УДК 681.3.06

**МАЗУРКОВ М.И., СОКОЛОВ А.В.**

# НЕЛИНЕЙНЫЕ $S$ -БЛОКИ ПОДСТАНОВКИ НА ОСНОВЕ КОМПОЗИЦИОННЫХ КОДОВ СТЕПЕННЫХ ВЫЧЕТОВ

*Одесский национальный политехнический университет*
*Украина, Одесса, 65044, пр-т Шевченко 1*

**Аннотация.** Предложен способ построения новых конструкций нелинейных $S$ -блоков подстановки длины $N = 256$ и объема $|S| = 8.6248 \cdot 10^{13}$ на основе композиционных кодов степенных вычетов. Синтезированные конструкции обладают хорошими криптографическими свойствами, существенно дополняют и расширяют класс конструкций Ниберга шифра Rijndael, а также обеспечивают возможность их применения в качестве долговременного ключа.

**Abstract.** The design method of the new constructions of nonlinear substitution $S$ -boxes of length $N = 256$ and volume $|S| = 8.6248 \cdot 10^{13}$ based on composite power residue codes are developed. The synthesized constructions with have good cryptographic properties, substantially amplifies and extends the class of Nyberg construction used in Rijndael cipher, as well as the opportunity to use it in the quality of long-term key are proposed.

**Ключевые слова:** криптографические шифры, нелинейные $S$ -блоки, методы синтеза, коды степенных вычетов, поля Галуа; cryptographic ciphers, nonlinear S-boxes, methods of synthesis, power residue codes, Galois fields.

Коды степенных вычетов широко используются для построения нормальных, композиционных и больших систем дискретных частотных (ДЧ) сигналов с большой базой и заданными структурными, дистанционными и корреляционными свойствами [1]. Вместе с тем, вопросы построения нелинейных $S$ -блоков подстановки на основе композиционных кодов степенных вычетов исследованы в литературе [2] недостаточно полно.

*Целью настоящей статьи является разработка способа построения нелинейных $S$ -блоков подстановки на основе композиционных кодов степенных вычетов, с хорошими криптографическими свойствами, применительно к шифру Rijndael/AES.*

Вне зависимости от выбранной архитектуры блочного симметричного шифра, будь то сеть Фейстеля или SP-сеть, основным компонентом, определяющим устойчивость криптопреобразования к основным видам атак криптоанализа, является надежность нелинейного $S$ -блока подстановки шифра, производящего отображение группы входных битов $x_i$ в группу выходных битов $y_i$ в соответствии с правилом кодирующей $Q$ -последовательности, которая полностью определяет структуру и криптографические свойства $S$ -блока подстановки. Пусть, например, задана кодирующая $Q$ -последовательность

$$Q_1 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}, \quad (1)$$

что соответствует отсутствию подстановки, т.е. прямому отображению входных битов $S$ -блока подстановки в выходные: $y_i = x_i$. Очевидно, что подобный $S$ -блок подстановки не обладает криптостойкостью, тем не менее, кодирующая $Q$ -последовательность (1) не содержит в себе повторяющихся элементов: операция подстановки, выполненная с помощью данного $S$ -блока подстановки является полностью обратимой. Такой $S$ -блок подстановки называется биективным [2], и может служить основой для построения криптографически высококачественных подстановочных конструкций.

Ввиду сильной взаимосвязи криптостойкости блочных симметричных шифров от примененных в них биективных $S$ -блоков подстановки задача построения больших мно-

жеств кодирующих $Q$-последовательностей, на базе которых могли бы быть построены криптографически качественные $S$-блоки подстановки является актуальной. Решению данной задачи посвящены работы многих исследователей, однако, оказывается, что существующие методы построения $Q$-последовательностей или приводят к криптографически уязвимым $S$-блокам подстановки, или позволяют построить лишь их небольшое количество.

Например, для построения $S$-блока подстановки шифра Rijndael/AES [3], его разработчики Даймен и Раймен выбрали за основу конструкцию К. Ниберг [2], которая представляет собой отображение, в виде мультипликативно обратных элементов поля $GF(2^k)$:

$$y = x^{-1} \operatorname{modd}[f(x), p], \quad y, x \in GF(2^k), \tag{2}$$

скомбинированное вместе с аффинным преобразованием

$$b = Ay + a, \quad a, b \in GF(2^k), \tag{3}$$

где $f(x) = x^8 + x^4 + x^2 + x + 1$ — неприводимый над полем $GF(2)$ полином, степени $k = 8$ используемый в Rijndael/AES [3], $A$ — невырожденная матрица аффинного преобразования, $a$ — вектор сдвига, $p = 2$ — характеристика поля, и принято, что $0^{-1} \equiv 0$.

