УДК 621.391.7

М.И. Мазурков, д-р техн. наук, проф.,
В.Я. Чечельницький, канд. техн. наук, доц.,
М.А. Мельник, специалист,
А.В. Соколов, бакалавр,
Одес. нац. политехн. ун-т

АЛГОРИТМ СИНТЕЗА ОПТИМАЛЬНЫХ КРИПТОГРАФИЧЕСКИХ БЛОКОВ ПОДСТАНОВКИ НА ОСНОВЕ РЕГУЛЯРНЫХ ОПЕРАТОРОВ ДЕЦИМАЦИИ, ПЕРЕСТАНОВКИ И *m*-СДВИГА

М.І. Мазурков, В.Я. Чечельницький, М.О. Мельник, А.В. Соколов. **Алгоритм синтезу оптимальних криптографічних блоків підстановки на основі регулярних операторів децимації, перестановки і *m*-зсуву.** На основі регулярних операторів: власної децимації, перестановки і *m*-зсуву, запропоновано алгоритм синтезу оптимальних криптографічних конструкцій — *S*-блоків підстановки, з максимальною відстанню нелінійності та іншими практично привабливими криптографічними властивостями.

Ключові слова: *S*-блок, булеві функції, алгебраїчна нормальна форма, афінні коди, *m*-зсув, циклічний часовий зсув.

М.И. Мазурков, В.Я. Чечельницкий, М.А. Мельник, А.В. Соколов. **Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и *m*-сдвига.** На основе регулярных операторов: собственной децимации, перестановки и *m*-сдвига, предложен алгоритм синтеза оптимальных подстановочных криптографических конструкций — *S*-блоков подстановки с максимальным расстоянием нелинейности, и другими практически привлекательными криптографическими свойствами.

Ключевые слова: *S*-блок, булевы функции, алгебраическая нормальная форма, аффинные коды, *m*-сдвиг, циклический временной сдвиг.

M.I. Mazurkov, V.Ya. Chechelnitskiy, M.O. Melnik, A.V. Sokolov. **Optimal cryptographic substitution boxes synthesis algorithm based on regular operators of decimation, permutation and *m*-shift.** On the basis of own decimation, permutation and *m*-shift regular operators an optimal cryptographic substitution boxes (*S*-boxes) synthesis algorithm is proposed. The obtained *S*-boxes have a maximum non-linearity distance and some other utilitarian cryptographic properties.

Key words: *S*-box, Boolean functions, algebraic normal form, affine codes, *m*-shift, cyclic time shift.

Подстановочные конструкции современных симметричных блочных шифров — криптографические S-блоки подстановки известны [1…3], в частности, подход, основанный на алгебраических методах описания S-блоков с помощью аппарата булевых функций. Известен метод построения S-блоков на основе операции собственной децимации и операции m-сдвига [4], в теории дискретных сигналов на конечных интервалах [5]. Однако, как показали исследования, криптографические свойства этих подстановочных конструкций могут быть существенно улучшены путем введения дополнительных операций циклического сдвига по времени (приведения) и перестановки, в рамках конструирования каждого S-блока подстановки.

Предлагается разработанный применительно к шифрам типа ГОСТ28147-89 [...] алгоритм синтеза оптимальных криптографических S-блоков подстановки на основе регулярных операторов собственной децимации, перестановки и m-сдвига с максимальным расстоянием нелинейности сбалансированных булевых функций.

Для создания такого алгоритма рассмотрены свойства операторов децимации, приведения и m-сдвига, выделены соотношения, позволяющие получить оптимальные S-блоки подста-

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

новки, обладающие максимальным расстоянием нелинейности компонентных булевых функций, проведена оценка объемов доступных оптимальных S-блоков подстановки, которые могут синтезированы.

Рассмотрим множество элементов (двоичных векторов) расширенного поля $GF(2^n)$, упорядоченных в естественном порядке возрастания натуральных чисел в виде двоичной матрицы $\mathbf{G}=[(0,0,\cdots,0);(0,0,\cdots,1);\cdots;(1,1,\cdots,1)]$, размера $(N\times n)$, где $N=2^n$ — количество отводов S-блока. Алгоритм синтеза семейств сбалансированных булевых функций — S-блоков подстановки — с максимальным расстоянием нелинейности представим в виде ряда процедур (шагов), а изложение важных технических деталей алгоритма будем сопровождать конкретным примером синтеза.

