

АНАЛИЗ НЕЛИНЕЙНЫХ АВТОМАТОВ С ЛАГОМ 2 НАД КОНЕЧНЫМ КОЛЬЦОМ

В. В. Скобелев, В. Г. Скобелев

Институт прикладной математики и механики НАН Украины, г. Донецк, Украина

E-mail: skbv@iamm.ac.donetsk.ua

Для обратимых нелинейных одномерных автоматов с лагом 2 над кольцом $\mathbb{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$ исследована структура автоматного графа, охарактеризованы множества эквивалентных состояний, решены задачи параметрической идентификации и идентификации начального состояния, охарактеризованы множества неподвижных точек отображений, реализуемых инициальными автоматами.

Ключевые слова: нелинейные автоматы, конечные кольца, симметричные поточные шифры, системы уравнений над конечными кольцами.

Введение

В [1, 2] показано, что как с позиции теории автоматов, так и с позиции современной криптографии представляет интерес исследование нелинейных обратимых автоматов над кольцом $\mathbb{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$, где p — простое число, а операции в кольце определены равенствами $a \oplus b = a + b \pmod{p^k}$ и $a \circ b = a \cdot b \pmod{p^k}$.

Замечание 1. С позиции криптографии интерес исследования обратимых автоматов над конечным кольцом обосновывается тем, что любой такой автомат может рассматриваться в качестве математической модели симметричного поточного шифра.

При фиксации параметров $a, b, c, d, e \in \mathbb{Z}_{p^k}$ система уравнений

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

определяет автомат Мура [3] M над кольцом $\mathbb{Z}_{p^k}$, для которого переменная x_{t+1} — входной символ в момент $t + 1$, переменная y_{t+1} — выходной символ в момент $t + 1$, а переменная $\mathbf{q}_t = (q_{t+1}, q_t)$ — состояние автомата M в момент t , $t \in \mathbb{Z}_+$. При этом фиксация в автомате M начального состояния $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ приводит к инициальному автомату Мура $(M, \mathbf{q}_0)$, осуществляющему отображение входной полугруппы $\mathbb{Z}_{p^k}^+$ в себя.

Замечание 2. В терминологии, принятой в [4], автомат M , определяемый системой уравнений (1), представляет собой автомат с задержкой.

Целью настоящей работы является исследование множества $\mathbf{M}$ всех таких автоматов M , определенных системой уравнений (1), что параметры a, b, c, d, e удовлетворяют условиям: $a, c \in \mathbb{Z}_{p^k}$, $b \in \mathbb{Z}_{p^k} \setminus \{0\}$, $d, e \in \mathbb{Z}_{p^k}^{\text{inv}}$, где $\mathbb{Z}_{p^k}^{\text{inv}}$ — множество всех обратимых элементов кольца $\mathbb{Z}_{p^k}$.

С алгебраической точки зрения инициальный автомат $(M, \mathbf{q}_0)$ ($M \in \mathbf{M}$, $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^2$) на каждом такте своего функционирования осуществляет фиксированное преобразование (т. е. сюръективное отображение на себя) множества $\mathbb{Z}_{p^k}$, представляющее собой

фиксированное линейное преобразование $u = e \circ v$ линейной комбинации $v = \alpha \oplus \beta$ фиксированной квадратичной формы $\alpha = b \circ q_{t+1}^2 \oplus c \circ q_t$ текущего состояния автомата M и фиксированного аффинного преобразования $\beta = a \oplus d \circ x_{t+1}$ множества $\mathbb{Z}_{p^k}$.

Замечание 3. Первое уравнение системы уравнений (1) представляет собой аналог над кольцом $\mathbb{Z}_{p^k}$ ряда модельных хаотических отображений, в частности отображения Эно [5]. Отсюда вытекает, что рассмотренный в [1, 2, 6] автомат Эно представляет собой специальный случай автомата (1).

Автоматом, обратным автомату $M \in \mathbf{M}$, является автомат Мили

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

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

Упорядоченная пара

$$((M, \mathbf{q}_0), (M^{\text{inv}}, \mathbf{q}_0)) \quad (M \in \mathbf{M}, \mathbf{q}_0 \in \mathbb{Z}_{p^k}^2) \quad (3)$$

определяет симметричный поточный шифр, секретным ключом которого является упорядоченный набор $(a, b, c, d, e, \mathbf{q}_0) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2 \times \mathbb{Z}_{p^k}^2$, причем параметры a, b, c, d, e — секретный ключ средней длительности, а начальное состояние $\mathbf{q}_0 = (q_1, q_0)$ — секретный сеансовый ключ. Таким образом, для симметричного поточного шифра (3):

1) длина в битах секретного ключа равна $7\lceil k \log p \rceil$, из которых $5\lceil k \log p \rceil$ бит представляют секретный ключ средней длительности, а $2\lceil k \log p \rceil$ бит — секретный сеансовый ключ;

2) мощность множества секретных ключей равна $p^{6k}(p^k - 1)(1 - p^{-1})^2$, мощность множества секретных ключей средней длительности равна $p^{4k}(p^k - 1)(1 - p^{-1})^2$, а при каждом фиксированном секретном ключе средней длительности мощность множества секретных сеансовых ключей равна p^{2k} .

Замечание 4. Симметричный поточный шифр (3) обладает тем свойством, что в процессе *шифрование* — *расшифрование* автоматы M и M^{inv} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

1. Структура автоматного графа исследуемой модели

В соответствии с [4, 7] считаем, что автоматный граф G_M автомата Мура $M \in \mathbf{M}$ — это размеченный орграф с петлями [8], содержащий p^{2k} вершин. Вершины графа G_M отмечены парами $(\mathbf{q}, y)$, где $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$; $y = e \circ q_1$ — выходной символ, вырабатываемый автоматом M при переходе в состояние $\mathbf{q}$ (т. е. имеется взаимно-однозначное соответствие между вершинами графа G_M и состояниями автомата M). Из вершины с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, q_0)$) в вершину с отметкой $(\tilde{\mathbf{q}}, \tilde{y})$ ($\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0)$) идет дуга тогда и только тогда, когда $\tilde{q}_0 = q_1$ и существует такой входной символ $x \in \mathbb{Z}_{p^k}$, что $\tilde{q}_1 = a \oplus b \circ q_1^2 \oplus c \circ q_0 \oplus d \circ x$. Эта дуга отмечена множеством всех входных символов, при которых автомат M переходит из состояния $\mathbf{q}$ в состояние $\tilde{\mathbf{q}}$.

Замечание 5. Так как $M \in \mathbf{M}$ — обратимый автомат Мура, то каждая дуга автоматного графа G_M отмечена единственным входным символом $x \in \mathbb{Z}_{p^k}$.

Охарактеризуем структуру автоматного графа G_M ($M \in \mathbf{M}$).

Теорема 1. Любой автомат $M \in \mathbf{M}$ является сильно связным автоматом, причем диаметр его автоматного графа G_M равен 2.

Доказательство. Пусть $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ — любые состояния автомата $M \in \mathbf{M}$.

Входной символ

$$x_1 = d^{-1} \circ (\tilde{q}_0 \ominus a \ominus b \circ q_1^2 \ominus c \circ q_0) \quad (4)$$

переводит состояние $\mathbf{q}$ автомата $M \in \mathbf{M}$ в состояние $\mathbf{q}_1 = (\tilde{q}_0, q_1) \in \mathbb{Z}_{p^k}^2$, а входной символ

$$x_2 = d^{-1} \circ (\tilde{q}_1 \ominus a \ominus b \circ \tilde{q}_0^2 \ominus c \circ q_1) \quad (5)$$

переводит состояние $\mathbf{q}_1$ автомата $M \in \mathbf{M}$ в состояние $\mathbf{q}_2 = \tilde{\mathbf{q}}$. Следовательно, входное слово x_1x_2 , определяемое равенствами (4) и (5), переводит любое состояние $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$ в любое состояние $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$, т. е. $M \in \mathbf{M}$ — сильно связный автомат, что и требовалось доказать.

Так как входное слово x_1x_2 , определяемое равенствами (4) и (5), переводит любое состояние $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$ в любое состояние $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$, то в автоматном графе G_M ($M \in \mathbf{M}$) расстояние между любыми двумя вершинами не превосходит 2.

