УДК 681.3 + 519.21

В.Г. СКОБЕЛЕВ, Э.Е. ЗАЙЦЕВА

АНАЛИЗ КЛАССА СЕМЕЙСТВ ЛЕГКО ВЫЧИСЛИМЫХ ПЕРЕСТАНОВОК

Ключевые слова: *поточные шифры, фракталы, конечные кольца, легко вычислимые перестановки*.

ВВЕДЕНИЕ

В последнее время значительное внимание уделяется приложению хаотических динамических систем к решению задач защиты информации [1], в частности при построении поточных шифров [2]. Общая схема нестационарного поточного шифра представлена на рис. 1. Предполагается, что задан генератор чисел, принадлежащих множеству $\mathbf{N}_m$, и класс алгоритмов $\mathbf{A} = \{A_i\}_{i \in \mathbf{N}_m}$, представленных в неявном виде. При генерации числа $i \in \mathbf{N}_m$ шифрование очередного фрагмента исходного текста осуществляется алгоритмом A_i.

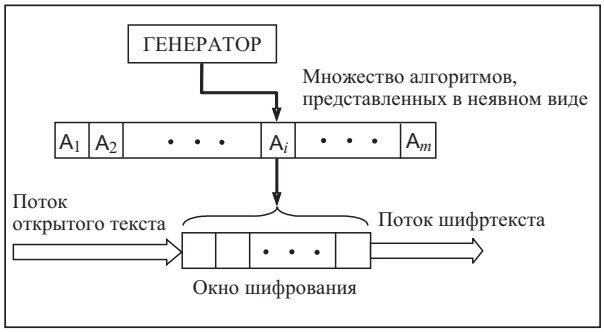


Рис. 1

Важной характеристикой широкого класса хаотических нелинейных динамических систем является наличие странных аттракторов. К ним относятся и фракталы, т.е. отображения, порождающие нерегулярные самоподобные структуры [3–5]. В [6] предложена следующая схема поточного шифра, основанного на применении фрактальных отображений. Сообщение (или изображение) представляется bmp-файлом, который последовательно обрабатывается пиксел за пикселом. При обработке каждого пиксела реализуется итерационный процесс, определяемый применяемым фрактальным отображением. При выполнении (либо нарушении) некоторого заданного условия осуществляется определяемая номером последней итерации перестановка на множестве цветов. Обработанный файл и представляет собой шифртекст. Корректность указанного подхода вытекает из обратимости перестановок. Предложенная схема реализована для одного из наиболее изученных фрактальных отображений — отображения Мандельброта [5], т.е. отображения $f: \mathbf{C} \to \mathbf{C}$ ($\mathbf{C}$ — множество комплексных чисел), определяемого равенством $f(z) = z^2 + c$ (c — константа) (рис. 2: *а* — комплексная плоскость; *б* — изображение на дисплее). Параметры шифра, определяющие число итераций, — это радиус R круга (R, O) и верхняя граница числа K итераций, применяемых к точке комплексной плоскости $\mathbf{C}$. Условие состоит в выходе образа за круг (R, O) в течение K итераций. Класс семейств перестановок определен равенствами:

$$\mathbf{f}_n: \begin{cases} r_n = (r_0 + n \cdot |\alpha_1^n \cdot a_1 - \alpha_2^n \cdot a_2 - \alpha_3^n \cdot a_3|) \pmod{256}, \\ g_n = (g_0 + n \cdot |\alpha_2^n \cdot a_2 - \alpha_1^n \cdot a_1 - \alpha_3^n \cdot a_3|) \pmod{256} \quad (n = 1, \ldots, 2^8 - 1), \\ b_n = (b_0 + n \cdot |\alpha_3^n \cdot a_3 - \alpha_1^n \cdot a_1 - \alpha_2^n \cdot a_2|) \pmod{256}. \end{cases} \quad (1)$$

Здесь r_0, g_0, b_0 и r_n, g_n, b_n — соответственно исходные и преобразованные компоненты цвета пиксела, а $\alpha_i, a_i \in \mathbf{Z}$ $(i = 1, 2, 3)$ — параметры, играющие роль секретного ключа. Рассмотренная схема — специальный случай нестационарного поточного шифра, для которого управление выбором алгоритма A_i $(i \in \mathbf{N}_m)$ осуществляется на основе динамических фрактальных отображений.

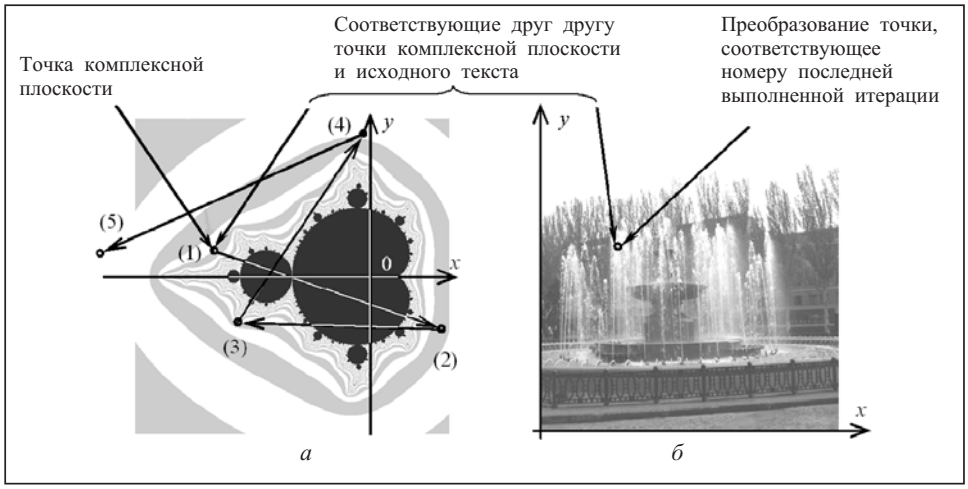


Рис. 2

При построении современных стандартов шифрования [7–10] наблюдается устойчивая тенденция к применению конечных алгебраических систем. Поэтому естественно перейти к перестановкам, определенным в терминах конечного кольца $Z_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ [7, 11] (p — простое число, $k \in \mathbf{N}$, а операции $\oplus$ и $\circ$ определены равенствами $a \oplus b = a + b \pmod{p^k}$ и $a \circ b = a \cdot b \pmod{p^k}$ для всех $a, b \in \mathbf{Z}_{p^k}$). Таким аналогом для (1) является класс семейств перестановок

$$\begin{cases} x_n^{(1)} = x_0^{(1)} \Theta n \circ \left(\overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \Theta 2 \circ \alpha_l^n \circ a_1 \right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (n = 1, \ldots, p^k - 1), \\ x_n^{(l)} = x_0^{(l)} \Theta n \circ \left(\overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \Theta 2 \circ \alpha_l^n \circ a_l \right) \end{cases} \tag{2}$$

где $\mathbf{x}_t = (x_t^{(1)}, \ldots, x_t^{(l)})^{\mathrm{T}} \in \mathbf{Z}_{p^k}$ $(t = 0, 1, \ldots, p^k - 1)$. Авторами был реализован поточный шифр, в котором управление классом перестановок (2) в случае, когда $p = 2$, $k = 8$ и $l = 3$, осуществляется отображением Мандельброта. Алгоритм реализован в среде Microsoft Visual C++ с использованием MFC App Wizard. В качестве примеров работы программы приведем результаты шифрования текста и изображения. Текстовому файлу объемом 64 Кбайт соответствует bmp-файл, изображенный на рис. 3, *а*. Зашифрованный bmp-файл того же размера (рис. 3, *б*) переводится в шифртекст.

