmatrix},\ \left| r_{\min\max} \right| = 0{,}25. \qquad (17)$$

Каждая последовательность, полученная из данной путем циклического сдвига влево, например, на заданную величину $\tau = \{0, 6, 7, 8, 14, 15\}$, обеспечивает построение S-блока подстановки с минимаксной корреляционной матрицей, подобной (17). Минимаксные Mg-последовательности длины $N = 32$ обеспечивают построение S-блоков подстановки с параметром $\left| r_{\min\max} \right| = 0{,}125$.

Основные результаты проведенных исследований:

— разработана методология синтеза полного класса алгебраических конструкций — двоичных Mg-последовательностей со свойством k-граммного распределения, что позволяет в четыре раза сократить объем памяти аппаратных устройств хранения таблицы подстановки шифров, особенно криптоалгоритмов ГОСТ 28147–89;

— установлено, что S–блоки подстановки на основе Mg-последовательностей обладают практически привлекательными структурными и криптографическими свойствами, так большинство S-блоков подстановки длины $N = 16$ имеют следующие параметры: максимальный по модулю коэффициент корреляции между выходными и входными векторами данных $0{,}25 \le r_{\max} \le 0{,}5$; расстояние нелинейности S–блоков $2 \le d_S \le 6$; при этом с ростом криптографические свойства S-блоков существенно улучшаются;

— исследованы периодические и апериодические корреляционные свойства Mg-последовательностей и сделан вывод, что гипотеза об оптимальном числе блоков символов

минимаксных сигналов справедлива только по отношению к линейному подклассу Mg-последовательностей.

Полученные результаты свидетельствуют также о том, что криптоалгоритм ГОСТ 28147-89 имеет большие потенциальные возможности как в плане уменьшения аппаратной сложности, так и в плане увеличения практической защищенности.

Литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. — М.: Горячая линия — Телеком, 2010. — 232 с.
2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. — Изд. 2-е, испр.: Пер. с англ. — М.: Изд. дом "Вильямс", 2003. — 1104 с.
3. Мазурков, М.И. Трехуровневая криптографическая система блочного шифрования данных / М.И. Мазурков, В.Я. Чечельницкий., К.К. Некрасов // Изв. вузов. Радиоэлектроника. — 2010. — Т. 57, № 7. — С. 43 — 47.
4. Мазурков, М.І. Основи теорії передавання інформації / М.І. Мазурков. — Одеса: Наука і техніка, 2005. — 168 с.
5. Сергиенко, Р.В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89 / Р.В. Сергиенко, И.В. Москвиченко // Харьковск. ун-т воздушн. сил им. Ивана Кожедуба, Системы обработки информации. — Харьков, 2007. — № 8(66). — С. 91 — 95.
6. Knuth, D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms / D. Knuth — USA, Commonwealth of Massachusetts: Addison — Wesley. — 1969. — P. 634.
7. De Bruijn, N.G. A combitorial problem / N.G. de Bruijn // Nederl. Akad. Wetensch. Proc. — 1946. — Vol. 49. — P. 758—764.
8. ГОСТ 28147-89. Системы обработки информации. Криптографическая защита. Алгоритм криптографического преобразования. — М: Изд-во стандартов, 1990. — 28 с.
9. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. — М.: Радио и связь, 1985. — 384 с.
10. OEIS. A048724. — Antti Karttunen, 1999 // http://oeis.org/A048724 . — 7.01.12
11. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Всеукр. міжвід. наук.-техн. зб. "Радіотехніка". — Харків, 2004 . — Т. 126. — С. 132 — 138.

References

1. Ryabko, B.Ya. Osnovy sovremennoy kriptografii i steganografii [Foundations of Modern Cryptography and Steganography] / B.Ya. Ryabko, A.N. Fionov. — Moscow, 2010. — 232 p.
2. Sklyar, B. Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie [Digital Communications. The Theoretical Basics and Practical Application] / B. Sklyar. — 2nd ed., rev.: Transl. from English. — Moscow, 2003. — 1104 p.
3. Mazurkov, M.I. Trekhurovnevaya kriptograficheskaya sistema blochnogo shifrovaniya dannykh [Three-Level Cryptographic System of Block Data Encryption] / M.I. Mazurkov, V.Ya. Chechelnitskiy., K.K. Nekrasov // Universities information. Electronics. — 2010. — Vol. 57. — #7. — pp. 43 — 47.
4. Mazurkov, M.I. Osnovy teorii peredavannia informatsii [Basics of Information Transfer Theory] / M.I. Mazurkov. — Odesa, 2005. — 168 p.
5. Sergienko, R.V. Issledovanie kriptograficheskikh svoystv nelineynykh uzlov zamen algoritma simmetrichnogo shifrovaniya GOST 28147-89 [Investigation of Nonlinear Properties of the Cryptographic Substitutions Units of the Symmetric Algorithm GOST 28147-89] / R.V. Sergienko, I.V. Moskvichenko // Kharkov. Univ. of air. forces of Ivan Kozhedub, Information processing systems. — Khar'kov, 2007. — # 8 (66). — pp. 91 — 95.
6. Knuth D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms / D. Knuth — USA, Commonwealth of Massachusetts: Addison-Wesley. — 1969. — p. 634.
7. De Bruijn N.G. A Combinatorial Problem // Nederl. Akad. Wetensch. Proc. — 1946. — Vol. 49. — pp. 758 — 764.
8. GOST 28147–89. Sistemy obrabotki informatsii. Kriptograficheskaya zashchita. Algoritm kriptograficheskogo preobrazovaniya [Information Processing Systems. Cryptographic Protection. The Algorithm of Cryptographic Transform]. — Moscow, 1990. — 28 p.
9. Varakin, L. Sistemy svyazi s shumopodobnymi signalami [Communication Systems with Noise-Like Signals]. —Moscow, 1985. — 384 p.
10. OEIS. A048724. — Antti Karttunen, 1999 // http://oeis.org/A048724 . — 7.01.12

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

11. Horbenko, I.D. Doslidzhennia analitychnykh i statystychnykh vlastyvostei bulevykh funktsii kryptoalhorytmu RIJNDAEL (FIPS 197) [Investigation of Analytical and Statistical Properties of Boolean Functions of Cryptographic Algorithm RIJNDAEL (FIPS 197)] / I.D. Horbenko, O.V. Potii, Yu.A. Izbenko // All-Ukrainian interdepartmental scientific and technical collection “Radio” — Kharkiv, 2004. — Volume 126. — pp. 132 — 138.

Рецензент д-р техн. наук, доц. Одес. нац. экон. ун-та Скопа А.А.

Поступила в редакцию 19 декабря 2011 г.