УДК 518.6+681.3

АНАЛИЗ FREE−RUNNING АВТОМАТА НАД КОНЕЧНЫМ КОЛЬЦОМ

В.В. СКОБЕЛЕВ

Исследован аналог над конечным кольцом хаотической динамической free-running системы. С позиции теории автоматов охарактеризована структура исследуемой модели. Решены задачи параметрической идентификации и идентификации начального состояния. Охарактеризована структура множества неподвижных точек словарной функции, реализуемой инициальным автоматом.

ВВЕДЕНИЕ

Успешное применение хаотических динамических систем при решении задач преобразования информации [1, 2] делает привлекательной разработку на их основе высокоскоростных вычислительно стойких поточных шифров. В простейшем случае построение такого шифра на основе динамической системы

$$\frac{d\bar{x}}{dt} = \bar{f}(\bar{x}, \bar{a}), \tag{1}$$

(где $\bar{x} = (x_1, \ldots, x_n)^T \in R^n$ — состояние системы в момент $t \in R_+$, а $\bar{a} = (a_1, \ldots, a_n)^T \in R^n$ — вектор параметров) состоит в дискретизации системы (1) и аддитивном внесении информационной переменной u, т.е. система (1) приводится к виду

$$\begin{cases} \bar{x}_{t+1} = h\bar{f}(\bar{x}_t, \bar{a}) + \bar{x}_t + h \cdot \alpha \cdot \bar{e}_j u_{t+1}, \\ y_{t+1} = x_{t+1}^{(j)}, \end{cases} \quad (t \in Z_+), \tag{2}$$

где $\bar{e}_j = (\underbrace{0,\ldots,0}_{j-1 \text{ раз}}, 1, \underbrace{0,\ldots,0}_{n-j \text{ раз}})^T$ и $\alpha \in R$.

Вычисления в поле действительных чисел R или, при компьютерном моделировании, в поле рациональных чисел Q наталкиваются на фактор накопления ошибок округления, из-за чего процесс «шифрование–расшифровка» теряет корректность. Чтобы избежать проблем, связанных с этими ошибками, следует перейти в (2) к вычислениям в конечной алгебраической системе. Тенденция перехода от чисто комбинаторных конструкций к конечным полям системы четко проявляется в криптографии [3, 4]. Известно, что поле — это специальный случай кольца. Наличие в кольце делителей нуля дает возможность охарактеризовать поиск через сложность решения алгебраических уравнений над кольцом. Итак, при переходе в (2) к действиям в кольце $(Z_{p^k}, \oplus, \circ)$ (где p — простое число, а операции опреде-

лены равенствами $a \oplus b = a + b \,(\mathrm{mod}\, p^k)$ и $a \circ b = a \cdot b \,(\mathrm{mod}\, p^k)$ для всех $a, b \in Z_{p^k}$) возникает класс нелинейных динамических систем над кольцом Z_{p^k}.

Актуальность исследования таких систем обусловлена следующими обстоятельствами. Во-первых, эти системы имеют нетривиальную область приложения — криптографию, так как при соответствующих ограничениях на параметры они определяют класс высокоскоростных поточных шифров, вычислительная стойкость которых может быть теоретически охарактеризована в терминах сложности решения уравнений над кольцом. Во-вторых, устанавливается связь между теорией динамических систем [5, 6] и современной криптологией [3, 4], так как сложность атаки для криптоаналитика характеризуется в терминах сложности решения классических задач теории динамических систем (управляемость, наблюдаемость, параметрическая идентификация). В-третьих, эти системы определяют новый класс конечных автоматов — класс нелинейных автоматов над кольцом, что дает возможность эффективно применить для их анализа теорию автоматов [7–10] и современную алгебру [11], т.е. устанавливается связь между теорией динамических систем, теорией автоматов и современной алгеброй. Эта связь — нетривиальная, так как такие чисто комбинаторные задачи абстрактной теории автоматов, как контрольный эксперимент с автоматом [12], для исследуемых систем сводятся к задаче параметрической идентификации, а исходя из подхода, развитого в [13], исследование управляемости и наблюдаемости для рассматриваемых систем — это задачи построения установочного и диагностического экспериментов со слабоинициальным автоматом. В-четвертых, для исследуемых систем решение классических задач теории динамических систем (таких, как параметрическая идентификация, управляемость, наблюдаемость) дает возможность выделить и изучить особенности, возникающие при переходе от поля характеристики нуль к конечным алгебраическим системам. В-пятых, применение теории конечных полей дает возможность выделить узкие классы дискретных систем, для которых решение ряда задач значительно проще, чем решение этих же задач для дискретных систем, определенных на абстрактных множествах. Примеры — исследование линейных последовательностных машин [14, 15], задач теории кодов, контролирующих ошибки [16] и многочисленные приложения, рассмотренные в работе [17].

