УДК 510.5+681.3

В.В. СКОБЕЛЕВ

О ДВУХ ТИПАХ НЕЛИНЕЙНЫХ АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

Ключевые слова: *эквивалентные состояния, идентификация состояний, параметрическая идентификация, неподвижные точки*.

ВВЕДЕНИЕ

В работе [1] в качестве модели поточного шифра предложено рассматривать обратимые нелинейные автоматы над кольцом $\mathcal{Z}_{p^k}=(\mathbf{Z}_{p^k},\oplus,\circ)$ (p — простое число, $k\in\mathbf{N}$), для которых «нелинейность» характеризуется тем, что изменение значений переменных состояний и выходных переменных представлено алгебраической суммой квадратичной и линейной форм от переменных состояний с линейной формой от входных переменных. Выбор этого типа «нелинейности» обусловлен тем, что аналоги над кольцом $\mathcal{Z}_{p^k}$ для большого числа модельных хаотических динамических систем [2] укладываются в рамки именно такой модели. Однако исследованные в [3] хаотические динамические системы Guckenheimer and Holmes cycle и free-running system не описываются моделью, рассмотренной в [1]. Изменение динамических переменных в первой системе представлено многочленами третьей степени, а во второй осуществляется с помощью показательной функции (как известно, дискретное логарифмирование — базовая конструкция современной криптографии). Кроме того, обе системы имеют нетривиальные группы симметрий (теория симметрий [4] представляет собой мощный аппарат анализа динамических систем). Поэтому как для теории автоматов, так и для криптографии представляет интерес исследование автоматов, являющихся аналогами над кольцом $\mathcal{Z}_{p^k}$ этих систем. Такие автоматы имеют соответственно вид (x — входная переменная, $q^{(i)}(i=1,2,3)$ — переменные состояния автомата, $y^{(i)}$ $(i=1,2,3)$ — выходные переменные)

$$M_{GH}=\begin{cases} q_{n+1}^{(1)}=q_n^{(1)}\circ(d\oplus a\circ(q_n^{(1)})^2\oplus b\circ(q_n^{(2)})^2\oplus c\circ(q_n^{(3)})^2)\oplus\alpha_1\circ x_{n+1},\\ q_{n+1}^{(2)}=q_n^{(2)}\circ(d\oplus c\circ(q_n^{(1)})^2\oplus a\circ(q_n^{(2)})^2\oplus b\circ(q_n^{(3)})^2)\oplus\alpha_2\circ x_{n+1},\\ q_{n+1}^{(3)}=q_n^{(3)}\circ(d\oplus b\circ(q_n^{(1)})^2\oplus c\circ(q_n^{(2)})^2\oplus a\circ(q_n^{(3)})^2)\oplus\alpha_3\circ x_{n+1},\\ y_{n+1}^{(i)}=q_{n+1}^{(i)}\quad(i=1,2,3;\ n\in\mathbf{Z}_+), \end{cases}\tag{1}$$

где $\alpha_1,\alpha_2,\alpha_3$ — фиксированные обратимые элементы кольца $\mathcal{Z}_{p^k}$, $a,b,c,d\in\mathbf{Z}_{p^k}\setminus\{0\}$ — фиксированные элементы кольца $\mathcal{Z}_{p^k}$;

$$M_{FR}=\begin{cases} q_{n+1}^{(1)}=f(q_n^{(1)})\circ\zeta^{q_n^{(3)}}\oplus\alpha_1\circ x_{n+1},\\ q_{n+1}^{(2)}=f(q_n^{(2)})\circ\zeta^{q_n^{(1)}}\oplus\alpha_2\circ x_{n+1},\\ q_{n+1}^{(3)}=f(q_n^{(3)})\circ\zeta^{q_n^{(2)}}\oplus\alpha_3\circ x_{n+1},\\ y_{n+1}^{(i)}=q_{n+1}^{(i)}\quad(i=1,2,3;\ n\in\mathbf{Z}_+), \end{cases}\tag{2}$$

где $f(x)=a\circ x\circ(1\Theta x)$, причем $\alpha_1,\alpha_2,\alpha_3,\zeta$ — фиксированные обратимые элементы кольца $\mathcal{Z}_{p^k}$, $a\in\mathbf{Z}_{p^k}\setminus\{0\}$ — фиксированный элемент кольца $\mathcal{Z}_{p^k}$. Отметим, что в [5] установлен ряд характеристик автоматов (1) и (2) в предположении, что $x_{n+1}\equiv 0$ $(n\in\mathbf{Z}_+)$.

Цель работы — исследование автоматов (1) и (2) при $x_{n+1}\in\mathbf{Z}_{p^k}$ $(n\in\mathbf{Z}_+)$. В разд. 1 определены основные конечно-автоматные характеристики моделей (1) и (2); в разд. 2 решены задачи параметрической идентификации и идентификации начального состояния; в разд. 3 приведен анализ множества неподвижных точек исследуемых автоматных отображений; заключение содержит ряд выводов.

1. СВОЙСТВА МОДЕЛЕЙ

Обозначим $\mathcal{A}_{GH}(p,k)$ и $\mathcal{A}_{FR}(p,k)$ множество всех автоматов соответственно (1) и (2) над кольцом $\mathcal{Z}_{p^k}$.

Утверждение 1. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ любой автомат $M_{GH}\in\mathcal{A}_{GH}(p,k)$, а также любой автомат $M_{FR}\in\mathcal{A}_{FR}(p,k)$ являются обратимыми.

