УДК 518.6, 681.3

КОМБИНАТОРНО-АЛГЕБРАИЧЕСКИЕ МОДЕЛИ В КРИПТОГРАФИИ

В. Г. Скобелев

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

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

В лекции охарактеризованы дескриптивные, алгоритмические и метрические аспекты применения комбинаторно-алгебраических моделей при решении задач современной криптографии; рассмотрено использование методов хаотической динамики; охарактеризованы линейные и нелинейные автоматы, представленные системой уравнений над кольцом Z_{p^k}; выделены подмножества обратимых автоматов, предназначенных для построения широкого класса симметричных поточных шифров.

Ключевые слова: *булевы функции, конечные автоматы, комбинаторный анализ, конечные алгебраические системы, хаотическая динамика, обратные задачи, конечные кольца, симметричные шифры.*

1. Математические основы

Характерной чертой современной криптологии (как любого научного направления, предназначенного для решения практических задач, определяемых современным состоянием технических средств) является использование широкого спектра, часто недостаточно проработанных именно с позиции решения задач криптологии, моделей и методов из различных разделов математики. К ним относятся классические разделы математики со своей сложившейся тематикой исследований (комбинаторный анализ, теория булевых функций, теория автоматов, теория алгоритмов, конечные алгебраические системы), а также формируемые в настоящее время разделы математики (теория квантовых алгоритмов, теория хаоса динамических систем, теория фракталов).

Именно широкий спектр недостаточно теоретически проработанных с позиции криптологии, часто плохо сравнимых друг с другом моделей и методов приводит к тому, что одним из основных методов анализа криптографических алгоритмов является статистический анализ их качества. Упущения, допускаемые при этом, в совокупности с интенсивным развитием средств вычислительной техники являются основной причиной достаточно частого пересмотра криптографических стандартов во всем мире. Осознание этой ситуации и стимулировало разработку математических основ современной криптологии. Цель настоящего раздела — попытка охарактеризовать дескриптивные, метрические и алгоритмичесие аспекты комбинаторно-алгебраических моделей и методов, предназначенных для решения задач современной криптологии, систематически изложенные в [1].

1.1. Булевы функции

В течение последних 20 лет наблюдается интенсивное развитие теории булевых функций, обусловленное именно исследованием проблем, связанных с криптологией. Математический анализ этих достижений, основанный на моделях и методах современной конечной алгебры, комбинаторного анализа и теории вероятностей, систематически представлен в [2].

Изложенные в [2] методы исследования криптографических примитивов могут быть эффективно применены на практике (безусловно, с использованием компьютеров) для анализа булевых вектор-функций

$$\mathbf{f} : \mathbf{E}^n \to \mathbf{E}^m \ \ (n, m \in \mathbb{N}),$$

где

$$\mathbf{E} = \{0, 1\},$$

при относительно небольших значениях числа $2^n \cdot m$. Существование эффективных методов «хорошей» декомпозиции (с точки зрения криптографии) графиков булевых вектор-функций $\mathbf{f} : \mathbf{E}^n \to \mathbf{E}^m$ при больших значениях чисел n и m вызывает сомнение.

Тем не менее представленные в [2] методы исследования булевых функций имеют огромное методологическое значение прежде всего потому, что они устанавливают нетривиальные глубокие внутренние связи между теорией булевых функций и современной алгеброй. Сказанное может быть проиллюстрировано следующим образом. При исследовании свойств булевой вектор-функции всегда можно перейти к булевой вектор-функции $\mathbf{f} : \mathbf{E}^n \to \mathbf{E}^m$, сохраняющей константу нуль. Для этого достаточно заменить исходную булеву вектор-функцию $\mathbf{g}(\mathbf{x})$ булевой вектор-функцией

$$\mathbf{f}(\mathbf{x}) = \mathbf{g}(\mathbf{x}) \oplus \mathbf{g}(\mathbf{0}).$$

Обозначим график такой булевой вектор-функции $\mathbf{f}$ через $\mathrm{graph}(\mathbf{f})$, а множество всех максимальных по включению подпространств линейного пространства $\mathbf{E}^{n+m}$, содержащихся во множестве $\mathrm{graph}(\mathbf{f})$, обозначим через $\mathbf{Lin}(\mathrm{graph}(\mathbf{f}))$. В [3] показано, что имеет место равенство

$$\mathrm{graph}(\mathbf{f}) = \bigcup_{\mathbf{V} \in \mathbf{Lin}(\mathrm{graph}(\mathbf{f}))} \mathbf{V}. \tag{1}$$

Следовательно, синтез булевой вектор-функции, обладающей заданными свойствами, по своей сути, сводится к построению множества $\mathbf{Lin}(\mathrm{graph}(\mathbf{f}))$ с соответствующими характеристиками.

Отметим, что представление булевой вектор-функции, сохраняющей константу нуль, в виде системы полиномов Жегалкина также основано на использовании подпространств линейного пространства $\mathbf{E}^{n+m}$. Однако такое представление по своей структуре значительно сложнее, чем представление (1), так как построение полинома Жегалкина, фактически, представляет собой вариант применения метода включения-исключения. Отсюда вытекает, что любые методы построения системы полиномов Жегалкина для булевых вектор-функций, обладающих заданными значениями криптографических примитивов, заведомо требуют учета нетривиальных соотношений между подпространствами пространства $\mathbf{E}^{n+m}$, а также нетривиальных свойств преобразований пространства $\mathbf{E}^{n+m}$.

По-видимому, одной из наиболее значимых для анализа и синтеза блочных шифров является парадигма *управляемой подстановочной операции* (УПО), для представления которой используется язык схемных реализаций, основанный на использовании комбинаторно-алгебраических конструкций. Попытка систематического исследования этой парадигмы предпринята в [4].

Соответствующая математическая модель представляет собой такую булеву вектор-функцию

$$\mathbf{f} : \mathbf{E}^{n+m} \to \mathbf{E}^l \ \ (\ m, n, l \in \mathbb{N};\ \ l \geqslant n),$$

представленную в виде $\mathbf{f}: \mathbf{E}^n \times \mathbf{E}^m \to \mathbf{E}^l$, т. е. в виде

$$\mathbf{y} = \mathbf{f}(\mathbf{x}, \mathbf{v}) \ (\mathbf{x} \in \mathbf{E}^n, \ \mathbf{v} \in \mathbf{E}^m),$$

что для каждого $\mathbf{v}_0 \in \mathbf{E}^m$ инъекцией является вектор-функция $\mathbf{g}_{\mathbf{v}_0}: \mathbf{E}^n \to \mathbf{E}^l$, определяемая равенством

$$\mathbf{g}_{\mathbf{v}_0}(\mathbf{x}) = \mathbf{f}(\mathbf{x}, \mathbf{v}_0) \ (\mathbf{x} \in \mathbf{E}^n).$$

Вектор $\mathbf{x} \in \mathbf{E}^n$ — информационный, а вектор $\mathbf{v} \in \mathbf{E}^m$ — управляющий. При этом управляющий вектор формируется из сеансового ключа.

Специальным случаем УПО является *блок управляемых перестановок* (БУП), характеризуемый тем, что:

1) $l = n$;

2) для каждого фиксированного $\mathbf{v}_0 \in \mathbf{E}^m$ вектор-функция $\mathbf{g}_{\mathbf{v}_0}$ представляет собой перестановку компонент информационного вектора;

3) если $\mathbf{v}_0 \neq \mathbf{v}_1$ $(\mathbf{v}_0, \mathbf{v}_1 \in \mathbf{E}^m)$, то $\mathbf{g}_{\mathbf{v}_0}$ и $\mathbf{g}_{\mathbf{v}_1}$ — различные перестановки компонент информационного вектора.

Для основных типов БУП и УПО в [4] исследованы эффективность и сложность схемных реализаций, принципы синтеза схем с заданными алгебраическими и вероятностно-статистическими свойствами, а также принципы, эффективность и сложность криптоанализа этих схем.

Тем не менее в настоящее время остается много нерешенных задач, связанных с анализом и синтезом как БУП и УПО, так и шифров, основанных на использовании этих парадигм.

Во-первых, задачи обнаружения и локализации неисправности схем, применяемых при построении шифров, остаются вне поля зрения криптографов (криптоаналитик, имея активный доступ к некоторым входам или выходам элементов таких схем, может успешно имитировать их неисправность, что существенно усложнит работу легального пользователя). Ясно, что эти задачи могут быть решены стандартными методами технической диагностики. Однако такие тесты будут значительно сложнее, чем оптимальные тесты, так как они не учитывают существенные характеристики соответствующих схем (в частности, свойство БУП и УПО «быть инъекцией при фиксированном управляющем векторе»). В [1] показано, что для основных типов БУП сложность таких тестов является полиномом не более третьей степени от сложности БУП. В этих тестах используется «бегущая единица» или «бегущий нуль». Поэтому криптоаналитик, даже имея только пассивный доступ к выходам некоторых элементов этих схем (т. е. производя пассивный эксперимент), может идентифицировать соответствующие подстановки или фрагменты ключа методами, отличными от линейного криптоанализа. Отсюда вытекает ряд нерешенных задач анализа вычислительной стойкости и устойчивости блочных шифров в условиях, когда криптоаналитик имеет доступ к входам или выходам УПО, на основе которых построен исследуемый шифр.

Во-вторых, наличие дешифратора в матричном БУП предполагает реализацию каждой из используемых перестановок в явном виде. Это обстоятельство существенно усложняет схемную реализацию БУП. Если же убрать дешифратор, то мы получим представление используемого семейства перестановок в неявном виде (что существенно упрощает схемную реализацию и усложняет криптоанализ), а именно в виде

$$S = \{f_1^{\alpha_1} \circ \cdots \circ f_m^{\alpha_m} | \alpha_i \in \mathbf{E} \ (i = 1, \ldots, m)\},$$

где $f_i^1 = f_i$ $(i = 1, \ldots, m)$ — заданная в явном виде перестановка, f_i^0 $(i = 1, \ldots, m)$ — тождественная перестановка, а $\circ$ — операция суперпозиции. При этом возникает ряд

нерешенных задач, связанных с выбором порождающих перестановок $f_1, \ldots, f_m$, обеспечивающих заданные алгебраические и вероятностно-статистические свойства семейства S.

1.2. Конечные автоматы

Осознание значимости теории конечных автоматов для математического анализа инъективных дискретных преобразователей информации относится к третьей четверти XX века [5–7]. Эти и аналогичные им исследования оперировали с *абстрактным автоматом*, т. е. моделью

$$A = (Q, X, Y, \delta, \lambda),$$

где Q, X, Y — соответственно конечные множество состояний, входной и выходной алфавиты; $\delta : Q \times X \to Q$ — функция переходов; а $\lambda : Q \times X \to Y$ — функция выходов. Так как на практике эффективно могут быть использованы абстрактные автоматы только при относительно небольших значениях числа $|Q| \cdot |X|$, то результаты исследований таких автоматов не оказали существенного влияния на разработку поточных шифров.

Высокая сложность решения задач анализа и синтеза для абстрактных автоматов (а также сетей, построенных из них) стимулировала исследование достаточно узких классов автоматов, для которых решение этих задач существенно проще. К таким классам относится класс линейных автоматов над полем $GF(p^k)$ (p — простое число, $k \in \mathbb{N}$). Систематический анализ этого класса автоматов с позиции классической теории систем представлен в [8, 9]. Однако эти исследования практически ничего не дали для решения задач криптологии, так как в них не рассматривались задачи исследования вычислительной стойкости поточных шифров, построенных на основе таких автоматов. Такие задачи, по своей сути, сводятся к задачам идентификации параметрически настраиваемых автоматов и к задачам теории экспериментов с автоматами над конечными полями. Этот пробел частично ликвидирован в [10–12].

Исследованная в [13] связка (посредством обратной связи)

операционный автомат — управляющий автомат

является теоретической основой возможности успешного применения конечных автоматов в процессе построения управляющих систем. При таком подходе естественно возникает проблема синтеза автомата по его внешнему поведению. Эта проблема является одной из центральных проблем теории конечных автоматов. В [14] выделены следующие четыре подхода приближенного построения (по своей сути, идентификации) конечного автомата по его внешнему поведению.

Первый подход к построению модели автомата основан на том, что на множестве всех автоматов с одним и тем же входным и выходным алфавитами вводится *функция близости*, использующая расстояние Хемминга между выходными словами. Предполагается, что задано число состояний искомого автомата. Функция близости применяется в процессе поиска наилучшего приближения искомого автомата во множестве всех автоматов с меньшим числом состояний. Известно, что эта задача решена для класса перестановочных автоматов, которые находят широкое применение в современной криптографии.

При втором подходе к построению модели автомата также предполагается, что задано число состояний искомого автомата. Построение модели $A = (Q, X, Y, \delta, \lambda)$ искомого автомата основано на построении его *статистического аналога*, т. е. такого

автомата $A' = (Q, X, Y, \delta', \lambda')$, что для любого состояния $q \in Q$ вероятности событий

$$\delta(q, x) = \delta'(q, x) \ (x \in X)$$

и

$$\lambda(q, x) = \lambda'(q, x) \ (x \in X)$$

больше соответственно величин $|Q|^{-1}$ и $|Y|^{-1}$.

При третьем подходе к построению модели автомата предполагается, что имеется дискретный преобразователь, являющийся *черным ящиком*, обеспечивающий при идеальных условиях требуемое поведение. Из-за отсутствия идеальных условий (шумы, воздействия внешней среды и т. д.) поведение дискретного преобразователя может отличаться от эталонного поведения. Построение модели автомата основано на построении его *следствия*, т. е. автомата, на который поступает входная и выходная последовательности исследуемого дискретного преобразователя и который, на основе поведения эталона на подмножестве входных слов фиксированной длины, корректирует выход дискретного преобразователя.

