F. M. Malyshev, Doubly transitive XLS-families of permutations, *Mat. Vopr. Kriptogr.*, 2010, Volume 1, Issue 2, 93–103

DOI: 10.4213/mvk11

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2010 Т. 1 № 2 С. 93–103

УДК 512.542.7

Дважды транзитивные XSL-семейства подстановок

Ф. М. Малышев

Академия криптографии Российской Федерации, Москва

Получено 22.IV.2010

Доказывается дважды транзитивность некоторых множеств подстановок, имеющих общую природу с преобразованиями, реализуемыми современными блочными шифраторами.

Ключевые слова: семейства подстановок, дважды транзитивность.

Doubly transitive XLS-families of permutations

F. M. Malyshev

Academy of Cryptography of Russian Federation, Moscow

Abstract. Conditions of 2-transitivity for some sets of permutations are established. These sets of permutations are similar to some mappings used in modern block ciphers.

Key words: families of permutations, double transitivity

Citation: *Mathematical Aspects of Cryptography*, 2010, vol. 1, no. 2, pp. 93–103 (Russian).

Введение

В работе рассматриваются семейства подстановок

$$\Pi_{L_1,...,L_r} = \{T_{x_1} SL_1 T_{x_2} SL_2 ... T_{x_r} SL_r \mid x = (x_1,...,x_r) \in F^{kr},\ x_i \in F^k, i = 1,...,r\}, \quad (1)$$

действующих на векторном пространстве $V_k = F^k$, $k \geq 1$. Здесь:

F — произвольное поле;

$T_{x_i}: V_k \to V_k$, $x_i \in V_k$, $i = 1,...,r$, оператор сдвига, $T_{x_i}(v) = v + x_i$, $v \in V_k$;

$L_i: V_k \to V_k, i = 1,...,r$, оператор умножения вектора на матрицу, обозначаемую той же буквой, $L_i \in \mathrm{GL}(k, F)$, $L_i(v) = vL_i$, $v \in V_k$;

$S: V_k \to V_k$, оператор замены координат вектора $v = (v_1,...,v_k) \in V_k$ на обратные к ним в поле F, $S(v_1,...,v_k) = (v_1^{-1},...,v_k^{-1})$ (по определению будем полагать $0^{-1} = 0, 0 \in F$).

Подстановки в произведении формулы (1) применяются в порядке слева направо.

Некоторые матрицы L_i в формуле (1) у нас будут мономиальными — с одним ненулевым элементом в каждой строке (а значит, и в каждом столбце). Ненулевые элементы в такой матрице располагаются по одной из $k!$ её диагоналей.

Если для какой-то матрицы $L_i, i = 1,...,r$, специально не оговорено, что она мономиальная, то будет предполагаться, что все k^2 её элементов ненулевые, причём у обратной матрицы L_i^{-1} тоже все k^2 элементов должны быть ненулевыми. В случае бесконечного поля F почти все матрицы размера $k \times k$ принадлежат $\mathrm{GL}(k, F)$ и обладают такими свойствами; их называют матрицами общего положения; это все матрицы, не входящие в некоторое алгебраическое многообразие [1]. Термин «почти все» здесь уместен как нигде, потому как у ненулевых многочленов одной переменной число нулей ограниченно его степенью.

Для конечных полей F достаточно большой мощности качественно такое положение сохраняется. Для практически интересных случаев $F = \mathrm{GF}(2^8)$, $k = 16, 24, 32$, отвечающих шифрпреобразованиям алгоритма AES, матрицы «общего положения» достаточно эффективно строятся путём их случайной генерации с последующей проверкой необходимых свойств. Примерами таких матриц L при $|F| \geq 2k$ являются, в частности, матрицы Коши $C = \|c_{ij}\|_{i,j=\overline{1,k}}$, $c_{ij} = \dfrac{1}{a_i - b_j}$, для произвольных попарно различных

$a_1,...,a_k,b_1,...,b_k \in F$ (см. монографию [3], а также упражнение 416 из задачника [4]). Дополнение к матрицам «общего положения» в множестве всех матриц $\|t_{ij}\|$ размера $k\times k$ над полем F состоит из корней многочлена $\det\|t_{ij}\|\prod_{i=1}^{k}\prod_{i=1}^{k}t_{ij}\prod_{i=1}^{k}\prod_{i=1}^{k}A_{ij}$ от k^2 переменных t_{ij}, $i, j=1,...,k$. Здесь A_{ij} — алгебраическое дополнение элемента t_{ij}. Мощность пересечения множества нулей этого многочлена с любой прямой, проходящей, например, через одну из матриц Коши, ограничена его степенью. Тем самым, и для конечного поля F достаточно большой мощности почти все матрицы являются матрицами «общего положения».

