2008 Прикладная теория автоматов № 1(1)
DOI 10.17223/20710410/1/21
УДК 681.3

ИДЕНТИФИКАЦИЯ АВТОМАТА В КЛАССЕ АВТОМАТОВ СПРОТТА

В.А. Сухинин, В.Г. Скобелев

Донецкий национальный университет
Институт прикладной математики и механики НАН Украины, г. Донецк

E-mail: vladimir.suhinin@gmail.com, skbv@iamm.ac.donetsk.ua

Решается задача идентификации автомата в классе автоматов Спротта над конечным кольцом $\mathbf{Z}_p{}^k = (\mathbf{Z}_p{}^k, \oplus, \circ)$. Оценка сложности решения задачи необходима для характеристики стойкости поточного шифра, определяемого автоматом Спротта при использовании информационного потока в качестве управления. Показано, что в подклассе автоматов Спротта задача решается проведением кратного эксперимента с автоматом.

Ключевые слова: *автоматы Спротта*, *идентификация*, *кратные эксперименты*, *поточные шифры*, *криптоанализ.*

На современном этапе развития информационных технологий актуальной проблемой является построение высокоскоростных поточных шифров. Значительные усилия исследователей направлены на разработку математического аппарата, предназначенного для решения задач преобразования информации, основанного на моделях и методах современной алгебры. Одним из таких направлений (см., напр., [1, 2]) является разработка средств и методов защиты информации на основе хаотических динамических систем [3]. При использовании информационного потока в качестве управления любая такая система определяет симметричный поточный шифр, причем расшифрование осуществляет обратная система. Ошибки округления, возникающие при использовании таких шифров над полем действительных чисел, устраняются за счет перехода к конечному кольцу $\mathbf{Z}_p{}^k = (\mathbf{Z}_p{}^k, \oplus, \circ)$. Такой переход приводит к конечным автоматам над конечным кольцом, что дает возможность непосредственно применять при анализе шифров модели и методы теории автоматов и теории колец. При этом параметры автомата и его начальное состояние являются составляющими секретного ключа шифра.

Структура работы следующая: в п. 1 представлена основная модель – аналоги над конечным кольцом систем Спротта с управлением; в п. 2 решена задача идентификации автомата в подклассе автоматов Спротта. Заключение содержит ряд выводов.

1. Основная модель

В дальнейшем все величины – элементы кольца $\mathbf{Z}_p{}^k = (\mathbf{Z}_p{}^k, \oplus, \circ)$, где p – простое число, $k \in \mathbf{N}$, а операции $\oplus$ и $\circ$ определяются равенствами

$$a \oplus b = a + b \pmod{p^k},$$
$$a \circ b = a \cdot b \pmod{p^k},$$

где $a, b \in \mathbf{Z}_p{}^k$, $\ominus$ – операция, обратная к операции $\oplus$, причем будем считать, что $p^k > 2$.

В работе исследуется класс автоматов Спротта – класс аналогов модельных динамических систем Спротта с нетривиальной структурой множества аттракторов [3]. Каждая из классических систем Спротта представляет собой систему трех дифференциальных уравнений. Поэтому информационная переменная может быть добавлена как во все уравнения системы (тогда выходом автомата является состояние автомата), так и в некоторые уравнения системы (соответственно выходом автомата является частичная информация о его состоянии). Положим $\mathrm{Y} = \{A, B, \ldots, S\}$. Автомат, соответствующий системе Спротта $x \in \mathrm{Y}$ в случае, когда информационная переменная добавляется во все уравнения системы, обозначим через M_x. В табл. 1 представлены автоматы M_x ($x \in \mathrm{Y}$) в скалярном виде, т.е. в виде систем уравнений над кольцом $\mathbf{Z}_p{}^k$, где $m_i = h \circ \alpha_i \circ x_{t+1}$ ($i = 1, 2, 3$), $t \in \mathbf{Z}_0$, а h и α_i ($i = 1, 2, 3$) – обратимые элементы кольца $\mathbf{Z}_p{}^k$. При переходе к кольцу $\mathbf{Z}_p{}^k$ ряд систем Спротта обобщен. Это обобщение состоит в том, что конкретные числовые коэффициенты классических систем Спротта заменены на произвольный фиксированный элемент β (возможно, с ин-

дексами) кольца $\mathbf{Z}_p^k$. Кроме того, в табл. 1 не указаны выходные переменные автоматов, так как для автоматов M_x ($x \in \mathrm{Y}$) выход автомата совпадает с его состоянием.

