2008 Математические методы криптографии № 2(2)

DOI 10.17223/20710410/2/12

УДК 519.7

СВОЙСТВА НЕКОТОРЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ФЕЙСТЕЛЯ ОТНОСИТЕЛЬНО ДВУХ ГРУПП СПЛЕТЕНИЯ[1]

М.А. Пудовкина

Московский инженерно-физический институт (*государственный университет*)

E-mail: maricap@rambler.ru

Одной из наиболее часто встречающихся конструкций, применяемой при синтезе блочных алгоритмов шифрования, является схема Фейстеля. В работе исследуются свойства некоторых алгоритмов шифрования на основе схемы Фейстеля относительно двух групп сплетений. Описаны слабости такого класса алгоритмов шифрования.

Ключевые слова: *алгоритм шифрования Фейстеля*, *сплетения групп подстановок*, *импримитивная группа.*

Одной из наиболее часто встречающихся конструкций, применяемых при синтезе блочных алгоритмов шифрования, является схема Фейстеля. Напомним (см., например, [1]), что схема Фейстеля задается преобразованием $g_{\pi_k} : V_m \times V_m \to V_m \times V_m$, $g_{\pi_k} : (\alpha,\beta) \to (\beta, \beta^{\pi_k} \oplus \alpha)$, где V_m – множество всех m-мерных двоичных векторов над полем $GF(2)$, $\pi_k: V_m \to V_m$, $k \in V_m$, $\oplus$ – операция векторного сложения в V_m. Преобразование π_k зависит от ключа k. Алгоритмы шифрования на основе схемы Фейстеля будем называть алгоритмами шифрования Фейстеля.

Групповые свойства алгоритмов шифрования Фейстеля приведены, например, в работах [2 – 4]. Так, в [4] рассматривался случай, когда подстановка π_k принадлежит импримитивной группе, и строилась система блоков импримитивности для алгоритма шифрования DES с измененными s-боксами.

Две импримитивные группы $S_2 \wr S_{2^{n-1}}$ и $S_{2^{n-1}} \wr S_2$ большого порядка, которые максимально близки к примитивным группам, неоднократно возникали в различных смежных областях, например в работе [5] при классификации групп автоморфизмов графов орбиталов подсхем схемы Хемминга и в работе [6]. Поэтому представляет интерес рассмотреть свойства алгоритмов шифрования Фейстеля с подстановкой π_k, принадлежащей двум этим группам.

В данной работе исследуются свойства алгоритмов шифрования Фейстеля таких, что $\pi \in \{S_2 \wr S_{2^{m-1}}, S_{2^{m-1}} \wr S_2\}$, а $\beta^{\pi_k} \in \{(\beta \oplus k)^{\pi}, \beta^{\pi} \oplus k\}$ для всех k, $\beta \in V_m$. Описаны слабости такого класса алгоритмов шифрования. Получено, что если $\pi \in S_{2^{m-1}} \wr S_2$, то по шифртексту возможно получить некоторую информацию об открытом тексте без знания ключа. Если же $\pi \in S_2 \wr S_{2^{m-1}}$, то на множестве ключей можно ввести отношение эквивалентности, и задача определения ключа сводится к проблеме нахождения какого-нибудь представителя из класса эквивалентности, которому принадлежит ключ.

Всюду ниже придерживаемся следующих обозначений: $S(X)$ – симметрическая группа подстановок на множестве X, N – множество натуральных чисел; $m \in N$; $n = 2m$; $\overline{a,b} = a, a+1, ..., b$, $a < b$; $\Phi_n = \{f_\pi \in S(V_m \times V_m) \mid f_\pi : (\alpha,\beta) \to (\beta, \beta^{\pi} \oplus \alpha)\}$ – множество алгоритмов шифрования Фейстеля; e – тождественная подстановка, $g^s = s^{-1}gs$ для подстановок g, $s \in S(X)$.

Будем отождествлять 2-адическое представление элемента a с представлением его в виде двоичного вектора.

1. Свойства алгоритмов шифрования Фейстеля относительно группы $S_2 \wr S_{2^{m-1}}$

Если подстановка $\pi \in S(V_m)$ фиксирована, $f_{\pi_k} \in \Phi_n$ и $\alpha^{\pi_k} \in \{(\alpha \oplus k)^{\pi}, \alpha^{\pi} \oplus k\}$ для любого $\alpha \in V_m$, то будем использовать обозначение $f_k = f_{\pi_k}$.