Обратим внимание, что внешний параметр $(L_1,...,L_r)\in \mathrm{GL}(k,F)^r$ в формуле (1) задаёт конкретное семейство $\Pi_{L_1,...,L_r}$, а внутренний параметр $x=(x_1,...,x_r)\in F^{kr}, x_i\in F^k, i=1,...,r$, задаёт конкретную подстановку $\Pi_{L_1,...,L_r;x}$ внутри семейства $\Pi_{L_1,...,L_r}$.

В криптографической литературе для реализации семейств подстановок (1) используются так называемые XSL — сети (см., например, [2]).

При наличии подполя $F_0\subset F$ класс семейств подстановок (1) может быть расширен за счёт использования для L_i более широкого множества линейных над F_0 преобразований из $\mathrm{GL}(mk,F_0)$, если $m=\dim_{F_0}F$.

Определение. Семейство подстановок (1) является дважды транзитивным на V_k, если для любых пар $(a,b),(a',b')\in(V_k)^2, a\neq b, a'\neq b'$, найдётся $x\in F^{kr}$, при котором $\Pi_{L_1,...,L_r;x}(a)=a'$, $\Pi_{L_1,...,L_r;x}(b)=b'$.

Теорема. *Семейство подстановок $\Pi_{L_1,...,L_r}$ является дважды транзитивным при выполнении любого из следующих условий:*

а) $k=1$; F — алгебраически замкнутое поле; $r\geq 2$.

б) $k=1$; $|F|\geq 5$; $r\geq 3$.

в) $k>1$; F — алгебраически замкнутое поле; $r\geq 4$.

г) $k>1$; если $\mathrm{char}F>2$, то $|F|>2k+1$; если $\mathrm{char}F=2$, то $|F|>2k+2$; при некотором $i\in\{1,...,r-4\}$ матрицы L_i, L_{i+2} мономиальные; $r\geq 6$.

д) $k>1$; $|F|>k+1$; $F\neq GF(2^2)$; при некотором $i\in\{1,...,r-6\}$ матрицы L_i, L_{i+2}, L_{i+4} мономиальные; $r\geq 7$.

В качестве комментариев к данной теореме приведём несколько замечаний.

ЗАМЕЧАНИЕ 1. Транзитивность семейства $\Pi_{L_1,\dots,L_r}$, в том смысле, что для любых $a,a'\in V_k$ найдётся $x\in F^{kr}$, при котором $\Pi_{L_1,\dots,L_r;x}(a)=a'$, очевидно имеет место при всех значениях параметров $F, k\geq 1, r\geq 1, L_i$, $i=1,\dots,r$.

ЗАМЕЧАНИЕ 2. Теорему достаточно доказывать только для наименьших значений параметра r, указанных в пунктах *а), б), в), г), д)* её формулировки. При доказательстве теоремы две последние подстановки SL_r в выражении (1) можно не принимать во внимание, они никак не влияют на справедливость утверждения теоремы.

