УДК 519.713+512.552

В.В. СКОБЕЛЕВ, В.Г. СКОБЕЛЕВ

О СЛОЖНОСТИ АНАЛИЗА АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

Ключевые слова: *конечные автоматы, конечные кольца, симметричные поточные шифры.*

ВВЕДЕНИЕ

Несмотря на большое многообразие используемых математических моделей (часто не сравнимых между собой) в последнее время в криптографии наметилась устойчивая тенденция перехода от чисто комбинаторных моделей к математическим моделям, построенным на основе конечных алгебраических систем. В то же время многочисленные попытки непосредственного применения хаотических динамических систем [1] при решении задач криптографии показали, что при этом возникает задача выбора точности вычислений, обеспечивающей корректность процесса «шифрование – расшифровка». С математической точки зрения для кусочно-линейных хаотических отображений ее решение не очень сложно [2, 3]. Однако даже для конкретных типов нелинейных хаотических динамических систем решение этой задачи пока не найдено. Естественным способом избежать ошибок, связанных с округлением, является переход в уравнениях, определяющих хаотическую динамическую систему, к операциям в конечной алгебраической системе. Перечисленные факторы стимулировали в последнее время интерес к исследованию автоматов, представленных системами уравнений над конечными алгебраическими системами.

Основы теории линейных автоматов над полем $GF(p^k)$ (где p — простое число, $k \in \mathbf{N}$) с позиции теории систем разработаны почти 40 лет тому назад [4, 5]. Однако эти исследования не дали эффективных результатов для решения задач криптографии в силу следующих причин.

Свойство «быть линейным автоматом» накладывает существенные ограничения на автоматное отображение, реализуемое инициальным автоматом (по-видимому, наиболее значимым приложением линейных автономных автоматов является их использование в качестве генераторов псевдослучайных последовательностей). В работах [4, 5] не рассматривались задачи, которые бы с позиции теории алгоритмов обосновывали вычислительную стойкость поточных шифров, построенных на основе автоматов над полем $GF(p^k)$. Такие задачи формируют специальное направление в теории экспериментов с автоматами (некоторые типы экспериментов с автоматами над конечными полями рассмотрены в [6–8]). Предметом его исследования является анализ сложности идентификации параметрически настраиваемых обратимых автоматов, множества неподвижных точек отображения, реализуемого инициальным обратимым автоматом, а также изменения поведения обратимого автомата при вариации его параметров и/или начального состояния.

Известно, что поле — специальный случай коммутативно-ассоциативного кольца с единицей [9]. При этом в кольце (в отличие от поля) наличие делителей нуля существенно усложняет структуру множеств решений уравнений (даже линейное уравнение может иметь экспоненциальное число решений), а также дает возможность охарактеризовать сложность поиска при решении задач идентификации в терминах мощности множеств решений соответствующих уравнений. По-видимому, именно это обстоятельство и послужило основным стимулом для исследования классов автоматов над конечными коммутативно-ассоциативными кольцами с единицей.

Систематический анализ автономных линейных и полилинейных автоматов над конечными кольцами представлен в [10, 11]. В работах [12–15] с позиции криптографии исследованы множества автоматов Мили и Мура над кольцом $\mathcal{Z}_m = (\mathbf{Z}_m, \oplus, \circ)$ (где $m \in \mathbf{N}$, $a \oplus b = a + b \pmod m$ и $a \circ b = a \cdot b \pmod m$) в случае, когда $m = p^k$ (где p — простое число, $k \in \mathbf{N}$). В [12] исследованы линейные автоматы, а в [13] — линейные одномерные автоматы с лагом l. В [14] рассмотрены нелинейные автоматы, у 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. В [15] исследованы нелинейные обратимые симметричные автоматы, построенные на основе Guckenheimer and Holms cycle и free-running system — двух модельных хаотических динамических симметричных систем.

Несмотря на то что в [12–15] выбрано кольцо $\mathcal{Z}_{p^k}$, полученные результаты могут быть естественным образом обобщены на любое конечное коммутативно-ассоциативное кольцо с единицей $\mathcal{K} = (K, +, \cdot)$ (в дальнейшем, для краткости, — кольцо $\mathcal{K}$). Настоящая работа посвящена анализу моделей и методов, лежащих в основе построения таких обобщений. В разд. 1 с позиции теории алгоритмов охарактеризована общая схема, предназначенная для вычисления оценок, основанных на мощности подмножеств заданного множества автоматов над кольцом $\mathcal{K}$. В разд. 2 предложен подход к решению над кольцом $\mathcal{K}$ систем полиномиальных уравнений с параметрами, основанный на использовании классов ассоциированных элементов кольца. Некоторые особенности применения этой схемы проиллюстрированы на примере решения конкретной системы. В разд. 3 установлен ряд общих характеристик автоматов над кольцом $\mathcal{K}$. Заключение содержит ряд выводов.

1. СХЕМА АНАЛИЗА КОНЕЧНО-АВТОМАТНЫХ ХАРАКТЕРИСТИК МОДЕЛЕЙ

Пусть множество $\mathbf{A}$ автоматов над кольцом $\mathcal{K}$ определяется конечным множеством S параметров, причем выбор значения каждого параметра осуществляется независимо из конечного множества Ω возможных значений. Тогда

$$|\mathbf{A}| = |\Omega|^{|S|}. \tag{1}$$

Анализ принадлежности автоматов нетривиальным подмножествам множества $\mathbf{A}$, характеризуемым в терминах теории автоматов («быть перестановочным автоматом», «быть приведенным автоматом», «быть сильносвязным автоматом», «иметь данную степень различимости состояний», «иметь данный диаметр графа переходов», «быть обратимым автоматом» и т.д.), укладывается в рамки следующей схемы.

Схема 1. Фиксируются непустые попарно непересекающиеся подмножества Ω_i $(i = 1, \ldots, l)$ множества Ω, а также непустые попарно непересекающиеся подмножества S_i $(i = 1, \ldots, l)$ множества S. Далее доказывается одно из следующих трех утверждений.

Утверждение 1 (достаточное условие). Если параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения из множества Ω_i, то автомат $M \in \mathbf{A}$ принадлежит подмножеству $\mathbf{A}_1$ множества $\mathbf{A}$.

Утверждение 2 (необходимое условие). Если автомат $M \in \mathbf{A}$ принадлежит подмножеству $\mathbf{A}_1$ множества $\mathbf{A}$, то параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения из множества Ω_i.

Утверждение 3 (критерий). Автомат $M \in \mathbf{A}$ принадлежит подмножеству $\mathbf{A}_1$ множества $\mathbf{A}$ тогда и только тогда, когда параметры, принадлежащие подмножеству S_i $(i = 1, \ldots, l)$, принимают значения из множества Ω_i.

Из схемы 1 вытекает следующая характеристика множества $\mathbf{A}_1$.

Теорема 1. Если истинно утверждение i $(i=1,2,3)$, то истинна оценка

$$|\mathbf{A}_1| \Diamond |\mathbf{A}| \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{2}$$

где

$$\Diamond = \begin{cases} \geq, \text{ если истинно утверждение 1,} \\ \leq, \text{ если истинно утверждение 2,} \\ =, \text{ если истинно утверждение 3.} \end{cases} \tag{3}$$

Доказательство. Из формулировки утверждений 1–3, а также определения множества автоматов $\mathbf{A}$ вытекает, что при построении автомата $M \in \mathbf{A}_1$ осуществляется независимый выбор из множества Ω_i $(i=1,\dots,l)$ значений параметров, принадлежащих подмножеству S_i, а также независимый выбор из множества Ω значений параметров, принадлежащих подмножеству $S \setminus (\bigcup_{i=1}^{l} S_i)$. При этом S_i $(i=1,\dots,l)$ — попарно непересекающиеся подмножества. Поэтому

$$|\mathbf{A}_1| \Diamond \prod_{i=1}^{l} |\Omega_i|^{|S_i|} |\Omega|^{|S| - \sum_{i=1}^{l} |S_i|} = |\Omega|^{|S|} \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{4}$$

где $\Diamond$ определяется формулой (3). Воспользовавшись в (4) формулой (1), получим (2).