Для нашего примера (1) можем выбрать один из неприводимых полиномов степени $k = 4$, например, $f(x) = x^4 + x + 1$, и в соответствии с (2) найти новое отображение в виде мультипликативно обратных элементов

$$Q_2 = \left\{0^{-1}, 1^{-1}, ..., 15^{-1}\right\} = \left\{0,1,2,4,8,9,11,15,7,14,5,10,13,3,6,12\right\}. \tag{4}$$

Очевидно, что подстановка (4) в отличие от (1) уже не является тривиальной. В [2,4] доказано, что криптографические $S$-блоки подстановки, построенные в соответствии с (2) являются сильно нелинейными, что делает их применение практически привлекательным. Однако подобных подстановочных конструкций (2), обладающих уникальной структурой, существует лишь ровно столько, сколько существует неприводимых $p$-ичных полиномов заданной степени $k$ [5]

$$\left|W_k\right| = \frac{1}{k} \sum_{d \;\vdots\; k} \mu(d) \cdot p^{(k/d)}, \tag{5}$$

где $d$ — делители числа $k$, $\mu(d)$ — функция Мёбиуса, а запись $d \;\vdots\; k$ означает, что $d$ делит $k$. Например, для степени неприводимого полинома $k = 8$, применяемой в криптопреобразовании Rijndael в соответствии с выражением (5) существует $\left|W_8\right| = 30$ неприводимых полиномов, из которых $\left|V_8\right| = \varphi\left(p^k - 1\right)/k = 16$ первообразных [6, 7], где $\varphi$ — функция Эйлера, что является недостаточным, например, для использования $S$-блока подстановки в качестве долговременного ключа. Возможность устранения данного недостатка может быть обнаружена в применении для построения кодирующих $Q$-последовательностей кодов степенных вычетов [1].

При $k = 8$, из анализа (2) с учетом теоремы о периоде элемента поля [8] запишем сравнение

$$x^{-1} \operatorname{modd}[f(x), p] \equiv x^{254} \operatorname{modd}[f(x), p], \tag{6}$$

которое показывает алгоритмическую возможность построения $S$-блоков подстановки конструкции (2) без использования операции обращения элементов, с помощью возведения в положительную степень по модулю первообразного неприводимого полинома, т.е. на основе кодов степенных вычетов.

Сравнение (6) есть строгое обоснование возможности построения $S$-блоков подстановки на базе кодов $r$-ичных степенных вычетов $i^r \bmod[f(z), p]$, $i = 0,1,...,255$, с хорошими криптографическими свойствами.

Представим произвольный $i$-ый степенной вычет композиционного кода [1] над полем $GF(p^k)$ в виде 4-х параметрического полинома $R^{(i,r,\omega,\nu)}(x)$ степени не более $k-1$, где через $(i,r,\omega,\nu)$ обозначены параметры полиномиального представления степенного вычета, т.е. основные параметры композиционного кода

$$R^{(i,r,\omega,\nu)}(x) = (\omega \cdot i^r + \nu) \bmod[f(x), p] = \alpha_{k-1}^{(i,r,\omega,\nu)} x^{k-1} + \alpha_{k-2}^{(i,r,\omega,\nu)} x^{k-2} + \cdots + \alpha_0^{(i,r,\omega,\nu)}, \quad i = 0,1,...,2^k - 1, \tag{7}$$

где коэффициенты $\alpha \in GF(p)$, $\omega = 1,2,..2^k - 1$, $\nu = 0,1,...,2^k - 1$.

Выражение (7) полностью определяет новый способ построения $Q$-последовательностей, а стало быть, и $S$-блоков подстановки на основе кодов степенных вычетов.

Для получения биективного $S$-блока подстановки с помощью $r$-ичных вычетов следует использовать такие значения чисел $r$, чтобы выполнялось условие отсутствия повторяющихся элементов в $Q$-последовательности

$$\text{НОД}(r, 2^k - 1) = 1, \tag{8}$$

где $k$ — степень расширения поля.