Рассмотрим двоичную последовательность $\overline{a} = a_1 a_2, ...,$

$$a_i = \begin{cases} 1, & \text{если } i \equiv 1, 2 \pmod 3, \\ 0, & \text{если } i \equiv 0 \pmod 3, \end{cases}$$

являющуюся решением рекуррентного соотношения $a_i = a_{i-1} \oplus a_{i-2}$ в $GF(2)$, $a_0 = 0$, $a_1 = 1$, $i = 2, 3, \ldots$

[1] Работа выполнена при поддержке гранта Президента РФ НШ №4.2008.10.

Утверждение 1. Пусть $\pi \in S_2 \wr S_{2^{m-1}}$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^{\pi}, \alpha^{\pi} \oplus k\}$ для любого $k \in V_m$. Тогда

1) $\pi_k \in S_2 \wr S_{2^{m-1}}$ для любого $k \in V_m$;

2) $$(\alpha,\beta)^{\prod_{i=1}^{l} f_{k_i} \oplus \theta_i} = \left(\alpha^{(l)} \oplus \sum_{i=1}^{l-1} a_{l-i}\theta_i, \beta^{(l)} \oplus \sum_{i=1}^{l} a_{l-i+1}\theta_i\right), \quad (1)$$

где $l \in N$, $(\alpha,\beta)^{\prod_{i=1}^{l} f_{k_i}} = (\alpha^{(l)}, \beta^{(l)})$ и $\theta_i \in \{\vec{0}, \vec{1}\}$, $i = \overline{1,l}$.

Доказательство. 1) Включение $s \in S_2 \wr S_{2^{m-1}}$ выполняется тогда и только тогда, когда $(\alpha \oplus \vec{1})^s = \alpha^s \oplus \vec{1}$ для любого $\alpha \in V_m$. Очевидно, что $(\alpha \oplus \vec{1})^{\pi} \oplus k = (\alpha \oplus k)^{\pi} \oplus \vec{1}$ для любого $k \in V_m$. Следовательно, $\pi_k \in S_2 \wr S_{2^{m-1}}$.

2) Пусть $\theta_i \in \{\vec{0}, \vec{1}\}$, $i = 1, 2, \ldots$ Рассмотрим последовательность $y_i = y_{i-1} \oplus y_{i-2} \oplus \theta_i$, $y_0 = y_{-1} = 0$, $i = 1, 2, \ldots$ Методом математической индукции нетрудно показать, что $y_i = \sum_{j=1}^{i} a_{i-j+1}\theta_j$.

Равенство

$$(\alpha,\beta)^{\prod_{i=1}^{l} f_{k_i} \oplus \theta_i} = \left(\alpha^{(l)} \oplus y_{l-1}, \beta^{(l)} \oplus y_l\right)$$

доказывается применением метода математической индукции с учетом следующих соотношений:

$$(\alpha,\beta)^{f_k \oplus \theta_1} = \left(\beta, \beta^{\pi_{k \oplus \theta_1}} \oplus \alpha\right) = \begin{cases} (\beta, ((k \oplus \theta_1) \oplus \beta)^{\pi} \oplus \alpha) \\ (\beta, (\beta^{\pi} \oplus (k \oplus \theta_1)) \oplus \alpha) \end{cases} = (\beta, \beta^{\pi_k} \oplus \alpha \oplus \theta_1) =$$

$$= (\alpha^{(1)}, \beta^{(1)} \oplus \theta_1) = (\alpha^{(1)} \oplus y_0, \beta^{(1)} \oplus y_1) = (\alpha \oplus \theta_1, \beta)^{f_k},$$

$$(\alpha,\beta)^{\prod_{i=1}^{2} f_{k_i} \oplus \theta_i} = (\beta^{\pi_{k_1}} \oplus \alpha \oplus \theta_1, (\beta^{\pi_{k_1}} \oplus \alpha)^{\pi_{k_2}} \oplus \beta \oplus \theta_1 \oplus \theta_2) = (\alpha^{(2)} \oplus y_1, \beta^{(2)} \oplus y_2).$$

Утверждение доказано.