Теорема доказана.

Следствие 1. Если на множестве Ω задано равномерное распределение, а $\mathbf{P}_{\mathbf{A}_1}$ — вероятность того, что случайно выбранный автомат $M \in \mathbf{A}$ принадлежит множеству $\mathbf{A}_1$, то

$$\mathbf{P}_{\mathbf{A}_1} \Diamond \prod_{i=1}^{l} \left(\frac{|\Omega_i|}{|\Omega|} \right)^{|S_i|}, \tag{5}$$

где $\Diamond$ определяется формулой (3).

Доказательство. Так как выбор значения каждого параметра, принадлежащего множеству S, осуществляется независимо из конечного множества Ω, на котором задано равномерное распределение, то на множестве $\mathbf{A}$ также задано равномерное распределение. Следовательно,

$$\mathbf{P}_{\mathbf{A}_1} = \frac{|\mathbf{A}_1|}{|\mathbf{A}|}. \tag{6}$$

Подставив (1) и (2) в (6), получим (5).

Следствие доказано.

Под «временной сложностью» будем понимать «временную сложность в худшем случае», т.е. наибольшее время, необходимое алгоритму для анализа объекта, если объект принадлежит заданному конечному множеству объектов.

Обозначим T_{S_i} $(i=1,\dots,l)$ временную сложность проверки принадлежности параметра $s \in S$ множеству S_i (т.е. временную сложность проверки того, что значение параметра $s \in S$ принадлежит множеству Ω_i), а $T_{\mathbf{A}_1}$ — временную сложность проверки принадлежности автомата $M \in \mathbf{A}$ множеству $\mathbf{A}_1$. Из формулировки утверждений 2 и 3 вытекает

$$T_{\mathbf{A}_1} \begin{cases} \geq \sum_{i=1}^{l} |S_i| T_{S_i}, \text{ если истинно утверждение 2,} \\ = \sum_{i=1}^{l} |S_i| T_{S_i}, \text{ если истинно утверждение 3.} \end{cases} \tag{7}$$

Выделим два специальных случая рассмотренной схемы.

Случай 1. Пусть $l = 1$. Тогда формулы (2), (5) и (7) принимают соответственно вид

$$|\mathbf{A}_1| \lozenge |\mathbf{A}| \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{8}$$

$$\mathbf{P}_{\mathbf{A}_1} \lozenge \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|}, \tag{9}$$

$$T_{\mathbf{A}_1} \begin{cases} \geq |S_1| T_{S_1}, \text{ если истинно утверждение 2,} \\ = |S_1| T_{S_1}, \text{ если истинно утверждение 3.} \end{cases} \tag{10}$$

Случай 2. Пусть $l = 2$ и $\Omega_1 \cup \Omega_2 = \Omega$. Тогда формулы (2), (5) и (7) принимают соответственно вид

$$|\mathbf{A}_1| \lozenge |\mathbf{A}| \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|} \left(1 - \frac{|\Omega_1|}{|\Omega|} \right)^{|S_2|}, \tag{11}$$

$$\mathbf{P}_{\mathbf{A}_1} \lozenge \left(\frac{|\Omega_1|}{|\Omega|} \right)^{|S_1|} \left(1 - \frac{|\Omega_1|}{|\Omega|} \right)^{|S_2|}, \tag{12}$$

$$T_{\mathbf{A}_1} \begin{cases} \geq (|S_1| + |S_2|) \min \{T_{S_1}, T_{S_2}\}, \text{ если истинно утверждение 2,} \\ = (|S_1| + |S_2|) \min \{T_{S_1}, T_{S_2}\}, \text{ если истинно утверждение 3.} \end{cases} \tag{13}$$

Подчеркнем, что все установленные в [12–15] оценки мощностей нетривиальных подмножеств автоматов получены в результате детализации формул (8) и (10) применительно к соответствующему подмножеству автоматов над кольцом $\mathcal{Z}_{p^k}$.

Проиллюстрируем схему анализа конечно-автоматных характеристик на примере обобщения ряда результатов, полученных в [12].

Пример 1. Пусть $m = \prod_{i=1}^{h} p_i^{k_i}$, где p_i $(i = 1, \ldots, h)$ — попарно различные простые числа, $k_i \in \mathbf{N}$ $(i = 1, \ldots, h)$, а $\mathbf{A}$ — множество всех линейных автоматов Мили над кольцом $\mathcal{Z}_m$, имеющих вид

$$\begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1} \ (t \in \mathbf{Z}_+), \end{cases}$$

где A, B, C, D — $(n \times n)$-матрицы над кольцом $\mathcal{Z}_m$, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathcal{Z}_m^n$ — вектор-столбцы, представляющие состояние автомата, входной и выходной символ в момент t.

В данном случае $S = \{A, B, C, D\}$, а Ω — множество всех $(n \times n)$-матриц над кольцом $\mathcal{Z}_m$. Следовательно, $|\Omega| = m^{n^2}$, откуда вытекает $|\mathbf{A}| = m^{4n^2}$.

Несложно показать, что автомат $M \in \mathbf{A}$ является обратимым автоматом тогда и только тогда, когда D — обратимая матрица над кольцом $\mathcal{Z}_m$. Обозначим Ω_1 множество всех обратимых $(n \times n)$-матриц над кольцом $\mathcal{Z}_m$. Так как $|\Omega_1| = m^{n^2} \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j})$ (см., например, [16]), имеем

$$\frac{|\Omega_1|}{|\Omega|} = \prod_{i=1}^{h} \prod_{j=1}^{n} (1 - p_i^{-j}).$$

Пусть $\mathbf{A}_1$ — множество всех обратимых перестановочных автоматов $M \in \mathbf{A}$.

Несложно показать, что автомат $M \in \mathbf{A}$ является перестановочным автоматом тогда и только тогда, когда A — обратимая матрица над кольцом $\mathcal{Z}_m$. Следовательно, $M \in \mathbf{A}_1$ тогда и только тогда, когда A, D — обратимые матрицы над кольцом $\mathcal{Z}_m$. Имеет место случай 1, где $S_1 = \{A, D\}$. Из (8)–(10) (с учетом того, что справедливо утверждение 3) вытекает

$$|\mathbf{A}_1| = m^{4n^2} \left(\prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\right)^2, \qquad \mathbf{P}_{\mathbf{A}_1} = \left(\prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\right)^2,$$

$$T_{\mathbf{A}_1} = 2T_{S_1},$$

где T_{S_1} — время, необходимое для проверки принадлежности $(n \times n)$-матрицы множеству обратимых матриц над кольцом $\mathcal{Z}_m$, т.е. время, необходимое для вычисления определителя матрицы и проверки его взаимной простоты с каждым из простых чисел p_i $(i = 1, \ldots, h)$.