Доказательство. Так как $\alpha_1,\alpha_2,\alpha_3$ — обратимые элементы кольца $\mathcal{Z}_{p^k}$, из первых трех уравнений систем (1) и (2) находим соответственно

$$\begin{cases} x_{n+1}=\alpha_1^{-1}\circ(q_{n+1}^{(1)}\Theta q_n^{(1)}\circ(d\oplus a\circ(q_n^{(1)})^2\oplus b\circ(q_n^{(2)})^2\oplus c\circ(q_n^{(3)})^2)),\\ x_{n+1}=\alpha_2^{-1}\circ(q_{n+1}^{(2)}\Theta q_n^{(2)}\circ(d\oplus c\circ(q_n^{(1)})^2\oplus a\circ(q_n^{(2)})^2\oplus b\circ(q_n^{(3)})^2)),\\ x_{n+1}=\alpha_3^{-1}\circ(q_{n+1}^{(3)}\Theta q_n^{(3)}\circ(d\oplus b\circ(q_n^{(1)})^2\oplus c\circ(q_n^{(2)})^2\oplus a\circ(q_n^{(3)})^2))\ (n\in\mathbf{Z}_+),\end{cases} \tag{3}$$

$$\begin{cases} x_{n+1}=\alpha_1^{-1}\circ(q_{n+1}^{(1)}\Theta f(q_n^{(1)})\circ\zeta^{q_n^{(3)}}),\\ x_{n+1}=\alpha_2^{-1}\circ(q_{n+1}^{(2)}\Theta f(q_n^{(2)})\circ\zeta^{q_n^{(1)}}),\\ x_{n+1}=\alpha_3^{-1}\circ(q_{n+1}^{(3)}\Theta f(q_n^{(3)})\circ\zeta^{q_n^{(2)}})\ (n\in\mathbf{Z}_+).\end{cases} \tag{4}$$

Из последних трех уравнений систем (1) и (2) имеем

$$q_n^{(i)}=y_n^{(i)}\quad(i=1,2,3) \tag{5}$$

для всех $n\in\mathbf{Z}_+$, причем $\mathbf{y}_0=\mathbf{q}_0$.

Подставив (5) в (3) и (4), а также заменив переменную x переменной y, переменную y — переменной x, получим

$$M_{GH}^{-1}=\begin{cases} y_{n+1}=\alpha_1^{-1}\circ(x_{n+1}^{(1)}\Theta x_n^{(1)}\circ(d\oplus a\circ(x_n^{(1)})^2\oplus b\circ(x_n^{(2)})^2\oplus c\circ(x_n^{(3)})^2)),\\ y_{n+1}=\alpha_2^{-1}\circ(x_{n+1}^{(2)}\Theta x_n^{(2)}\circ(d\oplus c\circ(x_n^{(1)})^2\oplus a\circ(x_n^{(2)})^2\oplus b\circ(x_n^{(3)})^2)),\\ y_{n+1}=\alpha_3^{-1}\circ(x_{n+1}^{(3)}\Theta x_n^{(3)}\circ(d\oplus b\circ(x_n^{(1)})^2\oplus c\circ(x_n^{(2)})^2\oplus a\circ(x_n^{(3)})^2))\\ \qquad (n\in\mathbf{Z}_+);\end{cases} \tag{6}$$

$$M_{FR}^{-1}=\begin{cases} y_{n+1}=\alpha_1^{-1}\circ(x_{n+1}^{(1)}\Theta f(x_n^{(1)})\circ\zeta^{x_n^{(3)}}),\\ y_{n+1}=\alpha_2^{-1}\circ(x_{n+1}^{(2)}\Theta f(x_n^{(2)})\circ\zeta^{x_n^{(1)}}),\\ y_{n+1}=\alpha_3^{-1}\circ(x_{n+1}^{(3)}\Theta f(x_n^{(3)})\circ\zeta^{x_n^{(2)}})\ \ (n\in\mathbf{Z}_+).\end{cases} \tag{7}$$

Утверждение доказано.

При использовании автомата (1) или (2) в качестве поточного шифра параметры представляют собой ключ средней длительности, а начальное состояние $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})$ — сеансовый ключ. При этом в процессе «шифрование-расшифровка» как автоматы $M_{GH} \in \mathcal{A}_{GH}(p,k)$ и M_{GH}^{-1}, так и автоматы $M_{FR} \in \mathcal{A}_{FR}(p,k)$ и M_{FR}^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Представим элементы кольца $\mathcal{Z}_{p^k}$ двоичными последовательностями длины $l = \lceil k \log p \rceil$. Рассмотрим очередную выходную последовательность $\gamma_1 \ldots \gamma_{3l}$, генерируемую автоматом $M_{GH} \in \mathcal{A}_{GH}(p,k)$ (соответственно автоматом $M_{FR} \in \mathcal{A}_{FR}(p,k)$). Предположим, что ошибки, состоящие в инвертировании значений битов, могут возникнуть только в процессе передачи информации по каналу связи. Подсоединим выходы автомата M_{GH}^{-1} (автомата M_{FR}^{-1}) к входам мажоритарной схемы. Из (6) и (7) вытекает, что в процессе расшифровки обнаружатся все такие ошибки, что $\gamma_{3i+1} \oplus \gamma_{3i+2} \oplus \gamma_{3i+3} \neq 0$ $(i \in \mathbf{Z}_l)$, а исправлены только те из них, для которых в каждой тройке битов $\gamma_{3i}, \gamma_{3i+2}, \gamma_{3i+3}$ $(i \in \mathbf{Z}_l)$ ошибка произошла не более чем в одном бите.

Утверждение 2. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$

$$|\mathcal{A}_{GH}(p,k)| = (p^k - 1)^4 p^{3k} (p^{-1}(p-1))^3, \tag{8}$$

$$|\mathcal{A}_{FR}(p,k)| = (p^k - 1) p^{4k} (p^{-1}(p-1))^4. \tag{9}$$

Доказательство. В автомате $M_{GH} \in \mathcal{A}_{GH}(p,k)$ параметры $\alpha_1, \alpha_2, \alpha_3$ — обратимые элементы кольца $\mathcal{Z}_{p^k}$, а $a,b,c,d \in \mathbf{Z}_{p^k} \setminus \{0\}$. Число обратимых элементов кольца $\mathcal{Z}_{p^k}$ равно $p^{k-1}(p-1)$, а выбор параметров $\alpha_1, \alpha_2, \alpha_3, a, b, c, d$ осуществляется независимо. Отсюда вытекает, что равенство (8) истинно.

В автомате $M_{FR} \in \mathcal{A}_{FR}(p,k)$ параметры $\alpha_1, \alpha_2, \alpha_3, \zeta$ — обратимые элементы кольца $\mathcal{Z}_{p^k}$, а $a \in \mathbf{Z}_{p^k} \setminus \{0\}$. Выбор параметров $\alpha_1, \alpha_2, \alpha_3, \zeta, a$ осуществляется независимо. Отсюда вытекает, что равенство (9) истинно.

Утверждение доказано.

Охарактеризуем структуру автоматов, принадлежащих множествам $\mathcal{A}_{GH}(p,k)$ и $\mathcal{A}_{FR}(p,k)$.

Утверждение 3. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ любой автомат $M_{GH} \in \mathcal{A}_{GH}(p,k)$, а также любой автомат $M_{FR} \in \mathcal{A}_{FR}(p,k)$ не являются сильно связными автоматами.