ЗАМЕЧАНИЕ 3. Для поля $F=\mathrm{GF}(2)$ или $F=\mathrm{GF}(3)$ подстановка S является тождественной на V_k, из-за чего при всех значениях параметров $k\geq 1, r\geq 1, L_i, i=1,\dots,r$, подстановка $\Pi_{L_1,\dots,L_r;x}$ является аффинным преобразованием, $\Pi_{L_1,\dots,L_r;x}(v)=vL_0+t(x)$, $v\in V_k$, в котором $L_0=L_1\cdot L_2\cdot\ldots\cdot L_r$ и от параметра $x\in F^{kr}$ зависит только вектор сдвига $t(x)\in V_k$. Всё вышесказанное можно повторить и для поля $F=\mathrm{GF}(2^2)$, когда S превращается в линейное преобразование V_k над полем $F_0=\mathrm{GF}(2)$, а $\Pi_{L_1,\dots,L_r;x}$ — в аффинное преобразование над полем F_0 с фиксированной линейной частью $L_0=$ $=S\cdot L_1\cdot S\cdot L_2\cdot\ldots\cdot S\cdot L_r$. В результате если $|F|<5$, то семейство подстановок $\Pi_{L_1,\dots,L_r}$ не будет дважды транзитивным ни при каких значениях параметров $k\geq 1, r\geq 1, L_i, i=1,\dots,r$, поскольку $\Pi_{L_1,\dots,L_r;x}(a)-\Pi_{L_1,\dots,L_r;x}(b)=(a-b)L_0$ для всех $a,b\in V_k, x\in (V_k)^r$. Исключением для последнего является совсем очевидный случай с $F=\mathrm{GF}(2)$, $k=1$, когда дважды транзитивность семейства подстановок $\Pi_{L_1,\dots,L_r}$, действующих на GF(2), эквивалентна транзитивности и имеет место для всех $r\geq 1$.

ЗАМЕЧАНИЕ 4. Пункт *б)* теоремы для конечного поля F характеристики 2 был доказан ранее Б. В. Березиным.

ЗАМЕЧАНИЕ 5. В работе [5] для поля $F=\mathrm{GF}(2^8)$, его простого подполя $F_0=\mathrm{GF}(2)$ и специальных матриц $L_i, i=1,\dots,r$, предусмотренных шифр-преобразованиями стандарта AES (см. [2]), дважды транзитивность семейства подстановок $\Pi_{L_1,\dots,L_r}$ при $(k,r)=(16,5),(24,7),(32,7)$ доказана с привлечением компьютерных вычислений. Обратим внимание, что как первый, так и два последних из трёх приведённых результатов работы [5] не следуют из пунктов *г)* и *д)* сформулированной здесь теоремы, потому как матрицы стандарта AES не удовлетворяют её условиям.

Доказательство. Каждый из пяти пунктов формулировки теоремы будем доказывать отдельно.

а) Достаточно проверить дважды транзитивность на F семейства $T_{x_1} SL_1 T_{x_2}$, что равносильно наличию решения у системы

$$\begin{cases} \dfrac{\alpha}{a + x_1} + x_2 = b \\ \dfrac{\alpha}{a' + x_1} + x_2 = b' \end{cases}$$

при $a \neq a', b \neq b', \alpha \neq 0.$ Вычитая одно уравнение из другого, получаем

$$\alpha \left(\frac{1}{a + x_1} - \frac{1}{a' + x_1} \right) = b - b'.$$

В качестве решения последнего уравнения можно взять любое решение уравнения

$$(a + x_1)(a' + x_1) = \frac{\alpha(a' - a)}{b - b'},$$

поскольку оно будет отлично и от $(-a),$ и от $(-a')$.

б) Проверка дважды транзитивности на F семейства подстановок $T_x SL_1 T_y SL_2 T_z$, $x, y, z \in F,$ равносильна доказательству разрешимости уравнения

$$\frac{\alpha_2}{\dfrac{\alpha_1}{x + d} + y} - \frac{\alpha_2}{\dfrac{\alpha_1}{x} + y} = D \tag{2}$$

относительно неизвестных $x, y \in F$ при любых ненулевых $\alpha_1, \alpha_2, d, D \in F.$ Чтобы в этом убедиться, достаточно в определении дважды транзитивности положить $a - a' = d,\ b - b' = D$. Ясно, что разрешимость уравнения (2) достаточно проверить только для $\alpha_1 = \alpha_2 = 1$. За исключением особых значений пар $x, y \in F$:

$$x = 0;\ x = -d;\ xy = -1;\ (x + d)y = -1, \tag{3}$$

уравнение (2) можно представить в эквивалентном виде

$$(xy + 1)(xy + 1 + yd) = dD^{-1}. \tag{4}$$

Разрешимость последнего уравнения достаточно проверить только для $d = 1$, при $d \neq 1$ можно воспользоваться заменой переменных $y' = ydz$, $x' = xd^{-1}$. Введение новых переменных