В работах [18, 19] систематически исследован класс нелинейных динамических систем над кольцом Z_{p^k} — автоматов Мили и Мура вида, соответственно,

$$\begin{cases} \overline{q}_{t+1} = A \circ \overline{q}_t \circ \overline{q}_t^{\,T} \circ \overline{b} \oplus C \circ \overline{q}_t \oplus \overline{d} \oplus E \circ \overline{x}_{t+1}, \\ \overline{y}_{t+1} = G \circ \overline{q}_t \oplus F \circ \overline{x}_{t+1}, \end{cases} \quad (t \in Z_0), \qquad (3)$$

и

$$\begin{cases} \overline{q}_{t+1} = A \circ \overline{q}_t \circ \overline{q}_t^{\,T} \circ \overline{b} \oplus C \circ \overline{q}_t \oplus \overline{d} \oplus E \circ \overline{x}_{t+1} \\ \overline{y}_{t+1} = G \circ \overline{q}_{t+1} \end{cases} \quad (t \in Z_0), \qquad (4)$$

где $\overline{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^T$, $\overline{x}_t = (x_t^{(1)}, \ldots, x_t^{(n)})^T$ и $\overline{y}_t = (y_t^{(1)}, \ldots, y_t^{(n)})^T$ — соответственно, состояние, входной и выходной символ в момент t, $\overline{b} = (b^{(1)}, \ldots, b^{(n)})^T$ и $\overline{d} = (d^{(1)}, \ldots, d^{(n)})^T$ — фиксированные векторы, а A, C, E, G, F — фиксированные $(n \times n)$-матрицы. К таким автоматам сводится широкий класс аналогов над конечным кольцом хаотических динамических систем [2]. Однако известны примеры хаотических динамических систем, которые не укладываются в рамки моделей (3) и (4). К ним, в частности, относится free-running система [20]. Ее особенностями является то, что, во-первых, в уравнения входит операция возведения в степень, а, во-вторых, система имеет нетривиальную группу симметрий. Как известно, вычисление дискретного логарифма — одна из базовых конструкций современной криптографии [3, 4], а теория симметрий [21] — мощный аппарат анализа динамических систем.

Цель работы — исследование аналога над кольцом Z_{p^k} free-running системы с позиции криптологии free-running автомата.

ИССЛЕДУЕМАЯ МОДЕЛЬ

Free-running система [20] имеет вид

$$\begin{cases} x_{n+1} = f(x_n) \cdot e^{-\gamma \cdot z_n}, \\ y_{n+1} = f(y_n) \cdot e^{-\gamma \cdot x_n}, \quad (n \in Z_+), \\ z_{n+1} = f(z_n) \cdot e^{-\gamma \cdot y_n}, \end{cases} \tag{5}$$

где $f(x) = a \cdot x \cdot (1 - x)$ — логистическое отображение с параметром $a \in (0;4)$. Добавим аддитивно информационную переменную u в каждое уравнение системы (5). Получим систему

$$\begin{cases} x_{n+1} = f(x_n) \cdot e^{-\gamma \cdot z_n} + \alpha_1 \cdot u_{n+1}, \\ y_{n+1} = f(y_n) \cdot e^{-\gamma \cdot x_n} + \alpha_2 \cdot u_{n+1}, \quad (n \in Z_+). \\ z_{n+1} = f(z_n) \cdot e^{-\gamma \cdot y_n} + \alpha_3 \cdot u_{n+1}, \end{cases} \tag{6}$$

Перейдем в (6) к действиям в кольце Z_{p^k} и к стандартным обозначениям теории автоматов. Получим free-running автомат Мура

$$M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) = \begin{cases} q_{n+1}^{(1)} = f(q_n^{(1)}) \circ \zeta^{q_n^{(3)}} \oplus \alpha_1 \circ x_{n+1}, \\ q_{n+1}^{(2)} = f(q_n^{(2)}) \circ \zeta^{q_n^{(1)}} \oplus \alpha_2 \circ x_{n+1}, \\ q_{n+1}^{(3)} = f(q_n^{(3)}) \circ \zeta^{q_n^{(2)}} \oplus \alpha_3 \circ x_{n+1}, \\ y_{n+1}^{(i)} = q_{n+1}^{(i)} \ (i = 1, 2, 3), \end{cases} \quad (n \in Z_+), \tag{7}$$

где $f(x) = a \circ x \circ (1 \Theta x)$ (через Θ обозначена операция, обратная операции $\oplus$, т.е. $a \Theta b = c$ тогда и только тогда, когда $a = b \oplus c$). Предполагается, что

$\alpha_1, \alpha_2, \alpha_3$ и ζ — обратимые элементы кольца Z_{p^k}, $a \in Z_{p^k} \setminus \{0\}$, x — входная переменная, а $y^{(i)}$ и $q^{(i)}$ $(i = 1,2,3)$ — соответственно, выходные переменные и переменные состояния.