Доказательство. Пусть $\mathbf{q}_0 = (q_0, q_0, q_0) \in \mathbf{Z}_{p^k}^3$. Из (1) (соответственно из (2)) вытекает, что $\mathbf{q}_1 = (q_1, q_1, q_1)$ для любого входного символа $x_1 \in \mathbf{Z}_{p^k}$. Индукцией по длине слова можно показать, что $\mathbf{q}_n = (q_n, q_n, q_n)$ для любого входного слова $x_1 \ldots x_n \in \mathbf{Z}_{p^k}^n$.

Поскольку α — обратимый элемент кольца $\mathcal{Z}_{p^k}$, из (1) (соответственно из (2)) вытекает, что для любых фиксированных состояний $\mathbf{q} = (q,q,q) \in \mathbf{Z}_{p^k}^3$ и $\tilde{\mathbf{q}} = (\tilde{q}, \tilde{q}, \tilde{q}) \in \mathbf{Z}_{p^k}^3$ автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ (автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$) существует единственный входной символ $x \in \mathbf{Z}_{p^k}$, переводящий состояние $\mathbf{q}$ в состояние $\tilde{\mathbf{q}}$.

Следовательно, собственное подмножество $S_1 = \{\mathbf{q} = (q,q,q) | q \in \mathbf{Z}_{p^k}\}$ состояний автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ (автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$) определяет компоненту сильной связанности. Отсюда вытекает, что автомат $M_{GH} \in \mathcal{A}_{GH}(p,k)$ (автомат $M_{FR} \in \mathcal{A}_{FR}(p,k)$) не является сильно связным автоматом.

Утверждение доказано.

Из доказательства утверждения 3 вытекает следствие.

Следствие 1. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ как подавтомат автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$, так и подавтомат автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$, определяемый множеством состояний $S_1 = \{\mathbf{q} = (q,q,q) | q \in \mathbf{Z}_{p^k}\}$, являются приведенными перестановочными автоматами, диаметр графа переходов которых равен 1.

Следующее утверждение показывает, что структура автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ может существенно отличаться от структуры его подавтомата, определяемого множеством состояний S_1.

Утверждение 4. Пусть

$$d \equiv 0(\bmod\ p^{\lceil 0,5k \rceil}). \tag{10}$$

Тогда для простого числа p при всех значениях числа $k \in \mathbf{N}$ множество состояний

$$S_2 = \{\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) | q^{(i)} \equiv 0(\bmod\ p^{\lceil 0,5k \rceil})\ (i = 1,2,3)\} \tag{11}$$

автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в одно и то же состояние

$$\mathbf{q}_1 = (\alpha_1 \circ x, \alpha_2 \circ x, \alpha_3 \circ x). \tag{12}$$

Доказательство. Пусть выполнено условие (10) и $\mathbf{q}_0 = (q^{(1)}, q^{(2)}, q^{(3)}) \in S_2$. Поскольку $q^{(i)} \equiv 0(\bmod\ p^{\lceil 0,5k \rceil})\ (i = 1,2,3)$, имеем

$$(q^{(i)})^2 = 0\ \ (i = 1,2,3). \tag{13}$$

Так как $q^{(i)} \equiv 0(\bmod\ p^{\lceil 0,5k \rceil})\ (i = 1,2,3)$ и $d \equiv 0(\bmod\ p^{\lceil 0,5k \rceil})$, получаем

$$q^{(i)} \circ d = 0 \quad (i = 1,2,3). \tag{14}$$

Из (1), (13) и (14) вытекает, что под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ состояние $\mathbf{q}_0$ переходит в состояние $\mathbf{q}_1$, определяемое равенством (12).

Утверждение доказано.

Из утверждения 4 вытекает следствие.

Следствие 2. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если $d \equiv 0(\bmod\ p^{\lceil 0,5k \rceil})$, то любой автомат $M_{GH} \in \mathcal{A}_{GH}(p,k)$ не является перестановочным автоматом.

Из (2) вытекает, что для автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ имеет место следующее утверждение.

Утверждение 5. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ множество состояний $S_3 = \{q = (q^{(1)}, q^{(2)}, q^{(3)}) | q^{(i)} \in \{0,1\} (i = 1,2,3)\}$ любого автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ под действием любого входного символа $x \in \mathbf{Z}_{p^k}$ переходит в одно и то же состояние $\mathbf{q}_1 = (\alpha_1 \circ x, \alpha_2 \circ x, \alpha_3 \circ x,)$.

Из утверждения 5 вытекает следствие.

Следствие 3. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ любой автомат $M_{FR} \in \mathcal{A}_{FR}(p,k)$ не является перестановочным автоматом.

Обозначим $K(\mathbf{q}, M_u)$ $(u \in \{GH, FR\})$ множество всех состояний автомата $M_u \in \mathcal{A}_u(p,k)$, эквивалентных состоянию $\mathbf{q} \in \mathbf{Z}^3_{p^k}$.

Теорема 1. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ для любого автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ и любого состояния $\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in \mathbf{Z}^3_{p^k}$ множество $K(\mathbf{q}, M_{GH})$ состоит из всех таких состояний $\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in \mathbf{Z}^3_{p^k}$, что истинны равенства

$$\begin{cases} \tilde{q}^{(1)} \circ (d \oplus a \circ (\tilde{q}^{(1)})^2 \oplus b \circ (\tilde{q}^{(2)})^2 \oplus c \circ (\tilde{q}^{(3)})^2) = \\ \qquad = q^{(1)} \circ (d \oplus a \circ (q^{(1)})^2 \oplus b \circ (q^{(2)})^2 \oplus c \circ (q^{(3)})^2), \\ \tilde{q}^{(2)} \circ (d \oplus c \circ (\tilde{q}^{(1)})^2 \oplus a \circ (\tilde{q}^{(2)})^2 \oplus b \circ (\tilde{q}^{(3)})^2) = \\ \qquad = q^{(2)} \circ (d \oplus c \circ (q^{(1)})^2 \oplus a \circ (q^{(2)})^2 \oplus b \circ (q^{(3)})^2), \\ \tilde{q}^{(3)} \circ (d \oplus b \circ (\tilde{q}^{(1)})^2 \oplus c \circ (\tilde{q}^{(2)})^2 \oplus a \circ (\tilde{q}^{(3)})^2) = \\ \qquad = q^{(3)} \circ (d \oplus b \circ (q^{(1)})^2 \oplus c \circ (q^{(2)})^2 \oplus a \circ (q^{(3)})^2). \end{cases} \tag{15}$$