$$Z = xy + 1,\ U = xy + 1 + y \tag{5}$$

сводит разрешимость уравнения (4) к разрешимости совсем простого уравнения:

$$ZU = D^{-1} \tag{6}$$

при любом ненулевом D^{-1}. Правда, учитывая особые значения пар $x, y \in F$ в списке (3), на пары новых неизвестных приходится вводить соответствующие запреты: $Z = 1$; $U = 1$; $Z = 0$; $U = 0$. К ним добавим ещё один запрет: $Z = U$. Незапрещённая пара Z, U получается с помощью равенств (5) из $x = \dfrac{Z-1}{U-Z}$ и $y = U - Z$, причём данные x и y избегают все особенности (3). Уравнение (6) имеет $|F|-1$ решений, запрещённых из которых не больше четырёх; по одному — для $Z = 1$ и $U = 1$, а также не более двух — для: $Z = U$. Тем самым, при $|F|-1 > 4$ утверждение пункта *б*) теоремы доказано. Для $F = \mathrm{GF}(5)$ разрешимость уравнения (2) при $\alpha_1 = \alpha_2 = d = 1$ и любом D проверяется непосредственно, достаточно положить $y = 0, 1, 2$ при $x = 0$ и $y = 2$ при $x = 1$. Когда $d \neq 1$, можно привлечь замену: $x' = xd^{-1}$, $y' = yd$, $D' = Dd^{-1}$.

в) Здесь будем доказывать дважды транзитивность на $V_k = F^k$ для семейства подстановок $T_{x_1} SL_1 T_{x_2} SL_2 T_{x_3} SL_3 T_{x_4}$, $(x_1, x_2, x_3, x_4) \in (V_k)^4$.

Через $e_1, \ldots, e_k$ обозначим стандартный базис V_k: у вектора e_i, $i = 1, \ldots, k$, i-я координата равна единице, а остальные координаты нулевые. Множество номеров ненулевых координат вектора $v = (v_1, \ldots, v_k) \in V_k$ будем называть носителем v и использовать обозначение $[v] = \{i \in \{1, \ldots, k\} \mid v_i \neq 0\}$.

Для $a, a' \in V_k$, $a \neq a'$, $b, b' \in V_k$, $b \neq b'$, обозначим $a - a' = d$, $b - b' = D$. Из приведённого выше доказательства утверждения *а*) теоремы следует, что

$$\{(T_{x_1} S)(a) - (T_{x_1} S)(a') \mid x_1 \in V_k\} =$$

$$= \{v = (v_1, \ldots, v_k) \in V_k \mid v_i = 0, i \notin [d], v_j \in F^*, j \in [d]\},\ F^* = F \setminus \{0\}.$$

Тогда

$$\{(T_{x_1} SL_1)(a) - (T_{x_1} SL_1)(a') \mid x_1 \in V_k\} = \left\{ \sum_{i \in [d]} v_i L_1(e_i) \mid v_i \in F^* \right\}. \tag{7}$$

Коль скоро у векторов $L_1(e_i)$, $i = 1, \ldots, k$, все координаты ненулевые, а поле F бесконечно, можно подобрать такие $v_i \in F^*$, $i \in [d]$, что у вектора $w_0 = \sum_{i \in [d]} v_i L_1(e_i)$ тоже все k координат будут ненулевые. Последнее, когда

$|[d]|=1$, очевидно. При $|[d]|>1$ положим $v_i=1$ для всех $i\in[d]\setminus\{i_0\}$ и какого-то $i_0\in[d]$. Затем для каждого $j=1,...,k$ определим элемент $v_{i_0}^{(j)}\in F$ таким образом, чтобы у вектора $v_{i_0}^{(j)}L_1(e_{i_0})+\sum\limits_{i\in[d]\setminus\{i_0\}}v_iL_1(e_i)$ была нулевой j-я координата. Если теперь выбрать $v_{i_0}\in F^*\setminus\{v_{i_0}^{(1)},...,v_{i_0}^{(k)}\}$, то у вектора $w_0=\sum\limits_{i\in[d]}v_iL_1(e_i)$ все координаты будут ненулевыми.