Пусть $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ — такие два состояния автомата $M \in \mathbf{M}$, что $q_1 \neq \tilde{q}_0$.

Входной символ $x_1 \in \mathbb{Z}_{p^k}$ переводит состояние $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата M в состояние $\mathbf{q}_1 = (q_2, q_1) \in \mathbb{Z}_{p^k}^2$, где

$$q_2 = a \oplus b \circ q_1^2 \oplus c \circ q_0 \oplus d \circ x_1.$$

Так как $q_1 \neq \tilde{q}_0$, то $\mathbf{q}_1 \neq \tilde{\mathbf{q}}$ для любого входного символа $x_1 \in \mathbb{Z}_{p^k}$. Следовательно, входное слово $x_1x_2 \in \mathbb{Z}_{p^k}^2$, определяемое равенствами (4) и (5), является минимальным входным словом, переводящим состояние $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата M в состояние $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($q_1 \neq \tilde{q}_0$). Это означает, что в автоматном графе G_M ($M \in \mathbf{M}$) расстояние от вершины с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2, y = e \circ q_1$) до вершины с отметкой $(\tilde{\mathbf{q}}, \tilde{y})$ ($\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2, \tilde{y} = e \circ \tilde{q}_1$) равно 2, если $q_1 \neq \tilde{q}_0$.

Отсюда вытекает, что диаметр автоматного графа G_M ($M \in \mathbf{M}$) равен 2, что и требовалось доказать. ■

Следствие 1. В автоматном графе G_M ($M \in \mathbf{M}$) существует петля в вершине с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2, y = e \circ q_1$) тогда и только тогда, когда $q_1 = q_0$. Эта петля отмечена входным символом

$$x = d^{-1} \circ (q_0 \ominus a \ominus b \circ q_0^2 \ominus c \circ q_0). \quad (6)$$

Доказательство. Автомат $M \in \mathbf{M}$ из состояния $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ под действием входного символа $x \in \mathbb{Z}_{p^k}$ переходит в состояние $\mathbf{q}_1 = (q_2, q_1)$, где

$$q_2 = a \oplus b \circ q_1^2 \oplus c \circ q_0 \oplus d \circ x. \quad (7)$$

Равенство $\mathbf{q} = \mathbf{q}_1$ истинно тогда и только тогда, когда $q_1 = q_0$ и $q_2 = q_1 (= q_0)$.

Положив $q_1 = q_0$ и $q_2 = q_0$ в равенстве (7), получим, что единственный входной символ $x \in \mathbb{Z}_{p^k}$, отмечающий петлю в вершине отметкой $((q_0, q_0), e \circ q_0)$ ($q_0 \in \mathbb{Z}_{p^k}$), определяется равенством (6). ■

Из доказательства теоремы 1 и из следствия 1 непосредственно вытекает, что истинны следующие два следствия.

Следствие 2. В автоматном графе G_M ($M \in \mathbf{M}$) множество вершин, находящихся на расстоянии 1 от вершины с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$, $y = e \circ q_1$), состоит из $p^k - 1$ вершин, отметки которых имеют вид $((q_2, q_1), e \circ q_2)$ ($q_2 \in \mathbb{Z}_{p^k} \setminus \{q_0\}$), если $q_1 = q_0$, и из p^k вершин, отметки которых имеют вид $((q_2, q_1), e \circ q_2)$ ($q_2 \in \mathbb{Z}_{p^k}$), если $q_1 \neq q_0$.

Следствие 3. В автоматном графе G_M ($M \in \mathbf{M}$) множество вершин, от которых вершина с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$, $y = e \circ q_1$) находится на расстоянии 1, состоит из $p^k - 1$ вершин, отметки которых имеют вид $((q_0, \tilde{q}_0), e \circ q_0)$ ($\tilde{q}_0 \in \mathbb{Z}_{p^k} \setminus \{q_0\}$), если $q_1 = q_0$, и из p^k вершин, отметки которых имеют вид $((q_0, \tilde{q}_0), e \circ q_0)$ ($\tilde{q}_0 \in \mathbb{Z}_{p^k}$), если $q_1 \neq q_0$.

Теорема 2. Для любых двух фиксированных вершин автоматного графа G_M ($M \in \mathbf{M}$) либо исходящие из них дуги, отмеченные любым входным символом $x \in \mathbb{Z}_{p^k}$, ведут в различные вершины графа G_M , либо исходящие из них дуги, отмеченные любым входным символом $x \in \mathbb{Z}_{p^k}$, ведут в одну и ту же вершину графа G_M .

Доказательство. Предположим, что в автоматном графе G_M ($M \in \mathbf{M}$) дуги, отмеченные входным символом $\tilde{x}$ ($\tilde{x} \in \mathbb{Z}_{p^k}$), ведут из двух фиксированных вершин с отметками соответственно $(\mathbf{q}^{(1)}, y^{(1)})$ ($\mathbf{q}^{(1)} = (q_1^{(1)}, q_0^{(1)}) \in \mathbb{Z}_{p^k}^2$, $y^{(1)} = e \circ q_1^{(1)}$) и $(\mathbf{q}^{(2)}, y^{(2)})$ ($\mathbf{q}^{(2)} = (q_1^{(2)}, q_0^{(2)}) \in \mathbb{Z}_{p^k}^2$, $y^{(2)} = e \circ q_1^{(2)}$) в одну и ту же вершину с отметкой $(\tilde{\mathbf{q}}, \tilde{y})$ ($\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$, $\tilde{y} = e \circ \tilde{q}_1$). Тогда $q_2^{(1)} = q_2^{(2)} (= \tilde{q}_1)$, т. е.

$$a \oplus b \circ (q_1^{(1)})^2 \oplus c \circ q_0^{(1)} \oplus d \circ \tilde{x} = a \oplus b \circ (q_1^{(2)})^2 \oplus c \circ q_0^{(2)} \oplus d \circ \tilde{x},$$

и $q_1^{(1)} = q_1^{(2)} (= \tilde{q}_0)$, т. е. $\mathbf{q}^{(1)} = (\tilde{q}_0, q_0^{(1)})$ и $\mathbf{q}^{(2)} = (\tilde{q}_0, q_0^{(2)})$.

Следовательно,

$$\begin{aligned} a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(1)} \oplus d \circ \tilde{x} &= a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(2)} \oplus d \circ \tilde{x} \Leftrightarrow \\ \Leftrightarrow a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(1)} &= a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(2)} \Leftrightarrow \\ \Leftrightarrow (\forall x \in \mathbb{Z}_{p^k}) (a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(1)} \oplus d \circ x &= a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(2)} \oplus d \circ x). \end{aligned}$$

Последнее утверждение означает, что дуги, отмеченные любым входным символом $x \in \mathbb{Z}_{p^k}$, ведут из вершин с отметками $(\mathbf{q}^{(1)}, y^{(1)})$ и $(\mathbf{q}^{(2)}, y^{(2)})$ в вершину с отметкой $(\mathbf{q}, y)$ ($\mathbf{q} = (q_1, \tilde{q}_0)$, $y = e \circ q_1$), где

$$q_1 = a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(1)} \oplus d \circ x (= a \oplus b \circ \tilde{q}_0^2 \oplus c \circ q_0^{(2)} \oplus d \circ x),$$

что и требовалось доказать. ■

2. Критерий эквивалентности состояний исследуемой модели

Два различных состояния автомата называются близнецами [9], если по любому входному символу они переходят в одно и то же состояние. Из теоремы 2 вытекает, что истинно следующее следствие.

Следствие 4. В любом автомате $M \in \mathbf{M}$ любые два состояния $\mathbf{q}, \tilde{\mathbf{q}} \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) либо являются близнецами, либо по любому входному символу $x \in \mathbb{Z}_{p^k}$ переходят в различные состояния автомата M .

Так как $M \in \mathbf{M}$ — автомат Мура, то эквивалентны любые состояния-близнецы $\mathbf{q}, \tilde{\mathbf{q}} \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$. Следующая теорема показывает, что понятие «состояния-близнецы» дает возможность полностью охарактеризовать эквивалентные состояния автомата $M \in \mathbf{M}$.