Таблица 1

$(M_A, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \ominus h \circ (q_t^{(2)})^2 \oplus m_3 \end{cases}$	$(M_B, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \ominus h \circ q_t^{(1)} \circ q_t^{(2)} \oplus m_3 \end{cases}$
$(M_C, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \ominus h \circ (q_t^{(1)})^2 \oplus m_3 \end{cases}$	$(M_D, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \oplus h \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \circ q_t^{(3)} \oplus \\ \quad \oplus \beta \circ h \circ (q_t^{(2)})^2 \oplus m_3 \end{cases}$
$(M_E, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ (q_t^{(1)})^2 \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \ominus h \circ \beta \circ q_t^{(1)} \oplus m_3 \end{cases}$	$(M_F, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ q_t^{(1)} \oplus h \circ \beta \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ (q_t^{(1)})^2 \ominus h \circ q_t^{(3)} \oplus m_3 \end{cases}$
$(M_G, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ \beta \circ q_t^{(1)} \oplus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \circ q_t^{(3)} \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \ominus h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus m_3 \end{cases}$	$(M_H, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus h \circ (q_t^{(3)})^2 \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \oplus h \circ \beta \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(3)} \oplus m_3 \end{cases}$
$(M_I, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ \beta \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \oplus h \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \oplus h \circ (q_t^{(2)})^2 \ominus \\ \quad \ominus h \circ q_t^{(3)} \oplus m_3 \end{cases}$	$(M_J, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ \beta \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ \beta \circ q_t^{(2)} \oplus h \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \ominus h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus \\ \quad \oplus h \circ (q_t^{(2)})^2 \oplus m_3 \end{cases}$
$(M_K, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(1)} \circ q_t^{(2)} \ominus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \oplus h \circ \beta \circ q_t^{(3)} \oplus m_3 \end{cases}$	$(M_L, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus h \circ \beta_1 \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ \beta_2 \circ (q_t^{(1)})^2 \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \ominus h \circ q_t^{(1)} \oplus m_3 \end{cases}$
$(M_M, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ (q_t^{(1)})^2 \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ \beta \oplus h \circ \beta \circ q_t^{(1)} \oplus \\ \quad \oplus h \circ (q_t^{(2)})^2 \oplus m_3 \end{cases}$	$(M_N, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ \beta \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \oplus h \circ (q_t^{(3)})^2 \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \oplus h \circ q_t^{(2)} \ominus h \circ \beta \circ q_t^{(1)} \oplus m_3 \end{cases}$
$(M_O, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \oplus h \circ q_t^{(1)} \circ q_t^{(3)} \oplus \\ \quad \oplus h \circ \beta \circ q_t^{(2)} \oplus m_3 \end{cases}$	$(M_P, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ \beta \circ q_t^{(2)} \oplus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ q_t^{(1)} \oplus h \circ (q_t^{(2)})^2 \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \oplus m_3 \end{cases}$
$(M_Q, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(3)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \ominus h \circ q_t^{(2)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ \beta_1 \oplus h \circ (q_t^{(2)})^2 \oplus \\ \quad \oplus h \circ \beta_2 \circ q_t^{(3)} \oplus m_3 \end{cases}$	$(M_R, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ \beta_1 \ominus h \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ \beta_2 \oplus h \circ q_t^{(3)} \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \circ q_t^{(1)} \circ q_t^{(2)} \ominus h \circ q_t^{(3)} \oplus m_3 \end{cases}$
$(M_S, \mathrm{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(1)} \ominus h \circ \beta \circ q_t^{(2)} \oplus m_1 \\ q_{t+1}^{(2)} = q_t^{(2)} \oplus h \circ q_t^{(1)} \oplus h \circ (q_t^{(3)})^2 \oplus m_2 \\ q_{t+1}^{(3)} = q_t^{(3)} \oplus h \oplus h \circ q_t^{(1)} \oplus m_3 \end{cases}$	

2. Идентификация автомата в классе автоматов M_x ($x \in Y$)

При атаках на шифрсистему, основанную на использовании автоматов M_x ($x \in Y$), важной информацией для криптоаналитика является знание x, то есть знание автомата, с которым работает шифрсистема. Предположим, что криптоаналитик может осуществлять требуемую инициализацию $(q_0^{(1)}, q_0^{(2)}, q_0^{(3)}) \in (\mathbf{Z}_{p^k})^3$ автомата M_x ($x \in Y$), а также имеет возможность управлять входом автомата M_x ($x \in Y$) и наблюдать его реакцию на поданную входную последовательность. Истинна следующая теорема.