Шаг 1. Найти оптимальные значения d_{opt} параметра собственной децимации [6], которые обеспечивают построение n-битных S-блоков подстановки с максимальным расстоянием нелинейности. Например, для 4-битного S-блока число отводов $N=2^4=16$. После осуществления последовательно собственную децимацию натурального ряда из $N=16$ чисел

$$\mathbf{G}=[\ 0\quad 1\quad 2\quad 3\quad 4\quad 5\quad 6\quad 7\quad 8\quad 9\quad 10\quad 11\quad 12\quad 13\quad 14\quad 15], \tag{1}$$

с параметром децимации $d\in\{3,5,7,9,11,13,15\}$, выполнения операции приведения последовательности, т.е. циклического сдвига полученных последовательностей так, чтобы старший элемент (2^n-1) находился в начале, а элемент $\mathbf{X}=(0,0,\cdots,0)$, состоящий из одних нулей, отображался в элемент $\mathbf{Y}=(1,1,\cdots,1)$, состоящий из одних единиц, получаются следующие кодирующие последовательности

$$\mathbf{D}=\begin{bmatrix}
\mathbf{D}_1=\{15 & 2 & 5 & 8 & 11 & 14 & 1 & 4 & 7 & 10 & 13 & 0 & 3 & 6 & 9 & 12\}\\
\mathbf{D}_2=\{15 & 4 & 9 & 14 & 3 & 8 & 13 & 2 & 7 & 12 & 1 & 6 & 11 & 0 & 5 & 10\}\\
\mathbf{D}_3=\{15 & 6 & 13 & 4 & 11 & 2 & 9 & 0 & 7 & 14 & 5 & 12 & 3 & 10 & 1 & 8\}\\
\mathbf{D}_4=\{15 & 8 & 1 & 10 & 3 & 12 & 5 & 14 & 7 & 0 & 9 & 2 & 11 & 4 & 13 & 6\}\\
\mathbf{D}_5=\{15 & 10 & 5 & 0 & 11 & 6 & 1 & 12 & 7 & 2 & 13 & 8 & 3 & 14 & 9 & 4\}\\
\mathbf{D}_6=\{15 & 12 & 9 & 6 & 3 & 0 & 13 & 10 & 7 & 4 & 1 & 14 & 11 & 8 & 5 & 2\}\\
\mathbf{D}_7=\{15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0\}
\end{bmatrix}. \tag{2}$$

Установлен ряд свойств оператора собственной децимации.

Утверждение 1. Для произвольного n и натуральной последовательности вида (1) существуют точно два оптимальных значения параметра децимации

$$\left.\begin{aligned} d_{opt1}&=2^{n-2}-1,\\ d_{opt2}&=2^n-1,\end{aligned}\right\} \tag{3}$$

каждый из которых определяет оптимальную кодирующую последовательность на основе натуральной последовательности вида (1), и, следовательно, оптимальный n-битный S-блок подстановки с наибольшим расстоянием нелинейности $d_s=2^{n-1}$. В примере это последовательности D_3 и D_7 из (2). Структурная схема S-блока подстановки приведена для последовательности D_3 (рис. 1).

Другие последовательности дают меньшее расстояние нелинейности S-блоков подстановки. Представим таблицу истинности компонентных булевых функций f_1,f_2,f_3,f_4, для S-блока (см. рисунок 1), и соответствующие векторы X и $\mathbf{D}_3$, (табл. 1).