Для нашего примера (1), можем выбрать первообразный неприводимый полином $f(x) = x^4 + x + 1$. В соответствии с (8), находим подходящие значения $r$

$$\{r\} = \{1,2,4,7,8,11,13,14\}, \tag{9}$$

и выбрав, например, значения $r = 7$, $\omega = 1$, $\nu = 0$, в соответствии с (7) строим новый $S$-блок подстановки

$$Q_3 = \{0,1,7,5,12,8,2,9,15,6,10,11,14,4,13,3\}. \tag{10}$$

В соответствии с [9], данная кодирующая последовательность (10) может быть представлена набором из $k = 4$ компонентных булевых функций $F_i$ как это показано с помощью таблиц истинности, табл. 1

*Таблица 1*

| $Q_3$ | 0 | 1 | 7 | 5 | 12 | 8 | 2 | 9 | 15 | 6 | 10 | 11 | 14 | 4 | 13 | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_1$ | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| $F_2$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| $F_3$ | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| $F_4$ | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |

Для исследования криптографических свойств $S$-блоков подстановки примем следующие критерии качества их применения [4]:

1. Минимальное значение максимального коэффициента корреляции $\min(\max\{r_{i,j}\})$ корреляционной матрицы $R = \|r_{i,j}\|$, которая определяет степень линейной связи между векторами выхода $y_j$ и входа $x_i$ $S$-блока подстановки, где коэффициенты корреляции [9]

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j})}{N/2},\ i, j = 1,2,...,k, \tag{11}$$

$N = 2^k$ — длина двоичной булевой функции, $\oplus$ — символ суммирование по $\mathrm{mod}\,2$.

В соответствии с (11) для нашего примера (10) находим

$$R = \begin{bmatrix} 0.25 & 0.5 & -0.25 & 0 \\ -0.25 & 0.25 & -0.25 & 0.5 \\ -0.25 & -0.25 & 0 & 0.25 \\ -0.25 & 0 & 0.25 & 0.25 \end{bmatrix}. \tag{12}$$

2. Количество $K^0$ нулевых значений матрицы коэффициентов корреляции: $r_{i,j} = 0$.

Нетрудно видеть, что для матрицы (12), данный параметр равен $K^0 = 3$.

3. Расстояние нелинейности $S$-блока подстановки — минимум расстояния Хэмминга между его компонентными булевыми функциями и всеми кодовыми словами аффинного кода

$$N_S = \min\left\{\mathrm{dist}(F_i, \varphi_j)\right\},\ i = 1,2,...,k,\ \ j = 1,2,...,2^{k+1}, \tag{13}$$

где $F_i$ — компонентные булевы функции $S$-блока подстановки, $\varphi_j$ — кодовые слова аффинного $A(N,k)$–кода.

В соответствии с определением аффинного кода, его кодовые слова определяются как $\varphi = \langle a, x \rangle + b$, где $\langle . \rangle$ — скалярное произведение по $\mathrm{mod}\,2$, $a, x \in V_k$, $V_k$ — линейное векторное пространство двоичных векторов длины $k$, $b \in \{0,1\}$. Построим все кодовые слова аффинного кода длины $N = 16$:

$$\begin{cases}\varphi_0=\{0000000000000000\};\\ \varphi_1=\{0101010101010101\};\\ \varphi_2=\{0011001100110011\};\\ \varphi_3=\{0110011001100110\};\\ \varphi_4=\{0000111100001111\};\\ \varphi_5=\{0101101001011010\};\\ \varphi_6=\{0011110000111100\};\\ \varphi_7=\{0110100101101001\};\\ \varphi_8=\{0000000011111111\};\\ \varphi_9=\{0101010110101010\};\\ \varphi_{10}=\{0011001111001100\};\\ \varphi_{11}=\{0110011010011001\};\\ \varphi_{12}=\{0000111111110000\};\\ \varphi_{13}=\{0101101010100101\};\\ \varphi_{14}=\{0011110011000011\};\\ \varphi_{15}=\{0110100110010110\};\end{cases}\quad\begin{cases}\varphi_{16}=\{1111111111111111\};\\ \varphi_{17}=\{1010101010101010\};\\ \varphi_{18}=\{1100110011001100\};\\ \varphi_{19}=\{1001100110011001\};\\ \varphi_{20}=\{1111000011110000\};\\ \varphi_{21}=\{1010010110100101\};\\ \varphi_{22}=\{1100001111000011\};\\ \varphi_{23}=\{1001011010010110\};\\ \varphi_{24}=\{1111111100000000\};\\ \varphi_{25}=\{1010101001010101\};\\ \varphi_{26}=\{1100110000110011\};\\ \varphi_{27}=\{1001100101100110\};\\ \varphi_{28}=\{1111000000001111\};\\ \varphi_{29}=\{1010010101011010\};\\ \varphi_{30}=\{1100001100111100\};\\ \varphi_{31}=\{1001011001101001\},\end{cases}\tag{14}$$

