МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.719.2+512.542.74 DOI 10.17223/20710410/54/2

ОБ ИНВАРИАНТНЫХ ПОДПРОСТРАНСТВАХ В XSL-ШИФРАХ

Д. И. Трифонов*, Д. Б. Фомин**

** Технический комитет по стандартизации «Криптографическая защита информации», г. Москва, Россия,*

*** Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия*

E-mail: d.arlekino@gmail.com, dfomin@hse.ru

Исследуется рассеивание подпространств, инвариантных относительно нелинейного преобразования XSL-шифра, линейным преобразованием. Приведён конструктивный способ поиска подпространств, инвариантных относительно одной итерации XSL-шифра. Показано, что подпространства, инвариантные относительно нелинейных преобразований из некоторых классов, не сохраняются любой матрицей, построенной из ненулевых элементов расширения поля $\mathbb{F}_2$. На основании теоретико-графового и группового подходов доказан ряд свойств множеств специального вида, инвариантных относительно раундовой функции XSL-шифра.

Ключевые слова: *XSL-шифр, SP-сеть, инвариантное подпространство.*

INVARIANT SUBSPACES IN SPN BLOCK CIPHER

D. I. Trifonov*, D. B. Fomin**

** Technical committee «Cryptography and Security Mechanism», Moscow, Russia,*

*** Higher School of Economics, Moscow, Russia*

Let there exist subsets of $\mathbb{F}_2^n$ that the non-linear layer of an SP-network maps to some other subset of $\mathbb{F}_2^n$. We study the possibility of existence of subsets of $\mathbb{F}_2^n$ that are invariant under the SP-layer. It is shown that subspaces invariant under nonlinear transformations from some classes are not preserved by any matrix without nonzero elements of the field extension $\mathbb{F}_2$. The paper also studies the question of the existence of invariant subsets of the form $A_{i_1} \times \ldots \times A_{i_m}$, where $n = m \cdot n'$, $A_{i_j} \subseteq \mathbb{F}_2^{n'}$, $j = 1, \ldots, m$. Some properties of such invariant sets of the round function of the SP-layer are proved on the basis of the graph-theoretic and group-theoretic approaches. We study the capacity of these sets and, using additional assumptions, show that A_{i_j}, $j = 1, \ldots, m$, should be cosets of some subspaces of $\left(\mathbb{F}_2^{n'}, +\right)$ of equal size. A constructive way of constructing such sets is proposed.

Keywords: *SP-network, SPN, invariant subspaces.*

Введение

С конца XX в. широкое распространение получили блочные криптографические алгоритмы. Большинство из них построено по итеративному принципу, где каждая итерация представляет собой чередование линейных и локальных нелинейных преобразований информационного блока.

В связи с появлением линейного и разностного методов криптографического анализа [1, 2] были сформулированы требования на выбор нелинейных и линейных рассеивающих преобразований для обеспечения стойкости относительно этих методов (см., например, [1, 3, 4] и др.). Изучению линейных и нелинейных преобразований посвящено много работ отечественных и зарубежных специалистов [2–26].

Таким образом, сформировался уже устоявшийся подход к построению блочных шифров, стойких относительно линейного и разностного методов: в качестве нелинейных необходимо использовать преобразования, обеспечивающие необходимые характеристики относительно линейного и разностного методов, а в качестве линейных — преобразования с достаточно высокими коэффициентами рассеивания. По такому принципу построено много криптографических алгоритмов, среди которых можно отметить российский стандарт блочного шифрования «Кузнечик» [27].

Вопрос о влиянии приводимости линейных преобразований на стойкость блочных криптографических алгоритмов поставлен в обзоре [28]. Изучению структурных свойств линейных преобразований посвящены работы [29–32].

В работе [32] наличие инвариантных подпространств у линейного преобразования позволило усилить разностную атаку на криптографический алгоритм ICEBERG (Involution Cipher Efficient for Block Encryption in Reconfigurable Hardware) [33]. В [34] построена атака на алгоритм Khazad [21], существенно использующая приводимость линейного преобразования. При этом в алгоритме используется максимально рассеивающее линейное преобразование и локальные нелинейные преобразования (подстановки) с высокими криптографическими характеристиками.

Наличие инвариантных подпространств у линейного преобразования делает необходимым при синтезе XSL-шифра исследовать вопрос, насколько хорошо данные подпространства рассеиваются нелинейным слоем. В данной работе предлагается несколько другой подход: сначала выделить подпространства, инвариантные для нелинейных преобразований, а затем изучить вопрос, насколько хорошо данные подпространства рассеиваются линейным слоем. Частично этот вопрос исследован в [35, 36].

1. Основные определения и обозначения

В работе используются следующие определения и обозначения. Через $\mathbb{F}_q$ обозначим конечное поле из q элементов, где $q = p^n$, p — простое число, $n \in \mathbb{N}$. Пусть $V_n(2^d)$ — векторное пространство размерности $n \in \mathbb{N}$ над полем $\mathbb{F}_{2^d}$. Обозначим полную линейную группу в её естественном действии на пространстве $V_n(2^d)$ через $\mathrm{GL}_n(2^d)$, при этом если $d = 1$, то будем писать $\mathrm{GL}_n = \mathrm{GL}_n(2)$.

Множество всех матриц из m строк и n столбцов с элементами из поля $\mathbb{F}_q$ обозначим $(\mathbb{F}_q)_{m,n}$, в случае поля $\mathbb{F}_2$ будем использовать обозначение $(\mathbb{F}_2)_{n,n} = M_n$. Кольцо многочленов от одного переменного x над полем $\mathbb{F}_q$ обозначим $\mathbb{F}_q[x]$; множество всех подстановок множества U — $S(U)$; $\mathbf{0}^{(l)} \in V_l$ — вектор $\mathbf{0}^{(l)} = (0, \ldots, 0)$.

Прежде чем сформулировать основные результаты, напомним несколько фактов из теории конечных полей [37].

Рассмотрим способ представления элементов конечного поля $\mathbb{F}_q$ с помощью матриц. Пусть $f(x) = x^n + f_{n-1}x^{n-1} + \ldots + f_1x + f_0 \in \mathbb{F}_q[x]$ есть унитарный многочлен степени

$n \in \mathbb{N}$. Его сопровождающей матрицей называется следующая квадратная матрица порядка n:

$$S(f(x)) = \begin{pmatrix} 0 & 0 & \dots & -f_0 \\ 1 & 0 & \dots & -f_1 \\ \dots & \dots & \dots & \dots \\ \dots & 1 & 0 & -f_{n-2} \\ 0 & \dots & 1 & -f_{n-1} \end{pmatrix}.$$

Из теоремы Гамильтона — Кэли (см., например, [38, с. 62, теорема 8]) следует, что матрица $A = S(f(x))$ удовлетворяет уравнению $f(A) = \mathbf{O}_{n,n}$, то есть

$$A^n + f_{n-1}A^{n-1} + \ldots + f_1 A + f_0 \mathbf{I}_{n,n} = \mathbf{O}_{n,n},$$

где $\mathbf{O}_{n,n}$ — нулевая матрица порядка n; $\mathbf{I}_{n,n}$ — единичная матрица порядка n.

Элементы поля $\mathbb{F}_{p^n}$ могут быть представлены всевозможными многочленами над $\mathbb{F}_p$ от матрицы $A = S(f(x))$ степеней меньше n. Далее многочлен $f(x)$ и соответствующую ему матрицу $S(f(x)) = A$ будем считать фиксированными.

Рассмотрим только случай $p = 2$. Элементы поля $\mathbb{F}_{2^{n'}}$, $n' \in \mathbb{N}$, могут быть представлены в виде матриц размера $n' \times n'$ над полем $\mathbb{F}_2$ следующим образом:

$$a_{n'-1} \cdot A^{n'-1} \oplus \ldots \oplus a_1 \cdot A \oplus a_0 \cdot \mathbf{I}_{n',n'}, \tag{1}$$

где $a_k \in \{0, 1\}$, $k = 0, \ldots, n' - 1$.

Пусть $\mathbb{F}_{2^{n'}} = \mathbb{F}_2[x]/f(x)$, $n' \in \mathbb{N}$, $\deg f(x) = n'$, $f[x] \in \mathbb{F}_2[x]$ неприводим и θ — класс вычетов по модулю $f(x)$, содержащий x. Пусть также $A = S(f(x))$. Элементам поля $\mathbb{F}_{2^{n'}}$ поставим во взаимно однозначное соответствие элементы вида (1) следующим образом: элементу $z_0 \oplus z_1 \cdot \theta \oplus \ldots \oplus z_{n'-1} \cdot \theta^{n'-1}$, $z_i \in \{0, 1\}$, $i = 0, 1, \ldots, n'-1$, соответствует элемент $z_0 \cdot \mathbf{I}_{n',n'} \oplus z_1 \cdot A \oplus \ldots \oplus z_{n'-1} \cdot A^{n'-1}$.

Через $\overline{\mathbb{F}}_{2^{n'}}$ будем обозначать описанное выше матричное представление поля из $2^{n'}$ элементов.