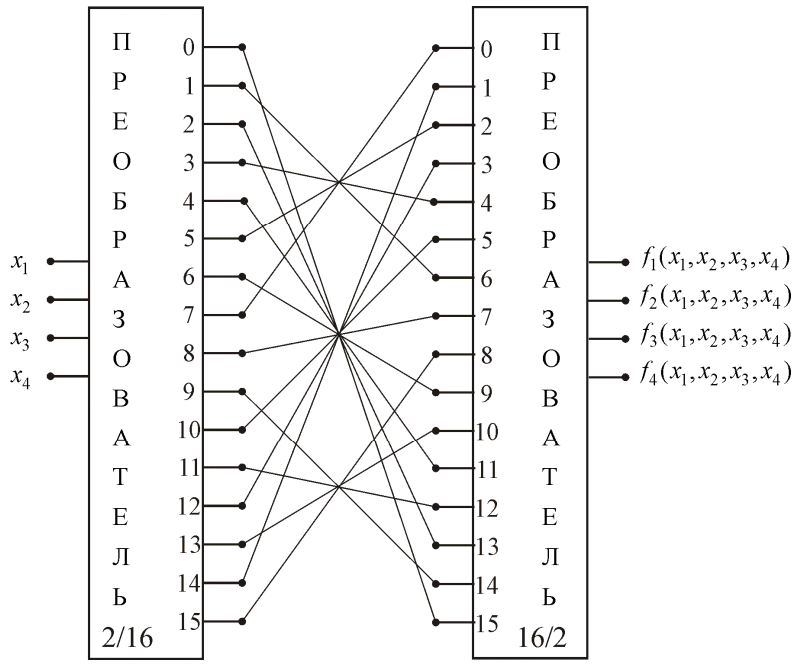

Рис. 1. Структурная схема S-блока подстановки для последовательности $\mathbf{D}_3$

Таблица 1

Таблицы истинности компонентных булевых функций f_1, f_2, f_3, f_4, *для* S *–блока подстановки для последовательности* $\mathbf{D}_3$

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	*15*
x_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	*1*
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	*1*
x_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	*1*
x_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	*1*
$\mathbf{D}_3$	15	6	13	4	11	2	9	0	7	14	5	12	3	10	1	*8*
f_1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	*1*
f_2	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	*0*
f_3	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	*0*
f_4	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*

Проведем анализ криптографических свойств S-блока подстановки (см. рисуок 1). Для нахождения максимального расстояния нелинейности каждой булевой функции $f_i(x_1,x_2,x_3,x_4)$, $i=\overline{1,4}$ (нелинейного порядка функции) составлена вспомогательная алгебраическая конструкция, содержащая всевозможные покоординатные суммы, а также таблица истинности всех линейных аффинных функций вида $\varphi=\alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \cdots \oplus \alpha_n x_n$, где $\alpha_i, x_i \in GF(2)$, и их номеров, и для удобства анализа рядом пропишем значения булевых функций (двоичных векторов), соответствующих кодирующей последовательности D_3.

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

Покоординатные суммы								Таблица истинности всех аффинных функций и их номеров: А(16б 4)-код													Булевы функции			
	x_1	$\oplus$	x_2	$\oplus$	x_3	$\oplus$	x_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	f_1	f_2	f_3	f_4
0.	0	$\oplus$	0	$\oplus$	0	$\oplus$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
1.	1	$\oplus$	0	$\oplus$	0	$\oplus$	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0
2.	0	$\oplus$	1	$\oplus$	0	$\oplus$	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	1	0	1
3.	1	$\oplus$	1	$\oplus$	0	$\oplus$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	0
4.	0	$\oplus$	0	$\oplus$	1	$\oplus$	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	0	1	1
5.	1	$\oplus$	0	$\oplus$	1	$\oplus$	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	0	1	0
6.	0	$\oplus$	1	$\oplus$	1	$\oplus$	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	0	0	1
7.	1	$\oplus$	1	$\oplus$	1	$\oplus$	0	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	0	0	0
8.	0	$\oplus$	0	$\oplus$	0	$\oplus$	1	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	1	1	1
9.	1	$\oplus$	0	$\oplus$	0	$\oplus$	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	1	1	0
10.	0	$\oplus$	1	$\oplus$	0	$\oplus$	1	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0	0	1	0	1
11.	1	$\oplus$	1	$\oplus$	0	$\oplus$	1	0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1	1	1	0	0
12.	0	$\oplus$	0	$\oplus$	1	$\oplus$	1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1
13.	1	$\oplus$	0	$\oplus$	1	$\oplus$	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	1	0	1	0
14.	0	$\oplus$	1	$\oplus$	1	$\oplus$	1	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	0	0	0	1
15.	1	$\oplus$	1	$\oplus$	1	$\oplus$	1	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	0	0	0

(4)

Оптимальный S-блок определим как такой, для которого набор булевых функций $f_i(x_1, x_2, \cdots, x_n)$, $i = \overline{1,n}$ удовлетворяет максиминному критерию, т.е. минимальное расстояние Хэмминга по заданному набору достигает максимального значения, среди всех других возможных наборов.