и в соответствии с (13) вычисляя минимум расстояния Хэмминга между каждой компонентной булевой функцией (табл. 1) и кодовыми словами аффинного кода (14) находим, что $N_s=4$, что является максимальным значением для биективного $S$-блока подстановки. Очевидно, бóльшее расстояние нелинейности, соответствует лучшему криптографическому качеству $S$-блока подстановки, т.к. затруднит его аппроксимацию аффинными функциями, что препятствует линейному криптоанализу.

4. Алгебраическая степень нелинейности $S$-блока подстановки, определяемая соотношением $\deg(S)=\min(\deg(\Phi_i)),\ i=1,2,...,k$ где $\deg(\Phi_i)=\max(\deg(term_i))$ — максимальная степень самого длинного слагаемого $term_i$ в полиноме Жегалкина (алгебраической нормальной форме) компонентной булевой функции $F_i$. Коэффициенты полинома Жегалкина могут быть найдены с помощью преобразования Рида-Маллера, с помощью умножения исходной компонентной булевой функции $F_i$ на матрицу $RM_k$ Рида-Маллера размера $2^k\times 2^k$, которую можно определить рекурсивно [10]:

$$RM_1=[1],\quad RM_k=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\otimes RM_{k-1}=\begin{bmatrix}RM_{k-1} & RM_{k-1}\\ 0 & RM_{k-1}\end{bmatrix},\tag{15}$$

где $\otimes$ — символ произведения Кронекера.

Для нашего примера (10), в соответствии с выражением (15), соответствующие полиномы Жегалкина, и их алгебраическая степень нелинейности имеют вид:

$$\begin{cases}\Phi_1=x_1+x_2+x_1x_2+x_1x_3+x_2x_3+x_4+x_1x_2x_4+x_3x_4+x_2x_3x_4,\quad \deg(\Phi_1)=3;\\ \Phi_2=x_2+x_1x_2+x_4+x_2x_4+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4,\quad \deg(\Phi_1)=3;\\ \Phi_3=x_2+x_3+x_1x_3+x_1x_2x_3+x_4+x_3x_4+x_1x_3x_4+x_2x_3x_4,\quad \deg(\Phi_1)=3;\\ \Phi_4=x_3+x_2x_3+x_1x_2x_3+x_4+x_1x_4+x_1x_2x_4+x_3x_4+x_2x_3x_4,\quad \deg(\Phi_1)=3,\end{cases}\tag{16}$$

соответственно, алгебраическая степень нелинейности $S$-блока подстановки равна $\deg(S)=\min(\deg(\Phi_i))=3$.

5. Период возврата $S$-блока в исходное состояние [9] — наименьшее общее кратное $T=\text{НОК}(z_1,z_2...)$, где $z_\xi$ — соответствующие длины циклов, на которые раскладывается подстановка $Q$ [11].

Найдем период возврата $S$-блока подстановки (10) в исходное состояние. Разложение (10) на циклы имеет вид

$$z_{\xi} = \begin{Bmatrix} 0 \to 0, & 1 \to 1, & 2 \to 7 \to 9 \to 6 \to 2, & 3 \to 5 \to 8 \to 15 \to 3, \\ & 4 \to 12 \to 14 \to 13 \to 4, & 10 \to 10, 11 \to 11 & \end{Bmatrix}, \quad (17)$$

тогда значение периода возврата $T = \text{НОК}(1,1,4,4,4,1,1) = 4$.