Теорема 1. Автомат M_x ($x \in Y$) можно идентифицировать 4-кратным экспериментом высоты 1.

Доказательство. Каждый автомат M_x ($x \in Y$) установим в одно из состояний $q_0 = (1, 0, 0)$, $q_0 = (0, 1, 0)$, $q_0 = (0, 0, 1)$ либо $q_0 = (0, 0, 0)$. В каждом из этих состояний подадим на автомат входной символ 0. Полученные выходы автоматов занесем в табл. 2.

Таблица 2

Автомат	$q_0 = (1,0,0)$	$q_0 = (0,1,0)$	$q_0 = (0,0,1)$	$q_0 = (0,0,0)$
(M_A,q_0)	$(1,\ominus h,h)$	$(h,1,0)$	$(0,0,1\oplus h)$	$(0,0,h)$
(M_B,q_0)	$(1,h,h)$	$(0,1\ominus h,h)$	$(0,0,1\oplus h)$	$(0,0,h)$
(M_C,q_0)	$(1,h,0)$	$(0,1\ominus h,h)$	$(0,0,1\oplus h)$	$(0,0,h)$
(M_D,q_0)	$(1,h,0)$	$(\ominus h,1,h\circ\beta)$	$(0,h,1)$	$(0,0,0)$
(M_E,q_0)	$(1,h,h\ominus h\circ\beta)$	$(0,1\ominus h,h)$	$(0,0,1\oplus h)$	$(0,0,h)$
(M_F,q_0)	$(1,\ominus h,h)$	$(h,1\oplus h\circ\beta,0)$	$(h,0,1\ominus h)$	$(0,0,0)$
(M_G,q_0)	$(1\oplus h\circ\beta,0,\ominus h)$	$(0,1\ominus h,h)$	$(h,0,1)$	$(0,0,0)$
(M_H,q_0)	$(1,h,h)$	$(\ominus h,1\oplus h\circ\beta,0)$	$(h,0,1\ominus h)$	$(0,0,0)$
(M_I,q_0)	$(1,h,h)$	$(\ominus h\circ\beta,1,h)$	$(0,h,1\ominus h)$	$(0,0,0)$
(M_J,q_0)	$(1,0,\ominus h)$	$(0,1\ominus h\circ\beta,2\circ h)$	$(h\circ\beta,h,1)$	$(0,0,0)$
(M_K,q_0)	$(1,h,h)$	$(0,1\ominus h,0)$	$(\ominus h,0,1\oplus h\circ\beta)$	$(0,0,0)$
(M_L,q_0)	$(1,h\circ\beta_2,0)$	$(h,1\ominus h,h)$	$(h\circ\beta_1,0,1\oplus h)$	$(0,0,h)$
(M_M,q_0)	$(1,\ominus h,2\circ h\circ\beta)$	$(0,1\ominus h,h\circ\beta\oplus h)$	$(\ominus h,0,1\oplus h\circ\beta)$	$(0,0,h\circ\beta)$
(M_N,q_0)	$(1,h,h\ominus h\circ\beta)$	$(\ominus h\circ\beta,1,2\circ h)$	$(0,h,1\oplus h)$	$(0,0,h)$
(M_O,q_0)	$(1,h,h)$	$(h,1,h\circ\beta)$	$(0,\ominus h,1)$	$(0,0,0)$
(M_P,q_0)	$(1,\ominus h,h)$	$(h\circ\beta,1\oplus h,h)$	$(h,0,1)$	$(0,0,0)$
(M_Q,q_0)	$(1,h,h\circ\beta_1)$	$(0,1\ominus h,h\circ\beta_1\oplus h)$	$(\ominus h,0,1\oplus h\circ\beta_1\oplus h\circ\beta_2)$	$(0,0,h\circ\beta_1)$
(M_R,q_0)	$(1\oplus h\circ\beta_1,h\circ\beta_2,0)$	$(h\circ\beta_1\ominus h,1\oplus h\circ\beta_2,0)$	$(h\circ\beta_1,h\circ\beta_2\oplus h,1\ominus h)$	$(h\circ\beta_1,h\circ\beta_2,0)$
(M_S,q_0)	$(1\ominus h,h,2\circ h)$	$(\ominus h\circ\beta,1,h)$	$(0,h,1\oplus h)$	$(0,0,h)$

Рассмотрим инициальный автомат (M_x, q_0) ($q_0 = (0, 0, 1)$). Возможны следующие случаи.