Теорема 3. Состояния $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) автомата $M \in \mathbf{M}$ эквивалентны тогда и только тогда, когда либо $q_1 = \tilde{q}_1$, а состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — близнецы, либо когда $q_1 \neq \tilde{q}_1$, а состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ по любому входному символу переходят в состояния-близнецы.

Доказательство. Пусть $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) — эквивалентные состояния автомата $M \in \mathbf{M}$.

Под действием входного символа $x_1 \in \mathbb{Z}_{p^k}$ состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ автомата M переходят соответственно в состояния $\mathbf{q}_1 = (q_2, q_1)$ и $\tilde{\mathbf{q}}_1 = (\tilde{q}_2, \tilde{q}_1)$, где

$$q_2 = a \oplus b \circ q_1^2 \oplus c \circ q_0 \oplus d \circ x_1, \quad (8)$$

$$\tilde{q}_2 = a \oplus b \circ \tilde{q}_1^2 \oplus c \circ \tilde{q}_0 \oplus d \circ x_1. \quad (9)$$

Так как $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — эквивалентные состояния автомата M , то $y_1 = \tilde{y}_1$ для любого входного символа $x_1 \in \mathbb{Z}_{p^k}$. Следовательно,

$$y_1 = \tilde{y}_1 \Leftrightarrow e \circ \tilde{q}_2 = e \circ q_2 \Leftrightarrow \tilde{q}_2 = q_2 \quad (10)$$

для любого входного символа $x_1 \in \mathbb{Z}_{p^k}$.

Из (10) вытекает, что для любого входного символа $x_1 \in \mathbb{Z}_{p^k}$ истинно равенство $\mathbf{q}_1 = \tilde{\mathbf{q}}_1$ тогда и только тогда, когда $\tilde{q}_1 = q_1$ и, кроме того, для любого входного символа $x_1 \in \mathbb{Z}_{p^k}$ истинно равенство $\tilde{q}_2 = q_2$.

Таким образом, $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — такие эквивалентные состояния автомата $M \in \mathbf{M}$, что $\tilde{q}_1 = q_1$ тогда и только тогда, когда $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — близнецы, что и требовалось доказать.

Пусть $\tilde{q}_1 \neq q_1$. Тогда $\mathbf{q}_1$ и $\tilde{\mathbf{q}}_1$ — такие эквивалентные состояния автомата $M \in \mathbf{M}$, что $\mathbf{q}_1 \neq \tilde{\mathbf{q}}_1$. Из равенства $\tilde{q}_2 = q_2$ вытекает, что под действием входного символа $x_2 \in \mathbb{Z}_{p^k}$ состояния $\mathbf{q}_1$ и $\tilde{\mathbf{q}}_1$ автомата M переходят соответственно в состояния $\mathbf{q}_2 = (q_3, q_2)$ и $\tilde{\mathbf{q}}_2 = (\tilde{q}_3, q_2)$, где

$$q_3 = a \oplus b \circ q_2^2 \oplus c \circ q_1 \oplus d \circ x_2, \quad (11)$$

$$\tilde{q}_3 = a \oplus b \circ q_2^2 \oplus c \circ \tilde{q}_1 \oplus d \circ x_2. \quad (12)$$

Так как $\mathbf{q}_1$ и $\tilde{\mathbf{q}}_1$ — эквивалентные состояния автомата M , то $y_2 = \tilde{y}_2$ для любого входного символа $x_2 \in \mathbb{Z}_{p^k}$. Следовательно,

$$y_2 = \tilde{y}_2 \Leftrightarrow e \circ \tilde{q}_3 = e \circ q_3 \Leftrightarrow \tilde{q}_3 = q_3 \quad (13)$$

для любого входного символа $x_2 \in \mathbb{Z}_{p^k}$.

Из равенства $\tilde{q}_2 = q_2$ и из (13) вытекает, что $\mathbf{q}_2 = \tilde{\mathbf{q}}_2$ для любого входного символа $x_2 \in \mathbb{Z}_{p^k}$, т. е. что состояния $\mathbf{q}_1$ и $\tilde{\mathbf{q}}_1$ — близнецы, что и требовалось доказать. ■

Из доказательства теоремы 3 вытекает, что истинно следующее следствие.

Следствие 5. Если $\mathbf{q}, \tilde{\mathbf{q}} \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) — неэквивалентные состояния автомата $M \in \mathbf{M}$, то существует входное слово $x_1 x_2 \in \mathbb{Z}_{p^k}^2$, различающее состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$.

Следствие 6. Состояния $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) автомата $M \in \mathbf{M}$ эквивалентны тогда и только тогда, когда либо

$$\begin{cases} \tilde{q}_1 = q_1, \\ c \circ (\tilde{q}_0 \ominus q_0) = 0, \end{cases} \quad (14)$$

либо

$$\begin{cases} \tilde{q}_1 \neq q_1, \\ b \circ (\tilde{q}_1^2 \ominus q_1^2) \oplus c \circ (\tilde{q}_0 \ominus q_0) = 0, \\ c \circ (\tilde{q}_1 \ominus q_1) = 0. \end{cases} \quad (15)$$

Доказательство. Пусть эквивалентные состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — близнецы. Тогда $\tilde{q}_1 = q_1$, а из (10) вытекает, что $\tilde{q}_2 = q_2$.

Подставив $\tilde{q}_1 = q_1$ и $\tilde{q}_2 = q_2$ в равенства (8) и (9) и вычитая равенство (9) из равенства (8), получим

$$c \circ (\tilde{q}_0 \ominus q_0) = 0,$$

что и требовалось доказать.

Пусть эквивалентные состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ не являются близнецами. Тогда $\tilde{q}_1 \neq q_1$ и, в силу (10), $\tilde{q}_2 = q_2$.

Подставив $\tilde{q}_2 = q_2$ в равенства (8) и (9) и вычитая равенство (9) из равенства (8), получим

$$b \circ (\tilde{q}_1^2 \ominus q_1^2) \oplus c \circ (\tilde{q}_0 \ominus q_0) = 0.$$

Из (13) вытекает, что $\tilde{q}_3 = q_3$. Подставив $\tilde{q}_3 = q_3$ в равенства (11) и (12) и вычитая равенство (12) из равенства (11), получим

$$c \circ (\tilde{q}_1 \ominus q_1) = 0,$$

что и требовалось доказать. ■

3. Вспомогательные результаты

Положив в равенствах (14)

$$\tilde{q}_0 \ominus q_0 = u, \quad (16)$$

а в равенствах (15)

$$\begin{cases} \tilde{q}_1 \ominus q_1 = u, \\ \tilde{q}_1 \oplus q_1 = v, \\ \tilde{q}_0 \ominus q_0 = w, \end{cases} \quad (17)$$

получим, что для того чтобы охарактеризовать структуру множества состояний, эквивалентных фиксированному состоянию $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$, достаточно охарактеризовать структуру множества S_1 решений u уравнения

$$c \circ u = 0 \quad (18)$$

и структуру множества S_2 решений (u, v, w) системы уравнений

$$\begin{cases} b \circ u \circ v \oplus c \circ w = 0, \\ c \circ u = 0. \end{cases} \quad (19)$$

В соответствии с [1] определим p -тип $\mathbf{t}_p(z)$ элемента $z \in \mathbb{Z}_{p^k}$ равенством

$$\mathbf{t}_p(z) = \begin{cases} k, & \text{если } z = 0; \\ 0, & \text{если } z \in \mathbb{Z}_{p^k}^{\text{inv}}; \\ r \ (1 \leq r \leq k-1), & \text{если } z \equiv 0 \pmod{p^r} \text{ и } z \not\equiv 0 \pmod{p^{r+1}}. \end{cases} \quad (20)$$

Замечание 6. Из (20) вытекает, что множество всех элементов кольца $\mathbb{Z}_{p^k}$, p -тип которых равен r ($0 \leq r \leq k-1$), представляет собой множество всех тех элементов $z \in \mathbb{Z}_{p^k}$, которые единственным образом представимы в виде $z = \alpha \circ p^r$, где $\alpha \in \mathbb{Z}_{p^{k-r}}^{\text{inv}}$.