Утверждение 2. Каждый оптимальный S-блок с параметром n имеет максимальное расстояние нелинейности d_S, удовлетворяющее условию

$$d_S = \max_{\text{наборы}} \min_{i=1:n} \{d_{f_i}\} = 2^{n-1}, \tag{5}$$

где d_{f_i} – расстояние нелинейности булевой функции $f_i(x_1, x_2, \cdots, x_n)$.

Расстояние Хэмминга между каждой булевой функцией $f_i(x_1, x_2, x_3, x_4)$ из семейства (4) и всеми кодовыми словами аффинного $A(16,4)$-кода, равно 8, поэтому расстояние нелинейности S-блока (см. рисунок 1) $d_S = 8$, что является максимально возможным.

Утверждение 3. Каждый аффинный $A(2^n, n)$-код является линейным эквидистантным кодом с кодовым расстоянием Хэмминга $d = 2^{n-1}$, т.е. достигает верхней границы Плоткина кодового расстояния [7], а также обладает свойством симметрии, поскольку $A = A^T$, где T — знак транспонирования. Следовательно, бинарный аффинный код (при отображении: $0 \to +1, 1 \to -1$) представляет собой ортогональную матрицу, что важно практически, поскольку существует большое количество ортогональных матриц заданного порядка, но различных структур [8, 9].

Общий вид произвольной булевой функции в алгебраической нормальной форме для параметра $n = 4$

$$f_i(x_1,x_2,x_3,x_4)=\sum_{i=0}^{15}a_iT_i=$$
$$=a_0T_0+a_1x_1+a_2x_2+a_3x_3+a_4x_4+a_5x_1x_2+a_6x_1x_3+a_7x_1x_4+a_8x_2x_3+a_9x_2x_4+ \quad (6)$$
$$+a_{10}x_3x_4+a_{11}x_1x_2x_3+a_{12}x_1x_2x_4+a_{13}x_1x_3x_4+a_{14}x_2x_3x_4+a_{15}x_1x_2x_3x_4,$$

где $a_i\in GF(2)$ — искомые коэффициенты;

a_i, x_i — слагаемые в виде произведений составляющих координат называются термами T_i, при этом каждый терм $T_i\in GF(2)$,

а все операции сложения выполняются по $\mathrm{mod}\,2$.

Из условия физической реализуемости S-блока (см. рисунок 1) полагаем, что значение терма

$$T_0=\begin{cases}1, & \text{если } x_1=x_2=x_3=x_4=0,\\ 0, & \text{при других значениях } x_i.\end{cases} \quad (7)$$

Построим таблицу численных значений всех термов T_i, при каждом конкретном значении входного вектора $\mathbf{X}=[x_1,x_2,x_3,x_4]$, и на основе этой таблицы составим общую систему из 16 уравнений для рекуррентного нахождения коэффициентов a_i:

$$\left.\begin{array}{ll}
0. & a_0 =\\
1. & a_1 =\\
2. & a_2 =\\
3. & a_1 \oplus a_2 \oplus a_5 =\\
4. & a_3 =\\
5. & a_1 \oplus a_3 \oplus a_6 =\\
6. & a_2 \oplus a_3 \oplus a_8 =\\
7. & a_1 \oplus a_2 \oplus a_3 \oplus a_5 \oplus a_6 \oplus a_8 \oplus a_{11} =\\
8. & a_4 =\\
9. & a_1 \oplus a_4 \oplus a_7 =\\
10. & a_2 \oplus a_4 \oplus a_9 =\\
11. & a_1 \oplus a_2 \oplus a_4 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{12} =\\
12. & a_3 \oplus a_4 \oplus a_{10} =\\
13. & a_1 \oplus a_3 \oplus a_4 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{13} =\\
14. & a_2 \oplus a_3 \oplus a_4 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{14} =\\
15. & a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} =
\end{array}\right\},(8)$$

где значения правых частей каждого уравнения определяются видом построенной (выбранной) булевой функции $f_i(x_1,x_2,x_3,x_4)$, $i=\overline{1,4}$.