Ключи, принадлежащие одному блоку импримитивности $A_k = \{k, k \oplus \vec{1}\}$, $k \in \overline{\{0, 2^{m-1} - 1\}}$, группы $S_2 \wr S_{2^{m-1}}$, будем называть 1-эквивалентными; также ключи $k^{(j)} = (k_1^{(j)}, \ldots, k_l^{(j)}) \in V_m{}^l$, $j = 1, 2$, будем называть 1-эквивалентными, если $k_i^{(1)}, k_i^{(2)}$ – 1-эквивалентны для любого $i \in \overline{\{1,l\}}$. Очевидно, что отношение 1-эквивалентности на множестве $V_m{}^l$ является отношением эквивалентности.

Предположим, что для l-раундового алгоритма шифрования Фейстеля с раундовыми функциями $f_{\pi_{k_i}}$, $i = \overline{1,l}$, удовлетворяющими условиям утверждения 1, ключи $k_1, \ldots, k_l$ выбираются случайно независимо и равновероятно из V_m. Опишем эквивалентные ключи такого алгоритма, где ключи считаются эквивалентными в смысле стандартного определения (см., например, [7]).

Следствие 1. Пусть выполнены условия утверждения 1, $l \geq 2$, $k = (k_1, \ldots, k_l) \in V_m{}^l$. Пусть также $\theta = (\theta_1, \ldots, \theta_l)$, $\theta' = (\theta'_1, \ldots, \theta'_l)$ – произвольные векторы из $\{\vec{0}, \vec{1}\}^l$. Тогда ключи $k + \theta$, $k + \theta'$ эквивалентны, если выполняются равенства: $\sum_{i=1}^{l-1} a_{l-i}(\theta_i \oplus \theta'_i) = \vec{0}$ и $\theta_l = \theta'_l$. Число эквивалентных ключей, являющихся также 1-эквивалентными, равно 2^{l-2}.

Доказательство. Условия $\sum_{i=1}^{l-1} a_{l-i}(\theta_i \oplus \theta'_i) = \vec{0}$ и $\theta_l = \theta'_l$ непосредственно следуют из равенства (1). Подсчитаем число эквивалентных ключей, являющихся также 1-эквивалентными, равное числу решений уравнения $\sum_{i=1}^{l-1} a_{l-i}\tilde{\theta}_i = \vec{0}$, и $\tilde{\theta}_l = \vec{0}$, где $\tilde{\theta}_i = \theta_i \oplus \theta'_i \in \{\vec{0}, \vec{1}\}$. Поскольку число нулей в последовательности $a_1, \ldots, a_{l-1}$ равно $\left\lfloor \frac{l-1}{3} \right\rfloor$, а число единиц – $l - 1 - \left\lfloor \frac{l-1}{3} \right\rfloor$, то число решений уравнения $\sum_{i=1}^{l-1} a_{l-i}\tilde{\theta}_i = \vec{0}$ равно $2^{\left\lfloor \frac{l-1}{3} \right\rfloor} \cdot 2^{l-1-\left\lfloor \frac{l-1}{3} \right\rfloor - 1} = 2^{l-2}$. Следствие доказано.

Следующий алгоритм при фиксированном открытом тексте $(\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t) \in V_{2m}$ и соответствующем шифртексте $(\alpha_1^{(l)},\beta_1^{(l)}),...,(\alpha_t^{(l)},\beta_t^{(l)})$, $l \geq 1$, полученном на неизвестном ключе $k = (k_1,...,k_l) \in {V_m}^l$, позволяет уменьшить трудоемкость определения ключа k по сравнению с полным перебором.