2. Постановка задачи

Рассмотрим XSL-шифр со следующими параметрами: n — размер блока в битах, m — число нелинейных биективных преобразований (подстановок) на подвекторах длины n', $n = n' \cdot m$.

При реализации изучаемых алгоритмов используются следующие преобразования:

- *наложение ключа* $\mathrm{X}[K]\colon V_n \to V_n$, где $\mathrm{X}[K](a) = K \oplus a$; $a, K \in V_n$;
- *нелинейное преобразование* $\mathrm{S}\colon V_n \to V_n$, $\mathrm{S}(a) = \mathrm{S}(a_1, \ldots, a_m) = (\pi(a_1), \ldots, \pi(a_m))$, $a_i \in V_{n'}$, $\pi \in S(V_{n'})$, $i = 1, \ldots, m$;
- *линейное преобразование* $\mathrm{L}\colon V_n \to V_n$, $\mathrm{L}(a) = a \cdot L'$, где $L' \in \mathrm{GL}_n$.

В [3, 4] отмечено, что для противодействия линейному и разностному методам криптографического анализа линейное преобразование должно обладать достаточно высоким коэффициентом рассеивания. Большинство способов построения максимально рассеивающих матриц из GL_n сводится к построению матриц из $\mathrm{GL}_m\left(2^{n'}\right)$ в известных классах: циркулянты, матрицы Коши, матрицы Коши — Адамара [3, 39] и некоторых других. Отметим также возможность построения при помощи направленного поиска максимально рассеивающих матриц с примитивным характеристическим многочленом [40]. Таким образом, широкое распространение получают матрицы из GL_n, полученные из матриц $\mathrm{GL}_m\left(2^{n'}\right)$. В рассматриваемом XSL-шифре будем использовать два типа матриц. Для их описания приведём необходимые определения.

Рассмотрим отображение $\varphi\colon \mathbb{F}_{2^{n'}} \to M_{n'}$, которое элементу $\alpha \in \mathbb{F}_{2^{n'}}$ ставит в соответствие матрицу из $M_{n'}$, определяемую равенством (1). Зададим также отображение $\psi\colon \mathrm{GL}_m(2^{n'}) \to \mathrm{GL}_{n'm}$, которое матрице $B = (\mathbf{B}_{i,j})_{m,m} \in \mathrm{GL}_m(2^{n'})$ ставит в соответствие следующую матрицу $\psi(B) \in \mathrm{GL}_{n'm}$:

$$\psi(B) = \begin{pmatrix} \varphi(\mathbf{B}_{1,1}) & \dots & \varphi(\mathbf{B}_{1,m}) \\ \vdots & \ddots & \vdots \\ \varphi(\mathbf{B}_{m,1}) & \dots & \varphi(\mathbf{B}_{m,m}) \end{pmatrix}.$$

Матрицами типа I будем называть матрицы $\psi(B)$, такие, что $\mathbf{B}_{i,j} \neq 0$ для всех $i, j = 1, \dots, m$.

Матрицами типа II будем называть матрицы $C \in M_{n'm}$ вида

$$C = \begin{pmatrix} C_{1,1} & \dots & C_{1,m} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,m} \end{pmatrix},$$

где $C_{i,j} \in M_{n'}$ невырождены, $i, j = 1, \dots, m$.

Замечание 1. Матрицы типа I являются матрицами типа II. Обратное, вообще говоря, неверно.

Большинство нелинейных биективных преобразований, используемых в современных криптографических алгоритмах, имеют достаточно простую алгебраическую структуру. Например, в AES [4], Grand-Cru [41], Mugi [42], Scream [43], Camelia [44], Square [45] используются подстановки, аффинно эквивалентные подстановке обращения ненулевых элементов поля $\mathbb{F}_{2^8}$. Подстановки белорусского стандарта [46] аффинно эквивалентны экспоненциальной подстановке, а подстановки российских стандартизированных алгоритмов «Кузнечик» [27] и «Стрибог» [47] имеют так называемую TU-декомпозицию, как и подстановки, рассматриваемые в [13, 14, 48, 49].

Наличие простой алгебраической структуры подстановки часто влечёт наличие смежных классов, инвариантных относительно данной подстановки. Например, нетрудно убедиться, что для подстановки обращения ненулевых элементов поля инвариантным подпространством будет любое подполе данного поля. Данное свойство подстановки может являться потенциальной слабостью относительно методов, использующих различные гомоморфизмы [50].

3. Основные результаты

Одним из основных вопросов, рассматриваемых в данной работе, является изучение случая, когда подмножество множества $V_{n'}^m$, которое является инвариантным относительно действия слоя подстановок, сохраняется линейным преобразованием.

Множество $W \subseteq V_n$ будем называть инвариантным относительно преобразования $g\colon V_n \to V_n$, если для любого $x \in W$ выполнено включение $g(x) \in W$. Для преобразования g определим множество $g(W)$, равное множеству образов всех элементов из W под действием преобразования g, то есть

$$g(W) = \{g(x)\colon x \in W\}.$$

В данных обозначениях множество W инвариантно относительно преобразования g, если $g(W) \subseteq W$. Будем использовать экспоненциальную форму записи действия произвольного отображения: $g(a) = a^g$, $a \in V_n$.

Пусть $K \in V_{n'}^m \cong V_n$ — раундовый ключ рассматриваемого блочного криптографического алгоритма. Интересен вопрос поиска множеств $G_K \subset V_n$, инвариантных относительно произведения преобразований $\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]$:

$$G_K = G_K^{\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]}.$$

Наличие таких множеств для большого числа ключей может говорить о возможных слабостях в раундовом преобразовании шифра [36].

Пусть множество $U \subset V_{n'}$ инвариантно относительно подстановки π. Рассмотрим множество

$$W = W_1 \times \ldots \times W_m,$$

где $W_i \in \{U, V_{n'}\}$, которое, очевидно, инвариантно относительно преобразования S. При фиксированном ключе $K \in V_{n'}^m$ для построения множества G_K необходимо изучить вопрос, в каких случаях множество W является инвариантным относительно линейного преобразования L.

Случай, когда для всех $i = 1, \ldots, m$ выполнено равенство $W_i = V_{n'}$, является тривиальным и не представляет интереса для построения множества G_K. Поэтому будем рассматривать следующие варианты построения множества W:

С л у ч а й 1. Существует единственный $i \in \{1, \ldots, m\}$, такой, что $W_i = U$.

С л у ч а й 2. Существуют $i_1 < \ldots < i_j$, $i_1, \ldots, i_j \in \{1, \ldots, m\}$, $j \in 1, \ldots, m-1$, такие, что $W_{i_1} = \ldots = W_{i_j} = U$.

С л у ч а й 3. Для всех $i = 1, \ldots, m$ выполнено равенство $W_i = U$.

Утверждение 1. Пусть подпространство $U < V_{n'}$, $U \neq V_{n'}$, инвариантно относительно подстановки π. Пусть для множества $W = W_1 \times \ldots \times W_m$, где $W_i \in \{U, V_{n'}\}$, не для всех $i = 1, \ldots, m$ выполнено $W_i = V_{n'}$. Кроме того, пусть в преобразовании L используется матрица $C = (C_{i,j})_{m,m} \in \mathrm{GL}_{n'm}$ типа II. Тогда справедливы следующие утверждения:

1) если существует $i \in \{1, \ldots, m\}$, такое, что $W_i = V_{n'}$, то множество W не является инвариантным относительно матрицы C;
2) если для любого $i = 1, \ldots, m$ выполнено $W_i = U$ и существуют $j_1, j_2 \in \in \{1, \ldots, m\}$, такие, что $C_{j_1,j_2}(U) \neq U$, то множество W не является инвариантным относительно матрицы C;
3) если для любого $i = 1, \ldots, m$ выполнено $W_i = U$ и $C_{j_1,j_2}(U) = U$ при всех $j_1, j_2 = 1, \ldots, m$, то $C(W) = W$.

Доказательство.

1) Покажем, что в данном случае при $C(W) = W'$, $W = W_1 \times \ldots \times W_i \times \ldots \times W_m$, $W' = W_1' \times \ldots \times W_i' \times \ldots \times W_m'$ и $W_i = V_{n'}$ получается, что для любых $j = 1, \ldots, m$ выполнено $W_j' \neq U$.

Во введённых обозначениях

$$W_j' = C_{1,j}(W_1) \oplus C_{2,j}(W_2) \oplus \ldots \oplus C_{m,j}(W_m),$$

где для множеств $A, B \subseteq V_n$ под множеством $A \oplus B$ будем понимать множество различных векторов $a \oplus b$ при всех $a \in A$ и $b \in B$.

Следовательно, в силу того, что $U \neq V_{n'}$, равенство $W_j' = U$, $j = 1, \ldots, m$ возможно лишь когда матрица $C_{i,j}$ вырождена, что противоречит условию утверждения. Таким образом, подпространство W не является инвариантным относительно матрицы C.