Отсюда, в частности, вытекает, что для любых $u, v \in \mathbb{Z}_{p^k}$

$$\begin{aligned} \mathfrak{t}_p(u \circ v) &= \min\{k, \mathfrak{t}_p(u) + \mathfrak{t}_p(v)\}, \\ \mathfrak{t}_p(u \oplus v) &\geq \min\{\mathfrak{t}_p(u), \mathfrak{t}_p(v)\}, \end{aligned}$$

причем

$$\mathfrak{t}_p(u \oplus v) = 0,$$

если $\mathfrak{t}_p(u) > 0$ и $\mathfrak{t}_p(v) = 0$.

Так как $M \in \mathbf{M}$, то

$$\begin{aligned} \mathfrak{t}_p(b) &\in \{0, 1, \dots, k-1\}, \\ \mathfrak{t}_p(c) &\in \{0, 1, \dots, k\}. \end{aligned}$$

Исследуем структуру множеств S_1 и S_2 при этих предположениях.

Случай 1. Пусть $\mathfrak{t}_p(c) = 0$, т. е. $c \in \mathbb{Z}_{p^k}^{\text{inv}}$.

Для уравнения (18) получим

$$c \circ u = 0 \Leftrightarrow u = 0 \Leftrightarrow S_1 = \{0\}. \quad (21)$$

Для системы уравнений (19) получим

$$\begin{aligned} \begin{cases} b \circ u \circ v \oplus c \circ w = 0, \\ c \circ u = 0, \end{cases} &\Leftrightarrow \begin{cases} u = 0, \\ v \in \mathbb{Z}_{p^k}, \\ c \circ w = 0, \end{cases} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} u = 0, \\ v \in \mathbb{Z}_{p^k}, \\ w = 0, \end{cases} \Leftrightarrow S_2 = \{(0, v, 0) | v \in \mathbb{Z}_{p^k}\}. \end{aligned} \quad (22)$$

Случай 2. Пусть $\mathfrak{t}_p(c) = k$, т. е. $c = 0$.

Для уравнения (18) получим

$$0 \circ u = 0 \Leftrightarrow S_1 = \mathbb{Z}_{p^k}. \quad (23)$$

Для системы уравнений (19) получим

$$\begin{aligned} \begin{cases} b \circ u \circ v \oplus 0 \circ w = 0, \\ 0 \circ u = 0, \end{cases} &\Leftrightarrow \begin{cases} u \in \mathbb{Z}_{p^k}, \\ b \circ u \circ v = 0, \\ w \in \mathbb{Z}_{p^k}, \end{cases} \Leftrightarrow \\ &\Leftrightarrow S_2 = \{(u, v, w) \in \mathbb{Z}_{p^k}^3 | \mathfrak{t}_p(v) \geq k - \mathfrak{t}_p(b) - \mathfrak{t}_p(u)\}. \end{aligned} \quad (24)$$

Случай 3. Пусть $\mathfrak{t}_p(c) \in \{1, \dots, k-1\}$, т. е. $c = \alpha \circ p^{\mathfrak{t}_p(c)}$, где $\alpha \in \mathbb{Z}_{p^{k-\mathfrak{t}_p(c)}}^{\text{inv}}$.

Для уравнения (18) получим

$$\alpha \circ p^{\mathfrak{t}_p(c)} \circ u = 0 \Leftrightarrow p^{\mathfrak{t}_p(c)} \circ u = 0 \Leftrightarrow$$

$$\Leftrightarrow S_1 = \{0\} \cup \bigcup_{l_1=k-\mathfrak{t}_p(c)}^{k-1} \{\delta_1 \circ p^{l_1} | \delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}}\}. \quad (25)$$

Рассмотрим систему уравнений (19). Из (25) вытекает, что

$$S_2 = S_2' \cup S_2'', \quad (26)$$

где S_2' — множество решений системы уравнений (19) при $u = 0$, а S_2'' — множество решений системы уравнений (19) при условии, что

$$u \in \bigcup_{l_1=k-\mathfrak{t}_p(c)}^{k-1} \{\delta_1 \circ p^{l_1} | \delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}}\}.$$

Отметим, что

$$S_2' \cap S_2'' = \emptyset.$$

Найдем множество S_2' :

$$\begin{cases} b \circ u \circ v \oplus \alpha \circ p^{\mathfrak{t}_p(c)} \circ w = 0, \\ \alpha \circ p^{\mathfrak{t}_p(c)} \circ u = 0, \\ u = 0, \end{cases} \Leftrightarrow \begin{cases} u = 0, \\ v \in \mathbb{Z}_{p^k}, \\ \alpha \circ p^{\mathfrak{t}_p(c)} \circ w = 0, \end{cases} \Leftrightarrow \\ \Leftrightarrow S_2' = \{(0, v, w) | v, w \in \mathbb{Z}_{p^k}, \mathfrak{t}_p(w) \geq k - \mathfrak{t}_p(c)\}. \quad (27)$$

Найдем множество S_2'' .

Положим

$$S_2''(\delta_1 \circ p^{l_1}) = \{(u, v, w) \in S_2 | u = \delta_1 \circ p^{l_1} (l_1 \in \{k - \mathfrak{t}_p(c), \dots, k - 1\}; \delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}})\}.$$

Так как множества $S_2''(\delta_1 \circ p^{l_1})$ ($l_1 \in \{k - \mathfrak{t}_p(c), \dots, k - 1\}; \delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}}$) попарно не пересекаются, причем

$$S_2'' = \bigcup_{l_1=k-\mathfrak{t}_p(c)}^{k-1} \bigcup_{\delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}}} S_2''(\delta_1 \circ p^{l_1}), \quad (28)$$

то для того, чтобы найти множество S_2'' , необходимо и достаточно найти множества $S_2''(\delta_1 \circ p^{l_1})$ ($l_1 \in \{k - \mathfrak{t}_p(c), \dots, k - 1\}; \delta_1 \in \mathbb{Z}_{p^{k-l_1}}^{\text{inv}}$).

Найдем эти множества.

Так как

$$\begin{cases} b \circ u \circ v \oplus \alpha \circ p^{\mathfrak{t}_p(c)} \circ w = 0, \\ u = \delta_1 \circ p^{l_1}, \end{cases} \Leftrightarrow \begin{cases} u = \delta_1 \circ p^{l_1}, \\ b \circ \delta_1 \circ p^{l_1} \circ v \oplus \alpha \circ p^{\mathfrak{t}_p(c)} \circ w = 0 \end{cases} \quad (29)$$

и $\mathfrak{t}_p(b) \in \{0, 1, \dots, k - 1\}$, то $b = \beta \circ p^{\mathfrak{t}_p(b)}$, где $\beta \in \mathbb{Z}_{p^{k-\mathfrak{t}_p(b)}}^{\text{inv}}$.

Следовательно, система уравнений (29) имеет вид

$$\begin{cases} u = \delta_1 \circ p^{l_1}, \\ (\beta \circ \delta_1) \circ p^{\mathfrak{t}_p(b)+l_1} \circ v \oplus \alpha \circ p^{\mathfrak{t}_p(c)} \circ w = 0. \end{cases} \quad (30)$$

Возможны следующие три случая.

Случай 3.1. Пусть $l_1 < \mathfrak{t}_p(c) - \mathfrak{t}_p(b)$.

Замечание 7. Так как $l_1 \geq k - \mathfrak{t}_p(c)$, то случай 3.1 имеет место тогда и только тогда, когда $\mathfrak{t}_p(c) > 0,5 \cdot (k + \mathfrak{t}_p(b))$.