Обозначим через $\mathrm{A}_{FR}(p,k)$ — множество всех автоматов (7) над кольцом Z_{p^k}. Автомат (7) при условии $x_{n+1} \equiv 0$ $(n \in Z_+)$ исследован в [22]. В настоящей работе этот автомат исследуется в предположении, что $x_{n+1} \in Z_{p^k}$ $(n \in Z_+)$.

КОНЕЧНО-АВТОМАТНЫЕ ХАРАКТЕРИСТИКИ ИССЛЕДУЕМОЙ МОДЕЛИ

Охарактеризуем структуру автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$.

Применение автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$ в качестве поточного шифра состоит в следующем: параметры $\alpha_1, \alpha_2, \alpha_3, \zeta, a$ — ключ средней длительности, а начальное состояние $\overline{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ — сеансовый ключ. Критерий корректности такого процесса «шифрование–расшифровка» — условие, состоящее в том, что $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a)$ — БПИ-автомат [23–25] (т.е. по выходной последовательности и по начальному состоянию автомата поданная на автомат входная последовательность определяется однозначно). Это условие эквивалентно тому, что для любого инициального автомата $(M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a), \overline{q}_0)$ существует обратный автомат.

Утверждение 1. Для любого простого числа p при всех значениях числа $k \in N$ любой автомат $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$ — БПИ-автомат.

Доказательство. Так как $\alpha_1, \alpha_2, \alpha_3$ — обратимые элементы кольца Z_{p^k}, то из первых трех уравнений системы (7) находим

$$\begin{cases} x_{n+1} = \alpha_1^{-1} \circ (q_{n+1}^{(1)} \Theta f(q_n^{(1)}) \circ \zeta^{q_n^{(3)}}), \\ x_{n+1} = \alpha_1^{-1} \circ (q_{n+1}^{(2)} \Theta f(q_n^{(2)}) \circ \zeta^{q_n^{(1)}}), \\ x_{n+1} = \alpha_1^{-1} \circ (q_{n+1}^{(3)} \Theta f(q_n^{(3)}) \circ \zeta^{q_n^{(2)}}). \end{cases} \tag{8}$$

Из последних трех уравнений системы (7) получим, что для всех $n \in Z_+$

$$q_n^{(i)} = y_n^{(i)} \quad (i = 1,2,3), \tag{9}$$

где $\overline{y}_0 = \overline{q}_0$. Подставим (9) в (8) и заменим x на y, а y на x. Получим

$$M_{FR}^{-1}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) = \begin{cases} y_{n+1} = \alpha_1^{-1} \circ (x_{n+1}^{(1)} \Theta f(x_n^{(1)}) \circ \zeta^{x_n^{(3)}}), \\ y_{n+1} = \alpha_1^{-1} \circ (x_{n+1}^{(2)} \Theta f(x_n^{(2)}) \circ \zeta^{x_n^{(1)}}), \\ y_{n+1} = \alpha_1^{-1} \circ (x_{n+1}^{(3)} \Theta f(x_n^{(3)}) \circ \zeta^{x_n^{(2)}}), \end{cases} \quad (n \in Z_+). \tag{10}$$

Утверждение доказано.

Замечание 1. Сравнивая (7) и (10), нетрудно заметить, что в процессе «шифрование-расшифровка» автоматы $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ и $M_{FR}^{-1}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ движутся по одной и той же траектории в пространстве состояний.

Замечание 2. Предположим, что элементы кольца Z_{p^k} представлены двоичными последовательностями длины $l=\lceil k\cdot\log p\rceil$. Рассмотрим очередную последовательность $\gamma_1\ldots\gamma_{3\cdot l}$, сгенерированную автоматом $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$. Предположим, что выходы автомата $M_{FR}^{-1}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ подсоединены к входам мажоритарной схемы. Из (10) вытекает, что в процессе расшифровки будут обнаружены все ошибки, возникшие в процессе передачи информации по каналу связи, состоящие в инвертировании значений битов и определяемые равенством $\gamma_i\oplus\gamma_{l+i}\oplus\oplus\gamma_{2\cdot l+i}\neq 0$ $(i\in\{1,\ldots,l\})$. При этом будут исправлены все ошибки, для которых в каждой тройке бит $\gamma_i,\gamma_{l+i},\gamma_{2\cdot l+i}$ ошибка произошла не более, чем в одном бите.

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

$$|\mathrm{A}_{FR}(p,k)|=(p^k-1)\cdot p^{4\cdot k}\cdot(p^{-1}\cdot(p-1))^4. \qquad (11)$$

Доказательство. В автомате $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in\mathrm{A}_{FR}(p,k)$ параметры $\alpha_1,\alpha_2,\alpha_3$ и ς — обратимые элементы кольца Z_{p^k}, а $a\in Z_{p^k}\setminus\{0\}$. Число обратимых элементов кольца Z_{p^k} равно $p^{k-1}\cdot(p-1)$. Выбор параметров $\alpha_1,\alpha_2,\alpha_3,\zeta,a$ осуществляется независимо. Сюда вытекает справедливость равенства (11).