2) Пусть $C(W) = W'$, $W = W_1 \times \ldots \times W_{j_1} \times \ldots \times W_m$, $W' = W'_1 \times \ldots \times W'_{j_1} \times \ldots \times W'_m$ и $W_i = U$, $i = 1, \ldots, m$. Тогда

$$W'_{j_2} = C_{1,j_2}(W_1) \oplus C_{2,j_2}(W_2) \oplus \ldots \oplus C_{m,j_2}(W_m).$$

В силу того, что $C_{j_1,j_2}(U) \neq U$, $W'_{j_2} \neq U$ при всех $j_2 = 1, \ldots, m$. Таким образом, подпространство W не является инвариантным относительно матрицы C.

3) В справедливости данного утверждения можно убедиться, рассмотрев доказательство п. 2 с условием $C_{j_1,j_2}(U) = U$ при всех $j_1, j_2 = 1, \ldots, m$. ■

Рассмотрим следующий случай. Пусть в рассматриваемом XSL-шифре $n' = 2n''$ и множество R_1 векторов вида

$$(\underbrace{0, \ldots, 0}_{n''}, x_{n''+1}, \ldots, x_{2n''}) \in V_{n'},$$

где $(x_{n''+1}, \ldots, x_{2n''}) \in V_{n''}$, инвариантно относительно преобразования π. При фиксированном ключе K шифра рассмотрим вопрос построения множества G_K, инвариантного относительно преобразования $\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]$.

Нетрудно убедиться, что множество

$$W = W_1 \times \ldots \times W_m,$$

где $W_i = R_1$, $i = 1, \ldots, m$, инвариантно относительно преобразования S. Для построения множества G_K необходимо рассмотреть условия, которым должна удовлетворять матрица $C = (C_{i,j})_{m,m}$, используемая в линейном преобразовании L. Согласно п. 3 утверждения 1, должны быть выполнены равенства $C_{i,j}(R_1) = R_1$, $i, j = 1, \ldots, m$. Ответ на вопрос, выполнимо ли последнее равенство при использовании матриц типа I, даёт следующая

Теорема 1. Пусть $\mathbf{B} \in \overline{\mathbb{F}}_{2^{n'}}$, $\mathbf{B} \neq 0$, $\mathbf{B} \neq 1$. Тогда множество R_1 не является инвариантным относительно матрицы $\varphi(\mathbf{B})$.

Доказательство. Введём следующее обозначение: $A \begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_l \end{pmatrix}$ — подматрица матрицы $A \in \mathrm{GL}_{n'}$, полученная из A удалением всех строк, кроме строк с номерами $i_1 < \ldots < i_k$, и всех столбцов, кроме столбцов с номерами $j_1 < \ldots < j_l$.

Переформулируем утверждение теоремы. Необходимо показать, что существует $x \in V_{n''}$, такой, что

$$(\mathbf{0}^{(n'')}, x) \cdot \varphi(\mathbf{B}) = (y_1, y_2),$$

где $y_1 \neq \mathbf{0}^{(n'')}$.

Доказательство теоремы будем проводить методом от противного. Предположим, что для любого $x \in V_{n''}$ выполнено

$$(\mathbf{0}^{(n'')}, x) \cdot \varphi(\mathbf{B}) = (\mathbf{0}^{(n'')}, y_2) \tag{2}$$

при некотором $y_2 \in V_{n''}$.

Рассмотрим первые n'' столбцов матрицы $\varphi(\mathbf{B})$, т. е. подматрицу $\varphi(\mathbf{B}) \begin{pmatrix} 1, \ldots, 2n'' \\ 1, \ldots, n'' \end{pmatrix}$. Заметим, что для выполнения равенства (2) для любых $x \in V_{n''}$ необходимо и достаточно, чтобы $\varphi(\mathbf{B}) \begin{pmatrix} n''+1, & \ldots, & 2n'' \\ 1, & \ldots, & n'' \end{pmatrix} = \mathbf{O}_{n'',n''}$.

Рассмотрим для элемента $\mathbf{B}$ поля $\overline{\mathbb{F}}_{2^{2n''}}$, которое задаётся неприводимым над $\mathbb{F}_2$ многочленом $f(x)$ степени $2n''$, представление в виде (1):

$$b_{2n''-1} \cdot S(f(x))^{2n''-1} \oplus \ldots \oplus b_1 \cdot S(f(x)) \oplus b_0 \cdot \mathbf{I}_{2n'',2n''}.$$

Непосредственной проверкой можно убедиться в следующем:

— при возведении матрицы $S(f(x))$ в степень i матрица $S(f(x))^i$ получается из матрицы $S(f(x))^{i-1}$ сдвигом всех столбцов на один влево и дописыванием последнего столбца, вид которого полностью определяется коэффициентами многочлена $f(x)$, $i = 2, \ldots, 2n'' - 1$;

— в матрицах $\mathbf{I}_{2n'',2n''}, S(f(x)), S(f(x))^2, \ldots, S(f(x))^{2n''-1}$ в первом столбце присутствует ровно одна единица, которая для матрицы $S(f(x))^i$ стоит в $(i+1)$-й строке, $i = 0, \ldots, 2n'' - 1$.

Таким образом, если рассмотреть элемент $\mathbf{B}$ поля $\mathbb{F}_{2^{2n''}}$ в виде (1), то равенство $\varphi(\mathbf{B}) \begin{pmatrix} n''+1, \ldots, 2n'' \\ 1, \ldots, n'' \end{pmatrix} = \mathbf{O}_{n'',n''}$ верно тогда и только тогда, когда выполнено одно из следующих условий:

1) $b_k = 0$, $k = 0, \ldots, 2n'' - 1$. Однако в этом случае $\mathbf{B} = 0$, что противоречит условию теоремы;
2) $b_0 = 1$, $b_k = 0$, $k = 1, \ldots, 2n'' - 1$. Однако в этом случае $\mathbf{B} = 1$, что противоречит условию теоремы.

Полученные противоречия завершают доказательство теоремы. ■

Замечание 2. Пусть $\mathbf{B} \in \overline{\mathbb{F}}_{2^{n'}}$, $\mathbf{B} = 1$. Тогда множество R_1 является инвариантным относительно матрицы $\varphi(\mathbf{B})$.

Утверждение 2. Пусть $n' = 2n''$, $n'' \in \mathbb{N}$, $m \geqslant 2$, $B = (\mathbf{B}_{i,j})_{m,m} \in \mathrm{GL}_m(2^{2n''})$ и матрица $\psi(B)$ является матрицей типа I. Тогда множества $W^{(1)}$, $W^{(2)}$, $W^{(3)}$ не являются инвариантными относительно преобразования $\psi(B)$, где

1) $W^{(1)} = W_1 \times \ldots \times W_m$ и существует единственный $i \in \{1, \ldots, m\}$, такой, что $W_i = R_1$;
2) $W^{(2)} = W_1 \times \ldots \times W_m$ и существуют $i_1 < \ldots < i_j$, $i_1, \ldots, i_j \in \{1, \ldots, m\}$, $j \in \in \{1, \ldots, m-1\}$, такие, что $W_{i_1} = \ldots = W_{i_j} = R_1$;
3) $W^{(3)} = W_1 \times \ldots \times W_m$ и для всех $i = 1, \ldots, m$ выполнено равенство $W_i = R_1$.

Доказательство. Справедливость утверждения следует из теоремы 1, а также п. 3 утверждения 1. ■

Аналогичные результаты можно сформулировать и для XSL-шифров, где в качестве линейного преобразования используется матрица типа II.

Утверждение 3. Пусть $n' \in \mathbb{N}$, $C = (c_{i,j}) \in M_{n'}$, $R_2 < V_{n'}$,

$$R_2 = \{(x_1, \ldots, x_{n'})\colon x_{j_1} = \ldots = x_{j_l} = 0, j_1 < \ldots < j_l; j_1, \ldots, j_l \in \{1, \ldots, n'\}; 1 \leqslant l < n'\}.$$

Тогда множество R_2 является инвариантным относительно матрицы C тогда и только тогда, когда $C \begin{pmatrix} \{1, \ldots, n'\} \setminus \{j_1, \ldots, j_l\} \\ j_1, \ldots, j_l \end{pmatrix} = \mathbf{O}_{n'-l,l}$.