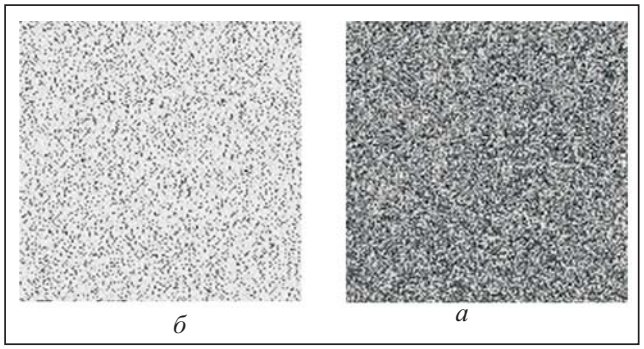
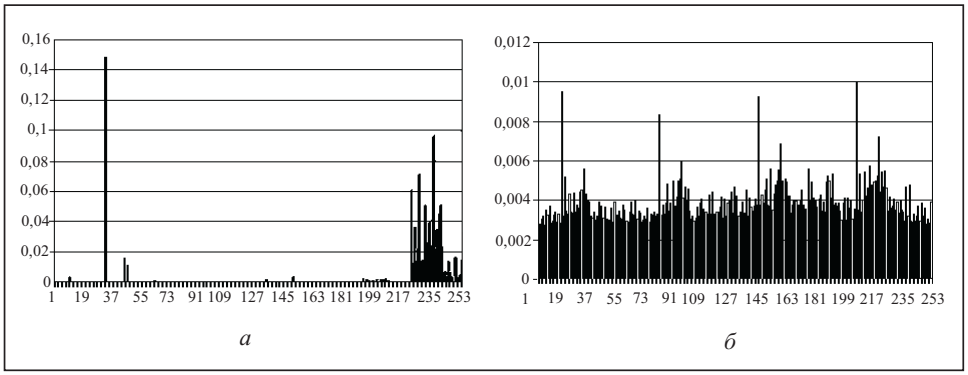


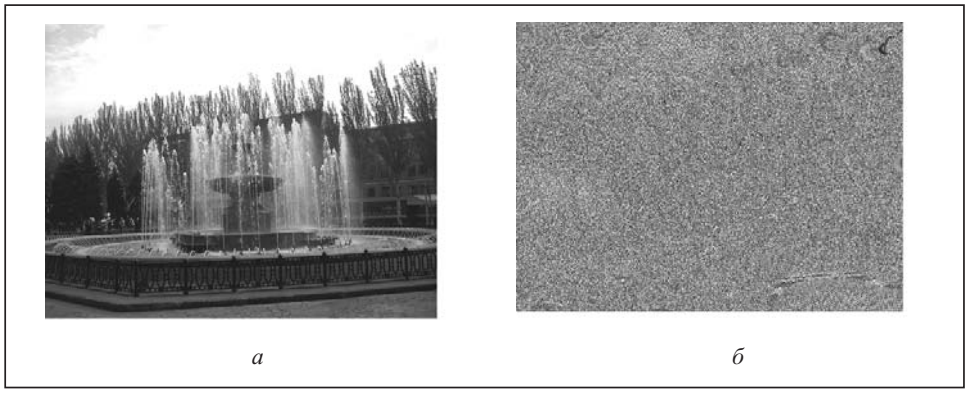
Рис. 3

Гистограммы распределения частот букв в исходном (*а*) и зашифрованном (*б*) текстовых файлах представлены на рис. 4. На рис. 5 приведен пример шифрования изображения: *а* — исходное; *б* — зашифрованное.



а *б*

Рис. 4



а *б*

Рис. 5

Перспективность и эффективность предложенного подхода обосновывает актуальность исследования классов семейств легко вычислимых перестановок, определенных в терминах кольца Z_{p^k}.

Цель настоящей работы — исследование класса семейств легко вычислимых перестановок, являющихся естественным обобщением класса (2). Структура работы следующая: разд. 1 содержит основные определения; в разд. 2 охарактеризована структура исследуемого класса семейств легко вычислимых перестановок, определенных в терминах кольца Z_{p^k}; в разд. 3 исследована сложность идентификации семейства перестановок, принадлежащих рассматриваемому классу. Заключение содержит ряд выводов.

1. ОСНОВНЫЕ ПОНЯТИЯ

Пусть S — конечное множество, а P_S — множество всех перестановок множества S. Если $S = \underset{i=1}{\overset{l}{\times}} S_i$ $(l>1)$, где $|S_i|>1$ $(i \in \mathbf{N}_l)$ и $\boldsymbol{f} = (f_1, \ldots, f_l)$, где $f_i \in P_{S_i}$ $(i \in \mathbf{N}_l)$, причем $\boldsymbol{f}(\mathbf{s}) = (f_1(s_1), \ldots, f_l(s_l))$ для всех $\mathbf{s} = (s_1, \ldots, s_l) \in S$, то перестановку $\boldsymbol{f} \in P_S$ назовем l-разложимой. Обозначим P_S^{l-s} множество всех l-разложимых перестановок множества S. Следуя [12], будем считать, что объем памяти v_S, необходимой для хранения любого элемента множества S, равен $O(\log |S|)$ $(|S| \to \infty)$. Перестановку $f \in P_S$ назовем легко вычислимой, если для любого

элемента $s \in S$ асимптотическая емкостная и временна́я сложность алгоритма A_j, реализующего перестановку f, соответственно равна $V_f = O(\log |S|)$ $(|S| \to \infty)$ и $T_f = O(\log^2 |S|)$ $(|S| \to \infty)$. Пусть P_S^{ec} — множество всех легко вычислимых перестановок $f \in P_S$.

Утверждение 1. Пусть $S = \underset{i=1}{\overset{l}{\times}} S_i$ $(l > 1)$, где $|S_i| > 1$ $(i \in \mathbf{N}_l)$ и $f_i \in P_{S_i}^{ec}$ $(i \in \mathbf{N}_l)$. Тогда $\boldsymbol{f} = (f_1, \ldots, f_l) \in P_S^{ec}$.

Доказательство. Предположим, что $f_i \in P_{S_i}^{ec}$ для всех $i \in \mathbf{N}_l$. Асимптотическая временна́я и емкостная сложность вычисления образа любого элемента $s_i \in S_i$ $(i \in \mathbf{N}_l)$ равна соответственно $T_{f_i} = O(\log^2 |S_i|)$ и $V_{f_i} = O(\log |S_i|)$. Так как вычисление $\boldsymbol{f}(\mathbf{s})$ $(\mathbf{s} = (s_1, \ldots, s_l) \in S)$ можно свести к независимым вычислениям $f_i(s_i)$ $(i \in \mathbf{N}_l)$, то

$$T_{\boldsymbol{f}} \le \sum_{i=1}^{l} T_{f_i} = O\left(\sum_{i=1}^{l} \log^2 |S_i|\right) = O\left(\left(\log \prod_{i=1}^{l} |S_i|\right)^2\right) = O(\log^2 |S|) \ (|S| \to \infty),$$

что и требовалось показать.