Разумеется, используя коды степенных вычетов (7), криптографически высококачественные $S$-блоки подстановки могут быть построены для любого значения $k$. Например, при значении $k = 8$, используемом в шифре Rijndael/AES [3] существует 128 таких чисел $r$, для которых выполняется условие (8). Множество чисел $\{r\}$ представлено в виде алгебраической конструкции (18)

$$\{r\} = \begin{bmatrix} 1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 22, 23, 26, 28, 29, 31, 32, 37, 38, 41, 43, 44, 46, 47, \\ 49, 52, 53, 56, 58, 59, 61, 62, 64, 67, 71, 73, 74, 76, 77, 79, 82, 83, 86, 88, 89, 91, \\ 92, 94, 97, 98, 101, 103, 104, 106, 107, 109, 112, 113, 116, 118, 121, 122, 124, 127 \\ 128, 131, 133, 134, 137, 139, 142, 143, 146, 148, 149, 151, 152, 154, 157 \quad 158 \\ 161, 163, 164, 166, 167, 169, 172, 173, 176, 178, 179, 181, 182, 184, 188 \quad 191 \\ 193, 194, 196, 197, 199, 202, 203, 206, 208, 209, 211, 212, 214, 217, 218 \quad 223 \\ 224, 226, 227, 229, 232, 233, 236, 239, 241, 242, 244, 247, 248, 251, 253 \quad 254 \end{bmatrix}. \quad (18)$$

Однако, ясно, что не все числа из множества $\{r\}$ могут обеспечить заданные криптографические свойства $S$-блока подстановки.

Проведенные исследования позволили установить оптимальные значения $r$, при которых $S$-блоки подстановки имеют наилучшие криптографические свойства: высокое расстояние нелинейности, высокую алгебраическую степень нелинейности, равномерную минимизацию элементов матрицы коэффициентов корреляции.

***Утверждение 1.*** Множество $\Omega$ оптимальных значений $r$-ичных степенных вычетов составляют все такие, и только такие числа $r$, которые в двоичном представлении имеют вес $wt((r)_2) = k - 1 = 7$, независимо от вида первообразного неприводимого полинома $f(x)$ степени $k$.

Для значения $k = 8$, множество $\Omega = \{127, 191, 223, 239, 247, 251, 253, 254\}$.

Следует отметить, что все числа данного множества являются членами последовательности A023689 [10] над полем $GF(2^8)$, предложенной Оливером Герардом, каждый элемент которой содержит точно 7 единиц в своем двоичном представлении.

Например, пусть $f(x) = x^8 + x^6 + x^5 + x^4 + 1$, $r = 127$, $\omega = 1$, $\nu = 0$, тогда, мы получаем $S$-блок подстановки $Q^{(r,\omega,\nu)} = Q^{(127,1,0)}$, который для краткости представим в виде шестнадцатеричной таблицы замены, (табл. 2):

*Таблица 2*

| $Q^{(r,\omega,\nu)}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 00 | 01 | CC | 7C | 8E | F4 | B0 | E4 | 66 | 4C | 44 | 4F | 3E | E0 | 18 | DF |
| 1 | 47 | A7 | 54 | 1B | 7A | BA | 1D | A1 | 58 | C0 | 0F | 5C | 72 | D8 | 9B | BC |
| 2 | 33 | 6E | 3C | 0D | 26 | 8B | 3B | CE | 22 | 50 | 95 | 9A | A9 | CF | AE | B6 |
| 3 | 1F | 4A | B7 | BE | 70 | D0 | 08 | 9C | 0C | AB | C5 | 64 | E1 | 15 | 07 | 7B |
| 4 | AD | 9D | 69 | 53 | DD | 98 | F5 | 02 | 2A | 4B | BD | 94 | 83 | A0 | 0B | DC |
| 5 | 3D | AA | 31 | 49 | 5D | 96 | 2D | 27 | 80 | 55 | C7 | A2 | DE | 90 | AC | 09 |
| 6 | 2C | 8A | C6 | 9F | 60 | 56 | 82 | 1C | 89 | 48 | EB | F2 | 2E | 6F | BF | AF |
| 7 | 39 | 51 | 05 | 46 | 6C | ED | C2 | 34 | C3 | A4 | 87 | E5 | 5E | 40 | EE | 6B |
| 8 | 97 | 0E | 73 | 10 | 37 | 41 | 78 | 76 | 1E | 2B | A8 | 3A | 88 | 30 | 85 | 7D |
| 9 | 13 | C1 | 0A | 99 | CB | 63 | 91 | 19 | 93 | 45 | 62 | 5A | 67 | 16 | D2 | F7 |
| A | 11 | D9 | C9 | D3 | 28 | D1 | 8F | 03 | C4 | B9 | 14 | 3F | 4D | 17 | E6 | F0 |
| B | DA | 79 | EA | B5 | E9 | FB | E7 | E3 | 57 | 24 | 86 | B1 | 5B | CA | E2 | F1 |
| C | 81 | 1A | 71 | 29 | 25 | 61 | F6 | C8 | D5 | F8 | A3 | 9E | 5F | 36 | 65 | B8 |
| D | 38 | 23 | 43 | F9 | 68 | 8C | D6 | D7 | 04 | A6 | A5 | 35 | 4E | 92 | 12 | 59 |
| E | 06 | BB | FD | 7E | DB | 77 | FF | 7F | EC | 20 | FA | 74 | 32 | 2F | F3 | B4 |
| F | FE | FC | 75 | E8 | 84 | CD | D4 | 42 | 8D | 52 | 6D | 21 | B3 | EF | B2 | 6A |