Доказательство. Зафиксируем состояние $\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in \mathbf{Z}^3_{p^k}$ автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$. Пусть $\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in K(\mathbf{q}, M_{GH})$. Из первых трех уравнений системы (1) находим, что для любого входного символа $x \in \mathbf{Z}_{p^k}$

$$\begin{cases} q_1^{(1)} = q^{(1)} \circ (d \oplus a \circ (q^{(1)})^2 \oplus b \circ (q^{(2)})^2 \oplus c \circ (q^{(3)})^2) \oplus \alpha_1 \circ x, \\ q_1^{(2)} = q^{(2)} \circ (d \oplus c \circ (q^{(1)})^2 \oplus a \circ (q^{(2)})^2 \oplus b \circ (q^{(3)})^2) \oplus \alpha_2 \circ x, \\ q_1^{(3)} = q^{(3)} \circ (d \oplus b \circ (q^{(1)})^2 \oplus c \circ (q^{(2)})^2 \oplus a \circ (q^{(3)})^2) \oplus \alpha_3 \circ x, \end{cases} \tag{16}$$

$$\begin{cases} \tilde{q}_1^{(1)} = \tilde{q}^{(1)} \circ (d \oplus a \circ (\tilde{q}^{(1)})^2 \oplus b \circ (\tilde{q}^{(2)})^2 \oplus c \circ (\tilde{q}^{(3)})^2) \oplus \alpha_1 \circ x, \\ \tilde{q}_1^{(2)} = \tilde{q}^{(2)} \circ (d \oplus c \circ (\tilde{q}^{(1)})^2 \oplus a \circ (\tilde{q}^{(2)})^2 \oplus b \circ (\tilde{q}^{(3)})^2) \oplus \alpha_2 \circ x, \\ \tilde{q}_1^{(3)} = \tilde{q}^{(3)} \circ (d \oplus b \circ (\tilde{q}^{(1)})^2 \oplus c \circ (\tilde{q}^{(2)})^2 \oplus a \circ (\tilde{q}^{(3)})^2) \oplus \alpha_3 \circ x. \end{cases} \tag{17}$$

Поскольку $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — эквивалентные состояния автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$, из последних трех уравнений системы (1) вытекает

$$q_1^{(i)} = \tilde{q}_1^{(i)} \quad (i = 1, 2, 3). \tag{18}$$

Из формул (16)–(18) следует (15).

Теорема доказана.

Из доказательства теоремы 1 вытекает следствие.

Следствие 4. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ любые эквивалентные один другому состояния любого автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ — близнецы.

Теорема 2. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ для любого автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ и любого состояния $\mathbf{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in \mathbf{Z}^3_{p^k}$ множество $K(\mathbf{q}, M_{FR})$ состоит из всех таких состояний $\tilde{\mathbf{q}} = (\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in \mathbf{Z}^3_{p^k}$, что истинны равенства

$$\begin{cases} f(\tilde{q}^{(1)}) \circ \zeta^{\tilde{q}^{(3)} - q^{(3)}} = f(q^{(1)}), \\ f(\tilde{q}^{(2)}) \circ \zeta^{\tilde{q}^{(1)} - q^{(1)}} = f(q^{(2)}), \\ f(\tilde{q}^{(3)}) \circ \zeta^{\tilde{q}^{(2)} - q^{(2)}} = f(q^{(3)}). \end{cases} \tag{19}$$

Доказательство. Зафиксируем состояние $\mathbf{q}=(q^{(1)}, q^{(2)}, q^{(3)})\in\mathbf{Z}^3_{p^k}$ автомата $M_{FR}\in\mathcal{A}_{FR}(p,k)$. Пусть $\widetilde{\mathbf{q}}=(\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)})\in K(\mathbf{q},M_{FR})$. Из первых трех уравнений системы (2) находим, что для любого входного символа $x\in\mathbf{Z}_{p^k}$

$$\begin{cases} q_1^{(1)}=f(q^{(1)})\circ\zeta^{q^{(3)}}\oplus\alpha_1\circ x_{n+1}, \\ q_1^{(2)}=f(q^{(2)})\circ\zeta^{q^{(1)}}\oplus\alpha_2\circ x_{n+1}, \\ q_1^{(3)}=f(q^{(3)})\circ\zeta^{q^{(2)}}\oplus\alpha_3\circ x_{n+1}, \end{cases} \tag{20}$$

$$\begin{cases} \widetilde{q}_1^{(1)}=f(\widetilde{q}^{(1)})\circ\zeta^{\widetilde{q}^{(3)}}\oplus\alpha_1\circ x_{n+1}, \\ \widetilde{q}_1^{(2)}=f(\widetilde{q}^{(2)})\circ\zeta^{\widetilde{q}^{(1)}}\oplus\alpha_2\circ x_{n+1}, \\ \widetilde{q}_1^{(3)}=f(\widetilde{q}^{(3)})\circ\zeta^{\widetilde{q}^{(2)}}\oplus\alpha_3\circ x_{n+1}. \end{cases} \tag{21}$$

Поскольку $\mathbf{q}$ и $\widetilde{\mathbf{q}}$ — эквивалентные состояния автомата M_{FR}, из последних трех уравнений системы (2) вытекает

$$q_1^{(i)}=\widetilde{q}_1^{(i)}\quad(i=1,2,3). \tag{22}$$

Из (20)–(22) следует

$$\begin{cases} f(q^{(1)})\circ\zeta^{q^{(3)}}\oplus\alpha_1\circ x_{n+1}=f(\widetilde{q}^{(1)})\circ\zeta^{\widetilde{q}^{(3)}}\oplus\alpha_1\circ x_{n+1}, \\ f(q^{(2)})\circ\zeta^{q^{(1)}}\oplus\alpha_2\circ x_{n+1}=f(\widetilde{q}^{(2)})\circ\zeta^{\widetilde{q}^{(1)}}\oplus\alpha_2\circ x_{n+1}, \Leftrightarrow \\ f(q^{(3)})\circ\zeta^{q^{(2)}}\oplus\alpha_3\circ x_{n+1}=f(\widetilde{q}^{(3)})\circ\zeta^{\widetilde{q}^{(2)}}\oplus\alpha_3\circ x_{n+1} \end{cases}$$

$$\Leftrightarrow\begin{cases} f(q^{(1)})\circ\zeta^{q^{(3)}}=f(\widetilde{q}^{(1)})\circ\zeta^{\widetilde{q}^{(3)}}, \\ f(q^{(2)})\circ\zeta^{q^{(1)}}=f(\widetilde{q}^{(2)})\circ\zeta^{\widetilde{q}^{(1)}}, \\ f(q^{(3)})\circ\zeta^{q^{(2)}}=f(\widetilde{q}^{(3)})\circ\zeta^{\widetilde{q}^{(2)}}. \end{cases} \tag{23}$$

Так как ζ — обратимый элемент кольца $\mathcal{Z}_{p^k}$, из (23) следуют равенства (19).