Поскольку $\mathbf{s} = (s_1, \ldots, s_l)$ и $V_{f_i} = O(\log |S_i|)$ $(i \in \mathbf{N}_l)$, то

$$V_{\boldsymbol{f}} = O\left(\sum_{i=1}^{l} V_{f_i}\right) = O\left(\sum_{i=1}^{l} \log |S_i|\right) = O(\log |S|) \ (|S| \to \infty).$$

Утверждение доказано.

Семейство легко вычислимых перестановок $S = \{f_j\}_{j \in \mathbf{N}}$ $(f_j \in P_S^{ec})$ назовем легко вычислимым, если существует такой алгоритм последовательной генерации элементов семейства S, что: 1) генерация алгоритма A_{f_1} осуществляется за время $T = O(\log |S|)$ $(|S| \to \infty)$; 2) преобразование алгоритма A_{f_j} $(j \in \mathbf{N})$ в алгоритм $A_{f_{j+1}}$ осуществляется за время $O(\log^2 |S|)$ $(|S| \to \infty)$.

Пусть $\mathbf{Z}_{p^k}^{inv}$ — множество всех обратимых элементов кольца Z_{p^k}, т.е. $(\mathbf{Z}_{p^k}^{inv}, \circ)$ — мультипликативная группа кольца Z_{p^k}. Отметим, что критерий принадлежности элемента $a \in \mathbf{Z}_{p^k}$ множеству $\mathbf{Z}_{p^k}^{inv}$ имеет вид $a \in \mathbf{Z}_{p^k}^{inv} \Leftrightarrow a \not\equiv 0 \pmod p$ (см., например, [13]).

Пусть l $(2 < l \le k)$ — такое фиксированное число, что $(l-2) \pmod{p^k} \in \mathbf{Z}_{p^k}^{inv}$. Зафиксируем элементы $\alpha_i, \beta_i, a_i \in \mathbf{Z}_{p^k}^{inv}$ $(i \in \mathbf{N}_l)$ кольца Z_{p^k}. Положим $A_i(n) = \underset{j=1}{\overset{l}{\oplus}} a_j \circ \alpha_j^n \ominus 2 \circ a_i \circ \alpha_i^n$ $(i \in \mathbf{N}_l, n \in \mathbf{N})$. Определим однопараметрические семейства аффинных отображений $S^{(i)} = \{f_n^{(i)} : \mathbf{Z}_{p^k} \to \mathbf{Z}_{p^k} \mid n \in \mathbf{N}\}$ $(i \in \mathbf{N}_l)$ равенством

$$f_n^{(i)}(x) = \beta_i^n \circ x \oplus n \pmod{p^k} \circ A_i(n) \ (x \in \mathbf{Z}_{p^k}, n \in \mathbf{N}). \tag{3}$$

Так как $\beta_i \in \mathbf{Z}_{p^k}^{inv}$ $(i \in \mathbf{N}_l)$, то $f_n^{(i)} \in P_{\mathbf{Z}_{p^k}}$ $(i \in \mathbf{N}_l, n \in \mathbf{N})$. Генерация алгоритма $A_{f_1^{(i)}}$ $(i \in \mathbf{N}_l)$ осуществляется за время $T_{f_1^{(i)}} = O(k \cdot \lceil \log p \rceil)$, а временна́я и емкостная сложность алгоритма $A_{f_1^{(i)}}$ $(i \in \mathbf{N}_l)$ равна соответственно $T_{f_1^{(i)}} = O((k \cdot \lceil \log p \rceil)^2)$ и $V_{f_1^{(i)}} = O(k \cdot \lceil \log p \rceil)$. При вычисленных значениях α_i^n, β_i^n $(i \in \mathbf{N}_l)$ преобразование алгоритма $A_{f_n^{(i)}}$ в алгоритм $A_{f_{n+1}^{(i)}}$ $(i \in \mathbf{N})$ осуществляется за время $T_{f_{n+1}^{(i)}} = O((k \cdot \lceil \log p \rceil)^2)$, а временна́я и емкостная сложность алгоритма $A_{f_{n+1}^{(i)}}$ $(i \in \mathbf{N}_l)$ рав-

на соответственно $T_{f_{n+1}^{(i)}} = O((k \cdot \lceil \log p \rceil)^2)$ и $V_{f_{n+1}^{(i)}} = O(k \cdot \lceil \log p \rceil)$. Следовательно, каждое семейство перестановок $S^{(i)}$ $(i \in \mathbf{N}_l)$ легко вычислимое.

Зафиксируем перестановку $h \in P_{\mathbf{N}_l}$. Определим семейство $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ отображений $\mathbf{f}_n : \mathbf{Z}_{p^k}^l \to \mathbf{Z}_{p^k}^l$ $(n \in \mathbf{N})$ следующим образом: для всех $\mathbf{x} = (x_1, \ldots, x_l)^{\mathrm{T}} \in \mathbf{Z}_{p^k}^l$

$$\mathbf{f}_n(\mathbf{x}) = (f_n^{(1)}(x_{h^n(1)}), \ldots, f_n^{(l)}(x_{h^n(l)}))^{\mathrm{T}}.$$

Ясно, что $\mathbf{f}_n \in P_{\mathbf{Z}_{p^k}^l}^{l-s} \cap P_{\mathbf{Z}_{p^k}^l}^{ec}$ $(n \in \mathbf{N})$.

Предметом исследования и является класс $\boldsymbol{K}$ таких $(3 \cdot l + 1)$-параметрических семейств перестановок $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$, что $h \in P_{\mathbf{N}_l}$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_l) \in (\mathbf{Z}_{p^k}^{inv})^l$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_l) \in (\mathbf{Z}_{p^k}^{inv})^l$ и $\mathbf{a} = (a_1, \ldots, a_l) \in (\mathbf{Z}_{p^k}^{inv})^l$. Так как l $(2 < l \le k)$ — фиксированное число, то из утверждения 1 вытекает, что $\boldsymbol{K}$ — легко вычислимый класс семейств перестановок. Схемная реализация класса $\boldsymbol{K}$ представлена на рис. 6.