Представим систему уравнений (30) в следующей эквивалентной форме:

$$\begin{cases} u = \delta_1 \circ p^{l_1}, \\ p^{\mathfrak{t}_p(b)+l_1} \circ (v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ p^{\mathfrak{t}_p(c)-\mathfrak{t}_p(b)-l_1} \circ w) = 0. \end{cases} \quad (31)$$

Из второго уравнения системы (31) вытекает, что либо

$$v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ p^{\mathfrak{t}_p(c)-\mathfrak{t}_p(b)-l_1} \circ w = 0,$$

либо

$$v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ p^{\mathfrak{t}_p(c)-\mathfrak{t}_p(b)-l_1} \circ w = \delta_2 \circ p^{l_2} \quad (k - \mathfrak{t}_p(b) - l_1 \leq l_2 \leq k - 1, \delta_2 \in \mathbb{Z}_{p^{k-l_2}}^{\text{inv}}).$$

Таким образом, если $l_1 < \mathfrak{t}_p(c) - \mathfrak{t}_p(b)$, то

$$\begin{aligned} S_2''(\delta_1 \circ p^{l_1}) &= \{(\delta_1 \circ p^{l_1}, \ominus \alpha \circ (\beta \circ \delta_1)^{-1} \circ p^{\mathfrak{t}_p(c)-\mathfrak{t}_p(b)-l_1} \circ w, w) | w \in \mathbb{Z}_{p^k}\} \cup \\ &\cup \bigcup_{l_2=k-\mathfrak{t}_p(b)-l_1}^{k-1} \bigcup_{w \in \mathbb{Z}_{p^k}} \{(\delta_1 \circ p^{l_1}, \delta_2 \circ p^{l_2} \ominus \alpha \circ (\beta \circ \delta_1)^{-1} \circ p^{\mathfrak{t}_p(c)-\mathfrak{t}_p(b)-l_1} \circ w, w) | \delta_2 \in \mathbb{Z}_{p^{k-l_2}}^{\text{inv}}\}. \end{aligned} \quad (32)$$

Случай 3.2. Пусть $l_1 = \mathfrak{t}_p(c) - \mathfrak{t}_p(b)$.

Замечание 8. Так как $l_1 \geq k - \mathfrak{t}_p(c)$, то случай 3.2 имеет место тогда и только тогда, когда $\mathfrak{t}_p(c) \geq 0,5(k + \mathfrak{t}_p(b))$.

Представим систему уравнений (30) в следующей эквивалентной форме:

$$\begin{cases} u = \delta_1 \circ p^{l_1}, \\ p^{\mathfrak{t}_p(c)} \circ (v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ w) = 0. \end{cases} \quad (33)$$

Из второго уравнения системы (33) вытекает, что либо

$$v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ w = 0,$$

либо

$$v \oplus \alpha \circ (\beta \circ \delta_1)^{-1} \circ w = \delta_3 \circ p^{l_3} \quad (k - \mathfrak{t}_p(c) \leq l_3 \leq k - 1, \delta_3 \in \mathbb{Z}_{p^{k-l_3}}^{\text{inv}}).$$

Таким образом, если $l_1 = \mathfrak{t}_p(c) - \mathfrak{t}_p(b)$, то

$$\begin{aligned} S_2''(\delta_1 \circ p^{l_1}) &= \{(\delta_1 \circ p^{l_1}, \ominus \alpha \circ (\beta \circ \delta_1)^{-1} \circ w, w) | w \in \mathbb{Z}_{p^k}\} \cup \\ &\cup \bigcup_{l_3=k-\mathfrak{t}_p(c)}^{k-1} \bigcup_{w \in \mathbb{Z}_{p^k}} \{(\delta_1 \circ p^{l_1}, \delta_3 \circ p^{l_3} \ominus \alpha \circ (\beta \circ \delta_1)^{-1} \circ w, w) | \delta_3 \in \mathbb{Z}_{p^{k-l_3}}^{\text{inv}}\}. \end{aligned} \quad (34)$$

Случай 3.3. Пусть $\mathfrak{t}_p(c) - \mathfrak{t}_p(b) < l_1 \leq k - 1$. Представим систему уравнений (30) в следующей эквивалентной форме:

$$\begin{cases} u = \delta_1 \circ p^{l_1}, \\ p^{\mathfrak{t}_p(c)} \circ (\beta \circ \delta_1 \circ \alpha^{-1} \circ p^{\mathfrak{t}_p(b)-\mathfrak{t}_p(c)+l_1} \circ v \oplus w) = 0. \end{cases} \quad (35)$$

Из второго уравнения системы (35) вытекает, что либо

$$\beta \circ \delta_1 \circ \alpha^{-1} \circ p^{\mathfrak{t}_p(b) - \mathfrak{t}_p(c) + l_1} \circ v \oplus w = 0,$$

либо

$$\beta \circ \delta_1 \circ \alpha^{-1} \circ p^{\mathfrak{t}_p(b) - \mathfrak{t}_p(c) + l_1} \circ v \oplus w = \delta_4 \circ p^{l_4} \quad (k - \mathfrak{t}_p(c) \leq l_4 \leq k - 1, \delta_4 \in \mathbb{Z}_{p^{k-l_4}}^{\text{inv}}).$$

Таким образом, если $\mathfrak{t}_p(c) - \mathfrak{t}_p(b) < l_1 \leq k - 1$, то

$$\begin{aligned} S_2''(\delta_1 \circ p^{l_1}) &= \{(\delta_1 \circ p^{l_1}, v, \ominus \beta \circ \delta_1 \circ \alpha^{-1} \circ p^{\mathfrak{t}_p(b) - \mathfrak{t}_p(c) + l_1} \circ v) | v \in \mathbb{Z}_{p^k}\} \cup \\ &\cup \bigcup_{l_4=k-\mathfrak{t}_p(c)}^{k-1} \bigcup_{v \in \mathbb{Z}_{p^k}} \{(\delta_1 \circ p^{l_1}, v, \delta_4 \circ p^{l_4} \ominus \beta \circ \delta_1 \circ \alpha^{-1} \circ p^{\mathfrak{t}_p(b) - \mathfrak{t}_p(c) + l_1} \circ v) | \delta_4 \in \mathbb{Z}_{p^{k-l_4}}^{\text{inv}}\}. \end{aligned} \quad (36)$$

4. Структура множеств эквивалентных состояний исследуемой модели

В соответствии с [10] автомат $M \in \mathbf{M}$ назовем приведенным, если все его состояния попарно неэквивалентные.

Теорема 4. Автомат $M \in \mathbf{M}$ является приведенным автоматом тогда и только тогда, когда $c \in \mathbb{Z}_{p^k}^{\text{inv}}$.

Доказательство. Из следствия 6 вытекает, что состояния $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) автомата $M \in \mathbf{M}$ являются близнецами тогда и только тогда, когда они удовлетворяют равенствам (14).

Пусть $c \in \mathbb{Z}_{p^k}^{\text{inv}}$. Из (21) вытекает, что уравнение (18) имеет единственное решение $u = 0$. Подставив это значение u в (16), получим, что $\tilde{q}_0 = q_0$. Отсюда вытекает, что состояния $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$ удовлетворяют равенствам (14) тогда и только тогда, когда $\mathbf{q} = \tilde{\mathbf{q}}$. Следовательно, никакие два различных состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ автомата $M \in \mathbf{M}$ не являются близнецами.

Отсюда (в силу теоремы 3) вытекает, что никакие два различных состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ автомата $M \in \mathbf{M}$ не являются эквивалентными состояниями, т. е. $M \in \mathbf{M}$ — приведенный автомат, что и требовалось доказать.

Пусть $c \notin \mathbb{Z}_{p^k}^{\text{inv}}$. Из (23) и (25) вытекает, что уравнение (18) имеет решение $u_0 \neq 0$. Подставив это решение в (16), получим $\tilde{q}_0 = q_0 \oplus u_0$. Так как u_0 — решение уравнения (18) и $u_0 \neq 0$, то $\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ и $\tilde{\mathbf{q}} = ((q_1, q_0 \oplus u_0) \in \mathbb{Z}_{p^k}^2$ — различные состояния автомата $M \in \mathbf{M}$, удовлетворяющие равенствам (14), т. е. состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ являются близнецами.

Отсюда (в силу теоремы 3) вытекает, что $\mathbf{q}$ и $\tilde{\mathbf{q}}$ ($\mathbf{q} \neq \tilde{\mathbf{q}}$) — эквивалентные состояния автомата $M \in \mathbf{M}$, т. е. автомат $M \in \mathbf{M}$ не является приведенным автоматом, что и требовалось доказать. ■

Обозначим через $\mathbf{M}_{NR}$ множество всех автоматов $M \in \mathbf{M}$, не являющихся приведенными автоматами.