Доказанное существование в множестве (7) вектора w_0 со всеми ненулевыми координатами гарантирует, согласно доказательству утверждения *а*) теоремы, вложение

$$\{(T_{x_1}SL_1T_{x_2}S)(a)-(T_{x_1}SL_1T_{x_2}S)(a')\,|\,x_1,x_2\in V_k\}\supset\left\{\sum_{i=1}^{k}v_ie_i\,|\,v_i\in F^*\right\}=Y.$$

После этого, принимая во внимание, что у матрицы L_2^{-1} все элементы ненулевые, можно утверждать, что в множестве

$$X=\{(T_{x_1}SL_1T_{x_2}SL_2)(a)-(T_{x_1}SL_1T_{x_2}SL_2)(a')\,|\,x_1,x_2\in V_k\}$$

содержится вектор w с любым наперёд заданным непустым носителем $A\subset\{1,...,k\}$. Проверим это. У вектора $L_2^{-1}(e_i)$, $i=1,...,k$, все координаты ненулевые — $L_2^{-1}(e_i)\in Y$. Тем самым, для $A=\{i\}$ наличие требуемого $w\in X$ установлено, причём для любого $i\in\{1,...,k\}$. В случае $|A|>1$ рассматриваем $w=\mu_{i_0}e_{i_0}+\sum\limits_{i\in A\setminus\{i_0\}}e_i$ для какого-либо $i_0\in A$. В последнем равенстве $\mu_{i_0}\in F^*\setminus\{\mu_{i_0}^{(1)},...,\mu_{i_0}^{(k)}\}$, а элементы $\mu_{i_0}^{(j)}\in F$, $j=1,...,k$, определяются таким образом, чтобы у вектора $\mu_{i_0}^{(j)}L_2^{-1}(e_{i_0})+\sum\limits_{i\in A\setminus\{i_0\}}L_2^{-1}(e_i)$ была нулевой j-я координата. Тогда $L_2^{-1}(w)=\mu_{i_0}L_2^{-1}(e_{i_0})+\sum\limits_{i\in A\setminus\{i_0\}}L_2^{-1}(e_i)\in Y$, а $w\in X$ и $[w]=A$.

Из существования таких векторов w и доказательства утверждения *а*) теоремы следует равенство

$$\{(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}S)(a)-(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}S)(a')\,|\,x_1,x_2,x_3\in V_k\}=V_k\setminus\{0\},$$

в частности, $(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}S)(a)-(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}S)(a')=L_3^{-1}(D)$ при некоторых $x_1,x_2,x_3\in V_k$. Так как $b-b'=D$, то существует $x_4\in V_k$, при котором $(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4})(a)=b$, $(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4})(a')=b'$.

г) Будем доказывать дважды транзитивность на $V_k=F^k$ для семейства подстановок $T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4}SL_4T_{x_5}SL_5T_{x_6}$, $(x_1,x_2,x_3,x_4,x_5,x_6)\in(V_k)^6$, в ко-

тором у матриц L_1 и L_3 только по одному ненулевому элементу в каждой строке.

Как и в предыдущем пункте доказательства для $a,a'\in V_k$, $a\neq a'$, $b,b'\in V_k$, $b\neq b'$, обозначим $a-a'=d$, $b-b'=D$. Мономиальная матрица L_1 представляется произведением диагональной матрицы и оператора $\hat{\pi}_1$ перестановки координат векторов из V_k по некоторой подстановке $\pi_1\in S_{1,\dots,k}$. Ненулевые элементы матрицы L_1 расположены на местах $(i,\pi_1(i))$, $i=1,\dots,k$. Оператор $\hat{\pi}_1$ перестановочен с операторами T_x, $x\in V_k$, и с оператором S. Благодаря такой перестановочности из приведённого выше доказательства утверждения *б)* теоремы следует, что

$$\{(T_{x_1}SL_1T_{x_2}S)(a)-(T_{x_1}SL_1T_{x_2}S)(a')\mid x_1,x_2\in V_k\}=$$

$$=\{v=(v_1,\dots,v_k)\in V_k\mid v_i=0, i\notin\pi_1([d]), v_j\in F^*, j\in\pi_1([d])\}.$$