Четвертый подход к построению модели искомого автомата основан на получении *следствий из соотношений, описывающих его функционирование*. Для абстрактных автоматов такие следствия получаются в терминах *обобщенных гомоморфизмов* автоматов и построении *обобщенного образа* автомата (т. е., по сути, некоторого класса автоматов). Обобщение понятия *гомоморфизма* состоит в рассмотрении (вместо отображений) бинарных отношений, определенных на прямых произведениях автоматных множеств. В случае, когда автомат представлен системой уравнений над конечной алгебраической системой, построение модели исследуемого автомата сводится к решению задачи параметрической идентификации соответствующей дискретной динамической системы.

Задачи анализа и синтеза поточных шифров оказались мощным катализатором появления новых направлений дискретного анализа, в которых переплетаются модели и методы теории конечных автоматов, современной алгебры и комбинаторного анализа. Рассмотрим кратко некоторые из таких направлений.

Первым типом модели структурного конечного автомата, часто применяемого при решении задач криптографии, является специальным образом подобранная комбинаторная структура, находящаяся под управлением псевдослучайного генератора. Основная сложность построения таких моделей конечного автомата связана именно с выбором комбинаторной структуры, так как здесь переплетаются все три аспекта исследования задач математической кибернетики:

1) дескриптивный аспект, состоящий в формальном определении класса возможных кандидатов;

2) алгоритмический аспект, состоящий в построении соответствующих алгоритмов и доказательстве их корректности;

3) метрический аспект, состоящий в анализе сложности предложенных алгоритмов и, в силу специфики криптографии, анализе вычислительной стойкости некоторых из них.

Проиллюстрируем сказанное на примере.

Пример 1. Естественным обобщением парадигмы УПО является *регулярная комбинаторная структура* (РКС), являющаяся, по своей сути, *представленным в неявном виде управляемым бинарным отношением*. РКС, по-видимому, впервые введена в [15] и предназначена для математического анализа решения задачи разрушения частот букв — модельной задачи криптографии. Рассмотрим кратко эти построения.

Пусть $L \subseteq \Sigma^+$ — заданный язык; $L(k) = \{u \in L | d(u) \leqslant k\}$ $(k \in \mathbb{N})$, где $d(u)$ — длина слова u; $n(u, \sigma)$ $(u \in \Sigma^+, \sigma \in \Sigma)$ — число вхождений буквы σ в слово u и

$$\nu(L(k), \sigma) = \frac{\sum\limits_{u \in L(k)} n(u, \sigma)}{\sum\limits_{u \in L(k)} d(u)} \quad (k \in \mathbb{N},\ \sigma \in \Sigma).$$

Предполагается, что для каждого $\sigma \in \Sigma$ существует предел

$$\lim_{k \to \infty} \nu(L(k), \sigma) = a(\sigma) > 0,$$

откуда вытекает, что для любого фиксированного положительного числа ε для каждого $\sigma \in \Sigma$ существует такое число $k_0(\sigma, \varepsilon) \in \mathbb{N}$, что для всех $k > k_0(\sigma, \varepsilon)$ $(k \in \mathbb{N})$

$$|\nu(L(k), \sigma) - a(\sigma)| < \varepsilon.$$

Зафиксируем такое положительное число ε, что

$$a(\sigma) - \varepsilon > 0$$

для всех $\sigma \in \Sigma$, и положим $k_0(\varepsilon) = \max\limits_{\sigma \in \Sigma} k_0(\sigma, \varepsilon)$.

Относительной частотой появления буквы $\sigma \in \Sigma$ в словах языка L назовем число

$$frqnc(L, \sigma) = \nu(L(k_0(\varepsilon)), \sigma).$$

Отметим, что из приведенных построений вытекает, что:
1) $frqnc(L, \sigma) > 0$ для всех $\sigma \in \Sigma$;
2) $\sum\limits_{\sigma \in \Sigma} frqnc(L, \sigma) = 1$.

Предположим, что каждое число $frqnc(L, \sigma)$ $(\sigma \in \Sigma)$ представлено двоичной дробью, вычисленной с точностью до 2^{-r} $(r \in \mathbb{N})$, причем выполнены оба приведенных выше условия.

Алгоритмом побуквенного кодирования назовем алгоритм, вычисляющий значения фиксированного инъективного отображения

$$cdng : \Sigma \to \mathbf{E}^{l_1} \ \ (l_1 = \lceil \log |\Sigma| \rceil)$$

с временной и емкостной сложностью, соответственно равной

$$T_{cdng} = O(l_1) \ \ (|\Sigma| \to \infty),$$

$$V_{cdng} = O(|\Sigma| \cdot l_1) \ \ (|\Sigma| \to \infty).$$

Ясно, что для всех $\sigma \in \Sigma$

$$frqnc(cdng(L), cdng(\sigma)) = frqnc(L, \sigma),$$

т. е. относительные частоты букв в словах языков L и $cdng(L)$ совпадают. Отсюда вытекает корректность построения комбинаторных структур в терминах языка $cdng(L)$ и относительных частот букв в словах языка L. В дальнейшем, для краткости, вместо записи $frqnc(L, \sigma)$ будем использовать запись $frqnc(\sigma)$.

Зафиксируем число $h \in \mathbb{N}$ $(h \geqslant r)$ и такое число $l_2 \in \mathbb{N}$, что $l_2 \geqslant l_1 + h$. *Регулярная комбинаторная структура* для языка L определена в [1, 16] как бинарное отношение $\Delta \subseteq \mathbf{E}^{l_1} \times \mathbf{E}^{l_2}$, удовлетворяющее следующим пяти условиям:

1) $pr_1\Delta = cdng(\Sigma)$;

2) $\Delta(cdng(\sigma)) = 2^r \cdot frqnc(\sigma)$ для всех $\sigma \in \Sigma$;

3) $\Delta(cdng(\sigma_1)) \cap \Delta(cdng(\sigma_2)) = \varnothing$ для всех $\sigma_1, \sigma_2 \in \Sigma$ $(\sigma_1 \neq \sigma_2)$;

4) каждое множество $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ представлено в неявном виде с емкостной сложностью $O(l_2)$ $(l_2 \to \infty)$;

5) существует алгоритм $\mathtt{A}$, который при фиксированной начинающейся с нуля нумерации элементов любого множества $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$ порождает 0-й элемент множества $\Delta(cdng(\sigma))$ и по j-му элементу $(j = 0, 1, \ldots, |\Delta(cdng(\sigma))| - 1)$ множества $\Delta(cdng(\sigma))$ порождает $(j+1)(\mathrm{mod}\ |\Delta(cdng(\sigma))|)$-й элемент множества $\Delta(cdng(\sigma))$ с временной и емкостной сложностью, равной $O(l_2)$ $(l_2 \to \infty)$.

В [1, 16] доказано, что множество регулярных комбинаторных структур для языка L непусто. Этот результат является, по своей сути, аналогом доказательства непротиворечивости построенного фрагмента теории и обосновывает исследование возможности построения математической модели дискретного преобразователя, основанного на использовании таких структур и предназначенного для разрушения частот букв в языке L. Такой дискретный преобразователь автоматного типа построен в [1, 16]. Псевдослучайный генератор применяется для инициализации значений элементов множеств $\Delta(cdng(\sigma))$ $(\sigma \in \Sigma)$. Доказана корректность предложенных алгоритмов. Показано, что при выполнении ряда предвычислений разрушение частот букв в языке L осуществляется с линейным замедлением. Исследована вычислительная стойкость реализуемого построенным дискретным преобразователем алгоритма (при его интерпретации в качестве поточного шифра).

Второй тип модели структурного конечного автомата, применяемого при решении задач криптографии, основан на использовании представленного в неявном виде семейства легко вычислимых перестановок заданного конечного множества, выбор элементов которого управляется посредством заданного быстрого алгоритма. Рассмотрим общую схему построения таких моделей.

Перестановка $f \in S$ элементов конечного множества S называется *легко вычислимой*, если существует алгоритм A_f, реализующий эту перестановку с временной и емкостной сложностью, соответственно равной

$$V_f = O(\log |S|)\ \ (|S| \to \infty),$$

$$T_f = O(\log^2 |S|)\ \ (|S| \to \infty).$$

Перестановка $\mathbf{f}$ элементов конечного множества

$$\mathbf{S} = S_1 \times \cdots \times S_l$$

называется *легко вычислимой разложимой* перестановкой, если существуют такие легко вычислимые перестановки

$$f_1, \ldots, f_l$$

элементов соответственно множеств $S_1, \ldots, S_l$, что для любого $\mathbf{s} = (s_1, \ldots, s_l) \in \mathbf{S}$

$$\mathbf{f}(\mathbf{s}) = (f_1(s_1), \ldots, f_l(s_l))$$

(несложно показать, что если $f_1, \ldots, f_l$ — легко вычислимые перестановки, то $\mathbf{f}$ — легко вычислимая перестановка множества $\mathbf{S}$, так что это определение корректно).

Пусть в неявном виде задано такое семейство легко вычислимых разложимых перестановок

$$\boldsymbol{F} = \{\mathbf{f}_i = (f_1^{(i)}, \ldots, f_l^{(i)})\}_{i \in \mathbb{Z}_m},$$

что:

1) генерация алгоритма $A_{\mathbf{f}_0}$ осуществляется за время $O(\log |\mathbf{S}|)$ $(|\mathbf{S}|) \to \infty$);

2) преобразование алгоритма $A_{\mathbf{f}_j}$ $(j \in \mathbb{Z}_m)$ в алгоритм $A_{\mathbf{f}_{(j+1) (\mathrm{mod}\, m)}}$ осуществляется за время $O(\log^2 |\mathbf{S}|)$ $(|\mathbf{S}|) \to \infty$).

Обозначим через B быстрый алгоритм, который (по заданному входу) генерирует такую последовательность натуральных чисел

$$n_0, n_1, n_2 \ldots, \tag{2}$$

что для всех $i \in \mathbb{N}$

$$n_i << m.$$

Соответствующий дискретный преобразователь автоматного типа преобразует любую последовательность

$$\mathbf{s}_0, \mathbf{s}_1, \mathbf{s}_2, \ldots$$

элементов множества $\mathbf{S}$ в последовательность

$$\mathbf{f}_{n_0}(\mathbf{s}_0), \mathbf{f}_{n_0+n_1}(\mathbf{s}_1), \mathbf{f}_{n_0+n_1+n_2}(\mathbf{s}_2), \ldots$$

Проиллюстрируем сказанное на примере.

Пример 2. В [1, 17, 18] предложен следующий подход к построению поточных шифров. Шифруемая входная последовательность разбивается на тройки байтов, которые интерпретируются как RGB-компоненты bmp-файла. Шифрование каждой такой тройки байтов (по своей сути, изменение цвета соответствующего пикселя) осуществляется посредством семейства легко вычислимых перестановок

$$\boldsymbol{F} = \{\mathbf{f}_i\}_{i \in \mathbb{Z}_{256}},$$

определяемого соотношениями

$$r_n = (r_0 + n \cdot |\alpha_1^n \cdot a_1 - \alpha_2^n \cdot a_2 - \alpha_3^n \cdot a_3|) \,(\mathrm{mod}\, 256),$$

$$g_n = (g_0 + n \cdot |\alpha_2^n \cdot a_2 - \alpha_1^n \cdot a_1 - \alpha_3^n \cdot a_3|) \,(\mathrm{mod}\, 256),$$

$$b_n = (b_0 + n \cdot |\alpha_3^n \cdot a_3 - \alpha_1^n \cdot a_1 - \alpha_2^n \cdot a_2|) \,(\mathrm{mod}\, 256),$$

где r_0, g_0, b_0 и r_n, g_n, b_n — соответственно исходные и преобразованные компоненты цвета пикселя, а $\alpha_i, a_i \in \mathbb{Z}$ $(i = 1, 2, 3)$ — параметры, играющие роль секретного сеансового ключа.

Последовательность натуральных чисел (2) вычисляется на основе номеров итераций построения на дисплее точек выбранного псевдофрактала.

Третий тип модели структурного конечного автомата, применяемого при решении задач криптографии, основан на представлении обратимых автоматов системами уравнений над конечной алгебраической системой. Значимость таких моделей обусловлена тем, что в последнее десятилетие в криптографии наметилась устойчивая тенденция

перехода от чисто комбинаторных конструкций к конечным алгебраическим системам. Эта тенденция проявляется в том, что практически во всех современных стандартах шифрования присутствует фрагментарное применение теории конечных полей, а значительное число схем поточного шифрования, представленных в рамках реализуемых в настоящее время европейского и японского проектов (соответственно NESSIE и CRYPTREC), основано на использовании автоматов над полем $GF(2^k)$. Известно, что *поле* — это специальный случай *кольца*. При этом наличие в кольце *делителей нуля* дает возможность охарактеризовать сложность *поиска* в терминах сложности решения уравнений над кольцом. Конечные автоматы над конечным кольцом, применяемые для решения задач криптографии, будут рассмотрены в последующих разделах. Сейчас отметим только, что исследование таких автоматов актуально для современной криптографии по следующим причинам.

Во-первых, при соответствующих ограничениях на параметры автоматы над конечным кольцом определяют класс поточных шифров, вычислительная стойкость которых может быть теоретически охарактеризована в терминах сложности решения уравнений над кольцом.

Во-вторых, устанавливается нетривиальная внутренняя связь между современной криптологией и теорией систем, так как сложность и эффективность успешных атак для криптоаналитика естественно характеризуется в терминах сложности решения таких классических задач теории динамических систем, как управляемость, наблюдаемость, параметрическая идентификация.