Случай 1. $q_1 = (0, 0, q_1^{(3)})$. Пользуясь табл. 2, находим, что в этом случае $x \in \{A, B, C, E, L, R\}$. Установим автомат M_x в состояние $q_2 = (0, 0, 0)$. Тогда, согласно табл. 2, возможны 2 случая.

Случай 1.1. $q_3 = (0, 0, q_3^{(3)})$, $q_3^{(3)} \neq 0$. Тогда $x \in \{A, B, C, E, L\}$. Установим автомат M_x в состояние $q_4 = (\ominus 1, 1, 0)$. Подадим на автомат M_x входной символ 0. Тогда, согласно табл. 1, если $x = A$, то $q_5 = (\ominus 1\oplus h, 1\oplus h, 0)$; если $x = B$, то $q_5 = (\ominus 1, 1\ominus 2\circ h, 2\circ h)$; если $x = C$, то $q_5 = (\ominus 1, 1\ominus 2\circ h, 0)$; если $x = E$, то $q_5 = (\ominus 1, 1, h\circ(\beta\oplus 1))$; если $x = L$, то $q_5 = (\ominus 1\oplus h, h\circ(\beta_2\ominus 1), 2\circ h)$. Возможны 5 случаев.

Случай 1.1.1. $q_5^{(1)} \neq \ominus 1$, $q_5^{(3)} = 0$. Тогда $x = A$.

Случай 1.1.2. $q_5^{(1)} \neq \ominus 1$, $q_5^{(3)} \neq 0$. Тогда $x = L$.

Случай 1.1.3. $q_5^{(1)} = \ominus 1$, $q_5^{(2)} = 1$. Тогда $x = E$.

Случай 1.1.4. $q_5^{(1)} = \ominus 1$, $q_5^{(2)} \neq 1$, $q_5^{(3)} \neq 0$. Тогда $x = B$.

Случай 1.1.5. $q_5^{(1)} = \ominus 1$, $q_5^{(2)} \neq 1$, $q_5^{(3)} = 0$. Тогда $x = C$.

Случай 1.2. $q_3 = (q_3^{(1)}, q_3^{(2)}, 0)$. Тогда $x = R$.

Случай 2. $q_1 = (0, q_1^{(2)}, q_1^{(3)})$, $q_1^{(2)} \neq 0$. Пользуясь табл. 2, находим, что в этом случае $x \in \{D, I, J, N, O, R, S\}$.

Случай 2.1. $q_1^{(3)} = 1$. Тогда $x \in \{D, J, O\}$. Установим автомат M_x в состояние $q_2 = (1, 0, 0)$. Тогда, согласно табл. 2, возможны 3 случая.

Случай 2.1.1. $q_3 = (1, q_3^{(2)}, 0)$, $q_3^{(2)} \neq 0$. Тогда $x = D$.

Случай 2.1.2. $q_3 = (1, 0, q_3^{(3)})$, $q_3^{(3)} \neq 0$. Тогда $x = J$.

Случай 2.1.3. $q_3 = (1, q_3^{(2)}, q_3^{(3)})$, $q_3^{(2)} \neq 0$, $q_3^{(3)} \neq 0$. Тогда $x = D$.

Случай 2.2. $q_1^{(3)} \neq 1$. Тогда $x \in \{I, N, R, S\}$. Установим автомат M_x в состояние $q_2 = (0, 1, 0)$. Тогда, согласно табл. 2, возможны 2 случая.

Случай 2.2.1. $q_3 = (q_3^{(1)}, q_3^{(2)}, q_3^{(3)})$, $q_3^{(3)} \neq 0$. Тогда $x \in \{I, N, S\}$. Установим автомат M_x в состояние $q_4 = (1, 0, \ominus 1)$. Подадим на автомат M_x входной символ 0. Тогда, согласно табл. 1, если $x = I$, то $q_5 = (1, 0, \ominus 1 \oplus 2 \circ h)$; если $x = N$, то $q_5 = (1, 2 \circ h, \ominus 1 \oplus h \circ (1 \ominus \beta))$; если $x = S$, то $q_5 = (1 \ominus h, 2 \circ h, \ominus 1 \oplus 2 \circ h)$. Возможны 3 случая.