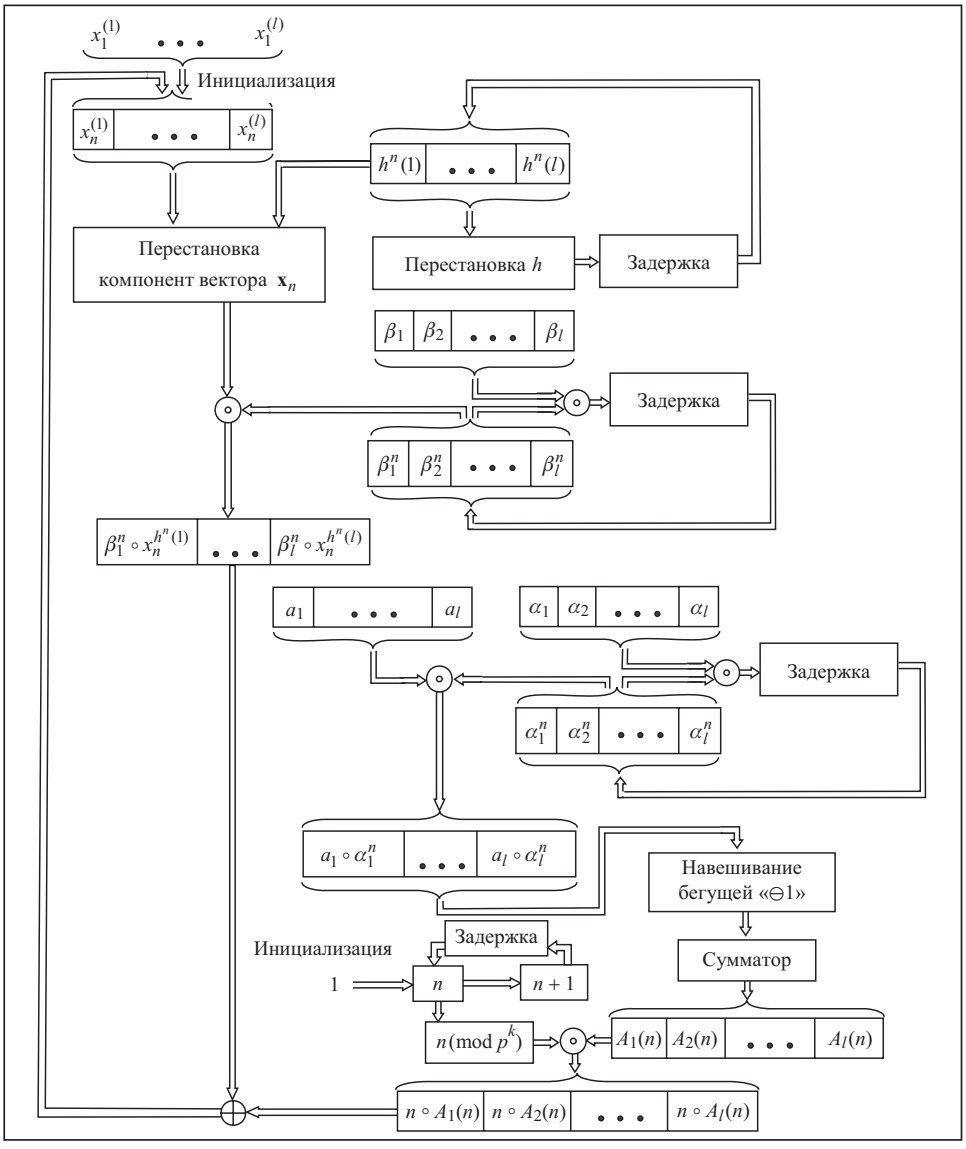


Рис. 6

2. СТРУКТУРА КЛАССА K

Отметим следующие свойства перестановок $f_n^{(i)} \in P^{ec}_{\mathbf{Z}_{p^k}}$ $(i \in \mathbf{N}_l, n \in \mathbf{N})$, определенных равенством (3).

Утверждение 2. Пусть $\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}^{inv}_{p^k}$ и $a_1 = \ldots = a_l = a \in \mathbf{Z}^{inv}_{p^k}$. В этом случае:

1) $f_i^{(n)} = f_n^{(j)}$ $(i, j \in \mathbf{N}_l, i \neq j)$ тогда и только тогда, когда $\beta_i^n = \beta_j^n$;

2) для каждого значения $n \in \mathbf{N}$ множество неподвижных точек перестановки $f_n^{(i)}$ $(i \in \mathbf{N}_l)$ совпадает со множеством решений уравнения

$$(1 \Theta \beta_i^n) \circ x = n \pmod{p^k} \circ (l-2) \circ a \circ \alpha^n. \tag{4}$$

Доказательство. Пусть $\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}^{inv}_{p^k}$ и $a_1 = \ldots = a_l = a \in \mathbf{Z}^{inv}_{p^k}$. Тогда равенства (3) принимают вид

$$f_n^{(i)}(x) = \beta_i^n \circ x \oplus n \pmod{p^k} \circ (l-2) \circ a \circ \alpha^n \quad (i \in \mathbf{N}_l). \tag{5}$$

Следовательно,

$$f_n^{(i)} = f_n^{(j)} \Leftrightarrow (\forall x \in \mathbf{Z}_{p^k})(f_n^{(i)}(x) = f_n^{(j)}(x)) \Leftrightarrow$$

$$\Leftrightarrow (\forall x \in \mathbf{Z}_{p^k})((\beta_i^n \Theta \beta_j^n) \circ x = 0) \Leftrightarrow \beta_i^n = \beta_j^n,$$

что и требовалось показать.

Пусть $x \in \mathbf{Z}_{p^k}$ — неподвижная точка перестановки $f_n^{(i)}$ $(i \in \mathbf{N}_l)$. Положим $f_n^{(i)}(x) = x$ в равенстве (5). Получим (4), что и требовалось показать.

Утверждение доказано.

Следствие 1. Пусть $\alpha_1 = \ldots = \alpha_l = \alpha \in \mathbf{Z}^{inv}_{p^k}$, $a_1 = \ldots = a_l = a \in \mathbf{Z}^{inv}_{p^k}$, $1 \Theta \beta_i^n \neq 0$, $n \pmod{p^k} \neq 0$ и r_1, r_2 — такие максимальные натуральные числа, что $1 \Theta \beta_i^n \equiv$ $\equiv 0 \pmod{p^{r_1}}$ и $n \pmod{p^k} \circ (l-2) \equiv 0 \pmod{p^{r_2}}$. Если $r_1 > r_2$, то перестановка $f_n^{(i)}$ не имеет неподвижных точек.

Истинность следствия 1 вытекает из того, что при сделанных предположениях уравнение (4) не имеет решений.

Пусть φ — функция Эйлера. Так как $\varphi(p^k) = p^k - p^{k-1}$, то показателями (по модулю p^k) элементов множества $\mathbf{Z}^{inv}_{p^k}$ могут быть только числа $p-1$, p^i и $(p-1) \cdot p^i$ $(i \in \mathbf{N}_{k-1})$.

Утверждение 3. Если $a_1 = \ldots = a_l = a \in \mathbf{Z}^{inv}_{p^k}$, то перестановка $f^{(i)}_{\varphi(p^k)}$ $(i \in \mathbf{N}_l)$ имеет неподвижные точки тогда и только тогда, когда $l-2 \equiv 0 (\text{mod } p)$.

Доказательство. Положим $a_1 = \ldots = a_l = a \in \mathbf{Z}^{inv}_{p^k}$ и $n = \varphi(p^k)$ в (3). Получим

$$f^{(i)}_{\varphi(p^k)}(x) = x \Theta p^{k-1} \circ (l-2) \circ a. \tag{6}$$

Положим $f^{(i)}_{\varphi(p^k)}(x) = x$ в (6). Получим $p^{k-1} \circ (l-2) \circ a = 0$. Последнее равенство истинно тогда и только тогда, когда $l-2 \equiv 0 (\text{mod } p)$.

Утверждение доказано.