В-третьих, устанавливается нетривиальная внутренняя связь между современной криптологией, теорией автоматов и современной алгеброй, что дает возможность при решении задач криптографии систематически и комплексно использовать модели и методы этих разделов математики, а также стимулировать формирование некоторых направлений исследований этих разделов математики, предназначенных именно для нужд криптографии.

1.3. Комбинаторный анализ

Об исключительной роли, которую комбинаторные конструкции играли и играют в криптографии, прежде всего свидетельствуют многочисленные примеры шифров и криптографических протоколов, основанных на их использовании (см., напр., [19]).

По-видимому, для современной криптографии важными являются следующие особенности, связанные с применением комбинаторного анализа.

Во-первых, это переосмысление известных комбинаторных конструкций в контексте задач современной криптографии.

Пример 3. В качестве регулярных комбинаторных структур, предназначенных для разрушения частот букв, в [15] использовались:

1) грани куба $\mathbf{E}^n$, которые, как известно, являются стандартной комбинаторной конструкцией в теории минимизации ДНФ;

2) система попарно непересекающихся шаров в пространстве $\mathbf{E}^n$, которая, как известно, применяется в теории кодов, контролирующих ошибки.

Во-вторых, это анализ возможности применения экстремальных и близких к ним комбинаторных объектов для решения задач криптографии.

Пример 4. В [20] было построено и исследовано семейство связных графов, удовлетворяющих следующим трем условиям:

1) граф имеет почти регулярную структуру (откуда вытекает возможность его эффективного представления в неявном виде);

2) число гамильтоновых путей между двумя фиксированными вершинами является субэкспонентой от числа ребер;

3) существует такой алгоритм, который порождает субэкспоненциальное число гамильтоновых путей на графе между этими фиксированными вершинами, причем каждый из этих путей порождается за время $O(n)$ $(n \to \infty)$, где n — число вершин графа.

В [15] показано, что такие графы могут быть эффективно применены при решении задачи диффузии информации — модельной задачи криптографии.

В-третьих, это необходимость метрического анализа комбинаторных конфигураций, определяемых в терминах *модульной арифметики*, в отличие от классического подхода комбинаторного анализа, основанного на использовании линейно или частично упорядоченных множеств (см., напр., [21, 22]).

Пример 5. В [23] исследована следующая комбинаторная конфигурация.

Пусть S — непустое конечное множество, а $a_1, \ldots, a_n \in \mathbb{N}$ — взаимно простые числа. Положим

$$F_{a_i}(S) = \{f | f : S \to \mathbb{Z}_{a_i}\} \ (i = 1, \ldots, m),$$
$$F(S) = \{f | f : S \to \mathbb{Z}_{\prod\limits_{i=1}^{m} a_i}\}.$$

Определим отображение $f_{\bmod a_i}$ $(f \in F(S);\ i = 1, \ldots, m)$ равенством

$$f_{\bmod a_i} = f(s) (\bmod a_i) \ (s \in S).$$

Зафиксируем подмножества $\widehat{F_{a_i}}(S) \subseteq F_{a_i}(S)$ $(i = 1, \ldots, m)$ и положим

$$\widetilde{F_{a_i}}(S) = \{f \in F(S) | f_{\bmod a_i} \in \widehat{F_{a_i}}(S)\} \ (i = 1, \ldots, m).$$

В [23] доказано, что

$$|\bigcap_{i=1}^{m} \widetilde{F_{a_i}}(S)| = \prod_{i=1}^{m} |\widehat{F_{a_i}}(S). \tag{3}$$

Нетривиальность равенства (3) обусловлена хотя бы тем, что оно дает возможность найти точное число обратимых матриц над кольцом $\mathbb{Z}_n$ $(n \in \mathbb{N})$, его следствиями являются *китайская теорема об остатках* и формула Эйлера для количества чисел, взаимно простых с данным числом.

1.4. А л г е б р а

К стандартному аппарату алгебры, применяемому в современной криптологии, относятся (см., напр., [24]) ряд разделов теории чисел (методы решения сравнений, использование первообразных корней, сведение задачи к поиску индекса (дискретного логарифма), применения цепных и подходящих дробей), ряд разделов теории конечных алгебр (конечные группы, конечные поля и векторные пространства над ними, кольца и модули линейных форм над ними), теория эллиптических кривых, а также теория алгебраических систем.

Формирование проблематики этих разделов математики осуществлялось без учета потребностей криптологии, и только в настоящее время начинают выделяться те их направления, которые существенно опираются на теорию алгоритмов и компьютерную математику и действительно могут стать мощным инструментом при исследовании задач защиты информации.

По-видимому, одним из самых тонких и сложных моментов, связанных с использованием систем уравнений над конечными алгебраическими системами в криптографии, является теоретическое исследование сложности их решения. Именно эта сложность, в конечном итоге, характеризует сложность идентификации сеансового ключа для шифра, определяемого этими системами уравнений.

Пример 6. В [25] исследовано семейство легко вычислимых перестановок

$$\boldsymbol{F} = \{\mathbf{f}_i = (f_1^{(i)}, \ldots, f_l^{(i)})\}_{i \in \mathbb{Z}_m},$$

которое является нетривиальным обобщением семейства перестановок из [17, 18]. Компоненты этих перестановок определяются уравнениями над кольцом

$$\boldsymbol{Z} = (\mathbb{Z}_{p^k}, \oplus, \circ),$$

где p — простое число. Показано, что параметрическая идентификация этого семейства перестановок сводится к решению системы высокостепенных уравнений над конечным кольцом, при этом необходимо решить l задач поиска дискретного логарифма.

По-видимому, заслуживает внимания исследование возможности применения для решения задачи выбора секретного ключа средней длительности для двух пользователей параметрических диофантовых уравнений (как известно, проблема поиска решения диофантовых уравнений алгоритмически неразрешима). На примерах простейших параметрических диофантовых уравнений нетрудно убедиться, что структура множества их решений может существенно варьироваться в зависимости от значений параметров. Поэтому даже передача открытым текстом номера решения, определяющего секретный сеансовый ключ, мало что даст криптоаналитику для идентификации этого ключа.

Одним из наиболее перспективных методов генерации ключей для электронно-цифровой подписи является применение эллиптических кривых над конечным полем. Это направление исследований в настоящее время интенсивно развивается (см., напр., [26, 27]). Однако в настоящее время отсутствует систематизация полученных результатов и системная характеристика тонких мест этого направления именно с позиции современной криптологии.

Наконец, следует отметить, что в последнее время при исследовании различных аспектов решения задачи защиты информации фрагментарно используются те или иные варианты многоосновных алгебраических систем. К таким исследованиям относятся анализ структуры гомоморфизмов универсальных многоосновных алгебр, применяемых при минимизации сложности решения уравнений, связанных с анализом блоков шифрования [28], попытка теоретической проработки основ построения системы компьютерного моделирования системы защиты информации (с применением системы автоматического вывода), предпринятая в [29], а также исследования формальных моделей систем компьютерной безопасности (см., напр., [30]).

Рассмотренные особенности комбинаторно-алгебраических моделей далеко не исчерпывают всего круга проблем, возникающих при их применении для исследования задач современной криптографии.

Во-первых, вне внимания криптографии остаются многочисленные комбинаторно-алгебраические конструкции, успешно применяемые в теории кодов, контролирующих

ошибки [31]. Применение таких конструкций (после соответствующей их модификации) дает возможность автоматически обнаруживать и исправлять некоторые случайно или преднамеренно внесенные ошибки, что повышает эффективность использования шифрсистем.

Во-вторых, как показал печальный опыт с *ранцевым алгоритмом шифрования*, требует самого тщательного теоретического обоснования сужение множества исходных данных NP-полных задач, которые естественно возникают при их применении в криптографии. Сложность такого теоретического обоснования весьма велика, так как оно, по своей сути, эквивалентно доказательству утверждения о том, что не существует эффективная атака того или иного типа. По-видимому, единственным эвристическим выходом из этой ситуации является использование семейства однотипных, имеющих различные размеры, комбинаторных конструкций, определяемых применяемой NP-полной задачей. Такой подход дает возможность в процессе сеанса шифрования динамически варьировать применяемые конструкции (и их размеры) с помощью псевдослучайного генератора. При таком подходе, по крайней мере, есть надежда, что криптоаналитик столкнется с трудной проблемой *тождества слов*.

В-третьих, в настоящее время интенсивно развивается теория квантовых вычислений [32]. Существенной особенностью этой теории является то, что она в корне изменяет взгляд на прикладную теорию алгоритмов, так как, во-первых, ее эффективным инструментом являются методы, осуществляющие построение решения с заданной вероятностью, а, во-вторых, в ее рамках возможно эффективно реализовать ряд методов поиска, имеющих экспоненциальную сложность в классической прикладной теории алгоритмов. По-видимому, серьезным предупреждением для криптографии является существование полиномиального квантового алгоритма для разложения числа на два простых сомножителя. Поэтому исследование комбинаторно-алгебраических моделей, для анализа которых не существует эффективных квантовых алгоритмов, является актуальным для современной криптографии.

Все сказанное выше, наряду с интенсивным развитием средств вычислительной техники, обосновывает актуальность теоретической проработки математических основ, обеспечивающих адекватное и эффективное применение комбинаторно-алгебраических моделей в процессе решения задач современной криптографии.

2. Модели хаотической динамики в анализе шифров

На протяжении последнего двадцатилетия усилия многочисленных коллективов ученых различных стран привели к значительным успехам в области исследования свойств детерминированного хаоса динамических систем (см., напр., [33, 34]).

Говоря неформально, *динамическая система* представляется таким набором из n динамических переменных, характеризующих *состояние* системы, что их значения в любой последующий момент времени получаются из набора исходных значений по определенному правилу, называемому *оператором эволюции* системы. *Динамику* (иными словами, *эволюцию*) такой системы можно представить как *движение точки* по *траектории* в *n-мерном фазовом пространстве*. Динамическую систему, представленную системой дифференциальных уравнений, часто называют *потоком*, а представленную системой рекуррентных соотношений — *отображением* (отметим, что при компьютерном моделировании динамических систем всегда происходит переход от потока к отображению). Динамическая система называется *хаотической*, если сколь угодно малое изменение начального состояния системы быстро нарастает во времени. Это означает, что сколь угодно малая неточность в задании начального состояния

системы делает невозможной предсказуемость ее эволюции на достаточно больших интервалах времени.

Выделим в фазовом пространстве динамической системы некоторую область (ее часто называют *облаком*) и рассмотрим эволюцию облака. Если с течением времени объем облака остается постоянным, то динамическая система называется *консервативной* (с физической точки зрения *консервативность* означает *сохранение энергии*). Если же с течением времени объем облака изменяется, то динамическая система называется *диссипативной*. Для диссипативных систем характерно то, что с течением времени облако *сжеживается* и *концентрируется* на одном или нескольких *аттракторах*, т. е. подмножествах фазового пространства, обладающих, как правило, нулевым фазовым объемом (наиболее известные примеры аттракторов — это *положение равновесия* и *предельный цикл*, т. е. замкнутая фазовая траектория, к которой с течением времени стремятся все близкие траектории). Множество всех точек фазового пространства, из которых траектории приходят к одному и тому же аттрактору, называется *бассейном* этого аттрактора.

В диссипативных системах хаос часто связан с наличием *странных аттракторов*, представляющих собой *фрактальные множества* (или, кратко, *фракталы*), т. е. множества, имеющие сложную самоподобную структуру и притягивающие к себе все траектории, принадлежащие бассейнам этих аттракторов.

В процессе исследования хаотических динамических систем большое внимание уделялось (и уделяется в настоящее время) применениям таких систем к решению задач преобразования информации. Здесь следует особо отметить исследования, связанные с разработкой методов записи и восстановления информации, основанные на использовании устойчивых циклов [35 – 38], которые, в конечном счете, привели к парадигме *хаотического процессора* [39], т. е. к математической модели, позволяющей работать с информацией как с траекторией в фазовом пространстве и управлять характером динамических явлений с целью осуществления базовых операций хаотического процессинга. Именно представление информации траекториями, а также обработка информации посредством хаотических динамических систем и составляют основу применения моделей и методов хаотической динамики в криптографии.

Подчеркнем, что применение любой схемы представления информации циклами, порождаемыми в фазовом пространстве хаотической динамической системой, по сути, приводит к шифрованию исходной информации, причем вычислительная стойкость такого шифра заведомо не меньше, чем вычислительная стойкость шифра замены, переводящего элементы исходной информации в циклы.

Цель настоящего раздела — проиллюстрировать основные из подходов, применяемых при использовании моделей и методов хаотической динамики для решения задач современной криптографии.

2.1. Модель хаотической динамики в криптографии с открытым ключом

В [40 – 42] предложен следующий подход к разработке шифрсистем с открытым ключом, основанный на неоднозначности обращения кусочно-линейных хаотических отображений.

В качестве кусочно-линейного хаотического отображения выбрано отображение *тент*, рекуррентное уравнение которого имеет вид

$$x_{n+1} = \begin{cases} \dfrac{x_n}{a}, & \text{если } 0 \leqslant x_n < a, \\ \dfrac{1-x_n}{1-a}, & \text{если } a \leqslant x_n \leqslant 1, \end{cases} \quad (n \in \mathbb{Z}_+), \tag{4}$$

где $a \in (0;1)$ — параметр.

В случае когда $a = 0{,}5$, решение рекуррентного уравнения (4) имеет вид

$$x_n = \frac{1}{\pi} \cdot \arccos(\cos(2^n \cdot \pi \cdot x_0)) \ (n \in \mathbb{Z}_+), \tag{5}$$

где x_0 — начальное значение.