Пусть $i \geq 1$. На i-м этапе опробования по схеме выбора без возвращения из множества всех блоков импримитивности $A = \{A(k),\ k = \overline{0, 2^{m-1}}\}$ упорядоченно выбираем l блоков, $r_1^{(i)}, ..., r_l^{(i)}$. Полагаем $k_1^{(i)} = k_{r_1^{(i)}},...,k_l^{(i)} = k_{r_l^{(i)}}$, где $k_j^{(i)}$ – j-й опробуемый ключ на i-м этапе, $k_{r_j^{(i)}}$ – произвольный элемент из $A(r_j^{(i)})$, $j = \overline{1,l}$. Если $(\alpha_j,\beta_j)^{f_{k_1^{(i)}...k_l^{(i)}}} = (\alpha_j^{(l,i)},\beta_j^{(l,i)}) \in \left\{(\alpha_j^{(l)},\beta_j^{(l)}),(\alpha_j^{(l)},\beta_j^{(l)}) + \vec{1}\right\}$, где $f_{k_1^{(i)}...k_l^{(i)}} = \prod_{j=1}^{i} f_{k_j^{(i)}}$, для любого $j \in \{\overline{1,l}\}$, то найден представитель $k^{(i)} = (k_1^{(i)},...,k_l^{(i)})$ класса 1-эквивалентности, содержащего истинный ключ. В противном случае переходим к этапу i+1.

Из следствия 1 следует способ нахождения ключа из класса эквивалентности, содержащего истинный ключ, по данному представителю $k^{(i)} = (k_1^{(i)},...,k_l^{(i)})$ класса 1-эквивалентности, которому принадлежит k. Для этого

- если $\beta_j^{(l)} = \beta_j^{(l,i)}$, то полагаем $k_l = k_l^{(i)}$, иначе $k_l = k_l^{(i)} + \vec{1}$;
- если $\alpha_j^{(l)} = \alpha_j^{(l,i)}$, то полагаем $k_{l-1} = k_{l-1}^{(i)}$, иначе $k_{l-1} = k_{l-1}^{(i)} + \vec{1}$;
- полагаем $k_j = k_j^{(i)}$, $j = \overline{1,l-2}$.

Трудоемкость предложенного алгоритма равна $2^{l(m-1)}$ э.о. и в 2^l раз меньше трудоемкости полного перебора, равной 2^{lm} э.о., где э.о. – элементарная операция.

2. Свойства алгоритмов шифрования Фейстеля относительно группы $S_{2^n-1} \int S_2$

Пусть $(\alpha,\beta)^{f_k} = (\beta, \alpha \oplus \beta^{\pi_k})$. Для векторов $(\alpha, \beta) \in V_m$, удовлетворяющих сравнению $||\alpha|| \equiv ||\beta|| \pmod 2$, будем использовать обозначение $\alpha \sim_2 \beta$. Также обозначим

$$(\alpha,\beta) \xrightarrow{f} (\alpha',\beta'),$$

если $(\alpha,\beta)^f = (\alpha^{(l)},\beta^{(l)})$, $f \in \Phi_n$, и $\alpha^{(l)} \sim_2 \alpha'$, $\beta^{(l)} \sim_2 \beta'$.

Утверждение 2. Пусть $\pi \in S_{2^m-1} \int S_2$, $f_k \in \Phi_n$, $\alpha^{\pi_k} \in \{(\alpha \oplus k)^\pi, \alpha^\pi \oplus k\}$ для любого $k \in V_m$. Тогда для любого натурального числа l и любых $k_1, \ldots, k_l \in V_m$ справедливо включение:

1. $\left(\prod_{j=1}^{l} f_{k_j}\right)^3 \in S_{2^n-1} \int S_2$, если $l \not\equiv 0 \pmod 3$.
2. $\left(\prod_{j=1}^{l} f_{k_j}\right)^2 \in S_{2^n-1} \int S_2$, если $l \equiv 0 \pmod 3$.

Доказательство. Методом математической индукции нетрудно показать, что для любого $i \in N$ справедливы равенства:

$$(\alpha,\beta) \xrightarrow{f_{k_1}...f_{k_{3\cdot i}}} (\alpha \oplus w_1^{(3i)}(k_1,...,k_{3i}), \beta \oplus w_2^{(3i)}(k_1,...,k_{3i})),$$

$$(\alpha,\beta) \xrightarrow{f_{k_1}...f_{k_{3\cdot i+1}}} (\beta \oplus w_1^{(3i+1)}(k_1,...,k_{3i+1}), \alpha \oplus \beta \oplus w_2^{(3i+1)}(k_1,...,k_{3i+1})),$$

$$(\alpha,\beta) \xrightarrow{f_{k_1}...f_{k_{3\cdot i+2}}} (\alpha \oplus \beta \oplus w_1^{(3i+2)}(k_1,...,k_{3i+2}), \alpha \oplus w_2^{(3i+2)}(k_1,...,k_{3i+2})),$$

где $w_j^{(3i+v)} : V_m^{3i+v} \to \{0,1\}$ – некоторые аффинные функции, $v \in \{0, 1, 2\}$, $j \in \{1, 2\}$.