Замечание 9. Так как $|\mathbf{M}| = p^{4k}(p^k - 1)(1 - p^{-1})^2$ и $|\mathbf{M}_{NR}| = p^{4k}(p^k - 1)(1 - p^{-1})^3$, то $|\mathbf{M}_{NR}| \cdot |\mathbf{M}|^{-1} = 1 - p^{-1}$. Значит, $|\mathbf{M}_{NR}| \cdot |\mathbf{M}|^{-1} \xrightarrow{p \rightarrow \infty} 1$, т. е. при $p \rightarrow \infty$ почти все автоматы $M \in \mathbf{M}$ не являются приведенными автоматами.

Обозначим через $C_M(\mathbf{q})$ ($\mathbf{q} = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$, $M \in \mathbf{M}_{NR}$) множество всех состояний автомата M , эквивалентных состоянию $\mathbf{q}$.

Из теоремы 3 вытекает, что множество $C_M(\mathbf{q})$ может быть представлено в виде

$$C_M(\mathbf{q}) = \{\mathbf{q}\} \cup C_M^{(1)}(\mathbf{q}) \cup C_M^{(2)}(\mathbf{q}), \quad (37)$$

где $C_M^{(1)}(\mathbf{q})$ — множество всех таких состояний $\tilde{\mathbf{q}} = (q_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($q_0 \neq \tilde{q}_0$), что состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ — близнецы, а $C_M^{(2)}(\mathbf{q})$ — множество всех таких состояний $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_0) \in \mathbb{Z}_{p^k}^2$ ($q_1 \neq \tilde{q}_1$), что состояния $\mathbf{q}$ и $\tilde{\mathbf{q}}$ по любому входному символу переходят в состояния-близнецы.

Из (14), (16), (23) и (25) вытекает, что

$$C_M^{(1)}(\mathbf{q}) = \{\tilde{\mathbf{q}} = (q_1, q_0 \oplus u) | u \in S_1 \setminus \{0\}\}, \quad (38)$$

а из (15), (17), (24) и (26) вытекает, что

$$C_M^{(2)}(\mathbf{q}) = \begin{cases} \{(\tilde{q}_1, \tilde{q}_0) | \tilde{q}_1 \neq q_1 \text{ \& } (\tilde{q}_1 \ominus q_1, \tilde{q}_1 \oplus q_1, \tilde{q}_0 \ominus q_0) \in S_2\}, & \text{если } \mathfrak{t}_p(c) = k; \\ \{(\tilde{q}_1, \tilde{q}_0) | \tilde{q}_1 \neq q_1 \text{ \& } (\tilde{q}_1 \ominus q_1, \tilde{q}_1 \oplus q_1, \tilde{q}_0 \ominus q_0) \in S_2''\}, & \text{если } 1 \leq \mathfrak{t}_p(c) \leq k-1. \end{cases}$$

Замечание 10. Из (23), (25) и (38) вытекает, что

$$|C_M^{(1)}(\mathbf{q})| = p^{\mathfrak{t}_p(c)} - 1.$$

В то же время из (24), (28), (32), (34) и (36) вытекает, что значение числа $|C_M^{(2)}(\mathbf{q})|$ представляется достаточно громоздкими суммами, вид которых существенно зависит от элемента $q_1 \in \mathbb{Z}_{p^k}$ кольца, а также от значений чисел $\mathfrak{t}_p(b)$ и $\mathfrak{t}_p(c)$. В настоящее время авторам не удалось получить простые оценки числа $|C_M^{(2)}(\mathbf{q})|$.

5. Задачи идентификации исследуемой модели

Рассмотрим задачу идентификации начального состояния $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата $M \in \mathbf{M}$.

Теорема 5. Для любого автомата $M \in \mathbf{M}$, если экспериментатору известен набор значений параметров $(a, b, c, d, e) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2$, то:

1) если $c \in \mathbb{Z}_{p^k}^{\text{inv}}$, то для любого входного слова $x_1 x_2 \in \mathbb{Z}_{p^k}^2$ начальное состояние $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ может быть вычислено по формулам

$$\begin{aligned} q_1 &= c^{-1} \circ (e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2), \\ q_0 &= c^{-1} \circ (e^{-1} \circ y_1 \ominus a \ominus b \circ q_1^2 \ominus d \circ x_1); \end{aligned} \quad (39)$$

2) если $c \in \mathbb{Z}_{p^k} \setminus \mathbb{Z}_{p^k}^{\text{inv}}$, то множество $C_M(\mathbf{q}_0)$ ($\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$) всех состояний автомата M , эквивалентных начальному состоянию $\mathbf{q}_0$, может быть вычислено по формуле

$$C_M(\mathbf{q}_0) = \bigcap_{x_1 x_2 \in \mathbb{Z}_{p^k}^2} S_{x_1 x_2}, \quad (40)$$

где $S_{x_1 x_2}$ ($x_1 x_2 \in \mathbb{Z}_{p^k}^2$) — множество всех решений (q_1, q_0) системы уравнений

$$\begin{cases} c \circ q_1 = e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2, \\ c \circ q_0 = e^{-1} \circ y_1 \ominus a \ominus b \circ q_1^2 \ominus d \circ x_1. \end{cases} \quad (41)$$

Доказательство. Из системы уравнений (1) вытекает, что

$$y_{t+1} = e \circ (a \oplus b \circ q_{t+1}^2 \oplus c \circ q_t \oplus d \circ x_{t+1}) \quad (t \in \mathbb{Z}_+). \quad (42)$$

Полагая $t = 0$ и 1 в (42), получим, что для любого входного слова $x_1x_2 \in \mathbb{Z}_{p^k}^2$ истинны равенства

$$\begin{aligned} & \begin{cases} y_1 = a \circ e \oplus b \circ e \circ q_1^2 \oplus c \circ e \circ q_0 \oplus d \circ e \circ x_1, \\ y_2 = a \circ e \oplus b \circ e \circ q_2^2 \oplus c \circ e \circ q_1 \oplus d \circ e \circ x_2, \end{cases} \Leftrightarrow \\ & \Leftrightarrow \begin{cases} y_1 = a \circ e \oplus b \circ e \circ q_1^2 \oplus c \circ e \circ q_0 \oplus d \circ e \circ x_1, \\ y_2 = a \circ e \oplus b \circ e^{-1} \circ y_1^2 \oplus c \circ e \circ q_1 \oplus d \circ e \circ x_2, \end{cases} \Leftrightarrow \\ & \Leftrightarrow \begin{cases} c \circ q_1 = e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2, \\ c \circ q_0 = e^{-1} \circ y_1 \ominus a \ominus b \circ q_1^2 \ominus d \circ x_1. \end{cases} \end{aligned} \quad (43)$$

Если $c \in \mathbb{Z}_{p^k}^{\text{inv}}$, то из (43) вытекает, что истинны равенства (39), что и требовалось доказать.

Если $c \in \mathbb{Z}_{p^k} \setminus \mathbb{Z}_{p^k}^{\text{inv}}$, то из (43) и следствия 5 вытекает, что истинны равенства (40), что и требовалось доказать. ■

Из теоремы 5 вытекает, что истинно следующее следствие.

Следствие 7. Для любого автомата $M \in \mathbf{M}$, если экспериментатору известен набор значений параметров $(a, b, c, d, e) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2$, то

1) если $c \in \mathbb{Z}_{p^k}^{\text{inv}}$, то идентификация начального состояния автомата M осуществима посредством простого эксперимента длины 2;

2) если $c \in \mathbb{Z}_{p^k} \setminus \mathbb{Z}_{p^k}^{\text{inv}}$, то идентификация множества всех состояний, эквивалентных начальному состоянию автомата M , осуществима посредством кратного эксперимента кратности p^{2k} и высоты 2.