Равенство (5) представляет собой подсемейство однопараметрического семейства отображений

$$T_k(x) = \frac{1}{\pi} \cdot \arccos(\cos(k \cdot \pi \cdot x_0)) \ (k \in \mathbb{N}). \tag{6}$$

В дальнейшем рассматривается именно семейство отображений (6), что совершенно не влияет на общность рассуждений.

Отметим, что семейство отображений (6) удовлетворяет *полугрупповому свойству*

$$T_{r \cdot s} = T_r \circ T_s \ (r, s \in \mathbb{N}), \tag{7}$$

где $\circ$ — операция суперпозиции отображений. Из (7), в свою очередь, вытекает, что семейство отображений (6) удовлетворяет также свойству *коммутативности*, т. е.

$$T_r \circ T_s = T_s \circ T_r \ (r, s \in \mathbb{N}).$$

Предполагается, что подлежащее шифрованию сообщение — это m-битовая последовательность, а M — целое число, представляющее эту последовательность.

В [41, 42] исследована следующая математическая модель шифрсистемы с открытым ключом.

Формирование ключей пользователем A осуществляется следующим образом:

1) генерируются такие натуральные числа p и q, что $n = p \cdot q > 2^m$;

2) ищется неустойчивая неподвижная точка $x_0 \in (0; 2^{-m})$ отображения T_n;

3) вычисляется открытый ключ $y_0 = T_p(x_0)$.

Пара (x_0, q) — личный секретный ключ пользователя A.

Для того чтобы отправить пользователю A сообщение M, пользователь B вычисляет и отправляет пользователю A шифртекст $c = T_M(y_0)$.

Для того чтобы расшифровать сообщение, пользователь A вычисляет значение

$$M = \frac{T_q(c)}{x_0}.$$

Действительно, с учетом того, что $M \cdot x_0 \leqslant 1$, получим

$$\frac{T_q(c)}{x_0} = \frac{T_q(T_M(y_0))}{x_0} = \frac{T_q(T_M(T_p(x_0)))}{x_0} = \frac{T_M(T_n(x_0))}{x_0} =$$

$$= \frac{T_M(x_0)}{x_0} = \frac{\arccos(\cos(\pi \cdot M \cdot x_0))}{\pi \cdot x_0} = \frac{\pi \cdot M \cdot x_0}{\pi \cdot x_0} = M.$$

В [41] исследована вычислительная стойкость рассмотренного шифра, а в [42] — точность вычислений, при которых процесс *шифрование — расшифрование* корректен.

Ясно, что рассмотренный выше подход к построению шифрсистемы с открытым ключом применим для любых кусочно-линейных хаотических отображений. Однако как анализ вычислительной стойкости соответствующего шифра, так и поиск условий, при которых процесс *шифрование – расшифрование* корректен, существенно зависят от используемого кусочно-линейного отображения.

2.2. Коммуникационная система на основе хаотического носителя

В [43] предложена следующая математическая модель вычислительно стойкой коммуникационной системы, содержащей хаотические динамические системы.

Используемая *передатчиком* управляемая хаотическая динамическая система, играющая роль *носителя*, предназначенного для *маскирования* зашифрованного аналогового сообщения $m(t)$, имеет следующий вид:

1) переходы состояний определяются системой уравнений

$$\begin{cases} \dot{q}_1 = 0{,}7 \cdot q_1 - q_2 - q_3, \\ \dot{q}_2 = q_1, \\ \dot{q}_3 = 3(q_1 - q_4), \\ \dot{q}_4 = 3q_3 - 30(q_4 - 1)H(q_4 - 1) - 30 \cdot e_{en}(t); \end{cases} \tag{8}$$

2) выход определяется уравнением

$$y(t) = (q_4(t) - 1)H(q_4(t) - 1) + \sum_{i=1}^{4} k_i \cdot q_i(t). \tag{9}$$

Обозначения в (8) и (9) следующие : $H(z)$ — функция Хевисайда, а $e_{en}(t)$ — функция шифрования, представляющая собой n-сдвиговый регистр, определяемый уравнением

$$e_{en}(t) = f_1(\dots f_1(f_1(m(t), K(t)), K(t)), \dots, K(t)), \tag{10}$$

где

$$f_1(x, K) = \begin{cases} x + K + 2 \cdot h, & \text{если } -2 \cdot h \leqslant x + K \leqslant -h, \\ x + K, & \text{если } -h < x + K < h, \\ x + K - 2 \cdot h, & \text{если } h \leqslant x + K \leqslant 2 \cdot h. \end{cases} \tag{11}$$

В (10) и (11) числа h и n представляют собой параметры шифра, а в качестве *ключа* $K(t)$ может быть выбрана любая функция от переменных состояния системы.

Сигнал, передаваемый *передатчиком*, имеет вид

$$z(t) = y(t) + e_{en}(t).$$

Используемая *приемником* управляемая хаотическая динамическая система имеет следующий вид:

1) переходы состояний определяются системой уравнений

$$\begin{cases} \dot{\widehat{q}}_1 = 0{,}7 \cdot \widehat{q}_1 - \widehat{q}_2 - \widehat{q}_3, \\ \dot{\widehat{q}}_2 = \widehat{q}_1, \\ \dot{\widehat{q}}_3 = 3(\widehat{q}_1 - \widehat{q}_4), \\ \dot{q}_4 = 3\widehat{q}_3 - 30(z(t) - \sum\limits_{i=1}^{4} k_i \cdot \widehat{q}_i(t)); \end{cases} \tag{12}$$

2) выход определяется уравнением

$$\widehat{e}_{en}(t) = z(t) - (\widehat{q}_4 - 1)\widehat{H}(\widehat{q}_4 - 1) - \sum_{i=1}^{4} k_i \cdot \widehat{q}_i(t).$$

Расшифрование выхода $\widehat{e}_{en}(t)$ осуществляет все тот же n-сдвиговый регистр

$$\widehat{m}(t) = f_1(\dots f_1(f_1(\widehat{e}_{en}(t), -\widehat{K}(t)), -\widehat{K}(t)), \dots, -\widehat{K}(t)).$$

Числа k_i $(i = 1, \dots, 4)$ подбираются таким образом, чтобы была обеспечена синхронизация систем (8) и (12). В этом случае для достаточно больших значений t

$$\widehat{x}_i(t) \to x_i(t) \ \ (i = 1, \dots, 4).$$

А так как ключи зависят только от переменных состояния, то

$$\widehat{K}(t) \to K(t).$$

Следовательно,

$$\widehat{e}_{en}(t) \to e_n(t),$$

откуда вытекает, что

$$\widehat{m}(t) \to m(t).$$

Высокая вычислительная стойкость рассмотренной коммуникационной системы обусловлена следующими обстоятельствами.

Во-первых, криптоаналитику достаточно сложно восстановить геометрическую структуру траектории используемой хаотической динамической системы в 4-мерном фазовом пространстве.

Во-вторых, даже если криптоаналитик сможет выделять зашифрованное сообщение

$$e_{en}(t) = z(t) - y(t),$$

у него возникнут проблемы с его расшифрованием, так как ключ не передается по каналу связи.

2.3. Поточные шифры на основе хаотических динамических систем

Рассмотренная выше коммуникационная система является системой с памятью (т. е., по своей сути, поточной системой) и основана на том обстоятельстве, что за счет синхронизации хаотических динамических систем восстанавливаемое аналоговое сообщение *сходится* к исходному. Однако *синхронизация хаотических динамических систем* — сложная проблема, исследованию которой посвящено значительное число конференций по хаотической динамике (см., напр., [44, 45]), и анализ *скорости синхронизации* требует индивидуального подхода к каждому типу систем. Ситуация еще более усложняется при компьютерном моделировании таких систем и переходе от аналогового сигнала к дискретному, т. е. при переходе к шифрсистемам в их обычном смысле в криптографии. Поэтому естественно избежать проблемы *синхронизации хаотических динамических систем*. Такой подход систематически изложен в [1] и состоит в следующем.

Рассмотрим хаотическую динамическую систему

$$\dot{\mathbf{q}} = \mathbf{f}(\mathbf{q}, \mathbf{a}), \tag{13}$$

где вектор динамических переменных $\mathbf{q} = (q^{(1)}, \ldots, q^{(n)})^T \in \mathbb{R}^n$ определяет состояние системы в момент $t \in \mathbb{R}_+$, а вектор $\mathbf{a} = (a_1, \ldots, a_m)^T \in \mathbb{R}^m$ определяет значение параметров системы.

Построение поточного шифра на основе динамической системы (13) осуществляется следующим образом.

Во-первых, осуществляется *дискретизация* системы (13) (этот этап не нужен, если исходная динамическая система является дискретной), т. е. приведение системы к виду

$$\mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t, \tag{14}$$

где h $(h > 0)$ — шаг дискретизации, а $t \in \mathbb{Z}_+$.

Во-вторых, с целью построения дискретной динамической системы с *функцией выхода* и с *внешним управлением* (т. е. модели автоматного типа) в систему (14) аддитивно вносится *информационная* переменная $\mathbf{x}_{t+1} = (x_{t+1}^{(1)}, \ldots, x_{t+1}^{(n)})^T$, определяющая значение блока информации, шифруемого в момент $t + 1$.

В результате таких построений можно выделить следующие два типа систем:

1) систему *типа Мили*

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t + h \cdot B \cdot \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \cdot \mathbf{q}_t + D \cdot \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+); \tag{15}$$

2) систему *типа Мура*

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t + h \cdot B \cdot \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \cdot \mathbf{q}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+). \tag{16}$$

В (15) и (16) A, B, C, D — $n \times n$-матрицы, $\mathbf{q}_0$ — начальное состояние, а $\mathbf{y}_{t+1}$ — результат шифрования блока информации $\mathbf{x}_{t+1}$.

Истинны следующие утверждения.

Утверждение 1. Динамическая система (15) представляет собой поточный шифр тогда и только тогда, когда D — невырожденная $n \times n$-матрица.

Следствие 1. Для поточного шифра (15) расшифрование осуществляет динамическая система

$$\begin{cases} \mathbf{q}_{t+1} = h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + (I - h \cdot B \cdot D^{-1} \cdot C) \cdot \mathbf{q}_t + h \cdot B \cdot D^{-1} \cdot \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = D^{-1} \cdot (\mathbf{x}_{t+1} - C \cdot \mathbf{q}_t), \end{cases} \quad (t \in \mathbb{Z}_+), \tag{17}$$

где I — единичная $n \times n$-матрица.

Утверждение 2. Динамическая система (16) представляет собой поточный шифр тогда и только тогда, когда B и C — невырожденные $n \times n$-матрицы.

Следствие 2. Для поточного шифра (16) расшифрование осуществляет динамическая система

$$\begin{cases} \mathbf{q}_{t+1} = C^{-1} \cdot \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = -h^{-1} \cdot B^{-1} \cdot (h \cdot \mathbf{f}(\mathbf{q}_t, \mathbf{a}) + \mathbf{q}_t) + h^{-1} \cdot B^{-1} \cdot C^{-1} \cdot \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+). \tag{18}$$

Итак, каждый из шифров (15) и (16) представляет собой симметричный поточный шифр. При этом секретным ключом для шифра (15) являются параметры $h, \mathbf{a}, B, C, D$ и начальное состояние $\mathbf{q}_0$, а для шифра (16) — параметры $h, \mathbf{a}, B, C$ и начальное состояние $\mathbf{q}_0$.

Следует особо отметить следующее свойство рассматриваемых шифров: в процессе *шифрование — расшифрование* как динамические системы (15) и (17), так и динамические системы (16) и (18) *движутся по одной и той же траектории в пространстве состояний*. Это свойство дает возможность за счет одновременного использования прямой и обратной системы осуществлять *контроль* (т. е. обнаружение и исправление) некоторых ошибок, возникающих именно в процессе передачи информации по каналу связи.

Вычисления в поле действительных чисел $\mathbb{R}$ (или в поле рациональных чисел $\mathbb{Q}$ при компьютерном моделировании) наталкивается на фактор *накопления ошибок округления*, в результате проявления которого процесс *шифрование — расшифрование* теряет свою корректность. Обеспечение корректности вычислений за счет повышения их точности связано с непростым анализом применяемой системы, приводит к существенному замедлению процесса *шифрование — расшифрование* в случае линейных систем и практически неосуществимо для нелинейных систем.

Именно это обстоятельство обосновывает целесообразность нивелирования ошибок округления за счет перехода к действиям в конечной алгебраической системе. Аргументы в пользу выбора конечного кольца в качестве такой алгебраической системы были изложены в разд. 1. В результате возникает новый класс симметричных поточных шифров, а именно *класс симметричных поточных шифров, построенных на основе аналогов хаотических динамических систем над конечным кольцом*. По своей сути такие шифры представляют собой *конечные автоматы над конечным кольцом*. Таким образом, мы приходим к новому разделу *теории автоматов*, имеющему нетривиальную область приложений, а именно современную криптологию.

В качестве конечного кольца всюду в дальнейшем выбрано кольцо

$$\boldsymbol{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ),$$

где p — простое число, $k \in \mathbb{N}$, а операции определены равенствами

$$a \oplus b = (a + b) \pmod{p^k},$$

$$a \circ b = (a \cdot b) \pmod{p^k}.$$

Проиллюстрируем построение таких шифров на основе модельных нелинейных хаотических динамических систем (см., напр., [34]).