Обозначим через ξ_i и ζ_i $(i \in \mathbf{N}_l)$ показатели (по модулю p^k) элементов β_i и α_i соответственно. Положим $[\xi_1, \ldots, \xi_l] = \delta$ и $[\zeta_1, \ldots, \zeta_l] = \lambda$ и $[\delta, \lambda] = \gamma$.

Из (3) вытекает, что для всех $i \in \mathbf{N}_l$

$$f^{(i)}_{m \cdot \delta}(x) = x \oplus (m \cdot \delta) (\text{mod } p^k) \circ A_i(m \cdot \delta) \quad (m \in \mathbf{N}), \tag{7}$$

$$f^{(i)}_{m\cdot\lambda}(x)=\beta_i^{m\cdot\lambda}\circ x\oplus(m\cdot\lambda)(\mathrm{mod}\,p^k)\circ\left(\bigoplus_{j=1}^{l}a_j\Theta 2\circ a_i\right)\ (m\in\mathbf{N}),\tag{8}$$

$$f^{(i)}_{m\cdot\gamma}(x)=x\oplus(m\cdot\gamma)(\mathrm{mod}\,p^k)\circ\left(\bigoplus_{j=1}^{l}a_j\Theta 2\circ a_i\right)\ (m\in\mathbf{N}).\tag{9}$$

Из (7)–(9) вытекает, что: 1) перестановка $f^{(i)}_{m\cdot\delta}$ $(i\in\mathbf{N}_l)$ не имеет неподвижных точек тогда и только тогда, когда $(m\cdot\delta)(\mathrm{mod}\ p^k)\circ A_i(m\cdot\delta)\neq 0$; 2) перестановка $f^{(i)}_{m\cdot\delta}$ $(i\in\mathbf{N}_l)$ тождественная тогда и только тогда, когда $(m\cdot\delta)(\mathrm{mod}\ p^k)\circ A_i(m\cdot\delta)=0$; 3) если $\bigoplus\limits_{j=1}^{l}a_j\Theta 2\circ a_i=0$ $(i\in\mathbf{N}_l)$, то множество неподвижных точек перестановки $f^{(i)}_{m\cdot\lambda}$ совпадает со множеством решений уравнения $(\beta_i^{m\cdot\lambda}\Theta 1)\circ x=0$; 4) если $\bigoplus\limits_{j=1}^{l}a_j\Theta 2\circ a_i=0$, то $f^{(i)}_{m\cdot\gamma}$ $(i\in\mathbf{N}_l)$ — тождественная перестановка.

Представим семейство перестановок $\boldsymbol{S}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)\in\boldsymbol{K}$ в явном виде:

$$\begin{cases}x^{(1)}_{n+1}=\beta_1^n\circ x_n^{h^n(1)}\oplus n(\mathrm{mod}\ p^k)\circ A_1(n),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ x^{(l)}_{n+1}=\beta_l^n\circ x_n^{h^n(l)}\oplus n(\mathrm{mod}\ p^k)\circ A_l(n),\end{cases}\tag{10}$$

где $A_i(n)=\bigoplus\limits_{j=1}^{l}a_j\circ\alpha_j^n\Theta 2\circ a_i\circ\alpha_i^n$ $(i\in\mathbf{N}_l,n\in\mathbf{N})$, $\beta_i,a_i,\alpha_i\in\mathbf{Z}^{inv}_{p^k}$ $(i\in\mathbf{N}_l)$ и $h\in P_{\mathbf{N}_l}$.

Для любых фиксированных чисел $n_0,n_1\in\mathbf{N}$ $(n_1\geq n_0)$ положим

$$\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)=\{\mathbf{f}_n\}_{n\in\mathbf{N}_{n_1}\setminus\mathbf{N}_{n_0-1}}.$$

Образом элемента $\mathbf{x}_0=(x_0^{(1)},\ldots,x_0^{(l)})^{\mathrm{T}}\in\mathbf{Z}^l_{p^k}$ при действии семейства $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ назовем последовательность

$$\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)(\mathbf{x})=\mathbf{x}_1\ldots\mathbf{x}_{n_1-n_0+1},$$

где $\mathbf{x}_i=(x_i^{(1)},\ldots,x_i^{(l)})^{\mathrm{T}}=\mathbf{f}_{n_0+i-1}(\mathbf{x}_{i-1})$ $(i\in\mathbf{N}_{n_1-n_0+1})$. Будем говорить, что $\mathbf{x}_0\in\mathbf{Z}^l_{p^k}$ — неподвижная точка для семейства $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ тогда и только тогда, когда $\mathbf{x}_i=\mathbf{x}_0$ для всех $i\in\mathbf{N}_{n_1-n_0+1}$.

Теорема 1. Пусть p — нечетное простое число. Тогда для всех $\boldsymbol{S}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)\in\boldsymbol{K}$ поиск семейства $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$ $(n\leq n_0)$, обладающего заданной неподвижной точкой $\mathbf{x}_0\in\mathbf{Z}^l_{p^k}$, при условии, что $n_0,n_1\in\mathbf{N}$ не являются показателями (по модулю p^k) ни одного из чисел $\alpha_i,\beta_i\in\mathbf{N}^{inv}_{p^k}$ $(i\in\mathbf{N}_l)$, сводится к решению системы многостепенных диофантовых уравнений с $2\cdot l$ неизвестными с последующей проверкой для каждого ее решения разрешимости $2\cdot l$ задач дискретного логарифмирования.

Доказательство. Пусть $\mathbf{x}_0\in\mathbf{Z}^l_{p^k}$ — неподвижная точка для семейства $\boldsymbol{S}_{n_0,n_1}(\boldsymbol{\alpha},\boldsymbol{\beta},\mathbf{a},h)$. Тогда $\mathbf{f}_{n_0+i-1}(\mathbf{x}_{i-1})=\mathbf{x}_0$ для всех $i\in\mathbf{N}_{n_1-n_0+1}$. Из (10) получим, что для всех $i\in\mathbf{N}_{n_1-n_0+1}$

$$(n_0+i-1)(\mathrm{mod}\ p^k)\circ A_j(n_0+i-1)\oplus\beta_j^{n_0+i-1}\circ x_0^{h^{n_0+i-1}(j)}=x_0^{(j)}\ \ (j\in\mathbf{N}_l).\tag{11}$$

Положив в (11)

$$u_j = \alpha_j^{n_0} \quad (j \in \mathbf{N}_l), \tag{12}$$

$$v_j = \beta_j^{n_0} \quad (j \in \mathbf{N}_l), \tag{13}$$

получим систему многостепенных диофантовых уравнений с $2 \cdot l$ неизвестными u_j, v_j $(j \in \mathbf{N}_l)$. Каждое решение этой системы диофантовых уравнений приводит к $2 \cdot l$ задачам дискретного логарифмирования, определяемым (12) и (13). Решение этой системы задач дискретного логарифмирования и определяет искомое семейство $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$.

Теорема доказана.

Отметим, что включение перестановки $h \in P_{\mathbf{N}_l}$ в число параметров, определяющих семейство перестановок $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$, целесообразно по следующим причинам. Во-первых, применение конструкции, предложенной в [14], дает возможность систематически строить перестановки $h \in P_{\mathbf{N}_l}$ порядка $e^{O(\sqrt{l})}$ $(l \to \infty)$, что приводит к существенному росту порядка перестановок $\mathbf{f}_n$ $(n \in \mathbf{N})$, формирующих семейство $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$. Во-вторых, существенно усложняется система многостепенных диофантовых уравнений, конструируемых при доказательстве теоремы 1. В-третьих, разрушается регулярность представления множества неподвижных точек семейства $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ $(n_0 \le n_1)$.