Замечание 11. Если $c = 0$, то система уравнений (41) принимает вид

$$\begin{aligned} & \begin{cases} e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2 = 0, \\ e^{-1} \circ y_1 \ominus a \ominus b \circ q_1^2 \ominus d \circ x_1 = 0, \end{cases} \Leftrightarrow \\ & \Leftrightarrow \begin{cases} e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2 = 0, \\ b \circ q_1^2 = e^{-1} \circ y_1 \ominus a \ominus d \circ x_1, \end{cases} \end{aligned}$$

где равенство

$$e^{-1} \circ y_2 \ominus a \ominus b \circ e^{-2} \circ y_1^2 \ominus d \circ x_2 = 0$$

не содержит переменных и является истинным равенством в кольце $\mathbb{Z}_{p^k}$. Следовательно, если $c = 0$, то для любого входного слова $x_1x_2 \in \mathbb{Z}_{p^k}^2$ множество $S_{x_1x_2}$ всех решений системы уравнений (41) состоит из всех таких пар (q_1, q_0) , что $q_0 \in \mathbb{Z}_{p^k}$, а q_1 является решением квадратного уравнения

$$b \circ q_1^2 = e^{-1} \circ y_1 \ominus a \ominus d \circ x_1.$$

Рассмотрим задачу параметрической идентификации автомата $M \in \mathbf{M}$ в предположении, что экспериментатор может проводить с автоматом M кратный эксперимент любой кратности.

Возможны следующие два случая.

Случай 1. Начальное состояние $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ автомата M известно экспериментатору.

Возможны следующие два случая.

Случай 1.1. Пусть $\mathbf{q}_0 = (q_1, q_0) = (0, 0)$. Полагая $t = 0, 1, \dots, l$ ($l \geq 6$) в (42), получим, что для любого входного слова $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$ истинны равенства

$$\begin{aligned} a \circ e \oplus d \circ e \circ x_1 &= y_1, \\ a \circ e \oplus b \circ e^{-1} \circ y_1^2 \oplus d \circ e \circ x_2 &= y_2, \\ a \circ e \oplus b \circ e^{-1} \circ y_2^2 \oplus c \circ y_1 \oplus d \circ e \circ x_3 &= y_3, \\ &\dots\dots\dots \\ a \circ e \oplus b \circ e^{-1} \circ y_{l-1}^2 \oplus c \circ y_{l-2} \oplus d \circ e \circ x_l &= y_l. \end{aligned} \quad (44)$$

Матрица A совместной системы уравнений (44) имеет следующий вид:

$$A = \begin{matrix} & a \circ e & b \circ e^{-1} & c & d \circ e \\ \begin{matrix} 1 \\ 2 \\ 3 \\ \vdots \\ l \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & x_1 \\ 1 & y_1^2 & 0 & x_2 \\ 1 & y_2^2 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & y_{l-1}^2 & y_{l-2} & x_l \end{pmatrix} \end{matrix}.$$

Найдем такое входное слово $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$ заранее неизвестной длины $l \geq 4$, что матрица A содержит обратимую подматрицу B 4-го порядка. Четыре уравнения системы уравнений (44), определяемые подматрицей B , образуют систему линейных уравнений, имеющую единственное решение:

$$\begin{cases} a \circ e = \alpha_1, \\ b \circ e^{-1} = \alpha_2, \\ c = \alpha_3, \\ d \circ e = \alpha_4. \end{cases} \quad (45)$$

Из (44) вытекает, что даже при отсутствии информации об истинном значении набора параметров $(a, b, c, d, e) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2$ решение (45) дает возможность моделировать работу автомата M на любом входном слове $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$, $l \in \mathbb{N}$, так как

$$\begin{aligned} y_1 &= \alpha_1 \oplus \alpha_4 \circ x_1, \\ y_2 &= \alpha_1 \oplus \alpha_2 \circ y_1^2 \oplus \alpha_4 \circ x_2, \\ y_3 &= \alpha_1 \oplus \alpha_2 \circ y_2^2 \oplus \alpha_3 \circ y_1 \oplus \alpha_4 \circ x_3, \\ &\dots\dots\dots \\ y_l &= \alpha_1 \oplus \alpha_2 \circ y_{l-1}^2 \oplus \alpha_3 \circ y_{l-2} \oplus \alpha_4 \circ x_l. \end{aligned} \quad (46)$$

А так как $\alpha_4 = d \circ e \in \mathbb{Z}_{p^k}^{\text{inv}}$, то решение (45) дает возможность по любому выходному слову $y_1 \dots y_l \in \mathbb{Z}_{p^k}^l$ однозначно вычислить поданное на автомат M входное слово $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$.

Случай 1.2. Пусть $\mathbf{q}_0 = (q_1, q_0) \neq (0, 0)$. Полагая $t = 0, 1, \dots, l$ ($l \geq 6$) в (42), получим, что для любого входного слова $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$ истинны равенства

$$\begin{aligned} a \circ e \oplus b \circ e \circ q_1^2 \oplus c \circ e \circ q_0 \oplus d \circ e \circ x_1 &= y_1, \\ a \circ e \oplus b \circ e^{-1} \circ y_1^2 \oplus c \circ e \circ q_1 \oplus d \circ e \circ x_2 &= y_2, \\ a \circ e \oplus b \circ e^{-1} \circ y_2^2 \oplus c \circ y_1 \oplus d \circ e \circ x_3 &= y_3, \\ &\dots\dots\dots \\ a \circ e \oplus b \circ e^{-1} \circ y_{l-1}^2 \oplus c \circ y_{l-2} \oplus d \circ e \circ x_l &= y_l. \end{aligned} \quad (47)$$

Матрица C совместной системы уравнений (47) имеет следующий вид:

$$C = \begin{matrix} & a \circ e & b \circ e & b \circ e^{-1} & c \circ e & c & d \circ e \\ \begin{matrix} 1 \\ 2 \\ 3 \\ \vdots \\ l \end{matrix} & \begin{pmatrix} 1 & q_1^2 & 0 & q_0 & 0 & x_1 \\ 1 & 0 & y_1^2 & q_1 & 0 & x_2 \\ 1 & 0 & y_2^2 & 0 & y_1 & x_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & y_{l-1}^2 & 0 & y_{l-2} & x_l \end{pmatrix} \end{matrix}.$$

Найдем такое входное слово $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$ заранее неизвестной длины $l \geq 6$, что матрица C содержит обратимую подматрицу D 6-го порядка. Шесть уравнений системы уравнений (47), определяемые подматрицей D , образуют систему линейных уравнений, имеющую единственное решение:

$$\begin{cases} a \circ e = \beta_1, \\ b \circ e = \beta_2, \\ b \circ e^{-1} = \beta_3, \\ c \circ e = \beta_4, \\ c = \beta_5, \\ d \circ e = \beta_6. \end{cases} \quad (48)$$

Из (47) вытекает, что даже при отсутствии информации об истинном значении набора параметров $(a, b, c, d, e) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2$ решение (48) дает возможность моделировать работу автомата M на любом входном слове $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$ ($l \in \mathbb{N}$), так как

$$\begin{aligned} y_1 &= \beta_1 \oplus \beta_2 \circ q_1^2 \oplus \beta_4 \circ q_0 \oplus \beta_6 \circ x_1, \\ y_2 &= \beta_1 \oplus \beta_3 \circ y_1^2 \oplus \beta_4 \circ q_1 \oplus \beta_6 \circ x_2, \\ y_3 &= \beta_1 \oplus \beta_3 \circ y_2^2 \oplus \beta_5 \circ y_1 \oplus \beta_6 \circ x_3, \\ &\dots\dots\dots \\ y_l &= \beta_1 \oplus \beta_3 \circ y_{l-1}^2 \oplus \beta_5 \circ y_{l-2} \oplus \beta_6 \circ x_l. \end{aligned} \quad (49)$$

А так как $\beta_6 = d \circ e \in \mathbb{Z}_{p^k}^{\text{inv}}$, то решение (48) дает возможность по любому выходному слову $y_1 \dots y_l \in \mathbb{Z}_{p^k}^l$ однозначно вычислить поданное на автомат M входное слово $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$.

Замечание 12. Ясно, что равенства (46) представляют собой специальный случай равенств (49). Действительно, если в (49) положить $q_1 = q_0 = 0$ и (в силу равенств (45) и (48)) $\beta_1 = \alpha_1$, $\beta_3 = \alpha_2$, $\beta_5 = \alpha_3$ и $\beta_6 = \alpha_4$, то получим равенства (46).