Тогда

$$\{(T_{x_1}SL_1T_{x_2}SL_2)(a)-(T_{x_1}SL_1T_{x_2}SL_2)(a')\mid x_1,x_2\in V_k\}=\left\{\sum_{i\in\pi_1([d])}v_iL_2(e_i)\mid v_i\in F^*\right\}. \quad (8)$$

У векторов $L_2(e_i)$, $i=1,\dots,k$, все координаты ненулевые, поэтому можно подобрать такие $v_i\in F^*$, $i\in\pi_1([d])$, что у вектора $w_0=\sum_{i\in\pi_1([d])}v_iL_2(e_i)$ тоже все k координат будут ненулевые. В этом убеждаемся как и в предыдущем пункте доказательства, полагая при $|[d]|>1$ $v_i=1$ для $i\in\pi_1([d])\setminus\{i_0\}$ при каком-либо $i_0\in\pi_1([d])$ и $v_{i_0}\in F^*\setminus\{v_{i_0}^{(1)},\dots,v_{i_0}^{(k)}\}$, где элемент $v_{i_0}^{(j)}\in F$, $j=1,\dots,k$, определяется так, что у вектора $v_{i_0}^{(j)}L_2(e_{i_0})+\sum_{i\in\pi_1([d])\setminus\{i_0\}}v_iL_2(e_i)$, $j=1,\dots,k$, j-я координата является нулевой. Такой выбор v_{i_0} возможен, поскольку в случае конечного поля F $|F|>2k+1>k+1$.

Доказанное существование в множестве (8) вектора w_0 со всеми ненулевыми координатами гарантирует, согласно доказательству утверждения *б)* теоремы, вложение

$$\{(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4}S)(a)-(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4}S)(a')\mid x_1,x_2,x_3,x_4\in V_k\}\supset$$

$$\supset\left\{\sum_{i=1}^{k}v_ie_i\mid v_i\in F^*\right\}.$$

Принимая во внимание, что у матрицы L_4^{-1} все элементы ненулевые, по аналогии с предыдущим пунктом доказательства заключаем, что в множестве

$$X = \{(T_{x_1} SL_1 T_{x_2} SL_2 T_{x_3} SL_3 T_{x_4} SL_4)(a) - \\ -(T_{x_1} SL_1 T_{x_2} SL_2 T_{x_3} SL_3 T_{x_4} SL_4)(a') \mid x_1, x_2, x_3, x_4 \in V_k\}$$

содержатся векторы w с любым наперёд заданным непустым носителем $A \subset \overline{1,k}$. Более того, в X содержатся все ненулевые векторы множества $V_A = \left\{ \sum_{i \in A} v_i e_i \mid v_i \in F \right\}$, за исключением, быть может, векторов из k', $0 \le k' \le k$, гиперплоскостей, являющихся образами при L_4 координатных гиперплоскостей.

Поскольку $xe_i^T = xL_4 L_4^{-1} e_i^T$, то образ при L_4 координатной гиперплоскости $V_{\overline{1,k} \setminus \{i\}} = \{x \in V_k \mid x \cdot e_i^T = 0\}$ будет равен $\{y \in V_k \mid y \cdot L_4^{-1} e_i^T = 0\}$. У вектора $L_4^{-1} e_i^T$ все координаты ненулевые, поэтому все k пересечений $L_4(V_{\overline{1,k} \setminus \{i\}}) \cap V_A$, $i = 1,...,k$, из которых какие-то совпадают, задаются в пространстве V_A уравнениями $\sum_{i \in A} c_i^{(j)} v_i = 0$, $j = 1,...,k'$, причём $c_i^{(j)} \in F^*$ для всех $i \in A$ и $j \in \overline{1,k'}$.

Множество $V_A \setminus \{0\}$ ненулевых векторов вида $\sum_{i \in A} v_i e_i$, за вычетом упомянутых гиперповерхностей $L_4(V_{1,...,k \setminus \{i\}}) \cap V_A$, обозначим через Y, $Y \subset X$.