Теорема доказана.

Из доказательства теоремы 2 вытекает следствие.

Следствие 5. Для любого простого числа p при всех значениях числа $k\in\mathbf{N}$ любые эквивалентные один другому состояния любого автомата $M_{FR}\in$ $\in\mathcal{A}_{FR}(p,k)$ — близнецы.

Множество $K(\mathbf{q},M_{FR})$ может быть вычислено следующим образом. Пусть ζ принадлежит показателю δ, т.е. δ — такое наименьшее натуральное число, что $\zeta^\delta\equiv1(\mathrm{mod}\ p^k)$. Представим компоненты состояния $\mathbf{q}=(q^{(1)}, q^{(2)}, q^{(3)})\in\mathbf{Z}^3_{p^k}$ в виде $q^{(i)}=\zeta^{h_i}\circ b_i$ $(i=1,2,3)$, где $(b_i,\zeta)=1$ $(i=1,2,3)$. Из (19) вытекает, что компоненты любого состояния $\widetilde{\mathbf{q}}=(\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)})\in K(\mathbf{q},M_{FR})$ удовлетворяют равенствам

$$\begin{cases} f(\widetilde{q}^{(1)})=\zeta^{l_3}\circ b_1, \\ f(\widetilde{q}^{(2)})=\zeta^{l_1}\circ b_2, \\ f(\widetilde{q}^{(3)})=\zeta^{l_2}\circ b_3. \end{cases} \tag{24}$$

Из (19) и (24) вытекает

$$\begin{cases} \tilde{q}^{(1)} \equiv h_1 \oplus q^{(1)} \Theta\, l_1 \,(\mathrm{mod}\,\delta), \\ \tilde{q}^{(2)} \equiv h_2 \oplus q^{(2)} \Theta\, l_2 \,(\mathrm{mod}\,\delta), \\ \tilde{q}^{(3)} \equiv h_3 \oplus q^{(3)} \Theta\, l_3 \,(\mathrm{mod}\,\delta). \end{cases} \tag{25}$$

Итак, для построения множества $K(\mathbf{q}, M_{FR})$ достаточно найти все решения $(\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)})$ систем сравнений (25) при всех значениях $l_1, l_2, l_3 \in \{0, 1, \dots, \delta - 1\}$. При этом $(\tilde{q}^{(1)}, \tilde{q}^{(2)}, \tilde{q}^{(3)}) \in K(\mathbf{q}, M_{FR})$ тогда и только тогда, когда истинны равенства (24).

2. ИДЕНТИФИКАЦИЯ МОДЕЛЕЙ

Рассмотрим задачу параметрической идентификации автомата $M_u \in \mathcal{A}_u(p,k)$ $(u \in GH, FR)$ в предположении, что экспериментатор может управлять входом и инициализацией автомата.

Утверждение 6. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ идентификация параметров $\alpha_1, \alpha_2, \alpha_3$ любого автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ и $M_{FR} \in \mathcal{A}_{FR}(p,k)$ осуществляется простым экспериментом длины 1.

Доказательство. Положим $q_0^{(1)} = q_0^{(2)} = q_0^{(3)} = 0$ и $x = 1$. Из равенств (1), (2) вытекает $\alpha_i = y_1^{(i)}$ $(i = 1, 2, 3)$.

Утверждение доказано.

Теорема 3. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$ идентификация параметров b и c любого автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ осуществляется кратным экспериментом кратности 2 и высоты 1.

Доказательство. Положив $\mathbf{q}_0 = (1, 0, 0)$ и $x_1 = 0$, из (1) находим

$$d \oplus a = y_1^{(1)}. \tag{26}$$

Положив $\tilde{\mathbf{q}}_0 = (1, 1, 0)$ и $x'_1 = 0$, из (1) получаем

$$\begin{cases} d \oplus a \oplus b = \tilde{y}_1^{(1)}, \\ d \oplus a \oplus c = \tilde{y}_1^{(2)}. \end{cases} \tag{27}$$

Из (26) и (27) имеем
$$\begin{cases} b = \tilde{y}_1^{(1)} \Theta\, y_1^{(1)}, \\ c = \tilde{y}_1^{(2)} \Theta\, y_1^{(1)}. \end{cases}$$

Теорема доказана.

Теорема 4. Для любого простого числа $p > 3$ при всех значениях числа $k \in \mathbf{N}$ идентификация параметров a и d любого автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$ сводится к решению системы двух линейных уравнений, сформированной в результате простого эксперимента длины 1.

Доказательство. Положив $\mathbf{q}_0 = (1, 2, 0)$ и $x_1 = 0$, из (1) находим

$$\begin{cases} d \oplus a \oplus 4 \circ b = y_1^{(1)}, \\ 2 \circ d \oplus (8 (\mathrm{mod}\ p)) \circ a \oplus 2 \circ c = y_1^{(2)} \end{cases} \Leftrightarrow \begin{cases} d \oplus a = y_1^{(1)} \Theta 4 \circ b, \\ 2 \circ d \oplus (8 (\mathrm{mod}\ p)) \circ a = y_1^{(2)} \Theta 2 \circ c \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} (8 (\mathrm{mod}\ p)\, \Theta\, 2) \circ a = y_1^{(2)} \Theta 2 \circ y_1^{(1)} \Theta 2 \circ c \oplus (8 (\mathrm{mod}\ p)) \circ b, \\ d = y_1^{(1)} \Theta\, 4 \circ b\, \Theta a. \end{cases} \tag{28}$$

Так как p — простое число и $p > 3$, элемент $8(\bmod\ p)\Theta 2$ является обратимым элементом кольца $\mathcal{Z}_{p^k}$.