Доказательство. Аналогично доказательству теоремы 1 с учётом того, что выполнимость условия утверждения означает существование в матрице C нулевой подматрицы $C \begin{pmatrix} \{1, \ldots, n'\} \setminus \{j_1, \ldots, j_l\} \\ j_1, \ldots, j_l \end{pmatrix}$. ■

Пример 1. Для иллюстрации теоремы 1 приведём конкретный пример. Пусть $n'' = 4$ и $\mathbf{B} \in \overline{\mathbb{F}}_{2^8}$, $\mathbf{B} \neq 0$, $\mathbf{B} \neq 1$. Поле $\overline{\mathbb{F}}_{2^8}$ задаётся неприводимым над $\mathbb{F}_2$ многочленом $f(x) = x^8 + \sum\limits_{i=0}^{7} f_i x_i$. Приведём в явном виде матрицы $A^i = (S(f(x)))^i$, $i = 0, \ldots, 7$:

$$E = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{array}\right), \quad A = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&0&0&f_0\\ 1&0&0&0&0&0&0&f_1\\ 0&1&0&0&0&0&0&f_2\\ 0&0&1&0&0&0&0&f_3\\ \hline 0&0&0&1&0&0&0&f_4\\ 0&0&0&0&1&0&0&f_5\\ 0&0&0&0&0&1&0&f_6\\ 0&0&0&0&0&0&1&f_7 \end{array}\right),$$

$$A^2 = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&0&f_0&*\\ 0&0&0&0&0&0&f_1&*\\ 1&0&0&0&0&0&f_2&*\\ 0&1&0&0&0&0&f_3&*\\ \hline 0&0&1&0&0&0&f_4&*\\ 0&0&0&1&0&0&f_5&*\\ 0&0&0&0&1&0&f_6&*\\ 0&0&0&0&0&1&f_7&* \end{array}\right), \quad A^3 = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&f_0&*&*\\ 0&0&0&0&0&f_1&*&*\\ 0&0&0&0&0&f_2&*&*\\ 1&0&0&0&0&f_3&*&*\\ \hline 0&1&0&0&0&f_4&*&*\\ 0&0&1&0&0&f_5&*&*\\ 0&0&0&1&0&f_6&*&*\\ 0&0&0&0&1&f_7&*&* \end{array}\right),$$

$$A^4 = \left(\begin{array}{cccc|cccc} 0&0&0&0&f_0&*&*&*\\ 0&0&0&0&f_1&*&*&*\\ 0&0&0&0&f_2&*&*&*\\ 0&0&0&0&f_3&*&*&*\\ \hline 1&0&0&0&f_4&*&*&*\\ 0&1&0&0&f_5&*&*&*\\ 0&0&1&0&f_6&*&*&*\\ 0&0&0&1&f_7&*&*&* \end{array}\right), \quad A^5 = \left(\begin{array}{cccc|cccc} 0&0&0&f_0&*&*&*&*\\ 0&0&0&f_1&*&*&*&*\\ 0&0&0&f_2&*&*&*&*\\ 0&0&0&f_3&*&*&*&*\\ \hline 0&0&0&f_4&*&*&*&*\\ 1&0&0&f_5&*&*&*&*\\ 0&1&0&f_6&*&*&*&*\\ 0&0&1&f_7&*&*&*&* \end{array}\right),$$

$$A^6 = \left(\begin{array}{cccc|cccc} 0&0&f_0&*&*&*&*&*\\ 0&0&f_1&*&*&*&*&*\\ 0&0&f_2&*&*&*&*&*\\ 0&0&f_3&*&*&*&*&*\\ \hline 0&0&f_4&*&*&*&*&*\\ 0&0&f_5&*&*&*&*&*\\ 1&0&f_6&*&*&*&*&*\\ 0&1&f_7&*&*&*&*&* \end{array}\right), \quad A^7 = \left(\begin{array}{cccc|cccc} 0&f_0&*&*&*&*&*&*\\ 0&f_1&*&*&*&*&*&*\\ 0&f_2&*&*&*&*&*&*\\ 0&f_3&*&*&*&*&*&*\\ \hline 0&f_4&*&*&*&*&*&*\\ 0&f_5&*&*&*&*&*&*\\ 0&f_6&*&*&*&*&*&*\\ 1&f_7&*&*&*&*&*&* \end{array}\right).$$

Здесь элементы, обозначенные «$*$», полностью определяются коэффициентами многочлена $f(x)$ и не приводятся из-за громоздкости их записи.

Покажем, что множество R_1 не инвариантно относительно матрицы $\varphi(\mathbf{B})$. Действительно, согласно доказательству теоремы 1, для того, чтобы множество R_1 было инвариантным относительно преобразования $\varphi(\mathbf{B})$, необходимо и достаточно, чтобы $\varphi(\mathbf{B}) \binom{5, \ldots, 8}{1, \ldots, 4} = \mathbf{O}_{n'', n''}$.

Рассмотрим элемент $\mathbf{B}$ в виде (1):

$$\mathbf{B} = a_7 \cdot A^7 \ \oplus \ a_6 \cdot A^6 \ \oplus \ \ldots \ \oplus \ a_1 \cdot A \ \oplus \ a_0 \cdot \mathbf{I}_{8,8},$$

$a_k \in \{0, 1\}$, $k = 0, \ldots, 7$. Отметим, что в первом столбце матрицы A^i присутствует ровно одна единица в строке с номером $i + 1$, $i = 0, \ldots, 7$. Таким образом,

$\varphi(\mathbf{B})\binom{5,\ldots,8}{1,\ldots,4} = \mathbf{O}_{n'',n''}$ тогда и только тогда, когда $a_k = 0$, $k = 0,\ldots,7$. Однако в этом случае $\varphi(\mathbf{B}) = \mathbf{O}_{8,8}$. Полученное противоречие подтверждает теорему 1.

Замечание 3. Существуют подстановки, обладающие высокими криптографическими характеристиками, относительно которых множество R_1 будет инвариантным. Примерами могут служить подстановки, исследуемые в [13, 14]. Ещё одним примером являются подстановки обращения ненулевых элементов поля $\mathbb{F}_{2^{2n'}}$. По теореме о башне полей [37], в поле $\mathbb{F}_{2^{2n'}}$ существует подполе $\mathbb{F}_{2^{n'}}$. Тогда можно подобрать подстановку, аффинно эквивалентную заданной, относительно которой множество R_1 будет инвариантным.

Рассмотрим XSL-шифр с линейным преобразованием, задаваемым матрицей типа II. Опишем один подход к поиску множеств $G_K \subset V_n$, инвариантных относительно композиции преобразований $\mathrm{X}[K]\circ\mathrm{L}\circ\mathrm{S}$. Пусть имеется пара семейств множеств $(\mathcal{A},\mathcal{B})$:

$$\mathcal{A} = \{A_1, A_2, \ldots, A_{e_a}\},\ A_i \subseteq V_{n'},$$
$$\mathcal{B} = \{B_1, B_2, \ldots, B_{e_b}\},\ B_i \subseteq V_{n'},$$

и для любого $i \in \{1,\ldots,e_a\}$ существует $j \in \{1,\ldots,e_b\}$, такой, что $A_i^{\pi} \subseteq B_j$. Рассмотрим семейства $\mathcal{A}^m$ и $\mathcal{B}^m$ — декартовы степени множеств $\mathcal{A}$ и $\mathcal{B}$. Тогда для любого элемента $A_{i_1} \times \ldots \times A_{i_m} \in \mathcal{A}^m$ существует элемент $B_{j_1} \times \ldots \times B_{j_m} \in \mathcal{B}^m$, такой, что

$$(A_{i_1} \times \ldots \times A_{i_m})^{\mathrm{S}} = \left(A_{i_1}^{\pi} \times \ldots \times A_{i_m}^{\pi}\right) \subseteq B_{j_1} \times \ldots \times B_{j_m}.$$

Множество G_K будем искать среди подмножеств множества $\mathcal{A}^m$, то есть его элементами являются множества вида $A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m} \in \mathcal{A}^m$.

Пусть $\mathcal{C}$ — такое семейство множеств, что для любого элемента $B_{j_1} \times \ldots \times B_{j_m} \in \mathcal{B}^m$ существует элемент C семейства $\mathcal{C}$, для которого выполняется включение

$$(B_{j_1} \times \ldots \times B_{j_m})^{\mathrm{L}} \subseteq C.$$

Пусть также существует такой $K \in V_{n'}^m$, что $\mathcal{C}^{\mathrm{X}[K]} = \mathcal{A}^m$, то есть верна следующая диаграмма:

$$\mathcal{A}^m \xrightarrow{\mathrm{S}} \mathcal{B}^m \xrightarrow{\mathrm{L}} \mathcal{C} \xrightarrow{\mathrm{X}[K]} \mathcal{A}^m. \tag{3}$$

Все дальнейшие рассуждения будем проводить в предположении выполнимости диаграммы (3). В этом случае, очевидно, выполняется равенство $|\mathcal{C}| = |\mathcal{A}^m|$. Действительно, рассмотрим элемент $A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m} \in \mathcal{A}^m$, $i_1,\ldots,i_m \in \{1,\ldots,e_a\}$. Пусть $K = (k_1, k_2, \ldots, k_m)$. Тогда

$$(A_{i_1} \oplus k_1) \times (A_{i_2} \oplus k_2) \times \ldots \times (A_{i_m} \oplus k_m) \in \mathcal{C}.$$

Таким образом, множество C состоит из прямого произведения множеств вида $A_j \oplus k_i$, $j \in \{1,\ldots,e_a\}$, $i \in \{1,\ldots,m\}$.

Утверждение 4. Пусть имеется XSL-шифр, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1,\ldots,m$, задаётся матрицей типа II. Рассмотрим множества

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}^m, \quad i_1,\ldots,i_m \in \{1,\ldots,e_b\},$$
$$C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C}, \quad j_1,\ldots,j_m \in \{1,\ldots,e_a\},$$

такие, что $B^{\mathrm{L}} \subseteq C$, и для некоторого ключа $K \in V_{n'}^m$ выполнена диаграмма (3). Тогда для любого $j \in \{j_1,\ldots,j_m\}$ выполнено неравенство $|C_j| \geqslant \max\limits_{i\in\{i_1,\ldots,i_m\}} |B_i|$.