Следующая теорема показывает, что для кольца Z_{2^k} можно выделить достаточно широкий класс семейств $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$, не имеющих неподвижных точек.

Теорема 2. Пусть $p = 2$, $\beta_i = 1$ $(i \in \mathbf{N}_l)$, l — нечетное число и $k \ge 3$. Тогда для всех $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, e) \in \boldsymbol{K}$ $(e \in P_{\mathbf{N}_l}$ — тождественная перестановка) ни одно семейство $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, e)$ $(n_0 \le n_1 < 2^k)$ не имеет неподвижных точек.

Доказательство. Пусть $p = 2$, $\beta_i = 1$ $(i \in \mathbf{N}_l)$, l — нечетное число, $k \ge 3$ и $e \in P_{\mathbf{N}_l}$ — тождественная перестановка.

Предположим противное, т.е. что существует неподвижная точка $\mathbf{x}_0 \in \mathbf{Z}_{2^k}^l$ для семейства $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, e)$ $(n_0 \le n_1 < 2^k)$. Из (10) получим, что для всех $i \in \mathbf{N}_{n_1 - n_0 + 1}$

$$(n_0 + i - 1) \,(\mathrm{mod}\, 2^k) \circ A_j(n_0 + i - 1) = 0 \quad (j \in \mathbf{N}_l).$$

Так как $a_i, \alpha_i \in \mathbf{Z}_{2^k}^{inv}$ $(i \in \mathbf{N}_l)$, то a_i, α_i $(i \in \mathbf{N}_l)$ — нечетные числа, а поскольку l — нечетное число, то $A_i(n) \ne 0$ $(i \in \mathbf{N}_l)$ для всех $n \in \mathbf{N}$. Следовательно, $n \circ A_i(n) \ne 0$ $(i \in \mathbf{N}_l)$ для всех $n \in \mathbf{N}_{n_1}$. Полученное противоречие означает, что предположение ложное. Отсюда вытекает, что ни одно семейство $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, e)$ $(n_0 \le n_1 < 2^k)$ не имеет неподвижных точек.

Теорема доказана.

3. ИДЕНТИФИКАЦИЯ СЕМЕЙСТВА $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$

Рассмотрим задачи идентификации семейства перестановок $\boldsymbol{S}_{n_0, n_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ при условии, что экспериментатору доступны некоторые точки съема информации и/или управления алгоритмом, реализующим перестановки $\mathbf{f}_n$ $(n \in \mathbf{N})$.

Теорема 3. Пусть известны значения векторов параметров $\mathbf{a}$ и $\boldsymbol{\alpha}$. Если в момент $n_0 \in \mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим перестановку $\mathbf{f}_{n_0}$, и наблюдать соответствующий выход, то идентификация вектора параметров $\boldsymbol{\beta}$ сводится к независимому решению l задач дискретного логарифмирования.

Доказательство. Предположим, что известны значения векторов параметров $\mathbf{a}, \boldsymbol{\alpha}$ и в момент $n_0 \in \mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим перестановку $\mathbf{f}_{n_0}$ и наблюдать соответствующий выход.

Выберем в качестве входа алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$, вектор $\mathbf{x}_{n_0} = (\underbrace{1,\ldots,1}_{l})^{\mathrm{T}}$. Из системы (10) получим следующую систему уравнений относительно неизвестных $\beta_1,\ldots,\beta_l \in \mathbf{Z}_{p^k}^{inv}$:

$$\begin{cases} \beta_1^{n_0} = x_{n_0+1}^{(1)} \Theta n_0 \pmod{p^k} \circ A_1(n_0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_l^{n_0} = x_{n_0+1}^{(l)} \Theta n_0 \pmod{p^k} \circ A_l(n_0). \end{cases} \tag{14}$$

Решение системы (14) сводится к независимому решению l задач дискретного логарифмирования.

Теорема доказана.

Теорема 4. Пусть p — нечетное простое число и известны значения векторов параметров $\mathbf{a}$ и $\boldsymbol{\beta}$. Если в момент $n_0 \in \mathbf{N}$, где $n_0 \pmod{p^k} \in \mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров $\boldsymbol{\alpha}$ сводится к независимому решению l задач дискретного логарифмирования.

Доказательство. Предположим, что p — нечетное простое число, известны значения векторов параметров $\mathbf{a}, \boldsymbol{\beta}$ и в момент $n_0 \in \mathbf{N}$ ($n_0 \pmod{p^k} \in \mathbf{Z}_{p^k}^{inv}$) экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$.

Из системы (10) получим следующую систему уравнений относительно неизвестных $\alpha_1,\ldots,\alpha_l \in \mathbf{Z}_{p^k}^{inv}$:

$$\begin{cases} \bigoplus\limits_{j=1}^{l} a_j \circ \alpha_j^{n_0} \Theta 2 \circ a_1 \circ \alpha_1^{n_0} = \gamma_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \bigoplus\limits_{j=1}^{l} a_j \circ \alpha_j^{n_0} \Theta 2 \circ a_l \circ \alpha_l^{n_0} = \gamma_l, \end{cases} \tag{15}$$

где $\gamma_i = (n_0 \pmod{p^k})^{-1} \circ (x_{n_0+1}^{(i)} \Theta \beta_i^{n_0} \circ x_{n_0}^{h^{n_0}(i)})$ $(i \in \mathbf{N}_l)$.

Так как

$$\Delta = \begin{vmatrix} \Theta a_1 & a_2 & \ldots & a_l \\ a_1 & \Theta a_2 & \ldots & a_l \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & \Theta a_l \end{vmatrix} = a_1 \circ \ldots \circ a_l \circ 2^{l-1} \circ (p^k - l + 2) \in \mathbf{Z}_{p^k}^{inv},$$

то система (15) эквивалентна системе

$$\begin{cases} a_1^{n_0} = c_1, \\ \ldots\ldots\ldots \\ a_l^{n_0} = c_l. \end{cases} \tag{16}$$

Решение системы (16) сводится к независимому решению l задач дискретного логарифмирования.

Теорема доказана.

Следствие 2. Пусть p — нечетное простое число и известны значения векторов параметров $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$. Если в момент $n_0 \in \mathbf{N}$, где $n_0 \,(\mathrm{mod}\ p^k) \in \mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего перестановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров **a** сводится к решению линейной системы уравнений.

Доказательство. Идентификация вектора параметров **a** сводится к решению линейной системы уравнений (15) относительно неизвестных $a_1, \ldots, a_l \in \mathbf{Z}_{p^k}^{inv}$.

Следствие доказано.

Следующая теорема показывает, что сложность задач идентификации существенно возрастает даже для семейства перестановок (2) в случае кольца Z_{2^k}, если это семейство встроено в поточный шифр, построенный на основе динамического фрактала, экспериментатор имеет только возможность анализировать исходный текст и шифртекст, и требуется идентифицировать два из трех векторов $\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}$ параметров.