Случай 2.2.1.1. $q_5^{(1)} \neq 1$. Тогда $x = S$.

Случай 2.2.1.2. $q_5^{(1)} = 1$, $q_5^{(2)} = 0$. Тогда $x = I$.

Случай 2.2.1.3. $q_5^{(1)} = 1$, $q_5^{(2)} \neq 0$. Тогда $x = N$.

Случай 2.2.2. $q_3 = (q_3^{(1)}, q_3^{(2)}, 0)$. Тогда $x = R$.

Случай 3. $q_1 = (q_1^{(1)}, 0, q_1^{(3)})$, $q_1^{(1)} \neq 0$. Пользуясь табл. 2, находим, что в этом случае $x \in \{F, G, H, K, L, M, P, Q, R\}$.

Случай 3.1. $q_1^{(3)} \neq 1$. Тогда $x \in \{F, H, K, L, M, Q, R\}$.

Случай 3.1.1. $q_1^{(1)} \oplus q_1^{(3)} = 1$. Тогда $x \in \{F, H, K, L, M, Q, R\}$. Установим автомат M_x в состояние $q_2 = (1, 0, 0)$. Тогда, согласно табл. 2, возможны 3 случая.

Случай 3.1.1.1. $q_3^{(1)} \neq 1$. Тогда $x = R$.

Случай 3.1.1.2. $q_3^{(1)} = 1$, $q_3^{(3)} \neq 0$. Тогда $x \in \{F, H, K, M, Q\}$. Установим автомат M_x в состояние $q_4 = (0, 1, 0)$. Тогда, согласно табл. 2, возможны 3 случая.

Случай 3.1.1.2.1. $q_5^{(1)} \neq 0$, $q_3^{(2)} \neq q_3^{(3)}$. Тогда $x = F$.

Случай 3.1.1.2.2. $q_5^{(1)} \neq 0$, $q_3^{(2)} = q_3^{(3)}$. Тогда $x = H$.

Случай 3.1.1.2.3. $q_5^{(1)} = 0$. Тогда $x \in \{K, M, Q\}$. Установим автомат M_x в состояние $q_6 = (1, 1, 0)$. Подадим на автомат M_x входной символ 0. Тогда, согласно табл. 1, если $x = K$, то $q_7 = (1 \oplus h, 1, h)$; если $x = M$, то $q_7 = (1, 1 \ominus 2 \circ h, 3 \circ h)$; если $x = Q$, то $q_7 = (1, 1, h \circ (\beta_1 \oplus 1))$. Возможны 3 случая.

Случай 3.1.1.2.3.1. $q_7^{(1)} \neq 1$. Тогда $x = K$.

Случай 3.1.1.2.3.2. $q_7^{(1)} = 1$, $q_7^{(2)} \neq 1$. Тогда $x = M$.

Случай 3.1.1.2.3.3. $q_7^{(1)} = 1$, $q_7^{(2)} = 1$. Тогда $x = Q$.

Случай 3.1.1.3. $q_3^{(1)} = 1$, $q_3^{(3)} = 0$. Тогда $x \in \{L, Q\}$. Установим автомат M_x в состояние $q_4 = (1, 1, 0)$. Подадим на автомат M_x входной символ 0. Тогда, согласно табл. 1, если $x = L$, то $q_5 = (1 \oplus h, 1 \oplus h \circ (\beta_2 \ominus 1), 0)$; если $x = Q$, то $q_5 = (1, 1, h \circ (\beta_1 \oplus 1))$. Возможны 2 случая.

Случай 3.1.1.3.1. $q_5^{(1)} \neq 1$. Тогда $x = L$.

Случай 3.1.1.3.2. $q_5^{(1)} = 1$. Тогда $x = Q$.

Случай 3.1.2. $q_1^{(1)} \oplus q_1^{(3)} \neq 1$. Тогда $x \in \{K, L, M, Q, R\}$. Установим автомат M_x в состояние $q_2 = (0, 1, 0)$. Тогда, согласно табл. 2, возможны 3 случая.

Случай 3.1.2.1. $q_3^{(1)} = 0$. Тогда $x \in \{K, M, Q\}$. Этот случай аналогичен случаю 3.1.1.2.3.