Доказательство. Пусть $x_v \in B_{i_v}$, $v = 1, \ldots, m$. Для произвольного $w \in \in \{1, \ldots, m\}$ рассмотрим следующую сумму:

$$S = \sum_{v=1}^{m} x_v \cdot l_{v,w}. \tag{4}$$

Так как $B^{\mathrm{L}} \subseteq C$, то $S \in C_{j_w}$ при любой фиксации $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\}$.

Заметим, что $|C_{j_w}|$ не меньше мощности множества различных значений сумм вида (4), получаемых при различных фиксациях значений $x_v \in B_{i_v}$, $v = 1, \ldots, m$. Фиксируем произвольное $v' \in \{1, \ldots, m\}$, а также $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\} \setminus \{v'\}$ и рассмотрим сумму

$$S_{v'} = \sum_{v \in \{1,\ldots,m\} \setminus \{v'\}} x_v \cdot l_{v,w}.$$

Тогда мощность множества

$$\left\{ S_{v'} + x_{v'} \cdot l_{v',w} : x_{v'} \in B_{i_{v'}} \right\},$$

во-первых, не больше мощности множества C_{j_w} и, во-вторых, равна мощности множества $B_{i_{v'}}$. Действительно, так как L — матрица типа II, то $l_{v',w}$ обратима и мощность множества

$$\left\{ x_{v'} \cdot l_{v',w} : x_{v'} \in B_{i_{v'}} \right\}$$

равна мощности множества $B_{i_{v'}}$. Отсюда для любого $v' \in \{1, \ldots, m\}$ выполняется равенство

$$|C_{j_w}| \geqslant \left| \left\{ x_{v'} \cdot l_{v',w} \in B_{i_{v'}} \right\} \right|,$$

которое завершает доказательство утверждения 4. ■

Из верности диаграммы 3 следует, что для любых $i_1, \ldots, i_m \in \{1, \ldots, e_a\}$ существуют такие $j_1, \ldots, j_m \in \{1, \ldots, e_a\}$, что верна диаграмма

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} A_{j_1} \times \ldots \times A_{j_m}.$$

Зададим на семействе $\mathcal{A}^m$ ориентированный граф Γ с помеченными дугами следующим образом. Вершинами этого графа являются элементы семейства $\mathcal{A}^m$, при этом вершины $X, Y \in \mathcal{A}^m$ соединены дугой с пометкой K тогда и только тогда, когда существует ключ K, такой, что $X^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} \to Y$. Если $V_{n'} \in \mathcal{A}$, то очевидно, что для произвольного ключа K

$$(V_{n'}^m)^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} = V_{n'}^m$$

есть цикл, который будем называть тривиальным. Для построения множества G_K необходимо уметь искать нетривиальные циклы в графе Γ. В частности, G_K — множество вершин графа Γ, лежащих на циклах длины 1 (петлях) с пометкой K. Однако далее рассмотрим и более общий случай, когда цикл состоит из более чем одной вершины. Предположим, что в графе Γ существует нетривиальный цикл длины r, задаваемый подсемейством семейства $\mathcal{A}^m$. Это эквивалентно тому, что некоторое подмножество $\mathcal{A}^m$ является инвариантным относительно r раундов рассматриваемого блочного шифра для некоторых ключей $K_1, \ldots, K_r$. Найдём необходимые условия существования нетривиального цикла и предложим конструктивный алгоритм его поиска.

Пусть здесь и далее $\mathcal{A}' \subset \mathcal{A}^m$ — множество вершин графа Γ, задающее некоторый нетривиальный цикл длины r. Обозначим $\mathcal{B}' = (\mathcal{A}')^{\mathrm{S}}$, $\mathcal{C}' = (\mathcal{B}')^{\mathrm{L}}$. При этом для каждого $A \in \mathcal{A}'$ существуют ключ K и множество $C \in \mathcal{C}'$, такие, что $C^{\mathrm{X}[K]} = A$.

Утверждение 5. Пусть имеется XSL-шифр, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ задают некоторый нетривиальный цикл графа Γ, $A_{a_1} \times \ldots \times A_{a_m} \in \mathcal{A}'$, и

$$B_{b_1} \times \ldots \times B_{b_m} \in \mathcal{B}',\ B_{b_1} \times \ldots \times B_{b_m} = \mathrm{S}\left(A_{a_1} \times \ldots \times A_{a_m}\right),$$
$$C_{c_1} \times \ldots \times C_{c_m} \in \mathcal{C}',\ C_{c_1} \times \ldots \times C_{c_m} = \mathrm{L}\left(B_{b_1} \times \ldots \times B_{b_m}\right).$$

Тогда:

1) $|A_{a_1}| = |B_{b_1}| = |C_{c_1}|$;
2) $|A_{a_1}| = |A_{a_2}| = \ldots = |A_{a_m}|$;
3) $|B_{b_1}| = |B_{b_2}| = \ldots = |B_{b_m}|$;
4) $|C_{c_1}| = |C_{c_2}| = \ldots = |C_{c_m}|$.

Доказательство. Множество $A_{a_1} \times \ldots \times A_{a_m} \in \mathcal{A}'$ лежит на цикле длины r. Тогда для некоторых ключей $K_1, \ldots, K_r$ верна следующая диаграмма, описывающая действие функций на соответствующие множества:

$$A_{a_1} \times \ldots \times A_{a_m} \xrightarrow{\mathrm{S}} \underbrace{B_{b_1} \times \ldots \times B_{b_m}}_{\in\mathcal{B}} \xrightarrow{\mathrm{L}} \underbrace{C_{c_1} \times \ldots \times C_{c_m}}_{\in\mathcal{C}'} \xrightarrow{\mathrm{X}[K_1]}$$
$$\xrightarrow{\mathrm{X}[K_1]} \underbrace{A_{d_1} \times \ldots \times A_{d_m}}_{\in\mathcal{A}'} \xrightarrow{\mathrm{X}[K_2]} \ldots \xrightarrow{\mathrm{X}[K_r]} \underbrace{A_{a_1} \times \ldots \times A_{a_m}}.$$

Отсюда следует, что $|C_{c_v}| = |A_{d_v}|$, $v = 1, \ldots, m$. Заметим, что по построению множеств $\mathcal{A}'$ и $\mathcal{B}'$ выполнено неравенство $|B_{b_v}| \geqslant |A_{a_v}|$, $v = 1, \ldots, m$, а по утверждению 4 — $|C_{c_v}| \geqslant |B_{b_w}|$, $v, w = 1, \ldots, m$.

Тогда, так как вершина $A_{a_1} \times \ldots \times A_{a_m}$ лежит на цикле в графе Γ, для любого $v = 1, \ldots, m$ имеет место

$$|A_{a_v}| \leqslant |B_{b_v}| \leqslant |C_{c_v}| = |A_{d_v}| \leqslant \ldots \leqslant |A_{a_v}|,$$

откуда следует доказательство п. 1 утверждения 5.

Для доказательства п. 2–4 достаточно доказать только один из них и воспользоваться цепочкой неравенств выше. Не теряя общности, покажем, что $|C_{c_1}| = |C_{c_2}|$. Для остальных пар индексов равенство доказывается аналогично.

Воспользуемся утверждением 4, а также фактом, что произвольное множество $A_{a_1} \times \ldots \times A_{a_m}$ лежит на цикле в графе Γ:

$$|C_{c_1}| = |A_{a_1}| \leqslant |B_{b_1}| \leqslant |C_{c_2}| = |A_{a_2}| \leqslant |B_{b_2}| \leqslant |C_{c_1}| \leqslant \ldots \leqslant |C_{c_1}|.$$

Утверждение доказано. ■

Следующее утверждение позволяет сформулировать алгоритм поиска циклов в графе Γ или доказать, что нетривиальных циклов нет.

Утверждение 6. Пусть для XSL-шифра, линейное преобразование которого $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ образуют некоторый нетривиальный цикл графа Γ. Пусть также

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}', \quad C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C}',$$

где $C = B^{\mathrm{L}}$. Тогда:

1) для произвольного $v \in \{1, \ldots, m\}$ множество B_{i_v} является смежным классом по некоторому подпространству пространства $V_{n'}$;
2) для произвольного $v \in \{1, \ldots, m\}$ множество C_{j_v} является смежным классом по некоторому подпространству пространства $V_{n'}$.