Пример 7. *Система Рёсслера* имеет вид

$$\begin{cases} \dot{x} = -y - z, \\ \dot{y} = x + a \cdot y, \\ \dot{z} = b + (x - r) \cdot y, \end{cases} \qquad (t \in \mathbb{R}_+). \tag{19}$$

Дискретизируем систему (19), внесем информационную переменную в 1-е уравнение, перейдем к вычислениям в кольце $\boldsymbol{Z}_{p^k}$ и к стандартным обозначениям теории

автоматов. Получим инициальный автомат

$$(M_R, \mathbf{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \ominus h \circ q_t^{(2)} \ominus h \circ q_t^{(3)} \ominus h \circ d \circ x_{t+1}, \\ q_{t+1}^{(2)} = h \circ q_t^{(1)} \oplus (a \circ h \oplus 1) \circ q_t^{(2)}, \\ q_{t+1}^{(3)} = h \circ b \oplus (1 \ominus h \circ r) \circ q_t^{(3)} \oplus h \circ q_t^{(1)} \circ q_t^{(3)}, \\ y_{t+1} = q_{t+1}^{(1)}, \end{cases} \qquad (t \in \mathbb{Z}_+), \tag{20}$$

где $\ominus$ — операция, обратная операции $\oplus$, а $a, b, d, h, r \in \mathbb{Z}_{p^k}$, причем d и h — обратимые элементы кольца $\boldsymbol{Z}_{p^k}$.

Пример 8. *1-я система Спротта* имеет вид

$$\begin{cases} \dot{x} = y, \\ \dot{y} = -x + y \cdot z, \\ \dot{z} = 1 - y^2, \end{cases} \qquad (t \in \mathbb{R}_+). \tag{21}$$

Дискретизируем систему (21), внесем информационную переменную в 1-е уравнение, перейдем к вычислениям в кольце $\boldsymbol{Z}_{p^k}$ и к стандартным обозначениям теории автоматов. Получим инициальный автомат

$$(M_S, \mathbf{q}_0): \begin{cases} q_{t+1}^{(1)} = q_t^{(1)} \oplus h \circ q_t^{(2)} \ominus h \circ a \circ x_{t+1}, \\ q_{t+1}^{(2)} = q_t^{(2)} \ominus h \circ q_t^{(1)} \oplus h \circ q_t^{(2)} \circ q_t^{(3)}, \\ q_{t+1}^{(3)} = h \oplus q_t^{(3)} \ominus h \circ (q_t^{(2)})^2, \\ y_{t+1} = q_{t+1}^{(1)}, \end{cases} \qquad (t \in \mathbb{Z}_+), \tag{22}$$

где $a, h \in \mathbb{Z}_{p^k}$ — обратимые элементы кольца $\boldsymbol{Z}_{p^k}$.

Пример 9. *Система Лоренца* имеет вид

$$\begin{cases} \dot{x} = a_1 \cdot (y - x), \\ \dot{y} = x \cdot (a_2 - z) - y, \\ \dot{z} = x \cdot y - a_3 \cdot z, \end{cases} \qquad (t \in \mathbb{R}_+). \tag{23}$$

Дискретизируем систему (23), внесем информационную переменную во 2-е уравнение, перейдем к вычислениям в кольце $\boldsymbol{Z}_{p^k}$ и к стандартным обозначениям теории автоматов. Получим инициальный автомат

$$(M_L, \mathbf{q}_0): \begin{cases} q_{t+1}^{(1)} = (1 \ominus h \circ a_1) \circ q_t^{(1)} \oplus h \circ a_1 \circ q_t^{(2)}, \\ q_{t+1}^{(2)} = (1 \ominus h) \circ q_t^{(2)} \oplus h \circ q_t^{(1)} \circ (a_2 \ominus q_t^{(3)}) \ominus h \circ a \circ x_{t+1}, \\ q_{t+1}^{(3)} = (1 \ominus h \circ a_3) \circ q_t^{(3)} \oplus h \circ q_t^{(1)} \circ q_t^{(2)}, \\ y_{t+1} = q_{t+1}^{(2)}, \end{cases} \qquad (t \in \mathbb{Z}_+), \tag{24}$$

где $a_1, a_2, a_3, a, h \in \mathbb{Z}_{p^k}$, причем a и h — обратимые элементы кольца $\boldsymbol{Z}_{p^k}$.

Пример 10. *Отображение Эно* имеет вид

$$\begin{cases} x_{n+1} = 1 - a \cdot x_n^2 - b \cdot y_n, \\ y_{n+1} = x_n, \end{cases} \qquad (n \in \mathbb{Z}_+). \tag{25}$$

Перейдем от (25) к отображению

$$x_{t+2} = 1 - a \cdot x_{t+1}^2 - b \cdot x_t \ \ (t \in \mathbb{Z}_+). \tag{26}$$

Добавим в (26) информационную переменную, перейдем к вычислениям в кольце $\boldsymbol{Z}_{p^k}$ и к стандартным обозначениям теории автоматов. Получим инициальный автомат

$$(M_H, \mathbf{q}_0) : \begin{cases} q_{t+2} = 1 \ominus a \circ q_{t+1}^2 \ominus b \circ q_t \oplus c \circ x_{t+1}, \\ y_{t+1} = q_{t+2}, \end{cases} \qquad (t \in \mathbb{Z}_+), \tag{27}$$

где $c \in \mathbb{Z}_{p^k}$ — обратимый элемент кольца $\boldsymbol{Z}_{p^k}$.

Отметим, что теоретический анализ вычислительной стойкости шифров (20), (22), (24) и (26) сводится к решению задач параметрической идентификации, идентификации начального состояния соответствующего автомата и к анализу множеств неподвижных точек отображений, реализуемых инициальными автоматами.

Выше были рассмотрены некоторые подходы к применению моделей и методов хаотической динамики для решения задач современной криптографии.

Среди попыток построения шифрсистем с открытым ключом следует также отметить предложенный в [46] протокол обмена ключами, основанный на использовании фракталов Мандельброта и Жюлиа для порождения открытых и секретных ключей. Хотя вычислительная стойкость предложенного протокола такая же, как и вычислительная стойкость протокола Диффи — Хеллмана, предложенный протокол использует ключи меньшего размера и работает быстрее, т. е. является более эффективным с точки зрения вычислений.

При построении коммуникационной системы на основе хаотического носителя в качестве такого носителя может быть выбрана практически любая хаотическая динамическая система. Основная проблема, которая здесь возникает, связана с построением схемы, обеспечевающей синхронизацию систем, расположенных в приемнике и передатчике. Ряд схем синхронизации модельных нелинейных хаотических динамических систем исследован в [44].

Исследованию линейных рекуррентных последовательностей над конечным кольцом (такие последовательности являются, по сути, автономными автоматами специального вида над конечным кольцом) посвящено значительное число публикаций. Их библиография представлена, например, в обзоре [47]. Однако исследования неавтономных автоматов над конечным кольцом, особенно в свете их приложения к решению задач криптографии, практически отсутствуют в настоящее время. В следующем разделе мы рассмотрим некоторые классы автоматов над кольцом $\boldsymbol{Z}_{p^k}$, которым, в частности, принадлежат автоматы, построенные в примерах 7–9.

3. Автоматы над конечным кольцом

В предыдущих двух разделах было показано, что как для теории автоматов, так и с точки зрения анализа математических основ современной криптографии актуально исследование автоматов, представленных системой уравнений над конечным кольцом. Такое исследование систематически изложено в [1].

В настоящем разделе мы рассмотрим основные характеристики ряда таких моделей как с точки зрения теории автоматов, так и с точки зрения современной криптографии. К стандартным задачам теории автоматов относится выделение основных нетривиальных подмножеств автоматов (в терминах критерия принадлежности автомата тому

или иному подмножеству), подсчет или оценка мощности этих подмножеств автоматов, поиск критериев эквивалентности состояний и автоматов, исследование сложности идентификации начального состояния автомата, а также исследование сложности идентификации автомата, принадлежащего заданному множеству автоматов (для модели, представленной системой уравнений, такое множество естественно определять в терминах вариации параметров).

Для криптографии объектом исследования является обратимый автомат, т. е. автомат, который при фиксации начального состояния реализует инъективное отображение входной полугруппы в выходную полугруппу. Ясно, что обратимый автомат и обратный ему автомат определяют симметричный поточный шифр. Поэтому с позиции криптографии представляет интерес выделение для исследуемых моделей подмножеств обратимых автоматов и решение для этих подмножеств автоматов перечисленных выше задач. При этом сложность решения задач идентификации начального состояния автомата и параметрической идентификации автомата характеризует с теоретической точки зрения сложность атаки криптоаналитика на секретный ключ соответствующего шифра.

Кроме перечисленных выше задач для криптографии представляет интерес исследование структуры множества неподвижных точек отображения, реализуемого инициальным обратимым автоматом (что дает возможность принять меры для предотвращения возможности появления критических фрагментов открытого текста на выходе шифра), а также изучение вариации поведения обратимого автомата при вариации его параметров или вариации начального состояния. Решение последней задачи представляет собой основу для разработки аналогов методов дифференциального и интегрального анализа поточных шифров, определяемых исследуемыми моделями (переход от булевой функции к словарной является принципиально новым моментом такого анализа для поточных шифров по сравнению с анализом блочных шифров).

В качестве конечного кольца выбрано кольцо $\boldsymbol{Z}_{p^k} = (\mathbb{Z}_{p^k}, \oplus, \circ)$. Такой выбор сделан только для того, чтобы упростить формулы, определяющие число автоматов, принадлежащих тем или иным подмножествам (остальные результаты истинны для любых конечных колец).

3.1. Исследуемые модели

Обозначим через $\mathtt{M}_n$ $(n \in \mathbb{N})$ множество всех $n \times n$-матриц над кольцом $\boldsymbol{Z}_{p^k}$.

В [1, 48, 49] исследовано множество $\mathsf{A}_{n,1}$ линейных автоматов Мили

$$(M_1, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+) \tag{28}$$

и множество $\mathsf{A}_{n,2}$ линейных автоматов Мура

$$(M_2, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+), \tag{29}$$

где $A, B, C, D \in \mathtt{M}_n$ — фиксированные матрицы, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathbb{Z}_{p^k}^n$ — вектор-столбцы, представляющие состояние автомата, входной символ и выходной символ в момент t.

Замечание 1. Интерес к исследованию множеств автоматов $\mathsf{A}_{n,1}$ и $\mathsf{A}_{n,2}$ обусловлен следующим. Как показывает предыдущий опыт (см., напр., [8, 9], для линейных автоматов решение многих задач значительно проще, чем в общем случае. Это дает возможность получить более завершенный (чем в общем случае) фрагмент теории и

понять ту внутреннюю сложность решения задач, которая возникает при переходе от конечного поля к конечному кольцу.

В [1, 50] исследовано множество $\widetilde{\mathsf{A}}_{l,1}$ линейных с лагом l одномерных автоматов Мили

$$(\widetilde{M}_1, \widetilde{\mathbf{q}}_0): \begin{cases} q_{t+1} = \bigoplus\limits_{i=1}^{n} a_i \circ q_{t+l-i} \oplus b \circ x_{t+1}, \\ y_{t+1} = \bigoplus\limits_{i=1}^{n} c_i \circ q_{t+l-i} \oplus d \circ x_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+) \tag{30}$$

и множество $\widetilde{\mathsf{A}}_{l,2}$ линейных с лагом l одномерных автоматов Мура

$$(\widetilde{M}_2, \widetilde{\mathbf{q}}_0): \begin{cases} q_{t+1} = \bigoplus\limits_{i=1}^{n} a_i \circ q_{t+l-i} \oplus b \circ x_{t+1}, \\ y_{t+1} = \bigoplus\limits_{i=1}^{n} c_i \circ q_{t+l+1-i}, \end{cases} \quad (t \in \mathbb{Z}_+), \tag{31}$$

где $q \in \mathbb{Z}_{p^k}$ — переменная состояния; $\widetilde{\mathbf{q}}_0 = (q_{l-1}, \ldots, q_1, q_0)^T$ — начальное состояние автомата; $x \in \mathbb{Z}_{p^k}$ и $y \in \mathbb{Z}_{p^k}$ — соответственно входная и выходная переменная; $a_i, c_i, b, d \in \mathbb{Z}_{p^k}$ $(i = 1, \ldots, l)$ — параметры.

Замечание 2. Интерес к исследованию множеств автоматов $\widetilde{\mathsf{A}}_{l,1}$ и $\widetilde{\mathsf{A}}_{l,2}$ обусловлен следующим. Применение при построении поточных шифров линейных сдвиговых регистров, реализующих вычисления в конечном кольце, привело к необходимости систематического анализа свойств линейных и полилинейных рекуррент над конечными коммутативными кольцами и модулями (см., напр., [47, 51]), а элементы множеств $\widetilde{\mathsf{A}}_{l,1}$ и $\widetilde{\mathsf{A}}_{l,2}$ являются математической моделью специального класса таких регистров с внешним управлением.

Автоматы (30) и (31) могут быть представлены в матричном виде

$$(\widetilde{M}_1, \widetilde{\mathbf{q}}_0): \begin{cases} \widetilde{\mathbf{q}}_{t+1} = \widetilde{A} \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{B} \circ \widetilde{\mathbf{x}}_{t+1}, \\ \widetilde{\mathbf{y}}_{t+1} = \widetilde{C} \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{D} \circ \widetilde{\mathbf{x}}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+),$$

$$(\widetilde{M}_2, \widetilde{\mathbf{q}}_0): \begin{cases} \widetilde{\mathbf{q}}_{t+1} = \widetilde{A} \circ \widetilde{\mathbf{q}}_t \oplus \widetilde{B} \circ \widetilde{\mathbf{x}}_{t+1}, \\ \widetilde{\mathbf{y}}_{t+1} = \widetilde{C} \circ \widetilde{\mathbf{q}}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+),$$

где

$$\widetilde{\mathbf{q}}_t = (q_{t+l-1}, \ldots, q_{t+1}, q_t)^T \ (t \in \mathbb{Z}_+), \tag{32}$$

$$\widetilde{\mathbf{x}}_{t+1} = (x_{t+1}, 0, 0, \ldots, 0)^T \ (t \in \mathbb{Z}_+), \tag{33}$$

$$\widetilde{\mathbf{y}}_{t+1} = (y_{t+1}, 0, 0, \ldots, 0)^T \ (t \in \mathbb{Z}_+), \tag{34}$$

$$\widetilde{A} = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_l \end{pmatrix}, \quad \widetilde{B} = \begin{pmatrix} b & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \tag{35}$$

$$\widetilde{C} = \begin{pmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & c_l \end{pmatrix}, \quad \widetilde{D} = \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}. \tag{36}$$

Отсюда вытекает, что для автоматов (30) и (31) заведомо истинны все результаты, полученные для автоматов (28) и (29), переформулированные с учетом равенств (32)–(36).