Пусть $\mathbf{A}_1$ — множество всех обратимых автоматов $M \in \mathbf{A}$, имеющих состояния-близнецы. Несложно показать, что если автомат $M \in \mathbf{A}$ имеет состояния-близнецы, то A, C — необратимые матрицы над кольцом $\mathcal{Z}_m$. Следовательно, если автомат $M \in \mathbf{A}$ принадлежит подмножеству $\mathbf{A}_1$, то D — обратимая матрица, а A, C — необратимые матрицы над кольцом $\mathcal{Z}_m$. Обозначим Ω_2 множество всех необратимых $(n \times n)$-матриц над кольцом $\mathcal{Z}_m$. Так как $\Omega_1 \cup \Omega_2 = \Omega$, имеет место случай 2, где $S_1 = \{D\}$ и $S_2 = \{A, C\}$. Из (11)–(13) (с учетом того, что справедливо утверждение 2) вытекает

$$|\mathbf{A}_1| \le m^{4n^2} \prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\left(1-\prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\right)^2,$$

$$\mathbf{P}_{\mathbf{A}_1} \le \prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\left(1-\prod_{i=1}^{h}\prod_{j=1}^{n}(1-p_i^{-j})\right)^2,$$

$$T_{\mathbf{A}_1} \ge 3\min\{T_{S_1}, T_{S_2}\},$$

где T_{S_2} — время, необходимое для проверки принадлежности $(n \times n)$-матрицы множеству необратимых матриц над кольцом $\mathcal{Z}_m$, т.е. время, необходимое для вычисления определителя матрицы и проверки его делимости хотя бы на одно простое число p_i $(i = 1, \ldots, h)$. Поскольку $T_{S_1} = T_{S_2}$, имеем $T_{\mathbf{A}_1} \ge 3T_{S_1}$.

2. РЕШЕНИЕ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ КОЛЬЦОМ

Для автоматов над кольцом $\mathcal{K} = (K, +, \cdot)$ задачи построения классов эквивалентных состояний автомата, идентификации начального состояния автомата, параметрической идентификации, а также построения множеств неподвижных точек автоматных отображений сводятся к решению соответствующих систем (линейных или нелинейных) уравнений (как правило, с параметрами) над кольцом $\mathcal{K}$ (что проиллюстрировано в [12–15] при исследовании автоматов над кольцом $\mathcal{Z}_{p^k}$).

Решение линейной системы уравнений над полем $GF(p^k)$ не вызывает особых затруднений. Однако ситуация изменяется при решении систем нелинейных уравнений над этим полем (известно, что даже при $p = 2$ задача решения систем квадратных уравнений от многих переменных — NP-полная). Значительно более сложной является разработка методов решения систем нелинейных уравнений над кольцом $\mathcal{K} = (K, +, \cdot)$ (что обусловлено, прежде всего, наличием в кольце делителей нуля).

В ряде случаев можно упростить поиск решения полиномиальной системы уравнений

$$\begin{cases} f_1(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_l(u_1, \ldots, u_n, a_1, \ldots, a_h) = 0 \end{cases} \tag{14}$$

над кольцом $\mathcal{K} = (K, +, \cdot)$, где $u_1, \ldots, u_n$ — переменные, а $a_1, \ldots, a_h$ — параметры.

Обозначим $\mathbf{B}$ множество классов ассоциированных элементов кольца $\mathcal{K}$, $<x>$ $(x \in K)$ — класс элементов, ассоциированных с элементом x, а $\mathbf{G} = (G, \cdot)$ $(G \subset K \setminus \{0\})$ — мультипликативную группу кольца $\mathcal{K}$. Тогда $\mathbf{B} = \{<0>, <1>\} \cup \mathbf{B}'$, где $<0> = \{0\}$, $<1> = G$, а $\mathbf{B}' = \{<x> | x \in (K \setminus \{0\}) \setminus G\}$ — множество классов, ассоциированных с необратимыми элементами кольца $\mathcal{K}$. Далее будем считать, что $|G| > 1$ и $|\mathbf{B}'| > 1$.

Определим на множестве $\mathbf{B}$ операцию умножения:

$$<x> \cdot <y> = <x \cdot y> \ (x, y \in K). \tag{15}$$

Такое определение корректно, поскольку $<x> = G \cdot x$ $(x \in K)$. Следовательно, $(\mathbf{B}, \cdot)$ — полугруппа. Положим

$$\mathbf{B}_0 = \{<x> | x \text{ — неприводимый элемент кольца } \mathcal{K}\}.$$

В дальнейшем предполагается, что каждый элемент множества $\mathbf{B}'$ единственным образом (с точностью до ассоциированного разложения) может быть представлен в виде произведения элементов множества $\mathbf{B}_0$. Отметим, что это требование более слабое, чем требование «$\mathbf{B}$ — гауссова полугруппа», так как не требуется выполнения «закона сокращения», который не имеет места даже в случае $\mathcal{K} = \mathcal{Z}_{p^k}$ $(k \geq 3)$.

Определим сумму элементов множества $\mathbf{B}$:

$$<x> + <y> = \{<z> \in \mathbf{B} \,|\, (\exists\, a \in <x>)(\exists\, b \in <y>)(a + b \in <z>)\} \ (x, y \in K). \tag{16}$$

Равенство (16) определяет на множестве $\mathbf{B}$ тернарное отношение, а не бинарную операцию (в алгебраическом смысле этого слова), что, в частности, истинно, даже если $\mathcal{K} = \mathcal{Z}_{p^k}$.

Таким образом, осуществлен переход от кольца $\mathcal{K} = (K, +, \cdot)$ к алгебраической системе $\mathcal{B} = (\mathbf{B}, +, \cdot)$, что дает возможность предложить следующую схему решения системы уравнений (14).

Схема 2. Заменив в (14) элементы кольца $\mathcal{K}$ элементами множества $\mathbf{B}$, а операции в кольце $\mathcal{K}$ — действиями в алгебраической системе $\mathcal{B}$, определяемыми равенствами (15) и (16), получим систему уравнений

$$\begin{cases} f_1(<u_1>, \ldots, <u_n>, <a_1>, \ldots, <a_h>) = <0>, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_l(<u_1>, \ldots, <u_n>, <a_1>, \ldots, <a_h>) = <0> \end{cases} \tag{17}$$

над алгебраической системой $\mathcal{B}$. Представим элементы $<a_1>, \ldots, <a_h> \in \mathbf{B}$ в виде произведения элементов, принадлежащих множеству $\mathbf{B}_0$. Найдем множество $\mathbf{S}$ решений системы уравнений (17) (где для каждого решения $(<u_1>, \ldots, <u_n>) \in \mathbf{S}$ каждый элемент $<u_i> \in \mathbf{B}$ представлен в виде произведения элементов, принадлежащих множеству $\mathbf{B}_0$). Исходя из множества $\mathbf{S}$, построим множество S решений системы уравнений (14). Для этого достаточно для каждого значения $\mathbf{u} = (<u_1>, \ldots, <u_n>) \in \mathbf{S}$ построить множество

$$S_{\mathbf{u}} = \{(u_1^{(0)}, \ldots, u_n^{(0)}) \,|\, u_i^{(0)} \in <u_i> (i = 1, \ldots, n)\}$$

и выделить в нем элементы множества S.

Очевидно, что сложность схемы 2 определяется именно сложностью поиска, осуществляемого при построении множества S из множества $\mathbf{S}$. Отсюда вытекает, что схема 2 будет эффективной при построении решений системы уравнений (14), если указанный поиск отсутствует либо его сложность невелика.

Следующий пример показывает, что схема 2 дает возможность эффективно строить множество решений по крайней мере для некоторых типов полиномиальных систем уравнений над конечными кольцами.

Пример 2. Найдем множество S решений (u_1, u_2, u_3) системы уравнений

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0, \\ a_2 \circ u_1 = 0 \end{cases} \tag{18}$$

с параметрами $a_1, a_2, a_3 \in \mathbf{Z}_{p^k}$ над кольцом $\mathcal{Z}_{p^k}$.