Пусть далее $A = \left[L_5^{-1}(D) \right]$, $L_5^{-1}(D) = \sum_{i \in A} D_i e_i$, $D_i \in F^*$, $i \in A$. Проверим теперь, что найдутся $d_i \in F^*$, $i \in A$, при которых разрешимо каждое из уравнений

$$\frac{1}{x + d_i} - \frac{1}{x} = D_i, \tag{9}$$

относительно $x \in F$ и $\sum_{i \in A} d_i e_i \in Y$. Этим будет завершено доказательство утверждения *г*) теоремы.

Обозначим через F_0 множество ненулевых элементов поля F, представимых в виде $x(x+1)$, $x \in F$. Равенство $x(x+1) = y(y+1)$ для различных $x, y \in F$ имеет место только при $x + y + 1 = 0$, поэтому в случае конечного

поля F имеем $|F_0|=\frac{|F|-2}{2}$ при $\mathrm{char}F=2$ и $|F_0|=\frac{|F|-3}{2}+1=\frac{|F|-1}{2}$ при $\mathrm{char}F>2$.

Обратимся теперь к уравнению (9). Ограничимся значениями $x\notin\{0,-d_i\}$. Уравнение (9) тогда можно представить в виде

$$-D_i^{-1}=d_i\frac{x}{d_i}\left(\frac{x}{d_i}+1\right),$$

откуда следует, что имеется по крайней мере $|F_0|$ возможностей для $d_i\in F^*$, при которых уравнение (9) разрешимо.

Зафиксируем некоторый номер $i_0\in A$. Для каждого $i\in A\setminus\{i_0\}$ выберем $d_i\in F^*$ одним из $|F_0|$ способов, при котором уравнение (9) разрешимо. Рассмотрим затем величины $d_{i_0}^{(j)}$, $j=1,...,k'$, удовлетворяющие равенствам $c_{i_0}^{(j)}d_{i_0}^{(j)}+\sum\limits_{i\in A\setminus\{i_0\}}c_i^{(j)}d_i=0$, $j=1,...,k'$. После этого d_{i_0} выбираем одним из $|F_0|$ способов, но так, чтобы $d_{i_0}\notin\{d_{i_0}^{(j)}\mid j=1,...,k'\}$. Это возможно, поскольку по условию теоремы $|F_0|>k\geq k'$. При таком выборе d_{i_0} имеем $d_{i_0}e_{i_0}+$ $+\sum\limits_{i\in A\setminus\{i_0\}}d_ie_i\in Y$. Этим устанавливается включение

$$\{(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4}SL_4T_{x_5}SL_5)(a)-$$
$$-(T_{x_1}SL_1T_{x_2}SL_2T_{x_3}SL_3T_{x_4}SL_4T_{x_5}SL_5)(a')\mid x_1,x_2,x_3,x_4\in V_k\}\ \ni\ D$$

и требуемая дважды транзитивность.

Справедливость доказываемого утверждения в случае мономиальных матриц L_2 и L_4 проверяется путём перехода к семейству из обратных подстановок в (1), при этом должны быть использованы равенства $T_{x_{i+1}}^{-1}L_i^{-1}=$ $=L_i^{-1}T_{-x_{i+1}L_i^{-1}}$ и учтено замечание 2.

∂) В этом случае доказательство проводится аналогично доказательству из предыдущего пункта без привлечения дополнительных особенностей.

Теорему можно считать полностью доказанной.

Автор благодарит А. М. Зубкова за внимательное прочтение исходного варианта статьи и сделанные замечания.

Список литературы

1. *Шафаревич И. Р.* Основы алгебраической геометрии. Т. 1, т. 2. — М.: Наука, 1988. .

2. *Зензин О. С., Иванов М. А.* Стандарт криптографической защиты AES. Конечные поля. — М.: КУДИЦ-ОБРАЗ, 2002, с. 176.
3. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.
4. *Проскуряков И. В.* Сборник задач по линейной алгебре. — М.: Наука, 1978.
5. *Глухов М. М.* О матрице частот переходов пар блоков в одной модификации криптосхемы Rijndael. — Обозрение прикл. и промышл. матем., 2004, т. 11, в. 2, с. 318–319.