В [1, 52, 53] исследовано:

1) множество $\mathtt{A}_{n,1}$ представленных в матричном виде нелинейных автоматов Мили

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = G \circ \mathbf{q}_t \oplus F \circ \mathbf{x}_{t+1}, \end{cases} \qquad (t \in \mathbb{Z}_+)$$

и множество $\mathtt{A}_{n,2}$ представленных в матричном виде нелинейных автоматов Мура

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = G \circ \mathbf{q}_{t+1}, \end{cases} \qquad (t \in \mathbb{Z}_+),$$

где $\mathbf{b}, \mathbf{d} \in \mathbb{Z}_{p^k}^n$ — фиксированные вектор-столбцы; $A, C, E, G, F \in \mathtt{M}_n$ — фиксированные матрицы; $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathbb{Z}_{p^k}^n$ — вектор-столбцы, представляющие состояние автомата, входной символ и выходной символ в момент t;

2) множество $\mathtt{A}_{n,3}$ представленных в матрично-скалярном виде нелинейных автоматов Мили

$$(M_3, \mathbf{q}_0): \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ (i = 1, \dots, r), \\ q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \ (i = r+1, \dots, n), \\ y_{t+1}^{(i)} = g_i \circ q_t^{(i)} \oplus f_i \circ x_{t+1}^{(i)} \ (i = 1, \dots, r), \end{cases} \qquad (t \in \mathbb{Z}_+)$$

и множество $\mathtt{A}_{n,4}$ представленных в матрично-скалярном виде нелинейных автоматов Мура

$$(M_4, \mathbf{q}_0): \begin{cases} q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \oplus e_i \circ x_{t+1}^{(i)} \ (i = 1, \dots, r), \\ q_{t+1}^{(i)} = \mathbf{q}_t^T \circ A_i \circ \mathbf{q}_t \oplus \mathbf{c}_i \circ \mathbf{q}_t \oplus d_i \ (i = r+1, \dots, n), \\ y_{t+1}^{(i)} = g_i \circ q_{t+1}^{(i)} \ (i = 1, \dots, r), \end{cases} \qquad (t \in \mathbb{Z}_+),$$

где r $(1 \leqslant r \leqslant n)$ — фиксированное число; $A_i \in \mathtt{M}_n$ — фиксированные матрицы; $\mathbf{c}_i \in \mathbb{Z}_{p^k}^n$ $(i = 1, \dots, n)$ — фиксированные векторы; $e_i, g_i, f_i \in \mathbb{Z}_{p^k}$ $(i = 1, \dots, r)$ — фиксированные обратимые элементы кольца $\boldsymbol{Z}_{p^k}$; $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in \mathbb{Z}_{p^k}^n$ — вектор-столбцы, представляющие состояние автомата, входной символ и выходной символ в момент t.

Замечание 3. Интерес к исследованию множеств автоматов $\mathtt{A}_{n,1}$, $\mathtt{A}_{n,2}$, $\mathtt{A}_{n,3}$ и $\mathtt{A}_{n,4}$ обусловлен тем, что значительное часть автоматов над кольцом $\boldsymbol{Z}_{p^k}$, построенных на основе модельных хаотических динамических систем, принадлежит именно этим множествам автоматов. В частности, все автоматы над кольцом $\boldsymbol{Z}_{p^k}$, построенные в разд. 2, принадлежат множеству $\mathtt{A}_{n,4}$.

В [1, 54, 55] исследовано множество A_{GH} симметричных нелинейных автоматов Мура

$$(M_{\mathrm{GH}}, \mathbf{q}_0): \begin{cases} q_{n+1}^{(1)} = q_n^{(1)} \circ (d \oplus a \circ (q_n^{(1)})^2 \oplus b \circ (q_n^{(2)})^2 \oplus c \circ (q_n^{(3)})^2 \oplus \alpha_1 \circ x_{n+1}, \\ q_{n+1}^{(2)} = q_n^{(2)} \circ (d \oplus c \circ (q_n^{(1)})^2 \oplus a \circ (q_n^{(2)})^2 \oplus b \circ (q_n^{(3)})^2 \oplus \alpha_2 \circ x_{n+1}, \\ q_{n+1}^{(3)} = q_n^{(3)} \circ (d \oplus b \circ (q_n^{(1)})^2 \oplus c \circ (q_n^{(2)})^2 \oplus a \circ (q_n^{(3)})^2 \oplus \alpha_3 \circ x_{n+1}, \\ y_{n+1}^{(i)} = q_{n+1}^{(i)} \ (i = 1, 2, 3), \end{cases} \quad (n \in \mathbb{Z}_+)$$

и множество A_{FR} симметричных нелинейных автоматов Мура

$$(M_{\mathrm{FR}}, \mathbf{q}_0): \begin{cases} q_{n+1}^{(1)} = f(q_n^{(1)}) \circ \zeta^{q_n^{(3)}} \oplus \alpha_1 \circ x_{n+1}, \\ q_{n+1}^{(2)} = f(q_n^{(2)}) \circ \zeta^{q_n^{(1)}} \oplus \alpha_2 \circ x_{n+1}, \\ q_{n+1}^{(3)} = f(q_n^{(3)}) \circ \zeta^{q_n^{(2)}} \oplus \alpha_3 \circ x_{n+1}, \\ y_{n+1}^{(i)} = q_{n+1}^{(i)} \ (i = 1, 2, 3), \end{cases} \quad (n \in \mathbb{Z}_+),$$

где $x_n \in \mathbb{Z}_{p^k}$, $\mathbf{y}_n = (y_n^{(1)}, y_n^{(2)}, y_n^{(3)})^T \in \mathbb{Z}_{p^k}^3$ и $\mathbf{q}_n = (q_n^{(1)}, q_n^{(2)}, q_n^{(3)})^T \in \mathbb{Z}_{p^k}^3$ — соответственно входной символ, выходной символ и состояние автомата в момент n; отображение $f(x) = a \circ x \circ (1 \ominus x)$ представляет собой аналог логистического отображения над кольцом $\boldsymbol{Z}_{p^k}$; $\alpha_1, \alpha_2, \alpha_3, \zeta \in \mathbb{Z}_{p^k}$ — фиксированные обратимые элементы кольца $\boldsymbol{Z}_{p^k}$; $a, b, c, d \in \mathbb{Z}_{p^k}$ — фиксированные элементы кольца $\boldsymbol{Z}_{p^k}$.

Подчеркнем, что автоматы M_{GH} и M_{FR} построены на основе модельных хаотических динамических систем, исследованных в [56], а именно: Guckenheimer and Holmes cycle (GH) и free-running system (FR).

Замечание 4. Интерес к исследованию автоматов M_{GH} и M_{FR} обусловлен следующими обстоятельствами.

Во-первых, оба автомата имеют нетривиальные группы симметрий, а, как известно, теория симметрий [57] — мощный аппарат анализа динамических систем.

Во-вторых, изменение динамических переменных Guckenheimer and Holmes cycle представлено многочленами 3-й степени, а, как известно, решение кубических уравнений над конечным кольцом — сложная задача.

В-третьих, изменение динамических переменных free-running system осуществляется с помощью показательной функции, а, как известно, дискретное логарифмирование (т. е. операция, обратная показательной функции) — базовая конструкция криптографии.

Анализ представленных автоматных моделей показывает, что если M — обратимый автомат, а M^{-1} — обратный ему автомат, то упорядоченная пара $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ — симметричный поточный шифр, причем в процессе *шифрование — расшифрование* автоматы M и M^{-1} движутся в пространстве состояний по одной и той же траектории. Отсюда вытекает, что за счет одновременного использования прямого и обратного автоматов возможно осуществлять контроль (т. е. обнаружение или исправление) некоторых ошибок, возникающих в процессе передачи информации по каналу связи.

Подчеркнем, что для шифра $((M, \mathbf{q}_0), (M^{-1}, \mathbf{q}_0))$ параметры представляют собой *ключ средней длительности*, а начальное состояние $\mathbf{q}_0$ — *сеансовый ключ*.

3.2. Конечно-автоматные характеристики исследуемых моделей

Анализ представленных автоматных моделей показывает, что каждое из множеств $\mathsf{A}_{n,3}$, $\mathsf{A}_{n,4}$, A_{GH} и A_{FR} состоит из обратимых автоматов.

Обозначим через $\mathrm{X}^{\mathrm{inv}}$ ($\mathrm{X} \in \{\mathsf{A}_{n,1}, \mathsf{A}_{n,2}, \widetilde{\mathsf{A}}_{l,1}, \widetilde{\mathsf{A}}_{l,2}, \mathtt{A}_{n,1}, \mathtt{A}_{n,2}\}$) множество всех обратимых автоматов $M \in \mathrm{X}$, через $\mathtt{M}_n^{\mathrm{inv}}$ — множество всех обратимых матриц $A \in \mathtt{M}_n$, а через $\mathtt{M}_n^{\text{non-inv}}$ — множество всех необратимых матриц $A \in \mathtt{M}_n$.

Принадлежность автомата множеству $\mathrm{X}^{\mathrm{inv}}$ ($\mathrm{X} \in \{\mathsf{A}_{n,1}, \mathsf{A}_{n,2}, \widetilde{\mathsf{A}}_{l,1}, \widetilde{\mathsf{A}}_{l,2}, \mathtt{A}_{n,1}, \mathtt{A}_{n,2}\}$) характеризуется следующим образом:

1) $M_1 \in \mathsf{A}_{n,1}$ — обратимый автомат тогда и только тогда, когда $D \in \mathtt{M}_n^{\mathrm{inv}}$;

2) $M_2 \in \mathsf{A}_{n,2}$ — обратимый автомат тогда и только тогда, когда $B, C \in \mathtt{M}_n^{\mathrm{inv}}$;

3) $\widetilde{M}_1 \in \widetilde{\mathsf{A}}_{l,1}$ — обратимый автомат тогда и только тогда, когда $d \in \mathbb{Z}_{p^k}$ — обратимый элемент кольца $\boldsymbol{Z}_{p^k}$;

4) $\widetilde{M}_2 \in \widetilde{\mathsf{A}}_{l,2}$ — обратимый автомат тогда и только тогда, когда $c_1, b \in \mathbb{Z}_{p^k}$ — обратимые элементы кольца $\boldsymbol{Z}_{p^k}$;

5) $M_1 \in \mathtt{A}_{n,1}$ — обратимый автомат тогда и только тогда, когда $F \in \mathtt{M}_n^{\mathrm{inv}}$;

6) $M_2 \in \mathtt{A}_{n,2}$ — обратимый автомат тогда и только тогда, когда $E, G \in \mathtt{M}_n^{\mathrm{inv}}$.

Именно на основании этих критериев и построены соответствующие обратные автоматы.

Пример 11.

1. Автоматы, обратные автоматам $M_i \in \mathsf{A}_{n,i}$ $(i = 1, 2)$, имеют вид

$$(M_1^{-1}, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = A_1 \circ \mathbf{q}_t \oplus B_1 \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $A_1 = A \ominus B \circ D^{-1} \circ C$, $B_1 = B \circ D^{-1}$, $C_1 = \ominus D^{-1} \circ C$, $D_1 = D^{-1}$, и

$$(M_2^{-1}, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = B_1 \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $B_1 = C^{-1}$, $C_1 = \ominus A$, $D_1 = B^{-1} \circ C^{-1}$.

2. Автоматы, обратные автоматам $M_i \in \mathtt{A}_{n,i}$ $(i = 1, 2)$, имеют вид

$$(M_1^{-1}, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C_1 \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E_1 \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = F^{-1} \circ (\mathbf{x}_{t+1} \ominus G \circ \mathbf{q}_t), \end{cases} \quad (t \in \mathbb{Z}_+),$$

где $C_1 = C \ominus E \circ F^{-1} \circ G$, $E_1 = E \circ F^{-1}$, и

$$(M_2^{-1}, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = G^{-1} \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = E^{-1} \circ (G^{-1} \circ \mathbf{x}_{t+1} \ominus (A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d})), \end{cases} \quad (t \in \mathbb{Z}_+).$$

Отметим, что построенные в примере 11 обратные автоматы — автоматы типа Мили.