Замечание 1. Несложно показать, что необходимость решения системы уравнений (18) возникает при исследовании структуры классов эквивалентных состояний такого обратимого автомата Мура

$$\begin{cases} q_{t+2} = a \oplus b \circ q_{t+1}^2 \oplus c \circ q_t \oplus d \circ x_{t+1}, \\ y_{t+1} = e \circ q_{t+2} \quad (t \in \mathbf{Z}_+) \end{cases}$$

над кольцом $\mathcal{Z}_{p^k}$, что параметры e и f — обратимые элементы кольца $\mathcal{Z}_{p^k}$. Отметим, что уравнение $q_{t+2} = a \oplus b \circ q_{t+1}^2 \oplus c \circ q_t$ представляет собой аналог над кольцом $\mathcal{Z}_{p^k}$ ряда модельных хаотических отображений, в том числе отображения Эно [1].

Классами ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ являются множество {0}, множество $\mathbf{Z}_{p^k}^{\text{inv}}$ всех обратимых элементов, а также множества $\{a \circ p^r \mid a \in \mathbf{Z}_{p^{k-r}}^{\text{inv}}\}$ $(r = 1, \ldots, k-1)$.

В соответствии с [17] определим p-тип $\mathbf{t}_p(z)$ элемента $z \in \mathbf{Z}_{p^k}$ равенством

$$\mathbf{t}_p(z) = \begin{cases} 0, \text{ если } z \in \mathbf{Z}_{p^k}^{\text{inv}}, \\ r \ (1 \le r \le k-1), \text{ если } z \equiv 0 (\text{mod } p^r) \text{ и } z \not\equiv 0 (\text{mod } p^{r+1}), \\ k, \text{ если } z = 0. \end{cases}$$

Из данного определения следуют утверждения:

1) $\mathbf{t}_p(u \circ v) = \min\{k, \mathbf{t}_p(u) + \mathbf{t}_p(v)\}$ $(u, v \in \mathbf{Z}_{p^k})$;

2) $\mathbf{t}_p(u \oplus v) \ge \min\{\mathbf{t}_p(u), \mathbf{t}_p(v)\}$ $(u, v \in \mathbf{Z}_{p^k})$;

3) $\mathbf{t}_p(u \oplus v) = 0$ $(u, v \in \mathbf{Z}_{p^k})$, если $\min\{\mathbf{t}_p(u), \mathbf{t}_p(v)\} = 0$, а $0 < \max\{\mathbf{t}_p(u), \mathbf{t}_p(v)\} < k$;

4) $\mathbf{t}_p(u) = \mathbf{t}_p(v)$ $(u, v \in \mathbf{Z}_{p^k})$ тогда и только тогда, когда элементы u и v принадлежат одному и тому же классу ассоциированных элементов кольца $\mathcal{Z}_{p^k}$.

Замечание 2. Из последнего свойства вытекает, что понятие p-тип элемента кольца $\mathcal{Z}_{p^k}$ определяет биекцию классов ассоциированных элементов кольца $\mathcal{Z}_{p^k}$ на множество $\mathbf{Z}_{k+1}$. Поэтому для того чтобы задать класс ассоциированных элементов кольца $\mathcal{Z}_{p^k}$, достаточно зафиксировать p-тип элемента, принадлежащего этому классу. Такой подход дает возможность выделять элементы множества S непосредственно в процессе построения множества $\mathbf{S}$ и тем самым избежать поиска или существенно его сократить при использовании схемы 2.

Для построения множества S рассмотрим следующие случаи.

Случай 3. Пусть $\mathbf{t}_p(a_1) = k$, т.е. $a_1 = 0$. Система уравнений (18) принимает вид

$$\begin{cases} 0 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0, \\ a_2 \circ u_1 = 0, \end{cases}$$

откуда вытекает

$$S = \begin{cases} \{(0, z, 0) \mid z \in \mathbf{Z}_{p^k}\}, \text{ если } \mathbf{t}_p(a_2) = 0, \\ \{(z_1, z, z_2) \in \mathbf{Z}_{p^k}^3 \mid k - \mathbf{t}_p(a_2) \le \mathbf{t}_p(z_i) \le k \ (i = 1, 2)\}, \text{ если } 1 \le \mathbf{t}_p(a_2) \le k-1, \\ \mathbf{Z}_{p^k}^3, \text{ если } \mathbf{t}_p(a_2) = k. \end{cases}$$

Случай 4. Пусть $\mathbf{t}_p(a_1) \neq k$ и $\mathbf{t}_p(a_2) = 0$. Тогда

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ a_2 \circ u_1 = 0 \end{cases} \Leftrightarrow \begin{cases} a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0 \\ u_1 = 0 \end{cases} \Leftrightarrow \begin{cases} 0 \circ u_2 \oplus a_2 \circ u_3 = 0, \\ u_1 = 0, \end{cases}$$

откуда следует $S = \{(0, z, 0) \mid z \in \mathbf{Z}_{p^k}\}$.

Случай 5. Пусть $\mathbf{t}_p(a_1) \neq k$ и $\mathbf{t}_p(a_2) = k$ (т.е. $a_2 = 0$). Система уравнений (18) принимает вид

$$\begin{cases} a_1 \circ u_1 \circ u_2 \oplus 0 \circ u_3 = 0, \\ 0 \circ u_1 = 0, \end{cases}$$

откуда вытекает $S = \{(u_1, u_2, u_3) \in \mathbf{Z}^3_{p^k} \mid k - \mathbf{t}_p(a_1) - \mathbf{t}_p(u_1) \leq \mathbf{t}_p(u_2) \leq k\}$.

Случай 6. Пусть $\mathbf{t}_p(a_1) \neq k$ и $\mathbf{t}_p(a_2) \in \{1, \ldots, k-1\}$. Представим множество S в виде $S = S_1 \cup S_2$, где

$$S_1 = \{(u_1, u_2, u_3) \in S \mid \mathbf{t}_p(u_1) = k\},$$
$$S_2 = \{(u_1, u_2, u_3) \in S \mid k - \mathbf{t}_p(a_2) \leq \mathbf{t}_p(u_1) \leq k-1\}.$$

Найдем множество S_1. Так как $\mathbf{t}_p(u_1) = k$ (т.е. $u_1 = 0$), система уравнений (18) принимает вид

$$\begin{cases} 0 \circ u_2 \oplus a_2 \circ u_3 = 0, \\ u_1 = 0, \end{cases}$$

откуда вытекает $S_1 = \{(0, z_1, z_2) \in \mathbf{Z}^3_{p^k} \mid k - \mathbf{t}_p(a_2) \leq \mathbf{t}_p(z_2) \leq k\}$.

Найдем множество S_2. Представим множество S_2 в виде $S_2 = S_2' \cup S_2''$, где

$$S_2' = \{(u_1, u_2, u_3) \in S \mid \max\{k - \mathbf{t}_p(a_1), k - \mathbf{t}_p(a_2)\} \leq \mathbf{t}_p(u_1) \leq k-1\},$$
$$S_2'' = \{(u_1, u_2, u_3) \in S \mid k - \mathbf{t}_p(a_2) \leq \mathbf{t}_p(u_1) < \max\{k - \mathbf{t}_p(a_1), k - \mathbf{t}_p(a_2)\}\}. \quad (19)$$

Из (18) следует

$$S_2' = \{(u_1, u_2, u_3) \in \mathbf{Z}^3_{p^k} \mid \max\{k - \mathbf{t}_p(a_1), k - \mathbf{t}_p(a_2)\} \leq$$
$$\leq \mathbf{t}_p(u_1) \leq k-1,\ \mathbf{t}_p(u_3) \geq k - \mathbf{t}_p(a_2)\},$$