Для построенных значений функций $f_i(x_1,x_2,x_3,x_4)$ (см. таблицу 1), определены значения коэффициентов a_i из (8), и на основании (6), с учетом (7) получены аналитические выражения булевых функций, описывающих оптимальный S-блок (см. рисунок 1),

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

$$\left.\begin{aligned}
f_1(x_1,x_2,x_3,x_4) &= \begin{cases} 1, \quad \text{если } x_1=x_2=x_3=x_4=0, \\ x_2+x_3+x_1x_2+x_1x_3+x_1x_4+ \\ +x_2x_3+x_2x_4+x_3x_4+x_1x_2x_3+ \\ +x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+ \\ +x_1x_2x_3x_4, \quad \text{при других } x_i. \end{cases} \\
f_2(x_1,x_2,x_3,x_4) &= \begin{cases} 1, \quad \text{если } x_1=x_2=x_3=x_4=0, \\ x_1+x_2+x_4+x_1x_2+x_1x_3+x_1x_4+ \\ +x_2x_3+x_2x_4+x_3x_4+x_1x_2x_3+ \\ +x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+ \\ +x_1x_2x_3x_4, \text{ при других } x_i. \end{cases} \\
f_3(x_1,x_2,x_3,x_4) &= \begin{cases} 1, \quad \text{если } x_1=x_2=x_3=x_4=0, \\ x_1+x_3+x_4+x_1x_2+x_1x_3+x_1x_4+ \\ +x_2x_3+x_2x_4+x_3x_4+x_1x_2x_3+ \\ +x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+ \\ +x_1x_2x_3x_4, \text{ при других } x_i. \end{cases} \\
f_4(x_1,x_2,x_3,x_4) &= \begin{cases} 1, \quad \text{если } x_1=x_2=x_3=x_4=0, \\ x_2+x_3+x_4+x_1x_2+x_1x_3+x_1x_4+ \\ +x_2x_3+x_2x_4+x_3x_4+x_1x_2x_3+ \\ +x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+ \\ +x_1x_2x_3x_4, \text{ при других } x_i. \end{cases}
\end{aligned}\right\}. \qquad (9)$$

Из анализа аналитических выражений полученных булевых функций (9) нетрудно найти ряд криптографических свойств этих функций, связанных с количеством термов.

Шаг 2. Рассмотрим правила размножения оптимальных кодирующих последовательностей на основе перестановок булевых функций f_i, $i=\overline{1,n}$, определяющих оптимальный S-блок.

Утверждение 4. Каждый оптимальный набор булевых функций f_i, $i=\overline{1,n}$ порождает, путем операции всевозможных их перестановок, точно $n!$ оптимальных S–блоков подстановки, с максимальным расстоянием нелинейности $d_S=2^{n-1}$.

Например, набор булевых функций f_i, $i=\overline{1,4}$, из (4) и (табл. 2),

Таблица 2

Набор булевых функций f_i, $i=\overline{1,4}$

f_i	*Таблица истинности*															
f_1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	*1*
f_2	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	*0*
f_3	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	*0*
f_4	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*

путем операции перестановок, порождает $4!=24$ оптимальных S-блока подстановки, кодирующие последовательности которых $\mathbf{\Pi}_i$, представлены в виде матрицы