Теорема 6. Для любого автомата $M \in \mathbf{M}$ при любом начальном состоянии $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$ множество $S_{\text{fxd}}^{(l)}(M, \mathbf{q}_0)$ ($l \in \mathbb{N}$) состоит из всех таких входных слов $x_1 \dots x_l \in \mathbb{Z}_{p^k}^l$, что $(x_1, \dots, x_l)$ — решение системы уравнений

[illegible]

Доказательство. Реакцией инициального автомата $(M, \mathbf{q}_0)$ на входное слово $x_1 \dots x_l \in S_{\text{fnd}}^{(l)}(M, \mathbf{q}_0)$ является такое выходное слово $y_1 \dots y_l \in \mathbb{Z}_{n_k}^l$, что

$$y_1 \dots y_l = x_1 \dots x_l.$$

[illegible]

Следствие 8. Для любого автомата $M \in \mathbf{M}$ при любом начальном состоянии $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$, если $1 \ominus \beta_6 \in \mathbb{Z}_{p^k}^{\text{inv}}$, то $|S_{\text{fixd}}^{(l)}(M, \mathbf{q}_0)| = 1$ для всех $l \in \mathbb{N}$.

Доказательство. Если $1 \ominus \beta_6 \in \mathbb{Z}_{p^k}^{\text{inv}}$, то для всех $l \in \mathbb{N}$ система уравнений (52) имеет единственное решение $(x_1, \dots, x_l)$, где

[illegible]

что и требовалось доказать. ■

Следствие 9. Для любого автомата $M \in \mathbf{M}$ при любом начальном состоянии $\mathbf{q}_0 = (q_1, q_0) \in \mathbb{Z}_{p^k}^2$, если $a \in \mathbb{Z}_{p^k}^{\text{inv}}$, $\mathbf{t}_p(b) > 0$, $\mathbf{t}_p(c) > 0$ и $\mathbf{t}_p(1 \ominus d \circ e) > 0$, то $S_{\text{fxd}}(M, \mathbf{q}_0) = \emptyset$.

Доказательство. Рассмотрим первое уравнение системы уравнений (52):

$$(1 \ominus \beta_6) \circ x_1 = \beta_1 \oplus \beta_2 \circ q_1^2 \oplus \beta_4 \circ q_0. \quad (53)$$

Так как $\mathbf{t}_p(1 \ominus d \circ e) > 0$, $\mathbf{t}_p(b) > 0$ и $\mathbf{t}_p(c) > 0$, то

$$\begin{aligned} \mathbf{t}_p(1 \ominus \beta_6) &= \mathbf{t}_p(1 \ominus d \circ e) > 0, \\ \mathbf{t}_p(\beta_2) &= \mathbf{t}_p(b \circ e) > 0, \\ \mathbf{t}_p(\beta_4) &= \mathbf{t}_p(c \circ e) > 0. \end{aligned}$$

А так как $a, e \in \mathbb{Z}_{p^k}^{\text{inv}}$, то

$$\mathbf{t}_p(\beta_1) = \mathbf{t}_p(a \circ e) = 0.$$

Следовательно, для любых $x_1, q_1, q_0 \in \mathbb{Z}_{p^k}$

$$\begin{aligned} \mathbf{t}_p((1 \ominus \beta_6) \circ x_1) &> 0, \\ \mathbf{t}_p(\beta_1 \oplus \beta_2 \circ q_1^2 \oplus \beta_4 \circ q_0) &= 0. \end{aligned} \quad (54)$$

Из (54) и (55) вытекает, что уравнение (53) не имеет решений, т. е.

$$S_{\text{fxd}}^{(1)}(M, \mathbf{q}_0) = \emptyset.$$

А так как

$$S_{\text{fxd}}^{(l+1)}(M, \mathbf{q}_0) \subseteq \{ux | u \in S_{\text{fxd}}^{(l)}(M, \mathbf{q}_0), x \in \mathbb{Z}_{p^k}\} \quad (l \in \mathbb{N}),$$

то

$$S_{\text{fxd}}^{(l)}(M, \mathbf{q}_0) = \emptyset$$

для всех $l \in \mathbb{N}$.

Отсюда вытекает, что $S_{\text{fxd}}(M, \mathbf{q}_0) = \emptyset$, что и требовалось доказать. ■

Заключение

В работе исследован класс $\mathbf{M}$ обратимых нелинейных одномерных автоматов Мура, определенных системой уравнений с лагом 2 над кольцом $\mathbb{Z}_{p^k}$, которые на каждом такте своего функционирования осуществляют линейное преобразование линейной комбинации квадратичной формы текущего состояния автомата и аффинного преобразования входного символа. Для исследуемой модели охарактеризованы структура автоматного графа и множества эквивалентных состояний, решены задачи параметрической идентификации и идентификации начального состояния, охарактеризованы множества неподвижных точек отображений, реализуемых инициальными автоматами.

Полученные результаты следующим образом характеризуют симметричный поточный шифр (3).

В п. 6 (следствие 9) выделены значения ключей (a, b, c, d, e) средней длительности, при которых отображение $f_{(M, \mathbf{q}_0)} : \mathbb{Z}_{p^k}^+ \rightarrow \mathbb{Z}_{p^k}^+$ не имеет неподвижных точек. Систематический анализ вариации таких отображений при вариации секретного сеансового ключа $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^2$ является одним из возможных направлений дальнейших исследований.

Если $c \in \mathbb{Z}_{p^k}^{\text{inv}}$, то любые сеансовые ключи неэквивалентны (теорема 4), т. е. не возникает задача выбора нового секретного сеансового ключа, неэквивалентного предыдущему секретному сеансовому ключу. Однако, если криптоаналитик располагает секретным ключом средней длительности (a, b, c, d, e) , то он без труда идентифицирует секретный сеансовый ключ (теорема 5 и следствие 7). Если же $c \notin \mathbb{Z}_{p^k}^{\text{inv}}$, то, даже располагая секретным ключом средней длительности (a, b, c, d, e) , для идентификации секретного сеансового ключа (с точностью до множества эквивалентных состояний) криптоаналитик вынужден решать совокупность систем квадратных уравнений над кольцом $\mathbb{Z}_{p^k}$, полученных посредством кратного эксперимента кратности p^{2k} и высоты 2 (теорема 5 и следствие 7). Однако при этом возникает задача выбора нового секретного сеансового ключа, неэквивалентного предыдущему секретному сеансовому ключу. Эта задача решается посредством кратного эксперимента кратности не более p^{2k} и высоты не более 2 (теорема 5).

В п. 5 показано, что вычислительная стойкость симметричного поточного шифра (3) полностью определяется сложностью поиска решения (51) (а не сложностью идентификации набора параметров (a, b, c, d, e)). Поэтому вторым из возможных направлений исследований является анализ с позиции криптографии подклассов автоматов, принадлежащих классу $\mathbf{M}$ и определяемых четверкой $(a \circ e, b \circ e^{-1}, c, d \circ e)$ $((a, b, c, d, e) \in \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k} \setminus \{0\}) \times \mathbb{Z}_{p^k} \times (\mathbb{Z}_{p^k}^{\text{inv}})^2)$ элементов кольца $\mathbb{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$.

Третьим возможным направлением исследований является анализ изменения вычислительной стойкости симметричного поточного шифра при сохранении функции переходов и замене линейной функции выхода на нелинейную функцию выхода, а также при переходе к автомату Мили.

ЛИТЕРАТУРА

1. Скобелев В. В., Скобелев В. Г. Анализ шифрсистем. Донецк: ИПММ НАН Украины, 2009. 479 с.
2. Скобелев В. Г. Комбинаторно-алгебраические модели в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 74–114.
3. Глушков В. М. Синтез цифровых автоматов. М.: Физматлит, 1962. 476 с.
4. Трахтенброт Б. А., Барздин Я. М. Конечные автоматы (поведение и синтез). М.: Наука, 1970. 400 с.
5. Кузнецов С. П. Динамический хаос. М.: Физматлит, 2001. 296 с.
6. Скобелев В. Г., Тубольцева О. В. Шифр на основе отображения Эно // Вестник Томского государственного университета. Приложение. 2005. № 14. С. 74–78.
7. Гилл А. Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.
8. Bollobas B. Modern graph theory. NY: Springer Verlag, 1998. 394 p.
9. Коршунов А. Д. О перечислении конечных автоматов // Проблемы кибернетики. Вып. 34. М.: Наука, 1978. С. 5–82.
10. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию конечных автоматов. М.: Наука, 1985. 320 с.