а из (18) и (19) вытекает

$$S_2'' = \begin{cases} \varnothing, \text{ если } 1 \leq \mathbf{t}_p(a_2) \leq \mathbf{t}_p(a_1), \\ \{(u_1, u_2, u_3) \in \mathbf{Z}^3_{p^k} \mid k - \mathbf{t}_p(a_2) \leq \mathbf{t}_p(u_1) < k - \mathbf{t}_p(a_1), \\ a_1 \circ u_1 \circ u_2 \oplus a_2 \circ u_3 = 0\}, \text{ если } \mathbf{t}_p(a_1) < \mathbf{t}_p(a_2) \leq k-1. \end{cases}$$

Представим множество S_2'' в явном виде в случае, когда $\mathbf{t}_p(a_1) < \mathbf{t}_p(a_2) \leq$ $\leq k-1$. Положив $a_1 = \alpha \circ p^{\mathbf{t}_p(a_1)}$ $(\alpha \in \mathbf{Z}^{\text{inv}}_{p^{k-\mathbf{t}_p(a_1)}})$, $a_2 = \beta \circ p^{\mathbf{t}_p(a_2)}$ $(\beta \in \mathbf{Z}^{\text{inv}}_{p^{k-\mathbf{t}_p(a_2)}})$ и $u_1 = \delta_1 \circ p^{\mathbf{t}_p(u_1)}$ $(\delta_1 \in \mathbf{Z}^{\text{inv}}_{p^{k-\mathbf{t}_p(u_1)}})$, получим

$$S_2'' = \bigcup_{l_1 = k - \mathbf{t}_p(a_2)}^{k - \mathbf{t}_p(a_1)} \bigcup_{\delta_1 \in \mathbf{Z}_{p^{k-l_1}}} S_2''(\delta_1 \circ p^{l_1}),$$

где

$$S_2''(\delta_1 \circ p^{l_1}) = \{(\delta_1 \circ p^{l_1}, u_2, u_3) \in$$
$$\in \mathbf{Z}^3_{p^k} \mid \alpha \circ \delta_1 \circ p^{\mathbf{t}_p(a_1) + l_1} \circ u_2 \oplus \beta \circ p^{\mathbf{t}_p(a_2)} \circ u_3 = 0\}. \quad (20)$$

Найдем множество $S_2''(\delta_1 \circ p^{l_1})$. Возможны следующие два случая.

Случай 6.1. Пусть $k - \mathbf{t}_p(a_2) \le l_1 \le \mathbf{t}_p(a_2) - \mathbf{t}_p(a_1)$ (что возможно тогда и только тогда, когда $\mathbf{t}_p(a_2) > 0{,}5\,(k + \mathbf{t}_p(a_1))$). Из (20) вытекает

$$S_2''(\delta_1 \circ p^{l_1}) = \{(\delta_1 \circ p^{l_1}, \Theta(\alpha \circ \delta_1)^{-1} \circ \beta \circ p^{\mathbf{t}_p(a_2)-\mathbf{t}_p(a_1)-l_1} \circ u_3, u_3) \mid u_3 \in \mathbf{Z}_{p^k}\} \cup$$

$$\cup \bigcup_{l_2=k-\mathbf{t}_p(a_1)-l_1}^{k-1} \bigcup_{\delta_2 \in \mathbf{Z}_{p^{k-l_2}}^{\mathrm{inv}}} \{(\delta_1 \circ p^{l_1}, \delta_2 \circ p^{l_2} \Theta(\alpha \circ \delta_1)^{-1} \circ$$

$$\circ \beta \circ p^{\mathbf{t}_p(a_2)-\mathbf{t}_p(a_1)-l_1} \circ u_3, u_3) \mid u_3 \in \mathbf{Z}_{p^k}\},$$

где Θ — операция, обратная операции $\oplus$.

Случай 6.2. Пусть $l_1 > \max\{\mathbf{t}_p(a_2) - \mathbf{t}_p(a_1), k - \mathbf{t}_p(a_2)\}$. Из (20) следует

$$S_2''(\delta_1 \circ p^{l_1}) = \{(\delta_1 \circ p^{l_1}, u_2, \Theta\alpha \circ \delta_1 \circ \beta^{-1} \circ p^{\mathbf{t}_p(a_1)+l_1-\mathbf{t}_p(a_2)} \circ u_2) \mid u_2 \in \mathbf{Z}_{p^k}\} \cup$$

$$\cup \bigcup_{l_3=k-\mathbf{t}_p(a_2)}^{k-1} \bigcup_{\delta_3 \in \mathbf{Z}_{p^{k-l_3}}^{\mathrm{inv}}} \{(\delta_1 \circ p^{l_1}, u_2, \delta_3 \circ p^{l_3} \Theta\alpha \circ \delta_1 \circ \beta^{-1} \circ$$

$$\circ p^{\mathbf{t}_p(a_1)+l_1-\mathbf{t}_p(a_2)} \circ u_2) \mid u_2 \in \mathbf{Z}_{p^k}\}.$$

3. ХАРАКТЕРИСТИКИ АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

Зафиксируем в кольце $\mathcal{K} = (K, +, \cdot)$ семейство таких отображений $f_i : K^n \to K$ $(i = 1, \ldots, n)$, что $|\mathrm{Val}\, f_i| > 1$ для всех $i = 1, \ldots, n$. Обозначим $\sim_i$ $(i = 1, \ldots, n)$ ядерную эквивалентность отображения f_i (т.е. $\mathbf{a} \sim_i \mathbf{b}$ $(\mathbf{a}, \mathbf{b} \in K^n)$ тогда и только тогда, когда $f_i(\mathbf{a}) = f_i(\mathbf{b})$), а π_i $(i = 1, \ldots, n)$ — разбиение $K^n / \sim_i$ множества K^n, определяемое ядерной эквивалентностью $\sim_i$, и положим $\pi = \prod_{i=1}^{n} \pi_i$. Определим отображение $\mathbf{f} : K^n \to K^n$ равенством $\mathbf{f}(\mathbf{a}) = (b_1, \ldots, b_n)^T$, где $b_i = f_i(\mathbf{a})$ $(i = 1, \ldots, n)$. Так как для любых элементов $\mathbf{a}, \mathbf{b} \in K^n$ $(\mathbf{a} \ne \mathbf{b})$ равенство $\mathbf{f}(\mathbf{a}) = \mathbf{f}(\mathbf{b})$ истинно тогда и только тогда, когда $\mathbf{a} \equiv \mathbf{b} (\mathrm{mod}\, \pi)$, то $\mathbf{f}$ — перестановка элементов множества K^n тогда и только тогда, когда π — нулевое разбиение множества K^n. Отметим, что для любого элемента $\mathbf{a} \in K^n$ решение системы уравнений $\mathbf{f}(\mathbf{u}) = \mathbf{a}$ эквивалентно поиску блока разбиения π, образом которого является элемент $\mathbf{a}$. Будем говорить, что отображение $\mathbf{f}$ стабильно на (непустом) подмножестве S множества K^n, если $\mathbf{f}(S) \subseteq S$.

Для любого фиксированного элемента $\vec{\beta} = (\beta_1, \ldots, \beta_n)^T \in K^n$ определим отображение $\mathbf{g}_{\vec{\beta}} : K^n \to K^n$ равенством $\mathbf{g}_{\vec{\beta}}(\mathbf{u}) = (\beta_1 \cdot u_1, \ldots, \beta_n \cdot u_n)^T$ $(\mathbf{u} = (u_1, \ldots, u_n)^T \in K^n)$. Из определения отображения $\mathbf{g}_{\vec{\beta}}$ вытекает, что: 1) $\mathbf{g}_{\vec{\beta}}$ — линейное отображение (т.е. $\mathbf{g}_{\vec{\beta}}(\mathbf{u} + \mathbf{v}) = \mathbf{g}_{\vec{\beta}}(\mathbf{u}) + \mathbf{g}_{\vec{\beta}}(\mathbf{v})$ и $\mathbf{g}_{\vec{\beta}}(\alpha \cdot \mathbf{u}) = \alpha \cdot \mathbf{g}_{\vec{\beta}}(\mathbf{u})$ для любых $\mathbf{u}, \mathbf{v} \in K^n$ и $\alpha \in K$); 2) $\mathbf{g}_{\vec{\beta}}(\mathbf{1}) = \vec{\beta}$, где $\mathbf{1} = (1, \ldots, 1)^T \in K^n$; 3) $\mathbf{g}_{\vec{\beta}}(\mathbf{0}) = \mathbf{0}$, где $\mathbf{0} = (0, \ldots, 0)^T \in K^n$; 4) $\mathbf{g}_{\vec{\beta}}$ — перестановка элементов множества K^n тогда и только тогда, когда все компоненты вектора $\vec{\beta}$ — обратимые элементы кольца $\mathcal{K}$.