Кодирующую десятичную $Q^{(r,\omega,\nu)}$-последовательность (кодовое слово композиционного кода $r$-ичных степенных вычетов) можно представить в виде

$$Q^{(r,\omega,\nu)} = \sum_{\mu=1}^{k} \alpha_{k-\mu}^{(i,r,\omega,\nu)} p^{k-\mu} = [F_1; F_2; F_3; F_4; F_5; F_6; F_7; F_8;], \quad i = 0,1,...,255, \tag{19}$$

где $F_i, i = 1,2,...,8$ — компонентные булевы функции, тогда матрица коэффициентов корреляции $S$-блока подстановки (табл. 2) имеет вид

$$R = \begin{bmatrix} -0.03125 & 0.046875 & -0.046875 & -0.09375 & 0.046875 & 0.015625 & 0 & 0.09375 \\ -0.046875 & 0.015625 & 0.09375 & 0.0625 & 0 & 0.09375 & -0.03125 & 0.046875 \\ -0.078125 & 0.078125 & 0.015625 & 0.046875 & -0.046875 & 0.0625 & 0.078125 & -0.10938 \\ 0.03125 & -0.03125 & 0 & -0.046875 & -0.09375 & 0.03125 & 0.015625 & -0.10938 \\ 0.09375 & 0.09375 & 0.046875 & -0.0625 & -0.03125 & -0.0625 & -0.0625 & 0.125 \\ 0.015625 & 0.09375 & 0.0625 & 0.03125 & -0.0625 & 0.125 & 0.09375 & 0.09375 \\ 0.046875 & 0.015625 & 0.078125 & -0.03125 & 0.09375 & 0.09375 & 0.015625 & 0.09375 \\ 0 & 0.09375 & 0.09375 & 0.046875 & 0.015625 & 0.09375 & 0.046875 & 0.015625 \end{bmatrix}, \tag{20}$$

Количество нулей в матрице коэффициентов корреляции $K^0$, расстояние нелинейности $N_S$, алгебраическая степень нелинейности $\deg(S)$ и период возврата $S$-блока подстановки в исходное состояние $T$ соответственно, равны

$$K^0 = 4, \quad N_S = 112, \quad \deg(S) = 7, \quad T = 8. \tag{21}$$

В табл.3 приведены значения основных показателей криптографического качества $S$-блоков подстановки основанных на $r$-ичных вычетах, где $r \in \Omega$ для первообразного полинома $f(x) = x^8 + x^6 + x^5 + x^4 + 1$

*Таблица 3*

| $r$ | $\max\{r_{i,j}\}$ | $K^0$ | $N_s$ | $\deg(S)$ | $T$ |
|---|---|---|---|---|---|
| 127 | 0.125 | 4 | 112 | 7 | 8 |
| 191 | 0.125 | 4 | 112 | 7 | 4 |
| 223 | 0.125 | 4 | 112 | 7 | 8 |
| 239 | 0.125 | 4 | 112 | 7 | 2 |
| 247 | 0.125 | 4 | 112 | 7 | 8 |
| 251 | 0.125 | 4 | 112 | 7 | 4 |
| 253 | 0.125 | 4 | 112 | 7 | 8 |
| 254 | 0.125 | 4 | 112 | 7 | 2 |

Мощность композиционного кода степенных вычетов (7) для построения оптимальных $S$-блоков подстановки (табл.3) определяется соотношением

$$|Q| = |\omega| \cdot |\nu| \cdot |V_k| \cdot |\Omega| = 255 \cdot 256 \cdot 16 \cdot 8 = 8\,355\,840. \qquad (22)$$

Дальнейшие исследования структурных свойств $Q$-последовательностей, представленных в виде компонентных булевых функций, позволили разработать регулярные правила их размножения:

***Утверждение 2.*** Каждая $Q$-последовательность позволяет построить свое подмножество новых структур $\tilde{Q}$-последовательностей, объема

$$\left|\tilde{Q}\right| = k! \cdot 2^k = 40320 \cdot 256 = 10\,321\,920, \qquad (23)$$

с хорошими криптографическими свойствами (табл.3) соответствующих $S$-блоков подстановки, по путем:

— осуществления $k! = 8! = 40320$ перестановок компонентных булевых функций $F_i,\ i = 1,2,...,8$;

— применения всевозможных $2^k = 2^8 = 256$ правил инвертирования компонентных булевых функций $F_i,\ i = 1,2,...,8$.

Таким образом, общий объем всех синтезируемых $S$-блоков подстановки определяется величиной

$$|S| = |Q| \cdot \left|\tilde{Q}\right| = 8\,355\,840 \cdot 10\,321\,920 = 8.6248 \cdot 10^{13}. \qquad (24)$$

Заметим, что для каждого $S$-блока из (24) всегда существует подходящее аффинное преобразование, которое обеспечивает период его возврата в исходное состояние не менее, чем период возврата $S$-блока Rijndael, который равен $T = 1\,531\,530$.

## ВЫВОДЫ

1. Обсуждаются конструктивные аспекты построения и размножения нового класса конструкций $S$-блоков подстановки на основе композиционных кодов степенных вычетов над расширенными полями $GF(2^k)$ с хорошими криптографическими свойствами (табл. 3) и большого объема $|S| = 8.6248 \cdot 10^{13}$.

2. Предложен способ синтеза $S$-блоков подстановки на основе кодов степенных вычетов над расширенными полями $GF(2^k)$, из которого класс конструкций Ниберга следует как частный случай.

3. Большой объем построенных высококачественных $S$-блоков композиционной конструкции делает возможным применение их в качестве долговременного ключа.

4. Разработан способ синтеза однобайтовых $S$-блоков подстановки композиционной конструкции, который может быть использован при разработке больших процессорно-ориентированых нелинейных подстановок современных программных шифров [10] с разрядностью процессора $m = (16, 32, 64, 128)$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Мазурков М.И.* Системы широкополосной радиосвязи: учебное пособие для студентов высших учебных заведений /М.И. Мазурков. — Одесса.: Наука и техника, 2010. — 340 с.

2. *Nyberg K*. Differentially uniform mappings for cryptography. I Advances in cryptology // Proceedings of EUROCRYPT'93 (1994) vol.765, Lecture Notes in Compuer Springer-Verlag, Berlin, Heidelberg, New York. P.55-65.

3. FIPS 197. Advanced encryption standard // см. http://csrc.nist.gov/publications/

4. Мазурков М.И. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов / М.И. Мазурков, А.В. Соколов // Труды Одесского национального политехнического университета. — №2(39). — 2012. — С.183—189.

5.*Берлекэмп Э.Р.* Алгебраическая теория кодирования / Э.Р. Берлекэмп. — М.: Мир. — 1971. — 477с.

6. *Мазурков М.И.* Конструктивный способ построения первообразных неприводимых полиномов над простыми полями Галуа / М.И. Мазурков // Радиоэлектроника. — 1999. — №2. — С. 41-45. (Изв. вузов).

7. *Мазурков М.И.* Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М.И., Конопака Е.А // Радиоэлектроника. — 2005. — № 11. — С. 58 — 65. (Изв. вузов).

8. *Свердлик М.Б.* Оптимальные дискретные сигналы / М.Б. Свердлик. — М.: Сов. радио, 1975. — 200 с.

9. *Мазурков М.И.* Регулярный метод синтеза подстановочных криптографических конструкций с максимальным расстоянием нелинейности / М.И. Мазурков // Радиоэлектроника. — 2012. — Том 55. — № 3. — С. 29—36. (Изв. вузов).

10. *Ростовцев А. Г.* Большие подстановки для программных шифров / А.Г. Ростовцев // Проблемы инф. безопасности. Компьютерные системы. — СПб.. — 2000. — № 3. — С. 31-34.

11. *Зайко Ю.Н*. Криптография глазами физика / Ю.Н. Зайко // Изв. Саратовского ун-та, т. 9 вып. 2 С. 34 — 48, 2009.

12. OEIS. A023689. — Olivier Gerard //см. http://oeis.org/A023689.