Рассмотрим три случая. Если $l \equiv 0 \pmod 3$, то

$$(\alpha,\beta) \xrightarrow{f_{k_1}...f_{k_l}} (\alpha \oplus w_1^{(l)}(k_1,...,k_l), \beta \oplus w_2^{(l)}(k_1,...,k_l)) \xrightarrow{f_{k_1}...f_{k_l}}$$
$$(\alpha \oplus w_1^{(l)}(k_1,...,k_l) \oplus w_1^{(l)}(k_1,...,k_l), \beta \oplus w_2^{(l)}(k_1,...,k_l) \oplus w_2^{(l)}(k_1,...,k_l)) \sim_2 (\alpha,\beta).$$

Если $l \equiv 1 \pmod 3$, то

$$(\alpha,\beta) \xrightarrow{f_{k_1}\dots f_{k_l}} (\beta \oplus w_1^{(l)}(k_1,\dots,k_l), \alpha \oplus \beta \oplus w_2^{(l)}(k_1,\dots,k_l)) \xrightarrow{f_{k_1}\dots f_{k_l}} (\alpha \oplus \beta \oplus w_2^{(l)}(k_1,\dots,k_l) \oplus w_1^{(l)}(k_1,\dots,k_l),$$

$$w_1^{(l)}(k_1,\dots,k_l) \oplus \alpha) \xrightarrow{f_{k_1}\dots f_{k_l}} (w_1^{(l)}(k_1,\dots,k_l) \oplus w_1^{(l)}(k_1,\dots,k_l) \oplus \alpha, \alpha \oplus \beta \oplus w_2^{(l)}(k_1,\dots,k_l) \oplus w_1^{(l)}(k_1,\dots,k_l) \oplus$$

$$\oplus w_1^{(l)}(k_1,\dots,k_l) \oplus \alpha \oplus w_2^{(l)}(k_1,\dots,k_l)) \sim_2 (\alpha,\beta).$$

Если $l \equiv 2 \pmod 3$, то

$$(\alpha,\beta) \xrightarrow{f_{k_1}\dots f_{k_l}} (\alpha \oplus \beta \oplus w_1^{(l)}(k_1,\dots,k_l), \alpha \oplus w_2^{(l)}(k_1,\dots,k_l)) \xrightarrow{f_{k_1}\dots f_{k_l}} (\beta \oplus w_2^{(l)}(k_1,\dots,k_l),$$

$$\alpha \oplus \beta \oplus w_1^{(l)}(k_1,\dots,k_l) \oplus w_2^{(l)}(k_1,\dots,k_l)) \xrightarrow{f_{k_1}\dots f_{k_l}} (\alpha,\beta).$$

Утверждение доказано.

Пусть $g_k = f_{k_1}\dots f_{k_l}$, где преобразования f_{k_j} удовлетворяют условию утверждения 2 для всех $j \in \{\overline{1,l}\}$, $l \geq 1$. Пусть также (α_1,β_1), …, (α_t, β_t) – неизвестный открытый текст длины $t \geq 1$, $(\alpha_1^{(l)},\beta_1^{(l)}),\dots,(\alpha_t^{(l)},\beta_t^{(l)})$ – известный шифртескт, где $(\alpha_i^{(l)},\beta_i^{(l)}) = (\alpha_i,\beta_i)^{g_k}$, $i = \overline{1,t}$.