Основные нетривиальные подмножества исследуемых автоматов характеризуются следующим образом:

1) граф переходов автомата $M_i \in \mathsf{A}_{n,i}$ $(i = 1, 2)$ — полный граф с петлями тогда и только тогда, когда $B \in \mathtt{M}_n^{\mathrm{inv}}$;

2) если $A \in \mathtt{M}_n^{\mathrm{inv}}$, то $M_i \in \mathsf{A}_{n,i}$ $(i = 1, 2)$ — перестановочный автомат;

3) если $C \in \mathtt{M}_n^{\mathrm{inv}}$, то $M_1 \in \mathsf{A}_{n,1}$ — приведенный автомат, и его степень различимости равна 1;

4) если $A, C \in \mathtt{M}_n^{\mathrm{inv}}$, то $M_2 \in \mathsf{A}_{n,2}$ — приведенный автомат, и его степень различимости равна 1;

5) если $A, C \in \mathtt{M}_n^{\text{non-inv}}$ и система уравнений

$$\begin{cases} A \circ \mathbf{u} = \mathbf{0}, \\ C \circ \mathbf{u} = \mathbf{0} \end{cases}$$

имеет ненулевое решение, то в автомате $M_1 \in \mathsf{A}_{n,1}$ существуют состояния-близнецы;

6) если $A \in \mathtt{M}_n^{\text{non-inv}}$, то в автомате $M_2 \in \mathsf{A}_{n,2}$ существуют состояния-близнецы;

7) для всех $l \in \mathbb{N}$ автомат $\widetilde{M}_j \in \widetilde{\mathsf{A}}_{l,j}$ $(j = 1, 2)$ является сильно связным автоматом тогда и только тогда, когда $b \in \mathbb{Z}_{p^k}$ — обратимый элемент кольца $\boldsymbol{Z}_{p^k}$;

8) для всех $l \in \mathbb{N}$, если автомат $\widetilde{M}_j \in \widetilde{\mathsf{A}}_{l,j}$ $(j = 1, 2)$ является сильно связным автоматом, то диаметр его графа переходов равен l;

9) для всех $l \in \mathbb{N}$ автомат $\widetilde{M}_j \in \widetilde{\mathsf{A}}_{l,j}$ $(j = 1, 2)$ является перестановочным автоматом тогда и только тогда, когда $a_l \in \mathbb{Z}_{p^k}$ — обратимый элемент кольца $\boldsymbol{Z}_{p^k}$;

10) если $E \in \mathtt{M}_n^{\text{inv}}$, то $M_i \in \mathtt{A}_{n,i}^{\text{inv}}$ $(i = 1, 2)$ — сильно связный перестановочный автомат, причем диаметр его графа переходов равен 1;

11) если $G \in \mathtt{M}_n^{\text{inv}}$, то $M_1 \in \mathtt{A}_{n,1}^{\text{inv}}$ — приведенный автомат;

12) $M_2 \in \mathtt{A}_{n,2}^{\text{inv}}$ — сильно связный перестановочный автомат, и диаметр его графа переходов равен 1;

13) если $E \in \mathtt{M}_n^{\text{non-inv}}$, то или автомат $M_1 \in \mathtt{A}_{n,1}^{\text{inv}}$ несвязен, или диаметр его графа переходов больше чем 1;

14) если $r = n$, то $M_i \in \mathtt{A}_{n,i}$ $(i = 3, 4)$ — сильно связный перестановочный автомат, и диаметр его графа переходов равен 1;

15) если $r < n$, то автомат $M_i \in \mathtt{A}_{n,i}$ $(i = 3, 4)$ не является сильно связным перестановочным автоматом или диаметр его графа переходов больше чем 1;

16) из каждого состояния $\mathbf{q} \in \mathbb{Z}_{p^k}^n$ автомата $M_i \in \mathtt{A}_{n,i}$ $(i = 3, 4)$ в точности $p^{k \cdot r}$ различных состояний автомата $M_i \in \mathtt{A}_{n,i}$ являются 1-достижимыми;

17) любой автомат $M_{\text{GH}} \in \mathsf{A}_{\text{GH}}$, а также любой автомат $M_{\text{FR}} \in \mathsf{A}_{\text{FR}}$ не является сильно связным автоматом;

18) подавтомат автомата $M_{\text{GH}} \in \mathsf{A}_{\text{GH}}$, а также подавтомат автомата $M_{\text{FR}} \in \mathsf{A}_{\text{FR}}$, определяемые множеством состояний

$$S_1 = \{\mathbf{q} = (q, q, q)^T | q \in \mathbb{Z}_{p^k}\},$$

являются приведенными перестановочными автоматами, причем диаметр графа переходов каждого из них равен 1;

19) если $d \equiv 0 \pmod{p^{\lceil 0{,}5 \cdot k \rceil}}$, то автомат $M_{\text{GH}} \in \mathsf{A}_{\text{GH}}$ не является перестановочным автоматом;

20) автомат $M_{\text{FR}} \in \mathsf{A}_{\text{FR}}$ не является перестановочным автоматом. Сформулированные выше утверждения характеризуют подмножества автоматов в терминах обратимых, необратимых и произвольных элементов или матриц над кольцом $\boldsymbol{Z}_{p^k}$. Отсюда вытекает следующий унифицированный способ оценки мощности подмножеств автоматов: если в характеристике автомата, принадлежащего заданному подмножеству, фигурирует γ_1 обратимых, γ_2 необратимых и γ_3 произвольных элементов или матриц над кольцом $\boldsymbol{Z}_{p^k}$, выбор которых осуществляется независимо, а число таких элементов или матриц над кольцом $\boldsymbol{Z}_{p^k}$ равно соответственно ρ_1, ρ_2 и ρ_3, то оценка мощности заданного подмножества автоматов имеет вид $\rho_1^{\gamma_1} \cdot \rho_2^{\gamma_2} \cdot \rho_3^{\gamma_3}$.

Пример 12. Число обратимых и необратимых элементов кольца $\boldsymbol{Z}_{p^k}$ равно (см., напр., [1]) соответственно $(p-1) \cdot p^{k-1}$ и p^{k-1}, и (см., напр., [23]) верны следующие

равенства:

$$|\mathtt{M}_n| = p^{n^2},$$

$$|\mathtt{M}_n^{\mathrm{inv}}| = |\mathtt{M}_n| \cdot \prod_{i=1}^{n}(1 - p^{-i}),$$

$$|\mathtt{M}_n^{\text{non-inv}}| = |\mathtt{M}_n|(1 - \prod_{i=1}^{n}(1 - p^{-i})).$$

На основании этих оценок в [58] установлены следующие оценки мощностей множеств автоматов:

1) для всех $n \in \mathbb{N}$ истинны равенства

$$|\mathsf{A}_{n,i}^{\mathrm{inv}}| = |\mathsf{A}_{n,i}| \cdot \prod_{j=1}^{n}(1 - p^{-j})^i \ \ (i = 1, 2),$$

где

$$|\mathsf{A}_{n,i}| = |\mathtt{M}_n|^{5-i} \ \ (i = 1, 2);$$

2) если $\mathtt{D}_n^{(1)}$ — множество всех диагональных матриц $X \in \mathtt{M}_n$, на главной диагонали которых расположены обратимые элементы кольца $\boldsymbol{Z}_{p^k}$,

$$\mathsf{B}_{n,1}^{\mathrm{inv}} = \{M_1 \in \mathsf{A}_{n,1}^{\mathrm{inv}} | D \in \mathtt{D}_n^{(1)}\},$$

$$\mathsf{B}_{n,2}^{\mathrm{inv}} = \{M_2 \in \mathsf{A}_{n,2}^{\mathrm{inv}} | B, C \in \mathtt{D}_n^{(1)}\},$$

то для всех $n \in \mathbb{N}$ истинны равенства

$$|\mathsf{B}_{n,i}^{\mathrm{inv}}| = |\mathsf{A}_{n,i}^{\mathrm{inv}}|((p-1)^n \cdot p^{(k-1-k\cdot n)\cdot n})^i \ \ (i = 1, 2);$$

3) если $\mathsf{G}_{n,i}$ $(i = 1, 2)$ — множество всех автоматов $M_i \in \mathsf{A}_{n,i}$, у которых граф переходов — полный граф с петлями, и

$$\mathsf{G}_{n,i}^{\mathrm{inv}} = \mathsf{G}_{n,i} \cap \mathsf{A}_{n,i}^{\mathrm{inv}} \ \ (i = 1, 2),$$

то для всех $n \in \mathbb{N}$ истинны равенства

$$|\mathsf{G}_{n,i}^{\mathrm{inv}}| = |\mathsf{A}_{n,i}| \cdot \prod_{j=1}^{n}(1 - p^{-j})^2 \ \ (i = 1, 2);$$

4) если $\mathsf{C}_{n,i}$ $(i = 1, 2)$ — множество всех перестановочных автоматов $M_i \in \mathsf{A}_{n,i}$ и

$$\mathsf{C}_{n,i}^{\mathrm{inv}} = \mathsf{C}_{n,i} \cap \mathsf{A}_{n,i}^{\mathrm{inv}} \ \ (i = 1, 2),$$

то для всех $n \in \mathbb{N}$ истинны равенства

$$|\mathsf{C}_{n,i}^{\mathrm{inv}}| = |\mathsf{A}_{n,i}| \cdot \prod_{j=1}^{n}(1 - p^{-j})^{i+1} \ \ (i = 1, 2);$$

5) если $\mathsf{D}_{n,i}$ $(i = 1, 2)$ — множество всех приведенных автоматов $M_i \in \mathsf{A}_{n,i}$ и

$$\mathsf{D}_{n,i}^{\mathrm{inv}} = \mathsf{D}_{n,i} \cap \mathsf{A}_{n,i}^{\mathrm{inv}} \ \ (i = 1, 2),$$

то для всех $n \in \mathbb{N}$ истинны неравенства

$$|\mathsf{D}_{n,i}^{\mathrm{inv}}| \geqslant |\mathsf{A}_{n,i}| \cdot \prod_{j=1}^{n}(1-p^{-j})^{i+1} \ (i=1,2);$$

6) если $\mathsf{E}_{n,i}$ $(i=1,2)$ — множество всех автоматов $M_i \in \mathsf{A}_{n,i}$, имеющих состояния-близнецы, и

$$\mathsf{E}_{n,i}^{\mathrm{inv}} = \mathsf{E}_{n,i} \cap \mathsf{A}_{n,i}^{\mathrm{inv}} \ (i=1,2),$$

то для всех $n \geqslant \mathbb{N}$ истинны неравенства

$$|\mathsf{E}_{n,i}^{\mathrm{inv}}| \geqslant |\mathsf{A}_{n,i}| \cdot (1-\prod_{j=1}^{n}(1-p^{-j}))^{3-i} \cdot \prod_{j=1}^{n}(1-p^{-j})^{i} \ (i=1,2);$$

7) если $\mathtt{D}_n^{(2)}$ — множество всех диагональных матриц $X \in \mathtt{M}_n$, у которых на главной диагонали расположены необратимые элементы кольца $\boldsymbol{Z}_{p^k}$,

$$\mathsf{F}_{n,1}^{\mathrm{inv}} = \{M_1 \in \mathsf{A}_{n,1}^{\mathrm{inv}} | A, C \in \mathtt{D}_n^{(2)}\}$$

и

$$\mathsf{F}_{n,2}^{\mathrm{inv}} = \{M_2 \in \mathsf{A}_{n,2}^{\mathrm{inv}} | A \in \mathtt{D}_n^{(2)}\},$$

то для всех $n \in \mathbb{N}$ истинны равенства

$$|\mathsf{F}_{n,i}^{\mathrm{inv}}| = |\mathsf{A}_{n,i}^{\mathrm{inv}}| \cdot p^{(3-i)\cdot n\cdot(k-1-k\cdot n)} \cdot \prod_{j=1}^{n}(1-p^{-j})^{i} \ (i=1,2);$$

8) для всех $n \in \mathbb{N}$ истинны равенства

$$|\widetilde{\mathsf{A}}_{l,j}^{\mathrm{inv}}| = |\widetilde{\mathsf{A}}_{l,j}| \cdot p^{-j}(p-1)^{j} \ (j=1,2),$$

где

$$|\widetilde{\mathsf{A}}_{l,j}| = p^{k\cdot(2\cdot l+3-j)} \ (j=1,2);$$

9) если $\widetilde{\mathsf{A}}_{l,j}^{sc}$ $(j=1,2)$ — множество всех сильно связных автоматов $\widetilde{M_j} \in \widetilde{\mathsf{A}}_{l,j}$ и

$$\widetilde{\mathsf{A}}_{l,j}^{\text{sc-inv}} = \widetilde{\mathsf{A}}_{l,j}^{sc} \cap \widetilde{\mathsf{A}}_{l,j}^{\mathrm{inv}} \ (j=1,2),$$

то для всех $l \in \mathbb{N}$ истинны равенства

$$|\widetilde{\mathsf{A}}_{l,j}^{\text{sc-inv}}| = |\widetilde{\mathsf{A}}_{l,j}| \cdot (1-p^{-1})^{2} \ (j=1,2);$$

10) если $\widetilde{\mathsf{A}}_{l,j}^{p}$ $(j=1,2)$ — множество всех перестановочных автоматов $\widetilde{M_j} \in \widetilde{\mathsf{A}}_{l,j}$ и

$$\widetilde{\mathsf{A}}_{l,j}^{\text{p-inv}} = \widetilde{\mathsf{A}}_{l,j}^{p} \cap \widetilde{\mathsf{A}}_{l,j}^{\mathrm{inv}} \ (j=1,2),$$

то для всех $l \in \mathbb{N}$ истинны равенства

$$|\widetilde{\mathsf{A}}_{l,j}^{\text{p-inv}}| = |\widetilde{\mathsf{A}}_{l,j}|(1-p^{-1})^{j+1} \ (j=1,2).$$

Отметим, что оценки мощностей подмножеств обратимых автоматов, установленные в примере 12, дают возможность оценить число ключей средней длительности для шифров, построенных на основе обратимых автоматов с соответствующей структурой.

3.3. Эквивалентность состояний исследуемых моделей

Исследование структуры множеств эквивалентных состояний исследуемых моделей представляет интерес не только с позиции теории автоматов, но и с позиции криптографии, так как эти результаты дают возможность охарактеризовать структуру множества эквивалентных сеансовых ключей поточных шифров, построенных на основе обратимых автоматов с соответствующей структурой.