$$\mathbf{\Pi} = \begin{bmatrix}
\mathbf{\Pi}_1 =15 & 6 & 11 & 2 & 13 & 4 & 9 & 0 & 14 & 7 & 10 & 3 & 12 & 5 & 8 & 1 \\
\mathbf{\Pi}_2 =15 & 5 & 11 & 1 & 14 & 4 & 10 & 0 & 13 & 7 & 9 & 3 & 12 & 6 & 8 & 2 \\
\mathbf{\Pi}_3 =15 & 6 & 13 & 4 & 11 & 2 & 9 & 0 & 14 & 7 & 12 & 5 & 10 & 3 & 8 & 1 \\
\mathbf{\Pi}_4 =15 & 5 & 14 & 4 & 11 & 1 & 10 & 0 & 13 & 7 & 12 & 6 & 9 & 3 & 8 & 2 \\
\mathbf{\Pi}_5 =15 & 3 & 14 & 2 & 13 & 1 & 12 & 0 & 11 & 7 & 10 & 6 & 9 & 5 & 8 & 4 \\
\mathbf{\Pi}_6 =15 & 3 & 13 & 1 & 14 & 2 & 12 & 0 & 11 & 7 & 9 & 5 & 10 & 6 & 8 & 4 \\
\mathbf{\Pi}_7 =15 & 10 & 7 & 2 & 13 & 8 & 5 & 0 & 14 & 11 & 6 & 3 & 12 & 9 & 4 & 1 \\
\mathbf{\Pi}_8 =15 & 9 & 7 & 1 & 14 & 8 & 6 & 0 & 13 & 11 & 5 & 3 & 12 & 10 & 4 & 2 \\
\mathbf{\Pi}_9 =15 & 12 & 7 & 4 & 11 & 8 & 3 & 0 & 14 & 13 & 6 & 5 & 10 & 9 & 2 & 1 \\
\mathbf{\Pi}_{10} =15 & 12 & 7 & 4 & 11 & 8 & 3 & 0 & 13 & 14 & 5 & 6 & 9 & 10 & 1 & 2 \\
\mathbf{\Pi}_{11} =15 & 10 & 7 & 2 & 13 & 8 & 5 & 0 & 11 & 14 & 3 & 6 & 9 & 12 & 1 & 4 \\
\mathbf{\Pi}_{12} =15 & 9 & 7 & 1 & 14 & 8 & 6 & 0 & 11 & 13 & 3 & 5 & 10 & 12 & 2 & 4 \\
\mathbf{\Pi}_{13} =15 & 12 & 11 & 8 & 7 & 4 & 3 & 0 & 14 & 13 & 10 & 9 & 6 & 5 & 2 & 1 \\
\mathbf{\Pi}_{14} =15 & 12 & 11 & 8 & 7 & 4 & 3 & 0 & 13 & 14 & 9 & 10 & 5 & 6 & 1 & 2 \\
\mathbf{\Pi}_{15} =15 & 10 & 13 & 8 & 7 & 2 & 5 & 0 & 14 & 11 & 12 & 9 & 6 & 3 & 4 & 1 \\
\mathbf{\Pi}_{16} =15 & 9 & 14 & 8 & 7 & 1 & 6 & 0 & 13 & 11 & 12 & 10 & 5 & 3 & 4 & 2 \\
\mathbf{\Pi}_{17} =15 & 9 & 14 & 8 & 7 & 1 & 6 & 0 & 11 & 13 & 10 & 12 & 3 & 5 & 2 & 4 \\
\mathbf{\Pi}_{18} =15 & 10 & 13 & 8 & 7 & 2 & 5 & 0 & 11 & 14 & 9 & 12 & 3 & 6 & 1 & 4 \\
\mathbf{\Pi}_{19} =15 & 6 & 11 & 2 & 13 & 4 & 9 & 0 & 7 & 14 & 3 & 10 & 5 & 12 & 1 & 8 \\
\mathbf{\Pi}_{20} =15 & 5 & 11 & 1 & 14 & 4 & 10 & 0 & 7 & 13 & 3 & 9 & 6 & 12 & 2 & 8 \\
\mathbf{\Pi}_{21} =15 & 6 & 13 & 4 & 11 & 2 & 9 & 0 & 7 & 14 & 5 & 12 & 3 & 10 & 1 & 8 \\
\mathbf{\Pi}_{22} =15 & 5 & 14 & 4 & 11 & 1 & 10 & 0 & 7 & 13 & 6 & 12 & 3 & 9 & 2 & 8 \\
\mathbf{\Pi}_{23} =15 & 3 & 14 & 2 & 13 & 1 & 12 & 0 & 7 & 11 & 6 & 10 & 5 & 9 & 4 & 8 \\
\mathbf{\Pi}_{24} =15 & 3 & 13 & 1 & 14 & 2 & 12 & 0 & 7 & 11 & 5 & 9 & 6 & 10 & 4 & 8
\end{bmatrix}, \quad (10)$$

где кодирующая последовательность $\mathbf{D}_3$ из (2), представляется теперь в виде последовательности $\mathbf{\Pi}_{21}$.