Доказательство. По п. 1 утверждения 5 верно равенство

$$C_{j_w} = \left\{ \sum_{v=1}^{m} b_v \cdot l_{v,w} : b_v \in B_{i_v},\ v \in \{1, \ldots, m\} \right\}.$$

Зафиксируем произвольные $v', v'' \in \{1, \ldots, m\}$, $x_v \in B_{i_v}$, $v \in \{1, \ldots, m\}$. Пользуясь п. 1 и 3 утверждения 5, запишем:

$$C_{j_w} = \left\{ \sum_{v \in \{1,\ldots,m\} \setminus \{v'\}} x_v \cdot l_{v,w} \oplus y_{v'} \cdot l_{v',w} : y_{v'} \in B_{i_{v'}} \right\},$$

$$C_{j_w} = \left\{ \sum_{v \in \{1,\ldots,m\} \setminus \{v''\}} x_v \cdot l_{v,w} \oplus y_{v''} \cdot l_{v'',w} : y_{v''} \in B_{i_{v''}} \right\}.$$

Отсюда следует, что множества

$$C'(x_{v''}) = \left\{ x_{v''} \cdot l_{v'',w} \oplus y_{v'} \cdot l_{v',w} : y_{v'} \in B_{i_{v'}} \right\} \text{ и } C''(x_{v'}) = \left\{ x_{v'} \cdot l_{v',w} \oplus y_{v''} \cdot l_{v'',w} : y_{v''} \in B_{i_{v''}} \right\}$$

равны. Запишем их в следующем виде:

$$C'\left(x_{v''}\right) = B_{i_{v'}} \cdot l_{v',w} \oplus x_{v''} \cdot l_{v'',w}, \quad C''\left(x_{v'}\right) = B_{i_{v''}} \cdot l_{v'',w} \oplus x_{v'} \cdot l_{v',w}.$$

Тогда

$$\forall\ x_{v'} \in B_{i_{v'}} \forall x_{v''} \in B_{i_{v''}} \left(C'(x_{v''}) = C''(x_{v'}) \right). \tag{5}$$

Из (5) следует, что

$$\left(B_{i'_v} + x_{v'} \right) \cdot l_{v',w} = \left(B_{i''_v} + x_{v''} \right) \cdot l_{v'',w}.$$

Так как $l_{v',w}$ невырождена, то

$$\forall x_1, x_2 \in B_{i_{v'}} \left(B_{i_{v'}} \oplus x_1 = B_{i_{v'}} \oplus x_2 \right). \tag{6}$$

Рассмотрим случай, когда $0 \in B_{i_{v'}}$. Пользуясь (6), получим

$$\forall x_1 \in B_{i_{v'}} \left(B_{i_{v'}} = B_{i_{v'}} \oplus x_1 \right).$$

Отсюда следует, что $B_{i_{v'}}$ замкнуто относительно операции сложения и является группой по сложению (векторным пространством).

Пусть теперь $0 \notin B_{i_{v'}}$. Фиксируем произвольное $x_1 \in B_{i_{v'}}$ и рассмотрим множество $H = x_1 \oplus B_{i_{v'}}$. Очевидно, что $0 \in H$. Покажем, что множество H замкнуто относительно операции сложения. Для этого покажем, что для любых $x_1, x_2 \in B_{i_{v'}}$ их сумма лежит в множестве $B_{i_{v'}}$. Действительно, пользуясь формулой (6), запишем:

$$B_{i_{v'}} = B_{i_{v'}} \oplus (x_1 \oplus x_2).$$

Таким образом, $B_{i_{v'}}$ является либо подпространством пространства $V_{n'}^m$, либо смежным классом по некоторому подпространству пространства $V_{n'}^m$. Для остальных индексов доказательство аналогично.

Для множеств C_{j_w} доказательство аналогично ввиду обратимости матрицы L. ■

Следствие 1. Пусть в условиях утверждения 6

$$A = A'_{i_1} \times A'_{i_2} \times \ldots \times A'_{i_m} \in \mathcal{A}'.$$

Тогда для любого $j \in \{1, \ldots, m\}$ множество A'_{i_j} является смежным классом по некоторому подпространству пространства $V_{n'}$.

Таким образом, нас в первую очередь интересуют такие пары множеств (A, B), что $A^{\pi} = B$, $A = H_A \oplus h_A$, $B = H_B \oplus h_B$, и H_A, H_B — подпространства пространства $V_{n'}$, $h_A, h_B \in V_{n'}$.

Предположим, имеется M пар таких множеств (A_i, B_i), $i \in \{1, \ldots, M\}$, при этом $A_i = H_{A,i} \oplus h_{A,i}$, $B_i = H_{B,i} \oplus h_{B,i}$, $|A_i| = |A_j|$ для всех $i, j \in \{1, \ldots, M\}$. Необходимость одинаковости мощностей множеств A_i обусловлена аналогичным требованием для множеств, образующих цикл в графе Г. Рассмотрим вектор $h \in V_{n'}^m$:

$$h = (h_{B,i_1}, h_{B,i_2}, \ldots, h_{B,i_m}), \ i_1, \ldots, i_m \in \{1, \ldots, M\}.$$

Всего таких векторов $|M|^m$.

Для каждых $v, w = 1, \ldots, m$ вычислим множество $C(h, v, w) \subset V_{n'}$:

$$C(h, v, w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} + y \cdot l_{v,w} : y \in H_{B,v} \right\}$$

— и проверим, существуют ли такие $g(w) \in V_{n'}$ и $j(w) \in \{1, \ldots, M\}$, зависящие от w, что

$$C(h, v, w) \oplus g(w) = A_{j(w)}.$$

То есть при разных v, но одинаковых w множество $A_{j(w)}$ и элемент $g(w)$ должны быть одинаковыми. Докажем следующую теорему.

Теорема 2. Пусть для XSL-шифра, линейное преобразование которого $L = (l_{a,b})_{m \times m}$, $l_{a,b} \in GL_{n'}(2)$, $a, b = 1, \ldots, m$, задаётся матрицей типа II, элементы семейства $\mathcal{A}'$ образуют некоторый нетривиальный цикл в графе Г. Пусть также $A_i = H_{A,i} \oplus h_{A,i}$, $H_{A,i}$ — подпространство пространства $V_{n'}$, $h_{A,i} \in V_{n'}$, $i \in \{1, \ldots, M\}$, при этом $|A_i| = |A_j|$ для всех $i, j \in \{1, \ldots, M\}$. Для множества $A \in \mathcal{A}'$,

$$A = A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m}, \ i_1, \ldots, i_m \in \{1, \ldots, M\},$$

существует такой ключ K, что $A^{\mathrm{L} \circ \mathrm{S} \circ \mathrm{X}[K]} = A' \in \mathcal{A}'$,

$$A' = A_{j_1} \times A_{j_2} \times \ldots \times A_{j_m}, \ j_1, \ldots, j_m \in \{1, \ldots, M\},$$

тогда и только тогда, когда для каждого $w \in \{1, \ldots, m\}$ существуют вектор $g(w) \in V_{n'}$ и номер $j(w) \in \{1, \ldots, M\}$, такие, что для любого $v \in \{1, \ldots, m\}$ выполнено равенство

$$C(h, v, w) \oplus g(w) = A_{j(w)},$$

где

$$C(h, v, w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} \oplus y \cdot l_{v,w} : y \in H_{B,v} \right\}.$$

Доказательство.

Докажем в прямую сторону методом от противного. Возможны два случая:

1) существует v, для которого не существует такого $g \in V_{n'}$, что $C(h, v, w) \oplus g \neq A_j$ хотя бы для одного $j \in \{1, \ldots, M\}$;
2) для некоторого w не существуют такие $g(w)$ и $A_{j(w)}$, что $C(h, v, w) \oplus g(w) = A_{j(w)}$.

В первом случае получаем противоречие с условием теоремы. Рассмотрим подробно второй случай.

Возьмём произвольный $x \in B$, $x = (x_1, x_2, \ldots, x_m)$. Так как для каждого $i \in \in \{1, \ldots, M\}$ верно $A_i = H_{A,i} \oplus h_{A,i}$, то $x = y \oplus h$, где $h = (h_{A,i_1}, h_{A,i_2}, \ldots, h_{A,i_m})$; $y = (y_1, y_2, \ldots, y_m)$; $y_i \in H_{A,i}$. Тогда

$$x \cdot L = y \cdot L \oplus h \cdot L.$$

Рассмотрим множество

$$Y_w = \left\{ y \cdot L_w^{\downarrow} : y \in H_{A,i_1} \times \ldots \times H_{A,i_m} \right\},$$

где $L_w^{\downarrow}$ — столбец матрицы L с номером w. Так как по условию теоремы $(Y_w \oplus h \cdot L) \oplus \oplus k = A_{j_w}$ для некоторого $k \in V_{n'}$, то $|A_{j_w}| = |Y_w|$; и по условию $|A_{i_a}| = |A_{j_b}|$ для всех $a, b \in \{1, \ldots, m\}$. Из мощностных соображений и того факта, что $0 \in H_{A,i_v}$ для всех $v \in \{1, \ldots, m\}$, получаем

$$\forall v \in \{1, \ldots, m\} \left(Y_w = \{ y_v \cdot l_{i_v,w} : y \in H_{A,i_v} \} \right).$$

Это противоречит тому, что для фиксированного w не существует таких $g(w)$ и $A_{j(w)}$, так как множество $\{ y_v \cdot l_{i_v,w} : y \in H_{A,i_v} \}$ одинаково для всех v.