Из утверждения 2 следует, что без знания ключа по известному шифртексту $(\alpha_1^{(l)},\beta_1^{(l)}),\dots,(\alpha_t^{(l)},\beta_t^{(l)})$ можно получить следующую информацию об открытом тексте:

1) если $l \equiv 0 \pmod 3$, то $(\alpha,\beta) \xrightarrow{g_k^2} (\alpha,\beta)$ и $(\alpha_i^{(l)},\beta_i^{(l)}) \xrightarrow{g_k} (\alpha_i,\beta_i)$ для любого $i = \{\overline{1,t}\}$;

2) если $l \not\equiv 0 \pmod 3$, то $(\alpha,\beta) \xrightarrow{g_k^3} (\alpha,\beta)$ и $(\alpha_i^{(l)},\beta_i^{(l)}) \xrightarrow{g_k^2} (\alpha_i,\beta_i)$ для любого $i = \{\overline{1,t}\}$;

3) если $l \equiv 2 \pmod 3$, то $\beta_i^{(l)} \oplus \beta_j^{(l)} \sim_2 \alpha_i \oplus \alpha_j$ и $\beta_i^{(l)} \oplus \beta_j^{(l)} \oplus \alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \beta_i \oplus \beta_j$ для любой пары $i, j \in \{\overline{1,t}\}$;

4) если $l \equiv 1 \pmod 3$, то $\alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \beta_i \oplus \beta_j$, и $\beta_i^{(l)} \oplus \beta_j^{(l)} \oplus \alpha_i^{(l)} \oplus \alpha_j^{(l)} \sim_2 \alpha_i \oplus \alpha_j$ для любой пары $i, j \in \{\overline{1,t}\}$;

5) если $l \equiv 0 \pmod 3$, то $\alpha_i^{(l)} \sim_2 \alpha_i$, $\beta_i^{(l)} \sim_2 \beta_i$ для любого $i \in \{\overline{1,t}\}$.

Утверждение 3. Для любых подстановок $s = (s_1, s_2) \in S(V_m) \times S(V_m)$, $\pi \in S(V_m)$, справедливо равенство

$$(\alpha,\beta)^{f_\pi^s} = \left(\beta^{s_2^{-1}s_1}, \left(\beta^{s_2^{-1}\pi} \oplus \alpha^{s_1^{-1}}\right)^{s_2}\right).$$

Доказательство следует из равенств

$$(\alpha,\beta)^{f_\pi^s} = \left(\alpha^{s_1^{-1}},\beta^{s_2^{-1}}\right)^{f_{\pi^s}} = \left(\beta^{s_2^{-1}},\beta^{s_2^{-1}\pi} + \alpha^{s_1^{-1}}\right)^s = \left(\beta^{s_2^{-1}s_1}, \left(\beta^{s_2^{-1}\pi} + \alpha^{s_1^{-1}}\right)^{s_2}\right).$$

Следствие 2. В условиях утверждения 2, если $s_2^{-1}s_1 \in S_{2^{m-1}} \int S_2$ и $(\alpha+\beta)^{s_2} \sim_2 \alpha^{s_2} \oplus \beta^{s_2}$ для любых $\alpha, \beta \in V_m$, то

$$(\alpha,\beta) \xrightarrow{f_\pi^s} \left(\beta, \beta^{s_2^{-1}\pi s_2} \oplus \alpha\right).$$

В частности, если $s_2 \in S_{2^{m-1}} \int S_2$ или $s_2 \in GL_m$, то соотношение $(\alpha \oplus \beta)^{s_2} \sim_2 \alpha^{s_2} \oplus \beta^{s_2}$ справедливо для любых $\alpha, \beta \in V_m$.

Доказательство следует из утверждения 3.

ЛИТЕРАТУРА

1. *Schneier B.* Applied Cryptography, Protocols, Algorithms, and Source Code in C. Second edition. New York: John Wiley and Sons, 1996.
2. *Pieprzyk J.*, *Zhang X.M.* Permutation generators of alternating groups // AUSCRYPT'90. 1990, LNCS 453.
3. *Caranti A., Volta F.D., Sala M., Villani F.* Imprimitive permutations groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis // Workshop on Coding and Cryptography, UC Cork. 2005.
4. *Paterson K.G.* Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers // FSE'99. 1999. LNCS 1636.
5. *Погорелов Б.А.*, *Пудовкина М.А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике, АК РФ. 2007. Т. 10.
6. *Погорелов Б.А.*, *Пудовкина М.А.* Линейные структуры групп подстановок векторных пространств // Труды 3-й Междунар. конф. «Проблемы безопасности и противодействия терроризму, 2007». М.: МЦНМО, 2008.
7. *Фомичев В.М.* Дискретная математика и криптология. М.: ЗАО «Диалог-МИФИ», 2003.