Обозначим $\mathbf{A}_{n,1}$ и $\mathbf{A}_{n,2}$ множество автоматов Мили и Мура над кольцом $\mathcal{K}$, определенных системами уравнений

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t) + \vec{\alpha} \cdot x_{t+1}, \\ \mathbf{y}_{t+1} = \mathbf{g}_{\vec{\beta}}(\mathbf{q}_t) + \vec{\gamma} \cdot x_{t+1} \ \ (t \in \mathbf{Z}_+), \end{cases} \tag{21}$$

$$\begin{cases} \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t) + \vec{\alpha} \cdot x_{t+1}, \\ \mathbf{y}_{t+1} = \mathbf{g}_{\vec{\beta}}(\mathbf{q}_{t+1}) \ \ (t \in \mathbf{Z}_+), \end{cases} \tag{22}$$

где $\mathbf{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^T \in K^n$, $x_t \in K$ и $\mathbf{y}_t \in K^n$ — соответственно состояние автомата, входной и выходной символ в момент t, а $\vec{\alpha}, \vec{\beta}, \vec{\gamma} \in K^n \setminus \{\mathbf{0}\}$ (где $\mathbf{0} = (0, \ldots, 0)$) — параметры. Положим $\mathbf{A}_n = \mathbf{A}_{n,1} \cup \mathbf{A}_{n,2}$.

Установим основные характеристики автоматов, принадлежащих множеству $\mathbf{A}_n$.

Предложение 1. Если для автомата $M \in \mathbf{A}_n$ хотя бы одна компонента вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ — обратимый элемент кольца $\mathcal{K}$, то любое состояние $\mathbf{q} \in K^n$ автомата M под действием различных входных символов переходит в различные состояния.

Доказательство. Предположим, что компонента α_i вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ — обратимый элемент кольца $\mathcal{K}$. Тогда система уравнений $\vec{\alpha} \cdot u = \mathbf{0}$ имеет единственное решение $u = 0$. Для любого состояния $\mathbf{q} \in K^n$ автомата M и любых входных символов $x, \tilde{x} \in K$ из первого уравнения систем (21) и (22) получим

$$\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot x = \mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot \tilde{x} \Leftrightarrow \vec{\alpha}\,(x - \tilde{x}) = \mathbf{0} \Leftrightarrow x - \tilde{x} = 0 \Leftrightarrow x = \tilde{x}.$$

Предложение доказано.

Предложение 2. Если для автомата $M \in \mathbf{A}_n$ все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ — необратимые элементы кольца $\mathcal{K}$, имеющие общий делитель, являющийся делителем нуля, то существует такое подмножество $S \subseteq K$ $(|S| > 1)$, что любое состояние $\mathbf{q} \in K^n$ автомата M под действием входных символов, принадлежащих множеству S, переходит в одно и то же состояние.

Доказательство. Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)^T \in K^n \setminus \{\mathbf{0}\}$ и $a \in K$ — общий делитель элементов $\alpha_1, \ldots, \alpha_n$, являющийся делителем нуля. Тогда существует такой элемент $< b > \in \mathbf{B}' \setminus < \{0\} >$, что $a \cdot < b > = < 0 >$. Положим $S = < b >$. Так как $< b > = G \cdot b$ и $|G| > 1$, то $|S| > 1$. Любой элемент $u \in S$ является решением системы уравнений $\vec{\alpha} \cdot u = \mathbf{0}$. Следовательно, для любого состояния $\mathbf{q} \in K^n$ автомата M и любых входных символов $x, \tilde{x} \in S$

$$\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot x - (\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot \tilde{x}) = \vec{\alpha} \cdot (x - \tilde{x}) = \mathbf{0}.$$

Предложение доказано.

Предложение 3. Диаметр автоматного графа любого автомата $M \in \mathbf{A}_n$ не меньше, чем n.

Доказательство. За один такт из каждого состояния $\mathbf{q} \in K^n$ автомата $M \in \mathbf{A}_n$ достижимо не более чем $|K|$ состояний. Следовательно, в течение $l \in \mathbf{N}$ тактов из состояния $\mathbf{q}$ достижимо не более чем $1 + |K| + \ldots + |K|^l = (|K|^{l+1} - 1)(|K| - 1)^{-1}$ состояний. Мощность множества состояний автомата M равна $|K|^n$. Из неравенства $(|K|^{l+1} - 1)(|K| - 1)^{-1} \geq |K|^n$ вытекает, что $l + 1 > n$, т.е. $l \geq n$.

Предложение доказано.

Предложение 4. Для автомата $M \in \mathbf{A}_n$ блоки разбиения π представляют собой множества состояний автомата M, переходящие по любому входному символу в одно и то же состояние, а состояния автомата M, принадлежащие разным блокам разбиения π, по любому входному символу переходят в различные состояния.

Доказательство. Если $\mathbf{q} \equiv \tilde{\mathbf{q}} (\mathrm{mod}\, \pi)$ $(\mathbf{q}, \tilde{\mathbf{q}} \in K^n)$, то $\mathbf{f}(\mathbf{q}) = \mathbf{f}(\tilde{\mathbf{q}})$. Следовательно, $\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot x = \mathbf{f}(\tilde{\mathbf{q}}) + \vec{\alpha} \cdot x$ для любого входного символа $x \in K$.

Если $\mathbf{q} \not\equiv \tilde{\mathbf{q}} (\mathrm{mod}\, \pi)$ $(\mathbf{q}, \tilde{\mathbf{q}} \in K^n)$, то $\mathbf{f}(\mathbf{q}) \neq \mathbf{f}(\tilde{\mathbf{q}})$. Таким образом, $\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot x \neq$ $\neq \mathbf{f}(\tilde{\mathbf{q}}) + \vec{\alpha} \cdot x$ для любого входного символа $x \in K$.

Предложение доказано.

Следуя [17], назовем состояния $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \tilde{\mathbf{q}})$ автомата $M \in \mathbf{A}_n$ близнецами, если автомат M из этих состояний под действием любого входного символа осуществляет переход в одно и то же состояние и при этом совпадают выходные символы, выдаваемые автоматом M.

Предложение 5. В автомате $M \in \mathbf{A}_{n,2}$ существуют состояния-близнецы тогда и только тогда, когда π — ненулевое разбиение множества K^n. При этом множествами состояний-близнецов являются все неодноэлементные блоки разбиения π.

Доказательство. В силу предложения 4, если π — нулевое разбиение множества K^n, то в автомате M близнецов нет (так как состояния, принадлежащие разным блокам разбиения π, по любому входному символу переходят в различные состояния).

Предположим, что π — ненулевое разбиение множества K^n и S — произвольный блок разбиения π, содержащий по крайней мере два элемента: $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \tilde{\mathbf{q}})$. В силу предложения 4 состояния $\mathbf{q}, \tilde{\mathbf{q}}$ переходят по любому входному символу в одно и то же состояние. При этом $\mathbf{g}_{\vec{\beta}}(\mathbf{f}(\mathbf{q})) = \mathbf{g}_{\vec{\beta}}(\mathbf{f}(\tilde{\mathbf{q}}))$ (так как $\mathbf{f}(\mathbf{q}) = \mathbf{f}(\tilde{\mathbf{q}})$).