Теорема 5. Пусть в шифр, построенный на основе динамического фрактала, встроено семейство перестановок (2) над кольцом Z_{2^k} $(k \ge 3)$, где $l\,(3 \le l \le k)$ — нечетное число. Тогда идентификация вектора параметров $(\mathbf{a}, \boldsymbol{\alpha})$ семейства (2) сводится к решению экспоненциального числа задач дискретного логарифмирования.

Доказательство. Предположим, что известны соответствующие пары $(\mathbf{x}_0, \mathbf{x}_n)$, $(n \in \mathbf{N}_{2^k-1})$ исходного текста и шифртекста. Из (2) вытекает, что

$$\begin{cases} n \circ \left(2 \circ \alpha_1^n \circ a_1 \Theta \overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \right) = c_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ n \circ \left(2 \circ \alpha_l^n \circ a_l \Theta \overset{l}{\underset{j=1}{\oplus}} \alpha_j^n \circ a_j \right) = c_l, \end{cases} \tag{17}$$

где $c_i = x_n^{(i)} \Theta x_0^{(i)}$ $(i \in \mathbf{N}_l)$. Перейдем от (17) к эквивалентной системе. Для этого первое уравнение оставим без изменений, а i-е $(i = 2, \ldots, l)$, умноженное на элемент $\Theta(l-2) \in \mathbf{Z}_{2^k}^{inv}$, сложим с суммой всех уравнений системы (17). Получим систему

$$\begin{cases} n \circ (\alpha_1^n \circ a_1 \Theta \alpha_2^n \circ a_2 \Theta \ldots \Theta \alpha_l^n \circ a_l) = c_1, \\ \Theta 2 \circ n \circ (l-2) \circ \alpha_2^n \circ a_2 = \overset{l}{\underset{j=1}{\oplus}} c_j \circ \Theta(l-2) \circ c_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \Theta 2 \circ n \circ (l-2) \circ \alpha_l^n \circ a_l = \overset{l}{\underset{j=1}{\oplus}} c_j \circ \Theta(l-2) \circ c_l. \end{cases} \tag{18}$$

Решим второе уравнение относительно $n \circ \alpha_2^n \circ a_2$. Так как $2 \in \mathbf{Z}_{2^k} \setminus \mathbf{Z}_{2^k}^{inv}$ и $(2, 2^k) = 2$, то для разрешимости этого уравнения достаточно, чтобы $2 \,\big|\, \overset{l}{\underset{j=1}{\oplus}} c_j \Theta \Theta(l-2) \circ c_2$. Положим $\overset{l}{\underset{j=1}{\oplus}} c_j \Theta(l-2) \circ c_2 = 2 \circ c_2'$. Сравнение $\Theta(l-2) \circ n \circ \alpha_2^n \circ a_2 \equiv c_2' \,(\mathrm{mod}\ 2^{k-1})$ имеет одно решение по модулю 2^{k-1} и два решения по модулю 2^k:

$$\begin{cases} n \circ \alpha_2^n \circ a_2 = v_2, \\ n \circ \alpha_2^n \circ a_2 = v_2 \oplus 2^{k-1}, \end{cases}$$

где $v_2 = \Theta c'_2 (l-2)^{-1}$. Аналогично i-е уравнение $(i = 3,\dots, l)$ системы (18) имеет два решения:

$$\left[\begin{array}{l} n \circ \alpha_i^n \circ a_i = v_i, \\ n \circ \alpha_i^n \circ a_i = v_i \oplus 2^{k-1}, \end{array}\right.$$

если $2 \Big| \mathop{\oplus}\limits_{j=1}^{l} c_j \Theta (l-2) \circ c_i$.

Из первого уравнения системы (18) вытекает, что $n \circ \alpha_1^n \circ a_1 = c_1 \oplus n \circ \alpha_2^n \circ a_2 \oplus \dots$ $\dots \oplus n \circ \alpha_l^n \circ a_l$, т.е.

$$\left[\begin{array}{l} n \circ \alpha_1^n \circ a_1 = c_1 \oplus \mathop{\oplus}\limits_{i=2}^{l} v_i, \\ n \circ \alpha_1^n \circ a_1 = c_1 \oplus \mathop{\oplus}\limits_{i=2}^{l} v_i \oplus 2^{k-1}. \end{array}\right.$$

Таким образом, система (17) имеет 2^{l-1} решений, т.е. построено 2^{l-1} систем вида

$$\left\{\begin{array}{l} n \circ \alpha_1^n \circ a_1 = z_1, \\ \dots\dots\dots\dots\dots \\ n \circ \alpha_l^n \circ a_l = z_l, \end{array}\right. \tag{19}$$

где $z_1 \in \{c_1 \oplus \mathop{\oplus}\limits_{i=2}^{l} v_i, c_1 \oplus \mathop{\oplus}\limits_{i=2}^{l} v_i \oplus 2^{k-1}\}$; $z_i \in \{v_i, v_i \oplus 2^{k-1}\}$ $(i = 2,\dots, l)$.

Для решения системы (19) рассмотрим следующую вход-выходную пару $(\mathbf{x}'_0, \mathbf{x}'_n)$ $(n' \in \mathbf{N}_{2^k-1})$. Система (17) принимает вид

$$\left\{\begin{array}{l} n' \circ \left(2 \circ \alpha_1^{n+n'} \circ a_1 \Theta \mathop{\oplus}\limits_{j=1}^{l} \alpha_j^{n+n'} \circ a_j \right) = c'_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ n' \circ \left(2 \circ \alpha_l^{n+n'} \circ a_l \Theta \mathop{\oplus}\limits_{j=1}^{l} \alpha_j^{n+n'} \circ a_j \right) = c'_l, \end{array}\right. \tag{20}$$

где значения n и n' известны, исходя из алгоритма. Решим (20) относительно $n' \circ \alpha_i^{n+n'} \circ a_i$ $(i \in \mathbf{N}_l)$ по аналогии с тем, как описано выше. В результате получим 2^{l-1} систем вида

$$\left\{\begin{array}{l} n' \circ \alpha_i^{n+n'} \circ a_1 = z'_1, \\ \dots\dots\dots\dots\dots \\ n' \circ \alpha_l^{n+n'} \circ a_l = z'_l, \end{array}\right.$$

т.е. полученная система имеет ту же структуру, что и система (19).

Решим систему (19) относительно $\alpha_i^n \circ a_i$ $(i \in \mathbf{N}_l)$.

Каждое уравнение системы (19) порождает $(n, 2^k) = 2^w$ уравнений вида $\alpha_i^n \circ a_i = u_i$, где $u_i \in \{\hat{z}_i \circ n_1^{-1}, \hat{z}_i \circ n_1^{-1} \oplus 2^{k-w}, \dots, \hat{z}_i \circ n_1^{-1} \oplus 2^{k-1}\}$, $n = 2^w \circ n_1$, $n_1 \in \mathbf{Z}_{2^k}^{inv}$, а $z_i = 2^w \circ \hat{z}_i$ $(i \in \mathbf{N}_l)$. Следовательно, количество решений систем (19) и (17) равно соответственно $l \cdot 2^w$ и $2^{l-1} \cdot l \cdot 2^w = l \cdot 2^{w+l-1}$. Аналогично получаем, что система (20) имеет $l \cdot 2^{w'+l-1}$ решений, где $(n', 2^k) = 2^{w'}$.