Утверждение доказано.

Утверждение 3. Для любого простого числа p при всех значениях числа $k\in N$ автомат $M_{FR}(\alpha,\alpha,\alpha,\zeta,a)\in\mathrm{A}_{FR}(p,k)$ не является сильно связным.

Доказательство. Пусть $\overline{q}_0=(q_0,q_0,q_0)\in Z_{p^k}^3$. Из (7) вытекает, что $\overline{q}_1=(q_1,q_1,q_1)$ для любого входного символа $x_1\in Z_{p^k}$. Индукцией по длине слова можно показать, что $\overline{q}_n=(q_n,q_n,q_n)$ для любого входного слова $x_1\ldots x_n\in Z_{p^k}^n$.

Так как α — обратимый элемент кольца Z_{p^k}, то из (7) вытекает, что для любых фиксированных состояний $\overline{q}_0=(q_0,q_0,q_0)\in Z_{p^k}^3$ и $\overline{q}_1=(q_1,q_1,q_1)\in Z_{p^k}^3$ автомата $M_{FR}(\alpha,\alpha,\alpha,\zeta,a)$ существует единственный входной символ $x\in Z_{p^k}$, переводящий состояние $\overline{q}_0$ в состояние $\overline{q}_1$.

Следовательно, собственное подмножество $S_1 = \{\overline{q} = (q,q,q) \mid q \in Z_{p^k}\}$ состояний автомата $M_{FR}(\alpha,\alpha,\alpha,\zeta,a)$ определяет компоненту сильной связанности, т.е. автомат $M_{FR}(\alpha,\alpha,\alpha,\zeta,a)$ не является сильно связным.

Утверждение доказано.

Из доказательства утверждения 3 вытекает следствие 1.

Следствие 1. Для любого простого числа p при всех значениях числа $k \in N$ подавтомат автомата $M_{FR}(\alpha,\alpha,\alpha,\zeta,a) \in \mathrm{A}_{FR}(p,k)$, определяемый множеством состояний $S_1 = \{\overline{q} = (q,q,q) \mid q \in Z_{p^k}\}$, является перестановочным приведенным автоматом, диаметр графа переходов которого равен 1.

Структура любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathrm{A}_{FR}(p,k)$ существенно отличается от структуры подавтомата автомата $M_{FR}(\alpha,\alpha,\alpha,\zeta,a) \in$ $\in \mathrm{A}_{FR}(p,k)$, определяемого множеством состояний $S_1 = \{\overline{q} = (q,q,q) \mid q \in$ $\in Z_{p^k}\}$. В частности, из (7) вытекает утверждение 4.

Утверждение 4. Для любого простого числа p при всех значениях числа $k \in N$ множество состояний $S_2 = \{\overline{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \mid q^{(i)} \in \{0,1\}$ $(i = 1,2,3)\}$ любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in A_{FR}(p,k)$ под действием любого входного символа $x \in Z_{p^k}$ переходит в одно и то же состояние $\overline{q}' = (\alpha_1 \circ x, \alpha_2 \circ x, \alpha_3 \circ x)$.

Из утверждения 4 вытекает следствие 2.

Следствие 2. Для любого простого числа p при всех значениях числа $k \in N$ любой автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathrm{A}_{FR}(p,k)$ не является перестановочным автоматом.

Обозначим через $K(\overline{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ множество всех состояний автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in \mathrm{A}_{FR}(p,k)$, эквивалентных состоянию $\overline{q} \in Z^3_{p^k}$.

Теорема 1. Для любого простого числа p при всех значениях числа $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ для любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a) \in$ $\in \mathrm{A}_{FR}(p,k)$ и любого состояния $\overline{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in Z^3_{p^k}$ множество $K(\overline{q}, M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ состоит из всех таких состояний $\overline{q}' = (\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)}) \in Z^3_{p^k}$, что истинны равенства

$$\begin{cases} f(\widetilde{q}^{(1)}) \circ \zeta^{\widetilde{q}^{(3)} - q^{(3)}} = f(q^{(1)}), \\ f(\widetilde{q}^{(2)}) \circ \zeta^{\widetilde{q}^{(1)} - q^{(1)}} = f(q^{(2)}), \\ f(\widetilde{q}^{(3)}) \circ \zeta^{\widetilde{q}^{(2)} - q^{(2)}} = f(q^{(3)}). \end{cases} \qquad (12)$$

Доказательство. Зафиксируем автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in$ $\in \mathrm{A}_{FR}(p,k)$ и состояние $\overline{q}=(q^{(1)},\ q^{(2)},\ q^{(3)})\in Z^3_{p^k}$. Пусть $\overline{q}'=(\widetilde{q}^{(1)},\ \widetilde{q}^{(2)},\ \widetilde{q}^{(3)})\in$ $\in K(\overline{q},M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$. Из первых трех уравнений системы (7) находим, что для любого входного символа $x\in Z_{p^k}$

$$\begin{cases} q_1^{(1)}=f(q^{(1)})\circ\zeta^{q^{(3)}}\oplus\alpha_1\circ x_{n+1},\\ q_1^{(2)}=f(q^{(2)})\circ\zeta^{q^{(1)}}\oplus\alpha_2\circ x_{n+1},\\ q_1^{(3)}=f(q^{(3)})\circ\zeta^{q^{(2)}}\oplus\alpha_3\circ x_{n+1}, \end{cases} \tag{13}$$