Предложение доказано.

Обозначим $\mathbf{D}_{K^n}$ множество всех таких $\mathbf{a} = (a_1, \ldots, a_n)^T \in K^n$, что $a_1 = \ldots = a_n$.

Предложение 6. Если для автомата $M \in \mathbf{A}_n$ $(n \geq 2)$ все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ равны между собой, а отображение $\mathbf{f}$ стабильно на множестве $\mathbf{D}_{K^n}$, то автомат M не является сильносвязным.

Доказательство. Предположим, что отображение $\mathbf{f}$ стабильно на множестве $\mathbf{D}_{K^n}$. Тогда $\mathbf{f}(\mathbf{q}) \in \mathbf{D}_{K^n}$ для всех $\mathbf{q} \in \mathbf{D}_{K^n}$. Так как все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ равны между собой, то $\vec{\alpha} \cdot u \in \mathbf{D}_{K^n}$ для всех $u \in K^n$. Следовательно, $\mathbf{f}(\mathbf{q}) + \vec{\alpha} \cdot u \in \mathbf{D}_{K^n}$ для всех $\mathbf{q} \in \mathbf{D}_{K^n}$ и $u \in K^n$. Отсюда вытекает, что собственное подмножество $\mathbf{D}_{K^n}$ множества состояний K^n автомата M определяет подавтомат автомата M.

Предложение доказано.

Следствие 2. Если для автомата $M \in \mathbf{A}_n$ все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ — равные между собой обратимые элементы кольца $\mathcal{K}$, а отображение $\mathbf{f}$ стабильно на множестве $\mathbf{D}_{K^n}$, то подавтомат автомата M, определяемый множеством состояний $\mathbf{D}_{K^n}$, является сильносвязным перестановочным автоматом, диаметр графа переходов которого равен 1.

Доказательство. Предположим, что все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ — равные между собой обратимые элементы кольца $\mathcal{K}$, а отображение $\mathbf{f}$ стабильно на множестве $\mathbf{D}_{K^n}$. Тогда для любых фиксированных состояний $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ автомата M уравнение $\vec{\alpha} \cdot x = \tilde{\mathbf{q}} - \mathbf{f}(\mathbf{q})$ имеет единственное решение $x \in K^n$.

Следствие доказано.

Охарактеризуем сложность идентификации параметров $\vec{\alpha}, \vec{\beta}, \vec{\gamma} \in K^n \setminus \{\mathbf{0}\}$ автомата $M \in \mathbf{A}_n$ в предположении, что экспериментатор может управлять входом автомата M, устанавливать автомат M в состояние, удовлетворяющее заданным условиям, а также полностью наблюдать выход автомата M.

Теорема 2. Если экспериментатор может управлять входом автомата $M \in \mathbf{A}_{n,1}$, устанавливать автомат M в состояние, удовлетворяющее заданным условиям, а также полностью наблюдать выход автомата M, то параметры $\vec{\gamma}, \vec{\beta}, \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) \in K^n \setminus \{\mathbf{0}\}$ идентифицируются кратным экспериментом кратности 3 и высоты 2.

Доказательство. Установим автомат M в состояние $\mathbf{q}_0 = \mathbf{0}$ и подадим на него входной символ $x_1 = 1$. Из второго уравнения системы уравнений (21) получим

$$\mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{0}) + \vec{\gamma} \cdot 1 \Leftrightarrow \vec{\gamma} = \mathbf{y}_1.$$

Установим автомат M в состояние $\mathbf{q}_0 = \mathbf{1}$ и подадим на него входной символ $x_1 = 0$. Из второго уравнения системы (21) следует

$$\mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{1}) + \vec{\gamma} \cdot 0 \Leftrightarrow \vec{\beta} = \mathbf{y}_1.$$

Установим автомат M в такое состояние $\mathbf{q}_0$, что $\mathbf{f}(\mathbf{q}_0) = \mathbf{0}$, и подадим на него входную последовательность $x_1 x_2 = 10$. Из первого уравнения системы (21) вытекает

$$\mathbf{q}_1 = \mathbf{f}(\mathbf{q}_0) + \vec{\alpha} \cdot 1 = \vec{\alpha},$$

из второго —

$$\mathbf{y}_2 = \mathbf{g}_{\vec{\beta}}(\mathbf{q}_1) + \vec{\gamma} \cdot 0 = \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) \Leftrightarrow \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) = \mathbf{y}_2.$$

Теорема доказана.

Теорема 3. Если экспериментатор может управлять входом автомата $M \in \mathbf{A}_{n,2}$, устанавливать автомат M в состояние, удовлетворяющее заданным условиям, а также полностью наблюдать выход автомата M, то параметры $\vec{\beta}, \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) \in$ $\in K^n \setminus \{\mathbf{0}\}$ идентифицируются кратным экспериментом кратности 2 и высоты 1.

Доказательство. Установим автомат M в такое состояние $\mathbf{q}_0$, что $\mathbf{f}(\mathbf{q}_0) = \mathbf{1}$, и подадим на него входной символ $x_1 = 0$. Из системы уравнений (22) получим

$$\mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{q}_1) \Leftrightarrow \mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{f}(\mathbf{q}_0) + \vec{\alpha} \cdot x_1) \Leftrightarrow \mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{1}) \Leftrightarrow \vec{\beta} = \mathbf{y}_1.$$

Установим автомат M в такое состояние $\mathbf{q}_0$, что $\mathbf{f}(\mathbf{q}_0) = \mathbf{0}$, и подадим на него входной символ $x_1 = 1$. Из системы уравнений (22) следует

$$\mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{q}_1) \Leftrightarrow \mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\mathbf{f}(\mathbf{q}_0) + \vec{\alpha} \cdot x_1) \Leftrightarrow \mathbf{y}_1 = \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) \Leftrightarrow \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) = \mathbf{y}_1.$$

Следствие 3. Параметр $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ автомата $M \in \mathbf{A}_n$ однозначно идентифицируется тогда и только тогда, когда все компоненты вектора $\vec{\beta} \in K^n \setminus \{\mathbf{0}\}$ — обратимые элементы кольца $\mathcal{K}$.

Доказательство. При фиксированном векторе $\vec{\beta} \in K^n \setminus \{\mathbf{0}\}$ уравнение $\mathbf{g}_{\vec{\beta}}(\vec{\alpha}) = \mathbf{a}$ (где $\mathbf{a} = \mathbf{y}_2$, если $M \in \mathbf{A}_{n,1}$, и $\mathbf{a} = \mathbf{y}_1$, если $M \in \mathbf{A}_{n,2}$) имеет единственное решение $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ тогда и только тогда, когда все компоненты вектора $\vec{\beta} \in K^n \setminus \{\mathbf{0}\}$ — обратимые элементы кольца $\mathcal{K}$.

Следствие доказано.

Из теорем 2 и 3 вытекает, что идентификация параметров $\vec{\gamma}, \vec{\beta}, \mathbf{g}_{\vec{\beta}}(\vec{\alpha}) \in K^n \setminus \{\mathbf{0}\}$ не вызывает затруднений, если экспериментатор может устанавливать автомат в состояние, удовлетворяющее заданным условиям. Однако часто именно это условие невыполнимо из-за наличия параметров, определяющих конкретный вид отображения $\mathbf{f}: K^n \to K^n$. Идентификация таких параметров, как правило, представляет основную сложность решения задач параметрической идентификации для автоматов над кольцом $\mathcal{K}$.