Поиск значений α_i и a_i $(i \in \mathbf{N}_l)$ сводится к решению $l^3 \cdot 2^{w+w'+2\cdot(l-1)}$ систем уравнений вида

$$\begin{cases} u^{\beta} \circ u^{\gamma} \circ v = h_1, \\ u^{\beta} \circ v = h_2. \end{cases} \tag{21}$$

Возможны следующие четыре случая.

Случай 1. Пусть u, v — обратимые элементы кольца Z_{2^k}. Тогда h_1 и h_2 — обратимые элементы. Из первого уравнения системы (21) находим $u^{\beta} \circ v = h_1 \circ u^{-\gamma}$. Отсюда следует, что $h_1 \circ u^{-\gamma} = h_2$, т.е.

$$u^{\gamma} = h_1 \circ h_2^{-1}. \tag{22}$$

Из уравнения (22) находим u, а из второго уравнения системы (21) находим v, т.е.

$$v = h_2 \circ u^{-\beta}. \tag{23}$$

Случай 2. Пусть u — обратимый, а v — необратимый элемент кольца Z_{2^k}. Тогда h_1 и h_2 — необратимые элементы. Из первого уравнения системы (21) находим $u^{\beta} \circ v = h_1 \circ u^{-\gamma}$. Отсюда следует, что $h_1 \circ u^{-\gamma} = h_2$, т.е.

$$h_2 \circ u^{\gamma} = h_1. \tag{24}$$

Пусть $(h_2, 2^k) = q \geq 2$. Уравнение (24) разрешимо, если $q \mid h_1$. При этом число решений равно q. Значения v находим из уравнения (23). Следовательно, система (22) имеет q решений.

Случай 3. Пусть u — необратимый, а v — обратимый элемент кольца Z_{2^k}. Тогда h_1 и h_2 — необратимые элементы. Пусть $u = 2^{\delta} \circ u_1$, где u_1 — обратимый элемент. Тогда

$$\begin{cases} 2^{k_1} \circ u_1^{\beta} \circ u_1^{\gamma} \circ v = h_1, \\ 2^{k_2} \circ u_1^{\beta} \circ v = h_2, \end{cases} \tag{25}$$

где $k_1 = \delta \cdot (\beta + \gamma)$, $k_2 = \delta \cdot \beta$. Система (25) разрешима, если $2^{k_1} \mid h_1$ и $2^{k_2} \mid h_2$. При этом порождается $2^{k_1+k_2}$ систем сравнений вида

$$\begin{cases} u_1^{\beta} \circ u_1^{\gamma} \circ v \equiv h_1' \pmod{2^{k-k_1}}, \\ u_1^{\beta} \circ v \equiv h_2' \pmod{2^{k-k_2}}, \end{cases} \tag{26}$$

где $h_1 = h_1' \circ 2^{k_1}$, $h_2 = h_2' \circ 2^{k_2}$. Каждая из систем (26) имеет одно решение, а система (25) — $2^{k_1+k_2}$ решений.

Случай 4. Пусть u и v — необратимые элементы кольца Z_{p^k}. Тогда h_1 и h_2 — необратимые элементы. Пусть $u = 2^{\delta} \circ u_1$, где u_1 — обратимый элемент, $v = 2^{\eta} \circ v_1$, v_1 — обратимый элемент. Тогда

$$\begin{cases} 2^{k_1} \circ u_1^{\beta} \circ u_1^{\gamma} \circ v_1 = h_1, \\ 2^{k_2} \circ u_1^{\beta} \circ v_1 = h_2, \end{cases} \tag{27}$$

где $k_1 = \delta \cdot (\beta + \gamma) + \eta$, $k_2 = \delta \cdot \beta + \eta$.

Система (27) разрешима, если $2^{k_1} \mid h_1$ и $2^{k_2} \mid h_2$. При этом порождается $2^{k_1+k_2}$ систем сравнений вида

$$\begin{cases} u_1^{\beta} \circ u_1^{\gamma} \circ v_1 \equiv h_1' \pmod{2^{k-k_1}}, \\ u_1^{\beta} \circ v_1 \equiv h_2' \pmod{2^{k-k_2}}, \end{cases} \tag{28}$$

где $h_1 = h_1' \circ 2^{k_1}$, $h_2 = h_2' \circ 2^{k_2}$. Каждая из систем (28) имеет одно решение, а система (27) — $2^{k_1+k_2}$ решений.

Итак, для идентификации вектора $(\mathbf{a}, \boldsymbol{\alpha})$ необходимо решить экспоненциальное число задач дискретного логарифмирования.

Теорема доказана.

ЗАКЛЮЧЕНИЕ

В работе изучены свойства класса семейств легко вычислимых перестановок, определенных в терминах конечного кольца. Актуальность задачи обусловлена возможностью применения этих классов перестановок при построении высокоскоростных вычислительно стойких поточных шифров.

Показано, что задачи идентификации для класса семейств перестановок $\boldsymbol{S}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \mathbf{a}, h)$ сводятся к решению систем многостепенных диофантовых уравнений и систем задач дискретного логарифмирования. Следовательно, эти задачи трудные, что обосновывает вычислительную стойкость поточного шифра, построенного на основе управления динамическим фракталом этим классом перестановок. Построение и сравнительный анализ таких классов семейств перестановок представляет одно из возможных направлений дальнейших исследований. Другое направление исследований связано с построением классов легко вычислимых перестановок над конечным кольцом, управляемых траекториями хаотических динамических систем с нетривиальным множеством аттракторов, таких как системы Лоренца Реслера, Спротта и т.д. [1].

СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов С.П. Динамический хаос. — М.: Физматлит, 2001. — 296 с.
2. Скобелев В.Г. Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. — 2006. — № 6. — С. 29–42.
3. Турбин А.Ф., Працевитый Н.В. Фрактальные множества, функции, распределения. — Киев: Наук. думка, 1992. — 208 с.
4. Працьовитий М.В. Фрактальний підхід у дослідженнях сингулярних розподілів. — Київ: НПУ ім. М.П. Драгоманова, 1998. — 296 с.
5. Пайтген Х.-О., Рихтер П.Х. Красота фракталов. Образы комплексных динамических систем. — М.: Мир, 1993. — 176 с.
6. Зайцева Э.Е., Скобелев В.Г. Шифры на основе фракталов // Тр. ИПММ НАН Украины. — 2006 — Вып. 12 — С. 63–68.
7. Харин Ю.С. и др. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 382 с.
8. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии. — М.: Гелиос АРВ, 2002. — 480 с.
9. Бабичев С.Г.,Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с.
10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2003. — 816 с.
11. Кострикин А.И. Введение в алгебру. — Т. 1–3. — М.: Наука, 1999–2000. — 912 с.
12. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979. — 536 с.
13. Скобелев В.В. Об обратимых матрицах над кольцом Z_{p^k} // Тр. ИПММ НАН Украины. — 2006. — **13.** — С. 185–192.
14. Скобелев В.Г. Построение нижних экспоненциальных оценок // Доп. НАН України. — 1997. — № 3. — С. 115–117.

Поступила 11.06.2007