Обратное очевидно. ■

С помощью теоремы 2 можно конструктивно строить инварианты для раундового преобразования XSL-шифра рассматриваемого вида. В общем случае можно воспользоваться методом нелинейных инвариантов [51]: функция $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ называется нелинейным инвариантом преобразования $g \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, если для любого $x \in \mathbb{F}_2^n$ и некоторой константы $c \in \mathbb{F}_2$ выполняется равенство

$$f(x) + f(g(x)) = c.$$

В работе [52] исследуются нелинейные инварианты раундовых преобразований XSL-алгоритмов и указаны условия на нелинейные биективные преобразования и матрицы, необходимые для существования таких инвариантов.

Авторы выражают благодарность Д. А. Довганю и Д. А. Бурову за конструктивные замечания в ходе обсуждения данной работы.

ЛИТЕРАТУРА

1. *Малышев Ф. М.* Двойственность разностного и линейного методов в криптографии // Матем. вопр. криптогр. 2014. Т. 5. Вып. 3. С. 35–48.
2. *Matsui M.* Linear cryptanalysis method for DES Cipher // LNCS. 1994. V. 765. P. 386–397.
3. *Малышев Ф. М., Трифонов Д. И.* Рассеивающие свойства XSLP-шифров // Матем. вопр. криптогр. 2016. Т. 7. Вып. 3. С. 47–60.
4. *Daemon J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin; Heidelberg: Springer, 2002. 238 p.
5. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Вып. 24. С. 15–42.

6. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
7. *Bilgin B., Nikova S., Nikov V., et al.* Threshold Implementations of all 3×3 and 4×4 S-boxes. IACR Cryptology ePrint Archive. 2012. `http://eprint.iacr.org/2012/300`.
8. *Bora A., Tolga M. S., and Ercan B.* Classifying 8-bit to 8-bit S-boxes based on power mappings from the point of DDT and LAT distributions // LNCS. 2008. V. 5130. P. 123–133.
9. *Biryukov A., De Cannière C., Braeken A., and Preneel B.* A toolbox for cryptanalysis: Linear and affine equivalence algorithms // LNCS. 2003. V. 2656. P. 33–50.
10. *Leander G. and Poschmann A.* On the classification of 4 bit S-boxes // LNCS. 2007. V. 4547. P. 159–176.
11. *Saarinen M. J. O.* Cryptographic analysis of all 4×4-bit S-boxes // LNCS. 2012. V. 7118. P. 118–133.
12. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С. 97–116.
13. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure // Матем. вопр. криптогр. 2019. Т. 10. Вып. 2. С. 169–180.
14. *Фомин Д. Б.* Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. Вып. 3. С. 121–138.
15. *Фомин Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m, m)$-функций // Матем. вопр. криптогр. 2020. Т. 11. Вып. 4. С. 133–149.
16. *Feistel H.* Cryptography and computer privacy // Scientific American. 1973. V. 225(5). P. 15–23.
17. *Feistel H., Notz W. A., and Smith J. L.* Some cryptographic techniques for machine to machine data communications // Proc. IEEE. 1975. V. 63(11). P. 1545–1554.
18. *Webster A. F. and Tavares S. E.* On the design of S-boxes // LNCS. 1986. V. 218. P. 523–534.
19. *Augot D. and Finiasz M.* Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. IACR Cryptology ePrint Archive. 2014. `http://eprint.iacr.org/2014/566`.
20. *Augot D. and Finiasz M.* Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions // IEEE Intern. Symp. Inform. Theory. 2013. P. 1551–1555.
21. *Barreto P. and Rijmen V.* The KHAZAD Legacy-Level Block Cipher. Submission to NESSIE. 2000. `https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher`.
22. *Gupta K. C. and Ray I. G.* On constructions of involutory MDS matrices // LNCS. 2013. V. 7918. P. 43–60.
23. *Junod P. and Vaudenay S.* Perfect diffusion primitives for block ciphers building efficient MDS matrices // LNCS. 2004. V. 3357. P. 84–99.
24. *Nakahara J. Jr. and Abrahao E.* A new involutory MDS matrix for the AES // Intern. J. Network Security. 2009. V. 9(2). P. 109–116.
25. *Poschmann A.* Lightweight Cryptography — Cryptographic Engineering for a Pervasive World. IACR Cryptology ePrint Archive. 2009. `http://eprint.iacr.org/2009/516`.
26. *Анашкин А. В.* Полное описание одного класса MDS-матриц над конечным полем характеристики 2 // Матем. вопр. криптогр. 2017. Т. 8. Вып. 4. С. 5–28.
27. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
28. D.STVL.9 — Ongoing Research Areas in Symmetric Cryptography. ECRYPT, 2008. 108 p.

29. *Погорелов Б. А., Пудовкина М. А.* Комбинаторная характеризация XL-слоёв // Матем. вопр. криптогр. 2013. Т. 4. Вып. 3. С. 99–129.
30. *Погорелов Б. А., Пудовкина М. А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25. № 3. С. 78–95.
31. *Погорелов Б. А., Пудовкина М. А.* О расстоянии от подстановок до объединения всех импримитивных групп с равными параметрами систем импримитивности // Дискретная математика. 2014. Т. 26. № 1. С. 103–117.
32. *Пудовкина М. А.* О вероятностях r-раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием // Прикладная дискретная математика. Приложение. 2014. № 7. С. 52–54.
33. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware // LNCS. 2004. V. 3017. С. 279–299.
34. *Burov D. A. and Pogorelov B. A.* An attack on 6 rounds of KHAZAD // Матем. вопр. криптогр. 2016. Т. 7. Вып. 2. С. 35–46.
35. *Burov D. A. and Pogorelov B. A.* The permutation group insight on the diffusion property of linear mappings // Матем. вопр. криптогр. 2018. Т. 9. Вып. 2. С. 47–58.
36. *Буров Д. А.* Подгруппы прямого произведения групп, инвариантные относительно действия подстановок на сомножителях // Дискретная математика. 2019. Т. 31. № 4. С. 3–19.
37. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т. Пер. с англ. М.: Мир, 1988.
38. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: учебник. В 2-х т. Т. 2. М.: Гелиос АРВ, 2003.
39. *Sim S. M., Khoo K., Oggier F. E., and Peyrin T.* Lightweight MDS involution matrices // FSE. 2015. P. 471–493.
40. *Coy Puente O. and de la Cruz Jiménez R. A.* Construction of orthomorphic MDS matrices with primitive characteristic polynomial // CTCrypt'20. 2020. `https://ctcrypt.ru/files/files/Oliver\CTCrypt2020.pdf`.
41. *Khan A. A. and Murtaza G.* Efficient Implementation of Grand Cru with TI C6x+ Processor. IACR Cryptology ePrint Archive. 2011. `http://eprint.iacr.org/2011/385`.
42. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI // LNCS. 2002. V. 2365. P. 179–194.
43. *Halevi S., Coppersmith D., and Jutla C. S.* Scream: A Software-Efficient Stream Cipher. IACR Cryptology ePrint Archive. 2002. `http://eprint.iacr.org/2002/019`.
44. `http://www.cryptonessie.org` — The New European Schemes for Signatures, Integrity and Encryption (NESSIE). 2003.
45. *Daeman J., Knudsen L. R., and Rijmen V.* The block cipher SQUARE // FSE'97. 1997. V. 1267. P. 149–156.
46. *Агиевич С. В., Галинский В. А., Микулич Н. Д., Харин Ю. С.* Алгоритм блочного шифрования BelT. `elib.bsu.by`.
47. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2012.
48. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372–402.
49. *Perrin L.* Partitions in the S-Box of Streebog and Kuznyechik. Cryptology ePrint Archive. 2019. `https://eprint.iacr.org/2019/092`.
50. *Горчинский Ю. Н.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. 1997. Т. 1. С. 67–84.

51. *Todo Y., Leander G., and Sasaki Y.* Nonlinear Invariant Attack — Practical Attack on Full SCREAM, iSCREAM, and Midori64. Cryptology ePrint Archive. 2016. `https://eprint.iacr.org/2016/732`.

52. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.