Случай 3.1.2.2. $q_3^{(1)} \neq 0$, $q_3^{(3)} \neq 0$. Тогда $x = L$.

Случай 3.1.2.3. $q_3^{(1)} \neq 0$, $q_3^{(3)} = 0$. Тогда $x = R$.

Случай 3.2. $q_1^{(3)} = 1$. Тогда $x \in \{G, K, M, P, Q\}$. Установим автомат M_x в состояние $q_2 = (0, \ominus 1, 0)$. Подадим на автомат M_x входной символ 0. Тогда $h = q_3^{(2)} \oplus 1$ для всех M_x ($x \in \{G, K, M, P, Q\}$). Установим автомат M_x в состояние $q_4 = (1, 0, 1)$. Подадим на автомат M_x входной символ 0. Тогда, согласно табл. 1, если $x = G$, то $q_5 = (1 \oplus h \circ (\beta \oplus 1), h, 1 \ominus h)$; если $x = K$, то $q_5 = (1 \ominus h, h, 1 \oplus h)$; если $x = M$, то $q_5 = (1 \ominus h, \ominus h, 1)$; если $x = P$, то $q_5 = (1 \ominus h, h, 1)$. Возможны 5 случаев.

Случай 3.2.1. $q_5^{(3)} = 1 \ominus h$. Тогда $x = G$.

Случай 3.2.2. $q_5^{(3)} = 1$, $q_5^{(2)} = \ominus h$. Тогда $x = M$.

Случай 3.2.3. $q_5^{(3)} = 1$, $q_5^{(2)} = h$. Тогда $x = Q$.

Случай 3.2.4. $q_5^{(3)} = 1 \oplus h$, $q_5^{(2)} = h$. Тогда $x = K$.

Случай 3.2.5. $q_5^{(3)} = 1 \oplus h$, $q_5^{(2)} = \ominus h$. Тогда $x = P$.

Случай 4. $q_1 = (q_1^{(1)}, q_1^{(2)}, q_1^{(3)})$, $q_1^{(1)} \neq 0$, $q_1^{(2)} \neq 0$. Пользуясь табл. 2, находим, что в этом случае $x \in \{J, R\}$.

Случай 4.1. $q_1^{(3)} = 1$. Тогда $x = J$.

Случай 4.2. $q_1^{(3)} \neq 1$. Тогда $x = R$.

Таким образом, каждый автомат M_x ($x \in Y$) можно идентифицировать n-кратным экспериментом высоты 1, где $n \leq 4$.

В случае, когда информационная переменная добавляется только в некоторые уравнения системы для автомата Спротта, задача значительно усложняется за счет того, что криптоаналитику становится недоступной для непосредственного наблюдения по крайней мере одна из фазовых переменных $q_t^{(i)}$ ($i = 1, 2, 3$).

Заключение

В работе решена задача идентификации автомата в подклассе автоматов Спротта, для которых информационная переменная добавлена во все уравнения, определяющие автоматы. Показано, что в этом случае криптоаналитик сможет идентифицировать автомат, проделав 4-кратный эксперимент высоты 1.

Задача идентификации автомата была решена в предположении, что экспериментатор может управлять входом автомата и осуществлять инициализацию автомата требуемое число раз. Ясно, что при том или ином ограничении этих возможностей сложность решения задачи возрастет. Детальное исследование роста такой сложности представляет собой одно из возможных направлений дальнейших исследований.

Актуальность задачи обусловлена применением исследуемых автоматов в качестве шифрсистем, такое исследование дает возможность теоретически и с единых позиций оценить стойкость поточного шифра, определяемого автоматом Спротта при использовании информационного потока в качестве управления.

ЛИТЕРАТУРА

1. *Сухинин В.А.*, *Скобелев В.Г.* Эквивалентность состояний систем Спротта // Труды ИПММ НАН Украины. 2007. Т. 14. С. 174 – 186.
2. *Сухинин В.А.*, *Скобелев В.Г.* Алгоритмы и сложность идентификации автоматов Спротта над кольцом $\mathbf{Z}_p^k$ // Труды VII Междунар. конф. «Идентификация систем и задачи управления» SICPRO'08. Москва, 28 – 31 января 2008 г. ИПУ РАН. С. 1107 – 1153.
3. *Кузнецов С.П.* Динамический хаос. М.: Физматлит, 2001. 296 с.