и

$$\begin{cases} \widetilde{q}_1^{(1)}=f(\widetilde{q}^{(1)})\circ\zeta^{\widetilde{q}^{(3)}}\oplus\alpha_1\circ x_{n+1},\\ \widetilde{q}_1^{(2)}=f(\widetilde{q}^{(2)})\circ\zeta^{\widetilde{q}^{(1)}}\oplus\alpha_2\circ x_{n+1},\\ \widetilde{q}_1^{(3)}=f(\widetilde{q}^{(3)})\circ\zeta^{\widetilde{q}^{(2)}}\oplus\alpha_3\circ x_{n+1}. \end{cases} \tag{14}$$

Так как $\overline{q}$ и $\overline{q}'$ — эквивалентные состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, то из последних трех уравнений системы (7) вытекает, что

$$q_1^{(i)}=\widetilde{q}_1^{(i)}\ \ (i=1,2,3). \tag{15}$$

Из (13)–(15) следует, что

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

$$\Leftrightarrow\begin{cases} f(q^{(1)})\circ\zeta^{q^{(3)}}=f(\widetilde{q}^{(1)})\circ\zeta^{\widetilde{q}^{(3)}},\\ f(q^{(2)})\circ\zeta^{q^{(1)}}=f(\widetilde{q}^{(2)})\circ\zeta^{\widetilde{q}^{(1)}},\\ f(q^{(3)})\circ\zeta^{q^{(2)}}=f(\widetilde{q}^{(3)})\circ\zeta^{\widetilde{q}^{(2)}}. \end{cases} \tag{16}$$

Так как ζ — обратимый элемент кольца Z_{p^k}, то из (16) вытекает (12).

Теорема доказана.

Состояния $q,q'\in Q$ автомата $M=(Q,X,Y,\delta,\lambda)$ — близнецы, если $\delta(q,x)=\delta(q',x)$ и $\lambda(q,x)=\lambda(q',x)$ для любого входного символа $x\in X$. Из доказательства теоремы 1 вытекает следствие 3.

Следствие 3. Для любого простого числа p при всех значениях числа $k\in N$ эквивалентные состояния любого автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in$ $\in \mathrm{A}_{FR}(p,k)$ — близнецы.

Множество $K(\overline{q},M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a))$ может быть вычислено следующим образом.

Пусть число ζ принадлежит показателю δ, т.е. δ — такое наименьшее натуральное число, что $\zeta^{\delta} \equiv 1 (\mathrm{mod}\, p^k)$. Представим компоненты состояния $\overline{q} = (q^{(1)}, q^{(2)}, q^{(3)}) \in Z_{p^k}^3$ в виде $q^{(i)} = \zeta^{h_i} \circ b_i$ $(i = 1,2,3)$, где $(b_i, \zeta) = 1$ $(i = 1,2,3)$. Из (12) вытекает, что компоненты любого состояния $\overline{q}' = (\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)}) \in K(\overline{q}, M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a))$ удовлетворяют равенствам

$$\begin{cases} f(\widetilde{q}^{(1)}) = \zeta^{l_3} \circ b_1, \\ f(\widetilde{q}^{(2)}) = \zeta^{l_1} \circ b_2, \\ f(\widetilde{q}^{(3)}) = \zeta^{l_2} \circ b_3. \end{cases} \tag{17}$$

Из (12) и (17) вытекает, что

$$\begin{cases} \widetilde{q}^{(1)} \equiv h_1 \oplus q^{(1)} \Theta l_1 \ (\mathrm{mod}\, \delta), \\ \widetilde{q}^{(2)} \equiv h_2 \oplus q^{(2)} \Theta l_2 \ (\mathrm{mod}\, \delta), \\ \widetilde{q}^{(3)} \equiv h_3 \oplus q^{(3)} \Theta l_3 \ (\mathrm{mod}\, \delta). \end{cases} \tag{18}$$

Итак, для построения множества $K(\overline{q}, M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a))$ достаточно найти все решения $(\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)})$ систем сравнений (18) при всех значениях $l_1, l_2, l_3 \in \{0,1,\ldots,\delta - 1\}$. При этом $(\widetilde{q}^{(1)}, \widetilde{q}^{(2)}, \widetilde{q}^{(3)}) \in$ $\in K(\overline{q}, M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a))$ тогда и только тогда, когда истинны равенства (17).