Из (28) вытекает

$$\begin{cases} a = (8(\bmod\ p)\Theta 2)^{-1} \circ (y_1^{(2)}\Theta 2 \circ y_1^{(1)}\Theta 2 \circ c \oplus (8(\bmod\ p)) \circ b), \\ d = y_1^{(1)}\Theta 4 \circ b\Theta(8(\bmod\ p)\Theta 2)^{-1} \circ (y_1^{(2)}\Theta 2 \circ y_1^{(1)}\Theta 2 \circ c \oplus (8(\bmod\ p)) \circ b). \end{cases}$$

Теорема доказана.

Теорема 5. Для любого простого числа $p > 3$ при всех значениях числа $k \in \mathbf{N}$, если известно, что a — обратимый элемент кольца $\mathcal{Z}_{p^k}$, то идентификация параметров a и ζ автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ сводится к решению системы двух уравнений, полученной в результате простого эксперимента длины 1.

Доказательство. Пусть a — обратимый элемент кольца $\mathcal{Z}_{p^k}$. Положив $\mathbf{q}_0 = (2,3,1)$ и $x_1 = 0$, из (2) находим

$$\begin{cases} \zeta \circ a \circ 2 \circ (p^k - 1) = y_1^{(1)}, \\ \zeta^2 \circ a \circ 3 \circ (p^k - 2) = y_1^{(2)}. \end{cases} \tag{29}$$

Поскольку p — простое число и $p > 3$, элементы 2, 3, $p^k - 1$ и $p^k - 2$ являются обратимыми элементами кольца $\mathcal{Z}_{p^k}$. Так как a — обратимый элемент кольца $\mathcal{Z}_{p^k}$ и система уравнений (29) совместная, $y_1^{(i)}$ $(i = 1, 2)$ — обратимые элементы кольца $\mathcal{Z}_{p^k}$.

Следовательно, из (29) вытекает

$$\begin{cases} \zeta = (y_1^{(1)})^{-1} \circ y_1^{(2)} \circ 2 \circ 3^{-1} \circ (p^k - 1) \circ (p^k - 2)^{-1}, \\ a = (y_1^{(1)})^2 \circ (y_1^{(2)})^{-1} \circ 4^{-1} \circ 3 \circ (p^k - 1)^{-2} \circ (p^k - 2). \end{cases}$$

Теорема доказана.

Отметим, что для автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ идентификация параметров a и ζ существенно усложняется, если a — необратимый элемент кольца $\mathcal{Z}_{p^k}$. В этом случае вначале необходимо найти все решения a и ζ системы уравнений (29), а затем обычными методами теории автоматов с помощью простого (или кратного) эксперимента [6] решить задачу идентификации автомата в классе всех допустимых автоматов $M_{FR} \in \mathcal{A}_{FR}(p,k)$.

Рассмотрим задачу идентификации начального состояния автомата $M_u \in \mathcal{A}_u(p,k)$ $(u \in \{GH, FR\})$ в предположении, что экспериментатору известны параметры автомата и он может управлять входом автомата. Ясно, что сложность решения этой задачи существенно зависит от возможности экспериментатора управлять параметрами автомата.

Рассмотрим автомат $M_{GH} \in \mathcal{A}_{GH}(p,k)$.

Предположим вначале, что экспериментатор может управлять параметрами автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$. Положив $(a,b,c,d) = (0,0,0,1)$ и $x_1 = 0$, из (1) находим, что $q_0^{(i)} = y_1^{(i)}$ $(i = 1,2,3)$.

Предположим теперь, что экспериментатор не может управлять параметрами автомата $M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d) \in \mathcal{A}_{GH}(p,k)$. Из (1) вытекает, что для любого входного символа $x \in \mathbf{Z}_{p^k}$ получим систему трех нелинейных уравнений

$$\begin{cases} q_0^{(1)} \circ (d \oplus a \circ (q_0^{(1)})^2 \oplus b \circ (q_0^{(2)})^2 \oplus c \circ (q_0^{(3)})^2) = y_1^{(1)} \Theta \alpha_1 \circ x, \\ q_0^{(2)} \circ (d \oplus c \circ (q_0^{(1)})^2 \oplus a \circ (q_0^{(2)})^2 \oplus b \circ (q_0^{(3)})^2) = y_1^{(2)} \Theta \alpha_2 \circ x, \\ q_0^{(3)} \circ (d \oplus b \circ (q_0^{(1)})^2 \oplus c \circ (q_0^{(2)})^2 \oplus a \circ (q_0^{(3)})^2) = y_1^{(3)} \Theta \alpha_3 \circ x. \end{cases} \quad (30)$$

Множество S решений $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)})$ системы (30) уравнений третьей степени над кольцом $\mathcal{Z}_{p^k}$ определяет множество всех допустимых кандидатов на начальное состояние исследуемого автомата. Неэквивалентные состояния автомата $M_{GH} \in \mathcal{A}_{GH}(p,k)$, принадлежащие множеству S (если такие имеются), необходимо различить обычными методами теории автоматов, т.е. с помощью диагностического эксперимента [6].

Рассмотрим автомат $M_{FR} \in \mathcal{A}_{FR}(p,k)$. Предположим вначале, что экспериментатор имеет возможность управлять параметрами этого автомата.

Пусть $p^k > 4$. Положим $a = 4$ и $\zeta = 1$. Из (2) вытекает, что для любого входного символа $x \in \mathbf{Z}_{p^k}$ получим следующую систему трех уравнений над кольцом $\mathcal{Z}_{p^k}$:

$$\begin{cases} (2 \circ q_0^{(1)} \Theta 1)^2 = \alpha_1 \circ x \Theta y_1^{(1)} \oplus 1, \\ (2 \circ q_0^{(2)} \Theta 1)^2 = \alpha_2 \circ x \Theta y_1^{(2)} \oplus 1, \\ (2 \circ q_0^{(3)} \Theta 1)^2 = \alpha_3 \circ x \Theta y_1^{(3)} \oplus 1. \end{cases} \quad (31)$$

Множество S решений $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)})$ системы уравнений (31) определяет множество всех допустимых кандидатов на начальное состояние исследуемого автомата. При этом $|S| = o(p^k)$, если $p \to \infty$ или $k \to \infty$.

Неэквивалентные состояния автомата M_{FR}, принадлежащие множеству S (если такие имеются), необходимо различить обычными методами теории автоматов, т.е. с помощью диагностического эксперимента.