REFERENCES

1. *Malyshev F. M.* Dvoystvennost' raznostnogo i lineynogo metodov v kriptografii [The duality of differential and linear methods in cryptography]. Matem. Vopr. Kriptogr., 2014, vol. 5, no. 3, pp. 35–48. (in Russian)
2. *Matsui M.* Linear cryptanalysis method for DES cipher. LNCS, 1994, vol. 765, pp. 386–397.
3. *Malyshev F. M. Trifonov D. I.* Rasseivayushchiye svoystva XSLP-shifrov [Diffusion properties of XSLP-ciphers]. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 3, pp. 47–60. (in Russian)
4. *Daemon J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin; Heidelberg, Springer, 2002. 238 p.
5. *Sidel'nikov V. M.* O vzaimnoy korrelyatsii posledovatel'nostey [Cross-correlation of sequences]. Problemy Kibernetiki, 1971, no. 24, pp. 15–42. (in Russian)
6. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 55–64.
7. *Bilgin B., Nikova S., Nikov V., et al.* Threshold Implementations of all 3×3 and 4×4 S-boxes. IACR Cryptology ePrint Archive. 2012. `http://eprint.iacr.org/2012/300`.
8. *Bora A., Tolga M. S., and Ercan B.* Classifying 8-bit to 8-bit S-boxes based on power mappings from the point of DDT and LAT distributions. LNCS, 2008, vol. 5130, pp. 123–133.
9. *Biryukov A., De Cannière C., Braeken A., and Preneel B.* A toolbox for cryptanalysis: Linear and affine equivalence algorithms. LNCS, 2003, vol. 2656, pp. 33–50.
10. *Leander G. and Poschmann A.* On the classification of 4 bit S-boxes. LNCS, 2007, vol. 4547, pp. 159–176.
11. *Saarinen M. J. O.* Cryptographic analysis of all 4×4-bit S-boxes. LNCS, 2012, vol. 7118, pp. 118–133.
12. *Menyachikhin A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 97–116.
13. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure. Matem. Vopr. Kriptogr., 2019, vol. 10, no. 2, pp. 169–180.
14. *Fomin D. B.* Postroenie podstanovok prostranstva V_{2m} s ispol'zovaniem $(2m, m)$-funktsiy [Construction of permutations on the space V_{2m} by means of $(2m, m)$-functions]. Matem. Vopr. Kriptogr., 2020, vol. 11, no. 3, pp. 121–138. (in Russian)
15. *Fomin D. B.* Ob algebraicheskoy stepeni i differentsial'noy ravnomernosti podstanovok prostranstva V_{2m}, postroennykh s ispol'zovaniem $(2m, m)$-funktsiy [On the algebraic degree and differential uniformity of permutations on the space V_{2m} constructed via $(2m, m)$-functions]. Matem. Vopr. Kriptogr., 2020, vol. 11, no. 4, pp. 133–149. (in Russian)
16. *Feistel H.* Cryptography and computer privacy. Scientific American, 1973, vol. 225(5), pp. 15–23.
17. *Feistel H., Notz W. A., and Smith J. L.* Some cryptographic techniques for machine to machine data communications. Proc. IEEE, 1975, vol. 63(11), pp. 1545–1554.
18. *Webster A. F. and Tavares S. E.* On the design of S-boxes. LNCS, 1986, vol. 218, pp. 523–534.

19. *Augot D. and Finiasz M.* Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. IACR Cryptology ePrint Archive. 2014. `http://eprint.iacr.org/2014/566`.
20. *Augot D. and Finiasz M.* Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. IEEE Intern. Symp. Inform. Theory, 2013, pp. 1551–1555.
21. *Barreto P. and Rijmen V.* The KHAZAD Legacy-Level Block Cipher. Submission to NESSIE. 2000. `https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher`.
22. *Gupta K. C. and Ray I. G.* On constructions of involutory MDS matrices. LNCS, 2013, vol. 7918, pp. 43–60.
23. *Junod P. and Vaudenay S.* Perfect diffusion primitives for block ciphers building efficient MDS matrices. LNCS, 2004, vol. 3357, pp. 84–99.
24. *Nakahara J. Jr. and Abrahao E.* A new involutory MDS matrix for the AES. Intern. J. Network Security, 2009, vol. 9(2), pp. 109–116.
25. *Poschmann A.* Lightweight Cryptography — Cryptographic Engineering for a Pervasive World. IACR Cryptology ePrint Archive, 2009. `http://eprint.iacr.org/2009/516`.
26. *Anashkin A. V.* Polnoe opisanie odnogo klassa MDS-matrits nad konechnym polem kharakteristiki 2 [Complete description of a class of MDS-matrices over finite field of characteristic 2]. Matem. Vopr. Kriptogr., 2017, vol. 8, no. 4, pp. 5–28. (in Russian)
27. GOST R 34.12-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. [GOST P 34.12-2015. Information Technology. Cryptographic Data Security. Block Ciphers]. Moscow, Standartinform, 2015. (in Russian)
28. D.STVL.9 — Ongoing Research Areas in Symmetric Cryptography. ECRYPT, 2008. 108 p.
29. *Pogorelov B. A. and Pudovkina M. A.* Kombinatornaya kharakterizatsiya XL-sloyov [Combinatorial characterization of XL-layers]. Matem. Vopr. Kriptogr., 2013, vol. 4, no. 3, pp. 99–129. (in Russian)
30. *Pogorelov B. A. and Pudovkina M. A.* On the distance from permutations to imprimitive groups for a fixed system of imprimitivity. Discr. Math. Appl., 2013, vol. 24(2), pp. 95–108.
31. *Pogorelov B. A. and Pudovkina M. A.* On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems. Discr. Math. Appl., 2014, vol. 24(3), pp. 163–173.
32. *Pudovkina M. A.* O veroyatnostyakh r-raundovykh par raznostey XSL-algoritma blochnogo shifrovaniya Markova s privodimym lineynym preobrazovaniyem [On probabilities of r-round differences of a Markov XSL block cipher with a reducible linear transformation]. Prikladnaya Diskretnaya Matematika. Prilozheniye, 2014, no. 7, pp. 52–54. (in Russian)
33. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware. LNCS, 2004, vol. 3017, pp. 279–299.
34. *Burov D. A. and Pogorelov B. A.* An attack on 6 rounds of KHAZAD. Matem. Vopr. Kriptogr., 2016, vol. 7, no. 2, pp. 35–46.
35. *Burov D. A. and Pogorelov B. A.* The permutation group insight on the diffusion property of linear mappings. Matem. Vopr. Kriptogr., 2018, vol. 9, no. 2, pp. 47–58.
36. *Burov D. A.* Podgruppy pryamogo proizvedeniya grupp, invariantnyye otnositel'no deystviya podstanovok na somnozhitelyakh [Subgroups of Cartesian Product of Groups that are Invariant on Nonlinear Layer]. Diskretnaya Matematika, 2019, vol. 31, no. 4, pp. 3–19. (in Russian)
37. *Lidl R. and Niederreiter H.* Finite Fields. Cambridge, Cambridge University Press, 1984.

38. *Gluhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Study Book. Moscow, Gelous ARV, 2003. (in Russian)
39. *Sim S. M., Khoo K., Oggier F. E., and Peyrin T.* Lightweight MDS involution matrices. FSE, 2015, pp. 471–493.
40. *Coy Puente O. and de la Cruz Jiménez R. A.* Construction of orthomorphic MDS matrices with primitive characteristic polynomial. CTCrypt'20, 2020. `https://ctcrypt.ru/files/files/Oliver\CTCrypt2020.pdf`.
41. *Khan A. A. and Murtaza G.* Efficient Implementation of Grand Cru with TI C6x+ Processor. IACR Cryptology ePrint Archive. 2011. `http://eprint.iacr.org/2011/385`.
42. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI. LNCS, 2002, vol. 2365, pp. 179–194.
43. *Halevi S., Coppersmith D., and Jutla C. S.* Scream: A Software-Efficient Stream Cipher. IACR Cryptology ePrint Archive. 2002. `http://eprint.iacr.org/2002/019`.
44. `http://www.cryptonessie.org` — The New European Schemes for Signatures, Integrity and Encryption (NESSIE), 2003.
45. *Daeman J., Knudsen L. R., and Rijmen V.* The block cipher SQUARE. FSE'97, 1997, vol. 1267, pp. 149–156.
46. *Agievich S. V., Galinskiy V. A., Mikulich N. D., and Kharin Yu. S.* Algoritm blochnogo shifrovaniya BelT. [BelT Block Cipher]. `elib.bsu.by`. (in Russian)
47. GOST R 34.11-2012. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya. [GOST P 34.11-2012. Information Technology. Cryptographic Data Security. Hash Function]. Moscow, Standartinform, 2012. (in Russian)
48. *Biryukov A., Perrin L., and Udovenko A.* Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1. LNCS, 2016, vol. 9665, pp. 372–402.
49. *Perrin L.* Partitions in the S-box of Streebog and Kuznyechik. Cryptology ePrint Archive, 2019. `https://eprint.iacr.org/2019/092`.
50. *Gorchinskiy Yu. N.* O gomomorfizmakh mnogoosnovnykh universal'nykh algebr v svyazi s kriptograficheskimi primeneniyami [On homomorphisms of multibase universal algebras in connection with cryptographic applications]. Trudy po Diskretnoy Matematike, 1997, vol. 1, pp. 67–84. (in Russian)
51. *Todo Y., Leander G., and Sasaki Y.* Nonlinear Invariant Attack — Practical Attack on Full SCREAM, iSCREAM, and Midori64. Cryptology ePrint Archive. 2016. `https://eprint.iacr.org/2016/732`.
52. *Burov D. A.* O sushchestvovanii nelineynykh invariantov spetsial'nogo vida dlya raundovykh preobrazovaniy XSL-algoritmov [About existence of the special nonlinear invariants for round functions of XSL-ciphers]. Diskretnaya Matematika, 2021, vol. 33, no. 2, pp. 31–45. (in Russian)