Шаг 3. Рассмотрим правила размножения оптимальных кодирующих последовательностей на основе оператора m-сдвига по отношению к каждой кодирующей последовательности $\mathbf{\Pi}_i$. Величина τ m-сдвига принимает значения в диапазоне $\tau = \overline{0, N-1}$.

Утверждение 5. Оператор m-сдвига, по отношению к каждой кодирующей последовательности $\mathbf{\Pi}_i$, порождает всего N последовательностей $Q_{i,\lambda}$, $\lambda = \overline{0, N-1}$, однако, одна половина этих последовательностей тождественно совпадает с другой. Иными словами, период ε_m цикличности оператора m-сдвига по отношению к каждой кодирующей последовательности $\mathbf{\Pi}_i$, определяется соотношением

$$\varepsilon_m = N / 2 = 2^{n-1}. \quad (11)$$

С учетом (11) устанавливаем

Утверждение 6. Мощность $W(n)$ предложенного регулярного алгоритма синтеза — количество синтезируемых оптимальных S-блоков с заданным параметром n и основанием сдвига $m = 2$ определяется соотношением

$$W(n) = 2 \cdot \varepsilon_m \cdot n! = 2^n \cdot n!. \quad (12)$$

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

В рассматриваемом примере $W(4) = 2^4 \cdot 4! = 384$ оптимальных S-блока подстановки.

Полученные результаты свидетельствуют о больших объемах $W(n)$ оптимальных n-битных S-блоков подстановок, что имеет важное практическое значение как при совершенствовании известных шифров, так и при разработке новых концепций построения криптографических шифров, например, путем оперативной смены таблиц подстановок в рамках каждого раунда зашифровывания открытой информации. Во многих случаях можно отказаться от засекречивания S-блоков подстановок, поскольку шифр ГОСТ 28147-89 имеет достаточную длину ключа — 256 бит, следовательно, возможна реализация концепции распределения объема $W(n) = 2^n \cdot n!$ оптимальных S-блоков подстановок между различными группами финансовых учреждений.

Основные результаты проведенных исследований:

— Разработан алгоритм и элементы теории синтеза оптимальных криптографических $n-$битных S-блоков подстановки по критерию максимума расстояния нелинейности, на основе регулярных операторов собственной децимации, перестановки и m-сдвига.

— Установлено, что при произвольном значении параметра n существует $(2^n)!$ различных подстановок, например, уже при $n = 128$ существует $2^{128} \approx 10^{38}$ подстановок — астрономическое число для криптоаналитика. Однако, техническая реализация S-блока с 10^{38} контактами является невозможной. Отбирая специальный класс подстановок, на основе предложенного алгоритма удается алгоритмически реализовать S-блоки подстановки, практически с произвольным значением параметра n и заданным уровнем практической защищенности.

— Представленный алгоритм позволяет синтез большого числа $W(n)$ n-битных S-блоков подстановки, причем, величина W стремительно растет с ростом n.

— Разработанный алгоритм может быть распространен на другие виды регулярных операторов преобразования, например, преобразования на основе многопетлевых циклических сдвигов, мегациклических сдвигов, ступенчато подобных циклических сдвигов и т.д., на выбор других значений основания m-сдвига $(m = 3,4,5,\cdots)$, на основе кодов Рида-Соломона, на основе композиционных систем ДЧ сигналов над простыми и расширенными полями Галуа.