Предположим, что экспериментатор не может управлять параметрами автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$. Из (2) следует, что для любого входного символа $x \in \mathbf{Z}_{p^k}$

$$\begin{cases} f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}} = y_1^{(1)} \Theta \alpha_1 \circ x_1, \\ f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}} = y_1^{(2)} \Theta \alpha_2 \circ x_1, \\ f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}} = y_1^{(3)} \Theta \alpha_3 \circ x_1. \end{cases} \quad (32)$$

Поскольку система уравнений (32) совместная, имеем

$$\begin{cases} y_1^{(1)} \Theta \alpha_1 \circ x_1 = b_1 \circ \zeta^{h_3}, \\ y_1^{(2)} \Theta \alpha_2 \circ x_1 = b_2 \circ \zeta^{h_1}, \\ y_1^{(3)} \Theta \alpha_3 \circ x_1 = b_3 \circ \zeta^{h_2}, \end{cases} \quad (33)$$

где $(b_i, \zeta) = 1$ $(i = 1, 2, 3)$. Из (32) и (33) получаем систему уравнений

$$\begin{cases} f(q_0^{(1)}) = \zeta^{l_3} \circ b_1, \\ f(q_0^{(2)}) = \zeta^{l_1} \circ b_2, \\ f(q_0^{(3)}) = \zeta^{l_2} \circ b_3. \end{cases} \quad (34)$$

Пусть число ζ принадлежит показателю δ. Подставив (33) и (34) в (32), получим

$$\begin{cases} q_0^{(1)} \equiv h_1 \Theta l_1 \pmod{\delta}, \\ q_0^{(2)} \equiv h_2 \Theta l_2 \pmod{\delta}, \\ q_0^{(3)} \equiv h_3 \Theta l_3 \pmod{\delta}. \end{cases} \tag{35}$$

Таким образом, для идентификации начального состояния любого автомата $M_{FR} \in \mathcal{A}_{FR}(p,k)$ достаточно найти множество S всех решений $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)})$ систем сравнений (35) при всех значениях чисел $l_1, l_2, l_3 \in \{0,1,\ldots,\delta-1\}$, вычислить подмножество $\widetilde{S}$, состоящее из всех элементов $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)}) \in S$, удовлетворяющих системе уравнений (34), и различить неэквивалентные состояния автомата M_{FR}, принадлежащие множеству $\widetilde{S}$ (если такие имеются), обычными методами теории автоматов, т.е. с помощью диагностического эксперимента.

3. НЕПОДВИЖНЫЕ ТОЧКИ МОДЕЛЕЙ

Охарактеризуем множества неподвижных точек ограниченно-детерминированных (о.-д.) функций [7], реализуемых инициальными автоматами $(M_{GH}, \mathbf{q}_0)$ и $(M_{FR}, \mathbf{q}_0)$. Пусть $X(M_u, \mathbf{q})$ $(u \in \{GH, FR\})$ — множество всех неподвижных точек о.-д. функции, реализуемой инициальным автоматом $(M_u, \mathbf{q})$. Положим $X^{(1)}(M_u, \mathbf{q}) = X(M_u, \mathbf{q}) \cap \mathbf{Z}_{p^k}$.

Рассмотрим автомат $M_{GH} \in \mathcal{A}_{GH}(p,k)$. Из (2) вытекает, что $x_1 \in X^{(1)}(M_{GH}, \mathbf{q}_0)$ тогда и только тогда, когда x_1 — решение системы уравнений

$$\begin{cases} (1\Theta\alpha_1)\circ x_1 = q_0^{(1)} \circ (d \oplus a\circ(q_0^{(1)})^2 \oplus b\circ(q_0^{(2)})^2 \oplus c\circ(q_0^{(3)})^2), \\ (1\Theta\alpha_2)\circ x_1 = q_0^{(2)} \circ (d \oplus c\circ(q_0^{(1)})^2 \oplus a\circ(q_0^{(2)})^2 \oplus b\circ(q_0^{(3)})^2), \\ (1\Theta\alpha_3)\circ x_1 = q_0^{(3)} \circ (d \oplus b\circ(q_0^{(1)})^2 \oplus c\circ(q_0^{(2)})^2 \oplus a\circ(q_0^{(3)})^2). \end{cases} \tag{36}$$

Из (36) вытекают следующие утверждения.

Утверждение 7. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если каждый элемент $1\Theta\alpha_i$ $(i = 1,2,3)$ является обратимым элементом кольца $\mathcal{Z}_{p^k}$, то имеет место следующее:

1) равенство $X^{(1)}(M_{GH}, \mathbf{q}_0) = \varnothing$ истинно тогда и только тогда, когда выполнено по крайней мере одно из условий:

$$(1\Theta\alpha_1)^{-1} \circ q_0^{(1)} \circ (d \oplus a\circ(q_0^{(1)})^2 \oplus b\circ(q_0^{(2)})^2 \oplus c\circ(q_0^{(3)})^2) \neq$$
$$\neq (1\Theta\alpha_2)^{-1} \circ q_0^{(2)} \circ (d \oplus c\circ(q_0^{(1)})^2 \oplus a\circ(q_0^{(2)})^2 \oplus b\circ(q_0^{(3)})^2), \tag{37}$$

$$(1\Theta\alpha_1)^{-1} \circ q_0^{(1)} \circ (d \oplus a\circ(q_0^{(1)})^2 \oplus b\circ(q_0^{(2)})^2 \oplus c\circ(q_0^{(3)})^2) \neq$$
$$\neq (1\Theta\alpha_3)^{-1} \circ q_0^{(3)} \circ (d \oplus b\circ(q_0^{(1)})^2 \oplus c\circ(q_0^{(2)})^2 \oplus a\circ(q_0^{(3)})^2) \tag{38}$$

или

$$(1\Theta\alpha_2)^{-1} \circ q_0^{(2)} \circ (d \oplus c\circ(q_0^{(1)})^2 \oplus a\circ(q_0^{(2)})^2 \oplus b\circ(q_0^{(3)})^2) \neq$$
$$\neq (1\Theta\alpha_3)^{-1} \circ q_0^{(3)} \circ (d \oplus b\circ(q_0^{(1)})^2 \oplus c\circ(q_0^{(2)})^2 \oplus a\circ(q_0^{(3)})^2); \tag{39}$$

2) равенство $|X^{(1)}(M_{GH}(\alpha_1, \alpha_2, \alpha_3, a, b, c, d), \mathbf{q}_0)| = 1$ истинно тогда и только тогда, когда ни одно из условий (37)–(39) не выполнено.