ЗАДАЧИ ИДЕНТИФИКАЦИИ ИССЛЕДУЕМОЙ МОДЕЛИ

Рассмотрим задачу параметрической идентификации автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$ в предположении, что экспериментатор может управлять входом и инициализацией автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a)$.

Утверждение 5. Для любого простого числа p при всех значениях числа $k \in N$ идентификация параметров $\alpha_1, \alpha_2, \alpha_3$ автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$ осуществляется простым экспериментом длины 1.

Доказательство. Положим $q_0^{(1)} = q_0^{(2)} = q_0^{(3)} = 0$ и $x = 1$. Из (7) вытекает, что $\alpha_i = y_1^{(i)}$ $(i = 1,2,3)$.

Утверждение доказано.

Теорема 2. Для любого простого числа $p \geq 3$ при всех значениях числа $k \in N$, если известны параметры $\alpha_1, \alpha_2, \alpha_3$ автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p,k)$, а также известно, что a — обратимый элемент кольца Z_{p^k}, то идентификация параметров a и ζ сводится к решению системы двух уравнений, полученной в результате простого эксперимента длины 1.

Доказательство. Пусть a — обратимый элемент кольца Z_{p^k}. Присвоив $q_0^{(1)} = 2$, $q_0^{(2)} = 2$ и $q_0^{(3)} = 1$. Из (7) вытекает, что для любого входного символа $x_1 \in Z_{p^k}$

$$\begin{cases} \zeta \circ a \circ 2 \circ (p^k - 1) = y_1^{(1)} \Theta \alpha_1 \circ x_1, \\ \zeta^2 \circ a \circ 2 \circ (p^k - 1) = y_1^{(2)} \Theta \alpha_2 \circ x_1. \end{cases} \tag{19}$$

Так как $p \geq 3$, то 2 и $p^k - 1$ — обратимые элементы кольца Z_{p^k}. А так как a — обратимый элемент кольца Z_{p^k} и система (19) — совместная, то $y_1^{(i)} \Theta \alpha_i \circ x_1$ $(i = 1, 2)$ — обратимые элементы кольца Z_{p^k}. Следовательно, из (19) вытекает, что

$$\begin{cases} \zeta = (y_1^{(1)} \Theta \alpha_1 \circ x_1)^{-1} \circ (y_1^{(2)} \Theta \alpha_2 \circ x_1), \\ a = (y_1^{(1)} \Theta \alpha_1 \circ x_1)^2 \circ (y_1^{(2)} \Theta \alpha_2 \circ x_1)^{-1} \circ 2^{-1} \circ (p^k - 1)^{-1}. \end{cases}$$

Теорема доказана.

Замечание 3. Метод доказательства, используемый в теореме 2, не применим, если $p = 2$. Действительно, пусть a — обратимый элемент кольца Z_{p^k}. Если $p = 2$ и $k = 1$, то $\zeta = 1$ и $a = 1$. Если же $p = 2$ и $k > 1$, то $x \circ (1 \Theta x)$ — необратимый элемент кольца Z_{p^k} для любого $x \in Z_{p^k}$. Поэтому, присвоив $q_0^{(1)} = 2$, $q_0^{(2)} = 1$ и $q_0^{(3)} = 0$, получим

$$\begin{cases} a \circ 2 \circ (p^k - 1) = y_1^{(1)} \Theta \alpha_1 \circ x_1, \\ \zeta^2 \circ a \circ 2 \circ (p^k - 1) = y_1^{(2)} \Theta \alpha_2 \circ x_1. \end{cases} \tag{20}$$

Все решения (a, ζ) этой системы обладают тем свойством, что при их подстановке в (7) получим эквивалентные друг другу автоматы. Это означает, что идентификация параметров a и ζ может быть осуществима только с точностью до множества решений системы (20).

Идентификация параметров a и ζ существенно усложняется, если a — необратимый элемент кольца Z_{p^k}. В этом случае вначале необходимо найти все решения a и ζ системы уравнений (19), а затем обычными методами теории автоматов с помощью кратного эксперимента решить задачу идентификации автомата в классе допустимых автоматов $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p, k)$.

Рассмотрим теперь задачу идентификации начального состояния автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a) \in \mathrm{A}_{FR}(p, k)$ в предположении, что экспериментатору известны параметры $\alpha_1, \alpha_2, \alpha_3, \zeta, a$ автомата и он может управлять входом автомата $M_{FR}(\alpha_1, \alpha_2, \alpha_3, \zeta, a)$.

Предположим вначале, что экспериментатор имеет возможность управлять также параметрами автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, а $p^k > 4$. Положим $a = 4$ и $\zeta = 1$. Из (7) вытекает, что для любого входного символа $x_1 \in Z_{p^k}$

$$\begin{cases} (2 \circ q_0^{(1)} \Theta 1)^2 = \alpha_1 \circ x_1 \Theta y_1^{(1)} \oplus 1, \\ (2 \circ q_0^{(2)} \Theta 1)^2 = \alpha_2 \circ x_1 \Theta y_1^{(2)} \oplus 1, \\ (2 \circ q_0^{(3)} \Theta 1)^2 = \alpha_3 \circ x_1 \Theta y_1^{(3)} \oplus 1. \end{cases} \tag{21}$$

Множество S решений $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)})$ системы уравнений (20) 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 $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, принадлежащие множеству S (если такие имеются), необходимо различить с помощью простого диагностического эксперимента.