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. Изд. 2-е, испр.: Пер. с англ. / Б. Скляр. — М.: Издат. дом “Вильямс”, 2003. — 1104 с.
3. Долгов, В.И. Подстановочные конструкции современных симметричных блочных шифров / Долгов В.И., Олейников Р.В., Лисицкая И.В. и др. // Радіоелектронні і компютерні системи, ХНУРЭ, — 2009, — № 6. — С. 89 — 93.
4. Мазурков, М.И. Трехуровневая криптографическая система блочного шифрования данных / М.И. Мазурков, В.Я. Чечельницкий., К.К. Некрасов // Изв. вузов. Радиоэлектроника. — 2010. — Том 57. — № 7. — С. 43 — 47.
5. Трахтман, А.М. Основы теории дискретных сигналов на конечных интервалах / А.М. Трахтман, В.А. Трахтман. — М.: Сов. радио, 1975. — 208 с.
6. Мазурков, М.И. Системы широкополосной радиосвязи: учеб. пособие для студентов высших учеб. заведений / М.И. Мазурков.— Одесса.: Наука и техника, 2010. — 340 с.
7. Блейхут, Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. — М.: Мир, 1986.— 576 с.
8. Мазурков, М.И. Быстрые ортогональные преобразования на основе совершенных двоичных решеток / М.И. Мазурков, М.Ю. Герасименко // Изв. вузов. Радиоэлектроника. — 2006. — № 9. — С. 54 — 60.

9. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Изв. вузов. Радиоэлектроника. — 2008. — Том 51. — № 11. — С. 53 — 57.

References

1. Ryabko, B.Ya. Osnovy sovremennoy kriptografii i stenografii [Modern Cryptography and Steganography] / B.Ya. Ryabko, A.N. Fionov. — Moscow: Hot line — Telecom, 2010. — 232 p.
2. Sklyar, B. Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie. [Digital Communications. The theoretical basics and practical application] / B. Sklyar. — 2nd edition, revised. Translation from English. — Moscow: Publishing house "Williams", 2003. — 1104 p.
3. Dolgov, V.I. Podstanovochnye konstruktsii sovremennykh simmetrichnykh blochnykh shifrov [Substitution Constructions of Modern Symmetric Block Ciphers.] / Dolgov V.I., Oleinikov R.V., Lisitskaja I.V., Sergienko R.V., Drobot'ko E.V. Melnichuk E.D. // Radioelectronic and computer systems, Kharkov national university of radioelectronics, — 2009, — # 6. — pp. 89 — 93.
4. Mazurkov, M.I. Trekhurovnevaya kriptograficheskaya sistema blochnogo shifrovaniya dannykh [Three-level Cryptographic System of Block Data Encryption] / M.I. Mazurkov, V.J. Chechelnitsky., K.K. Nekrasov // Universities information. Electronics. — 2010. — Vol. 57. — #7. — pp. 43 — 47.
5. Trakhtman, A.M. Osnovy teorii diskretnykh signalov na konechnykh intervalakh [Basics of Theory of Discrete Signals on Finite Intervals] / A.M. Trakhtman, V.A. Trakhtman. — Moscow: Soviet Radio, 1975. — 208 p.
6. Mazurkov, M.I. Sistemy shirokopolosnoy radiosvyazi: uchebnoe posobie dlya studentov vysshykh uchebnykh zavedeniy [The Broadband Wireless Systems: tutorial for higher school students]. — Odessa; Science and technology, 2010. — 340 p.
7. Bleikhut, R. Teoriya i praktika kodov, kontrolliruyushchikh oshibki [Theory and Practice of Error Control Codes.] / Trans. From English. — Moscow: Mir, 1986. — 576 p.
8. Mazurkov M.I. Bystrye ortogonal'nye preobrazovaniya na osnove sovershennykh dvoichnykh reshetok [Fast Orthogonal Transforms on the Base of Perfect Binary Arrays] / M.I. Mazurkov, M.Yu. Gerasimenko // Universities information. Radioelectronics. — 2006. — # 9. pp. 54 — 6.
9. Mazurkov M.I. Metod zashchity informatsii na osnove sovershennykh dvoichnykh reshetok [Data Protection Method on the Base of Perfect Binary Arrays] / M.I. Mazurkov, V.Y. Chechelnitskiy, P. Murr // Universities information. Radioelectronics. — 2008. — Vol. 51. — # 11. — pp. 53 — 57.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Кобозева А.А.

Поступила в редакцию 30 ноября 2011 г.