Утверждение 8. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если по крайней мере один из элементов $1\Theta\alpha_i$ $(i = 1, 2, 3)$ — необратимый элемент кольца $\mathcal{Z}_{p^k}$, то равенство $X^{(1)}(M_{GH}, \mathbf{q}_0) = \varnothing$ истинно, если выполнено по крайней мере одно из условий:

1) $q_0^{(1)} \circ (d \oplus a \circ (q_0^{(1)})^2 \oplus b \circ (q_0^{(2)})^2 \oplus c \circ (q_0^{(3)})^2)$ — обратимый элемент кольца $\mathcal{Z}_{p^k}$, а $1\Theta\alpha_1$ — необратимый элемент кольца $\mathcal{Z}_{p^k}$;

2) $q_0^{(2)} \circ (d \oplus c \circ (q_0^{(1)})^2 \oplus a \circ (q_0^{(2)})^2 \oplus b \circ (q_0^{(3)})^2)$ — обратимый элемент кольца $\mathcal{Z}_{p^k}$, а $1\Theta\alpha_2$ — необратимый элемент кольца $\mathcal{Z}_{p^k}$;

3) $q_0^{(3)} \circ (d \oplus b \circ (q_0^{(1)})^2 \oplus c \circ (q_0^{(2)})^2 \oplus a \circ (q_0^{(3)})^2)$ — обратимый элемент кольца $\mathcal{Z}_{p^k}$, а $1\Theta\alpha_3$ — необратимый элемент кольца $\mathcal{Z}_{p^k}$.

Рассмотрим автомат $M_{FR} \in \mathcal{A}_{FR}(p, k)$. Из (2) вытекает, что $x_1 \in X^{(1)}(M_{FR}, \mathbf{q}_0)$ тогда и только тогда, когда x_1 является решением системы уравнений

$$\begin{cases} (1\Theta\alpha_1) \circ x_1 = f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}}, \\ (1\Theta\alpha_2) \circ x_1 = f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}}, \\ (1\Theta\alpha_3) \circ x_1 = f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}}. \end{cases} \tag{40}$$

Из (40) вытекают следующие утверждения.

Утверждение 9. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если каждый элемент $1\Theta\alpha_i$ $(i = 1, 2, 3)$ является обратимым элементом кольца $\mathcal{Z}_{p^k}$, то имеет место следующее:

1) равенство $X^{(1)}(M_{FR}, \mathbf{q}_0) = \varnothing$ истинно тогда и только тогда, когда выполнено по крайней мере одно из условий:

$$(1\Theta\alpha_1)^{-1} \circ f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}} \neq (1\Theta\alpha_2)^{-1} \circ f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}}, \tag{41}$$

$$(1\Theta\alpha_1)^{-1} \circ f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}} \neq (1\Theta\alpha_3)^{-1} \circ f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}} \tag{42}$$

или

$$(1\Theta\alpha_2)^{-1} \circ f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}} \neq (1\Theta\alpha_3)^{-1} \circ f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}}; \tag{43}$$

2) равенство $|X^{(1)}(M_{FR}, \mathbf{q}_0)| = 1$ истинно тогда и только тогда, когда ни одно из условий (41)–(43) не выполнено.

Утверждение 10. Для любого простого числа p при всех значениях числа $k \in \mathbf{N}$, если существует такое значение $i \in \{1, 2, 3\}$, что $1\Theta\alpha_i$ и $f(q_0^{(i)})$ — соответственно необратимый и обратимый элементы кольца $\mathcal{Z}_{p^k}$, то $X^{(1)}(M_{FR}, \mathbf{q}_0) = \varnothing$.

ЗАКЛЮЧЕНИЕ

В настоящей работе исследованы классы $\mathcal{A}_{GH}(p,k)$ и $\mathcal{A}_{FR}(p,k)$ нелинейных автоматов над кольцом $\mathcal{Z}_{p^k}$, являющихся аналогами модельных симметрических хаотических динамических систем Guckenheimer and Holmes cycle и free-running system соответственно. Показано, что автоматы, принадлежащие этим классам, могут быть использованы в качестве кандидата на поточный шифр, способный контролировать ошибки, возникшие в процессе передачи информации по каналу связи и состоящие в инвертировании значений битов. С позиции теории автоматов охарактеризована структура автоматов, принадлежащих классам $\mathcal{A}_{GH}(p,k)$ и $\mathcal{A}_{FR}(p,k)$.

Более тонкий анализ компонентов связанности этих автоматов и множеств неподвижных точек о.-д. функций, реализуемых инициальными автоматами, — одно из возможных направлений дальнейших исследований. Второе направление предполагает детальный анализ сложности решения задач параметрической идентификации и идентификации начального состояния автоматов, принадлежащих указанным классам. Он дает возможность выбрать наиболее подходящие значения параметров при использовании такого автомата в качестве поточного шифра. Третье направление основано на разработке средств автоматизации решения задач построения классов эквивалентных состояний, параметрической идентификации и идентификации начального состояния автоматов, принадлежащих классам $\mathcal{A}_{GH}(p,k)$ и $\mathcal{A}_{FR}(p,k)$. Четвертое направление исследований связано с компьютерным анализом вычислительной стойкости шифров, построенных на основе автоматов, принадлежащих этим классам.

СПИСОК ЛИТЕРАТУРЫ

1. Скобелев В.Г. Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. — 2006. — № 6. — С. 29–42.
2. Кузнецов С.П. Динамический хаос. — М.: Физматлит, 2001. — 296 с.
3. Ashwin P., Rucklidge A.M., Sturman R. Cyclic attractors of coupled cell systems and dynamics with symmetry // Synchronization: Theory and application. NATO Science Series. — 2003. — **109**. — P. 5–23.
4. Голод П.И., Климык А.У. Математические основы теории симметрий. — Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. — 528 с.
5. Скобелев В.В. Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Тр. ИПММ НАНУ. — 2005. — **10**. — С. 184–189.
6. Гилл А. Введение в теорию конечных автоматов. — М.: Наука, 1966. — 272 с.
7. Кудрявцев В.Б., Подколзин А.С., Ушчумлич Ш. Введение в теорию конечных автоматов. — М.: Наука, 1985. — 320 с.

Поступила 15.01.2009