Предположим теперь, что экспериментатор не может управлять параметрами автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$. Из (7) вытекает, что для любого входного символа $x_1 \in Z_{p^k}$

$$\begin{cases} f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}} = y_1^{(1)} \Theta \alpha_1 \circ x_1, \\ f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}} = y_1^{(2)} \Theta \alpha_2 \circ x_1, \\ f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}} = y_1^{(3)} \Theta \alpha_3 \circ x_1. \end{cases} \tag{22}$$

Так как система уравнений (22) — совместная, то

$$\begin{cases} y_1^{(1)} \Theta \alpha_1 \circ x_1 = b_1 \circ \zeta^{h_3}, \\ y_1^{(2)} \Theta \alpha_1 \circ x_1 = b_2 \circ \zeta^{h_1}, \\ y_1^{(3)} \Theta \alpha_1 \circ x_1 = b_3 \circ \zeta^{h_2}, \end{cases} \tag{23}$$

где $(b_i, \zeta) = 1$ $(i = 1,2,3)$. Из (22) и (23) следует, что

$$\begin{cases} f(q_0^{(1)}) = \zeta^{l_3} \circ b_1, \\ f(q_0^{(2)}) = \zeta^{l_1} \circ b_2, \\ f(q_0^{(3)}) = \zeta^{l_2} \circ b_3. \end{cases} \tag{24}$$

Пусть число ζ принадлежит показателю δ. Подставим (23) и (24) в (22). Получим

$$\begin{cases} q_0^{(1)} = h_1 \Theta l_1 \pmod{\delta}, \\ q_0^{(2)} = h_2 \Theta l_2 \pmod{\delta}, \\ q_0^{(3)} = h_3 \Theta l_3 \pmod{\delta}. \end{cases} \tag{25}$$

Таким образом, для идентификации начального состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathrm{A}_{FR}(p,k)$ достаточно найти множество S_1 всех решений $(q_0^{(1)},q_0^{(2)},q_0^{(3)})$ систем сравнений (25) при всех значениях $l_1,l_2,l_3\in\{0,1,\ldots,\delta-1\}$, вычислить подмножество S_2, состоящее из всех элементов $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)})\in S_1$, удовлетворяющих системе уравнений (24) и различить неэквивалентные состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, принадлежащие множеству S_2 (если такие имеются) с помощью простого диагностического эксперимента.

НЕПОДВИЖНЫЕ ТОЧКИ ИССЛЕДУЕМОЙ МОДЕЛИ

Зафиксируем автомат $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)\in \mathrm{A}_{FR}(p,k)$ и начальное состояние $\overline{q}=(q_0^{(1)},q_0^{(2)},q_0^{(3)})$. Обозначим через $X(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)$ множество всех неподвижных точек словарной функции, реализуемой инициальным автоматом $(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)$. Положим

$$X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)=X(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)\cap Z_{p^k}.$$

Из (7) вытекает, что $x_1\in X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)$ тогда и только тогда, когда x_1 является решением системы уравнений

$$\begin{cases}(1\Theta\alpha_1)\circ x_1=f(q_0^{(1)})\circ\zeta^{q_0^{(3)}},\\ (1\Theta\alpha_2)\circ x_1=f(q_0^{(2)})\circ\zeta^{q_0^{(1)}},\\ (1\Theta\alpha_3)\circ x_1=f(q_0^{(3)})\circ\zeta^{q_0^{(2)}}.\end{cases}\qquad(26)$$

Из (26) вытекают утверждение 6 и 7.

Утверждение 6. Для любого простого числа p при всех значениях числа $k\in N$, если каждый элемент $1\Theta\alpha_i$ $(i=1,2,3)$ — обратимый элемент кольца Z_{p^k}, то:

- $X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)=\varnothing$ тогда и только тогда, когда

$$|\{(1\Theta\alpha_1)^{-1}\circ f(q_0^{(1)})\circ\zeta^{q_0^{(3)}},(1\Theta\alpha_2)^{-1}\circ f(q_0^{(2)})\circ\zeta^{q_0^{(1`)}},$$

$$(1\Theta\alpha_3)^{-1}\circ f(q_0^{(3)})\circ\zeta^{q_0^{(2)}}\}|\ge 2;$$

- $|X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)|=1$ тогда и только тогда, когда

$$|\{(1\Theta\alpha_1)^{-1}\circ f(q_0^{(1)})\circ\zeta^{q_0^{(3)}},(1\Theta\alpha_2)^{-1}\circ f(q_0^{(2)})\circ\zeta^{q_0^{(1`)}},$$

$$(1\Theta\alpha_3)^{-1}\circ f(q_0^{(3)})\circ\zeta^{q_0^{(2)}}\}|=1.$$

Утверждение 7. Для любого простого числа p при всех значениях числа $k \in N$, 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 Z_{p^k}, то $X^{(1)}(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0) = \varnothing$.