Обозначим $\mathbf{A}_{n,1}^{\text{inv}}$ множество всех обратимых автоматов $M \in \mathbf{A}_{n,1}$ (характеризуемых тем, что все компоненты вектора $\vec{\gamma} \in K^n \setminus \{\mathbf{0}\}$ — обратимые элементы кольца $\mathcal{K}$), а $A_{n,2}^{\text{inv}}$ — множество всех обратимых автоматов $M \in \mathbf{A}_{n,2}$ (все компоненты векторов $\vec{\alpha}, \vec{\beta} \in K^n \setminus \{\mathbf{0}\}$ — обратимые элементы кольца $\mathcal{K}$). Положим $\mathbf{A}_n^{\text{inv}} = \mathbf{A}_{n,1}^{\text{inv}} \cup \mathbf{A}_{n,2}^{\text{inv}}$. Для любого автомата $M \in \mathbf{A}_n^{\text{inv}}$ истинны предложения 1, 3–6, теоремы 2, 3, а также следствия 2, 3. Эти утверждения представляют собой общие конечно-автоматные характеристики симметричного поточного шифра, построенного на основе автомата $M \in \mathbf{A}_n^{\text{inv}}$.

Множество автоматов $\mathbf{A}_n$ построено на основе произвольного фиксированного семейства таких отображений $f_i : K^n \to K$ $(i = 1, \ldots, n)$, что $|\text{Val } f_i| > 1$ для всех $i = 1, \ldots, n$. Рассмотрим теперь семейство отображений $f_i : K^n \to K$ $(i = 1, \ldots, n)$. Зафиксируем такое произвольное отображение $f : K^n \to K$, что $|\text{Val } f| > 1$, и произвольную циклическую подстановку $\varphi \in S_n$ (где S_n — симметрическая группа). Положим

$$f_i(u_1, \ldots, u_n) = f(u_{\varphi^{i-1}(1)}, \ldots, u_{\varphi^{i-1}(n)}) \ (i = 1, \ldots, n),$$

где φ^0 — тождественная подстановка (т.е. единица группы S_n). Отображение $\mathbf{f} : K^n \to K^n$, определяемое семейством отображений $f_i : K^n \to K$ $(i = 1, \ldots, n)$, характеризуется тем, что оно является:

1) симметричным отображением относительно преобразований координат, определяемых циклической группой, порожденной подстановкой φ;

2) стабильным отображением на множестве $\mathbf{D}_{K^n}$.

Множество автоматов $\mathbf{A}_n$, построенное на основе отображения $\mathbf{f} : K^n \to K^n$, назовем множеством симметрических автоматов над кольцом $\mathcal{K}$. В силу предложения 6 любой симметрический автомат $M \in \mathbf{A}_n$ $(n \geq 2)$ не является сильносвязным автоматом, если все компоненты вектора $\vec{\alpha} \in K^n \setminus \{\mathbf{0}\}$ равны между собой. Отметим, что симметрические автоматы над кольцом $\mathcal{Z}_{p^k}$, исследованные в [15], являются специальным случаем таких автоматов.

ЗАКЛЮЧЕНИЕ

В работе с позиции сложности вычислений рассмотрены методы анализа автоматов над конечным коммутативно-ассоциативным кольцом $\mathcal{K}$ с единицей.

Предложенная схема вычисления оценок, основанных на мощности подмножеств заданного множества автоматов над конечным кольцом, является основой для исследования свойств, формулируемых в терминах «для почти всех автоматов …», «доля автоматов …» и т.д., доказательство которых часто осуществляется с применением методов теории вероятностей. Проработка этой схемы для решения таких задач — одно из возможных направлений исследований.

Схема решения над кольцом $\mathcal{K}$ систем полиномиальных уравнений с параметрами, основанная на использовании классов ассоциированных элементов, дает возможность эффективно находить решения для специальных типов таких систем над кольцом $\mathcal{Z}_{p^k}$, что проиллюстрировано примером 2. Из него вытекает, что эффективное применение предложенной схемы для кольца $\mathcal{K}$ должно быть основано на понятии «тип» для элемента кольца $\mathcal{K}$. По-видимому, такой «тип» должен представлять собой вектор, компонентами которого являются показатели степеней элементов множества $\mathbf{B}_0$ в разложении элемента кольца $\mathcal{K}$ в произведение неприводимых элементов. При этом, в отличие от кольца $\mathcal{Z}_{p^k}$, множество типов элементов частично упорядочено, что усложняет анализ возможных случаев при построении множества решений. Детальная проработка этих аспектов — другое направление дальнейших исследований.

Установленные в разд. 3 общие характеристики автоматов над кольцом $\mathcal{K}$ допускают обобщение в следующих двух направлениях: исследование случаев, когда отображение $\mathbf{g}_{\tilde{\beta}}$ является либо произвольным линейным отображением, либо нелинейным отображением специального вида; переход от автоматов, осуществляющих отображение вида $K^+ \to (K^n)^+$ к автоматам, осуществляющим отображение вида $(K^m)^+ \to (K^n)^+$.

Авторы выражают искреннюю благодарность академику НАН Украины, профессору Александру Адольфовичу Летичевскому за внимание к работе, полезные советы и идеи, возможно, не в полной мере реализованные в процессе выполнения настоящего исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов С.П. Динамический хаос. — М.: Физматлит, 2001. — 296 с.
2. Костенко П.Ю., Антонов А.В., Костенко Т.П. Обратные задачи хаотической динамики и статистический анализ при обеспечении информационной скрытности в коммуникационных системах и сетях // Кибернетика и системный анализ. — 2006. — № 5. — С. 96–106.
3. Костенко П.Ю., Антонов А.В., Костенко Т.П. Развитие концепции односторонних функций для систем криптографической защиты информации с использованием достижений хаотической динамики // Там же. — 2006. — № 6. — С. 136–146.
4. Гилл А. Линейные последовательностные машины. — М.: Наука, 1974. — 298 с.
5. Фараджев Р.Г. Линейные последовательностные машины. — М.: Сов. радио, 1975. — 248 с.
6. Агибалов Г.П. Распознавание операторов, реализуемых в линейных автономных автоматах // Изв. АН СССР. Техн. кибернетика. — 1970. — № 3. — С. 99–108.
7. Агибалов Г.П., Юфит Я.Г. О простых экспериментах для линейных инициальных автоматов // Автоматика и вычисл. техника. — 1972. — № 2. — С. 17–19.
8. Сперанский Д.В. Эксперименты с линейными и билинейными конечными автоматами. — Саратов: Изд-во Саратов. ун-та, 2004. — 144 с.
9. Курош А.Г. Лекции по общей алгебре. — М.: Наука, 1973. — 400 с.
10. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности // Тр. по дискрет. математике. — М.: Науч. изд-во «ТВП», 1997. — **1**. — С. 139–202.
11. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) // Там же. — 1998. — **2**. — С. 191–222.
12. Скобелев В.В. Анализ структуры класса линейных автоматов над кольцом $\mathcal{Z}_{p^k}$ // Кибернетика и системный анализ. — 2008. — № 3. — С. 60–74.
13. Скобелев В.В. Характеристики линейных одномерных автоматов с лагом l над конечным кольцом // Тр. ИПММ НАН Украины. — 2008. — **16**. — С. 190–196.
14. Скобелев В.Г. Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. — 2006. — № 6. — С. 29–42.
15. Скобелев В.В. О двух типах нелинейных автоматов над конечным кольцом // Там же. — 2009. — № 4. — С. 57–68.
16. Скобелев В.В. Точная формула для числа обратимых матриц над конечным кольцом // Тр. ИПММ НАН Украины. — 2009. — **18**. — С. 155–158.
17. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. — Донецк: ИПММ НАН Украины, 2009. — 479 с.

Поступила 23.03.2010