ВЫВОДЫ

В работе определен и исследован класс $\mathrm{A}_{FR}(p,k)$ автоматов $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$, являющихся аналогами над кольцом Z_{p^k} хаотической динамической free-running системы. Показано, что автоматы, принадлежащие классу $\mathrm{A}_{FR}(p,k)$, 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 автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$. Более тонкий анализ компонент связанности автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ и множества неподвижных точек словарной функции, реализуемой инициальным автоматом $(M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a),\overline{q}_0)$, представляет собой одно из возможных направлений дальнейших исследований.

Второе направление исследований связано с детальным анализом сложности решения задач параметрической идентификации и идентификации начального состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ с целью выделения наиболее подходящих значений параметров $\alpha_1,\alpha_2,\alpha_3,\zeta,a$ при использовании автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$ в качестве поточного шифра.

Третье направление исследований связано с разработкой средств автоматизации решения задач построения классов эквивалентных состояний, параметрической идентификации и идентификации начального состояния автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$.

Четвертое направление исследований связано с компьютерным анализом вычислительной стойкости шифра, построенного на основе автомата $M_{FR}(\alpha_1,\alpha_2,\alpha_3,\zeta,a)$.

ЛИТЕРАТУРА

1. *Андреев Ю.В., Дмитриев А.С., Куминов Д.А.* Хаотические процессоры // Радиотехника и электроника. — 1997. — **42,** Вып. 10. — С. 50–79.
2. *Кузнецов С.П.* Динамический хаос. — М.: Физматлит, 2001. — 296 с.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — М.: ТРИУМФ, 2003. — 816 с.
4. *Харин Ю.С., Берник В.И., Матвеев Б.В.* Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 382 с.
5. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. — М.: Мир, 1971. — 400 с.

6. *Льюнг Л.* Идентификация систем. Теория для пользователя. — М.: Наука, 1991. — 432 с.
7. *Глушков В.М.* Синтез цифровых автоматов. — М.: Физматлит, 1962. — 476 с.
8. *Гилл А.* Введение в теорию конечных автоматов. — М.: Наука, 1966. — 272 с.
9. *Трахтенброт Б.А.* Конечные автоматы (поведение и синтез). — М.: Наука, 1970. — 400 с.
10. *Кудрявцев В.Б.*, *Подколзин А.С.* Введение в теорию конечных автоматов. — М.: Наука, 1985. — 320 с.
11. *Кострикин А.И.* Введение в алгебру. — Т. 1–3. — М.: Наука, 1999–2000. — 818 с.
12. *Hennie F.C.* Finite state models for logical machines. — NY: John Wiley&Sons, Inc., 1962. — 466 p.
13. *Горяшко А.П.* Проектирование легко тестируемых дискретных устройств: идеи, методы, реализация // АиТ. — 1984. — № 7. — С. 5–35.
14. *Гилл А.* Линейные последовательностные машины. — М.: Наука, 1974. — 287 с.
15. *Фараджев Р.Г.* Линейные последовательностные машины. — М.: Сов. Радио, 1975. — 248 с.
16. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. — М.: Мир, 1986. — 576 с.
17. *Лидл Р., Нидеррайтер Г.* Конечные поля. — Т. 1–2. — М.: Мир, 1988. — 820 с.
18. *Скобелев В.Г.* Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. — 2006. — № 6. — С. 29–42.
19. *Скобелев В.Г.* О некоторых свойствах нелинейных БПИ-автоматов над кольцом Z_{p^k} // Прикладная радиоэлектроника. — 2007. — **6.** — № 2. — С. 288–299.
20. *Aswin P.*, *Ruclidge A.M.*, *Sturman R.* Cyclic attractors of coupled cell systems and dynamics with symmetry // Syncronization: Theory and Application. NATO Science Series. II. Mathematics, Physics and Chemistry. Kluver Academic Publishers. — 2003. — **109**. — P. 5–23.
21. *Голод П.И.*, *Климык А.У.* Математические основы теории симметрий. — Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. — 528 с.
22. *Скобелев В.В.* Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Труды ИПММ НАНУ. — 2005. — **10.** — С. 184–189.
23. *Even S.* On information lossless automata of finite order // IEEE Transactions Election Computation — 1965. — **C-14**, № 4. — P. 561–569.
24. *Huffman D.A.* Canonical forms for information-lossless finite stste logical machines // IRE Transactions on Circuit Theory. Special Supplement,1959. — **CT-6.** — P. 41–59.
25. *Курмит А.* Автоматы без потери информации конечного порядка. — Рига: Зинатне, 1972. — 266 с.

Поступила 02.07.2008