В [1, 48, 49] показано, что:

1) инициальные автоматы $(M_1, \mathbf{q}_0)$ и $(M_1', \mathbf{q}_0')$ $(M_1, M_1' \in \mathsf{A}_{n,1})$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

а) $D = D'$;

б) $C' \circ \mathbf{q}_0' \ominus C \circ \mathbf{q}_0 = \mathbf{0}$;

в) $C' \circ (A')^t \circ \mathbf{q}_0' \ominus C \circ A^t \circ \mathbf{q}_0 = \mathbf{0}$ $(t = 1, \ldots, 2 \cdot p^{k \cdot n} - 2)$;

г) $C' \circ (A')^t \circ B' \ominus C \circ A^t \circ B = O$ $(t = 1, \ldots, 2 \cdot p^{k \cdot n} - 3)$ (через O обозначена нулевая $n \times n$ -матрица);

д) $C' \circ B' \ominus C \circ B = O$;

2) инициальные автоматы $(M_2, \mathbf{q}_0)$ и $(M_2', \mathbf{q}_0')$ $(M_2, M_2' \in \mathsf{A}_{n,2})$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

а) $C' \circ B' \ominus C \circ B = O$;

б) $C' \circ (A')^t \circ \mathbf{q}_0' \ominus C \circ A^t \circ \mathbf{q}_0 = \mathbf{0}$ $(t = 1, \ldots, 2 \cdot p^{k \cdot n} - 1)$;

в) $C' \circ (A')^t \circ B' \ominus C \circ A^t \circ B = O$ $(t = 1, \ldots, 2 \cdot p^{k \cdot n} - 2)$.

Из этих критериев вытекает, что:

1) состояния $\mathbf{q}_0$ и $\mathbf{q}_0'$ автомата $M_1 \in \mathsf{A}_{n,1}$ эквивалентны тогда и только тогда, когда выполнены следующие условия:

а) $C \circ (\mathbf{q}_0' \ominus \mathbf{q}_0) = \mathbf{0}$;

б) $C \circ A^t \circ (\mathbf{q}_0' \ominus \mathbf{q}_0) = \mathbf{0}$ для всех $t = 1, \ldots, p^{k \cdot n} - 2$;

2) состояния $\mathbf{q}_0$ и $\mathbf{q}_0'$ автомата $M_2 \in \mathsf{A}_{n,2}$ эквивалентны тогда и только тогда, когда $C \circ A^t \circ (\mathbf{q}_0' \ominus \mathbf{q}_0) = \mathbf{0}$ для всех $t = 1, \ldots, p^{k \cdot n} - 2$.

Отметим, что из этих утверждений, в частности, следует, что:

1) если $C \in \mathtt{M}_n^{\text{inv}}$, то $M_1 \in \mathsf{A}_{n,1}$ — приведенный автомат;

2) если $A, C \in \mathtt{M}_n^{\text{inv}}$, то $M_2 \in \mathsf{A}_{n,2}$ — приведенный автомат.

В [1, 52, 53] показано, что:

1) если $G \in \mathtt{M}_n^{\text{non-inv}}$, то $\mathbf{q}_0$ и $\mathbf{q}_0'$ — эквивалентные состояния автомата $M_1 \in \mathtt{A}_{n,1}^{\text{inv}}$ тогда и только тогда, когда выполнены следующие условия:

а) $G \circ (\mathbf{q}_0' \ominus \mathbf{q}_0) = \mathbf{0}$;

б) $G \circ (\mathbf{q}_t' \ominus \mathbf{q}_t) = \mathbf{0}$ $(t = 1, \ldots, p^{k \cdot n} - 2)$ для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbb{Z}_{p^k}^{n \cdot t}$;

2) состояния автомата $M_2 \in \mathtt{A}_{n,2}^{\text{inv}}$ эквивалентны тогда и только тогда, когда они являются близнецами;

3) состояния $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ автомата $M_3 \in \mathsf{A}_{n,3}$ эквивалентны тогда и только тогда, когда для всех $i = 1, \ldots, r$ выполнены следующие условия:

а) $\widetilde{q}_0^{(i)} \ominus q_0^{(i)} = 0$;

б) $\widetilde{q}_t^{(i)} \ominus q_t^{(i)} = 0$ для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbb{Z}_{p^k}^{r \cdot t}$ $(t = 1, \ldots, p^{k \cdot n} - 2)$;

4) состояния $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ автомата $M_4 \in \mathtt{A}_{n,4}$ эквивалентны тогда и только тогда, когда $\widetilde{q}_t^{(i)} \ominus q_t^{(i)} = 0$ $(i = 1, \ldots, r)$ для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in \mathbb{Z}_{p^k}^{r \cdot t}$ $(t = 1, \ldots, p^{k \cdot n} - 1)$.

В [1, 55] показано, что:

а) состояния автомата $M_{\text{GH}} \in \mathsf{A}_{\text{GH}}$ эквивалентны тогда и только тогда, когда они являются близнецами;

б) состояния автомата $M_{\mathrm{FR}} \in \mathsf{A}_{\mathrm{FR}}$ эквивалентны тогда и только тогда, когда они являются близнецами.

Приведенные выше критерии эквивалентности состояний исследуемых моделей дают возможность для поточных шифров, построенных на основе обратимых автоматов с соответствующей структурой, представить в виде множества решений систем уравнений над конечным кольцом множество всех состояний автомата, эквивалентных заданному состоянию (т. е., по своей сути, множество всех сеансовых ключей соответствующего поточного шифра, эквивалентных заданному сеансовому ключу).

Пример 13. В [1] показано, что для автомата $M_2 \in \mathtt{A}_{n,2}^{\mathrm{inv}}$ множество всех состояний $\widetilde{\mathbf{q}}$, эквивалентных заданному состоянию $\mathbf{q}_0$, совпадает с множеством решений следующей системы нелинейных уравнений:

$$A \circ (\widetilde{\mathbf{q}} \circ \widetilde{\mathbf{q}}^T \ominus \mathbf{q}_0 \circ \mathbf{q}_0^T) \circ \mathbf{b} \oplus \circ(\widetilde{\mathbf{q}} \ominus \mathbf{q}_0) = \mathbf{0}.$$

Дополнительный учет факторов, вытекающих из структуры уравнений, которые определяют построенный на основе конкретной модельной хаотической динамической системы обратимый автомат, дает возможность детализировать приведенные выше критерии эквивалентности состояний, а также провести более тщательный их анализ.

Проиллюстрируем сказанное на примере автоматов, построенных в разд. 2.

Пример 14.

1. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_R \in \mathtt{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} \ominus (a \oplus h^{-1}) \circ \Delta, \\ \widetilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta, \\ \widetilde{q}_0^{(3)} = q_0^{(3)} \ominus (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta, \end{cases}$$

где Δ — решение нелинейного уравнения

$$(a \circ h \oplus 1) \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1) \circ \Delta^2 \ominus (q_0^{(3)} \circ (a \circ h \oplus 1) \oplus$$

$$\oplus q_0^{(1)} \circ (a \oplus h^{-1} \oplus h) \oplus (1 \ominus h \circ r) \circ (a \circ h^{-1} \oplus h^{-2} \oplus 1)) \circ \Delta = 0.$$

Отсюда, в частности, вытекает, что:

1) если у двух различных состояний $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_R \in \mathtt{A}_{3,4}$ совпадают вторые компоненты, то состояния $\mathbf{q}_0$ и $\widetilde{\mathbf{q}}_0$ являются неэквивалентными состояниями автомата $M_R \in \mathtt{A}_{3,4}$;

2) любые эквивалентные состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_R \in \mathtt{A}_{3,4}$ являются близнецами.

2. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_S \in \mathtt{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} (\widetilde{q}_0^{(1)} \ominus q_0^{(1)}) \oplus h \circ (\widetilde{q}_0^{(2)} \ominus q_0^{(2)}) = 0, \\ (\widetilde{q}_0^{(2)} \ominus q_0^{(2)}) \ominus h \circ (\widetilde{q}_0^{(1)} \ominus q_0^{(1)}) \oplus h \circ (\widetilde{q}_0^{(2)} \circ \widetilde{q}_0^{(3)} \ominus q_0^{(2)} \circ q_0^{(3)}) = 0, \\ \widetilde{q}_t^{(2)} \circ \widetilde{q}_t^{(3)} \ominus q_t^{(2)} \circ q_t^{(3)} = 0 \ \ (t = 1, \ldots, p^{3 \cdot k} - 3) \end{cases}$$

для всех $x_1 \ldots x_t \in \mathbb{Z}_{p^k}^t$.

Из этого утверждения, в частности, вытекает, что состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_S \in \mathtt{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} \ominus h \circ \Delta, \\ \widetilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta, \\ \widetilde{q}_0^{(3)} = q_0^{(3)} \oplus 2 \circ h \circ q_0^{(2)} \circ \Delta \oplus h \circ \Delta^2, \end{cases}$$

где Δ — решение нелинейного уравнения

$$\Delta^3 \oplus 3 \circ q_0^{(2)} \circ \Delta^2 \oplus (2 \circ (q_0^{(2)})^2 \oplus h^{-1} \circ q_0^{(3)} \oplus 1 \oplus h^{-2}) \circ \Delta = 0.$$

3. Состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_L \in \mathtt{A}_{3,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} a_2 \circ (\widetilde{q}_0^{(1)} \ominus q_0^{(1)}) \oplus (h^{-1} \ominus 1) \circ (\widetilde{q}_0^{(2)} \ominus q_0^{(2)}) \ominus (\widetilde{q}_0^{(1)} \circ \widetilde{q}_0^{(3)} \ominus q_0^{(1)} \circ q_0^{(3)}) = 0, \\ a_2 \circ (\widetilde{q}_t^{(1)} \ominus q_t^{(1)}) \ominus (\widetilde{q}_t^{(1)} \circ \widetilde{q}_t^{(3)} \ominus q_t^{(1)} \circ q_t^{(3)}) = 0 \ \ (t = 1, \ldots, p^{3 \cdot k} - 2) \end{cases}$$

для всех $x_1 \ldots x_t \in \mathbb{Z}_{p^k}^t$.

Из этого утверждения, в частности, вытекает, что состояния $\mathbf{q}_0 = (q_0^{(1)}, q_0^{(2)}, q_0^{(3)})^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_0^{(1)}, \widetilde{q}_0^{(2)}, \widetilde{q}_0^{(3)})^T$ автомата $M_L \in \mathtt{A}_{3,4}$ являются близнецами тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_0^{(1)} = q_0^{(1)} \oplus \Delta_1, \\ \widetilde{q}_0^{(2)} = q_0^{(2)} \oplus \Delta_2, \\ \widetilde{q}_0^{(3)} = q_0^{(3)} \oplus \Delta_3, \end{cases}$$

где $(\Delta_1, \Delta_2, \Delta_3)$ — решение нелинейной системы уравнений

$$\begin{cases} (h^{-1} \ominus a_1) \circ \Delta_1 \oplus a_1 \circ \Delta_2 = 0, \\ (a_2 \ominus q_0^{(3)}) \circ \Delta_1 \oplus (h^{-1} \ominus 1) \circ \Delta_2 \ominus q_0^{(1)} \circ \Delta_3 \ominus \Delta_1 \circ \Delta_3 = 0, \\ q_0^{(2)} \circ \Delta_1 \oplus q_0^{(1)} \circ \Delta_2 \oplus (h^{-1} \ominus a_3) \circ \Delta_3 \oplus \Delta_1 \circ \Delta_2 = 0. \end{cases}$$

4. Состояния $\mathbf{q}_0 = (q_1, q_0)^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_1, \widetilde{q}_0)^T$ автомата $M_H \in \mathtt{A}_{2,4}$ являются эквивалентными состояниями тогда и только тогда, когда

$$\begin{cases} a \circ (\widetilde{q}_1^2 \ominus q_1^2) \ominus b \circ (\widetilde{q}_0 \ominus q_0) = 0, \\ b \circ (\widetilde{q}_1 \ominus q_1) = 0. \end{cases}$$

Из этого утверждения, в частности, вытекает, что:

1) если $b \in \mathbb{Z}_{p^k}$ — обратимый элемент кольца $\boldsymbol{Z}_{p^k}$, то $M_H \in \mathtt{A}_{2,4}$ — приведенный автомат;

2) состояния $\mathbf{q}_0 = (q_1, q_0)^T$ и $\widetilde{\mathbf{q}}_0 = (\widetilde{q}_1, \widetilde{q}_0)^T$ автомата $M_H \in \mathtt{A}_{2,4}$ являются близнецами тогда и только тогда, когда

$$\begin{cases} \widetilde{q}_1 = q_1, \\ b \circ (\widetilde{q}_0 \ominus q_0) = 0. \end{cases}$$

В заключение отметим, что из установленных выше критериев вытекает, что для нелинейных автоматов над кольцом $\boldsymbol{Z}_{p^k}$ построение в явном виде множества состояний, эквивалентных заданному состоянию, является трудной задачей, сводимой к решению систем нелинейных уравнений над кольцом $\boldsymbol{Z}_{p^k}$. Такая особенность структуры множеств эквивалентных состояний, по-видимому, свидетельствует о том, что минимизация нелинейного автомата может существенно усложнить систему уравнений, представляющую такой автомат.

3.4. Параметрическая идентификация исследуемых моделей

С позиции теории автоматов сложность решения задачи параметрической идентификации исследуемых моделей характеризует сложность решения задачи распознавания автомата в классе, полученном вариацией значений параметров, а с позиции криптографии — сложность атаки криптоаналитика на ключ средней длительности поточного шифра, построенного на основе соответствующего обратимого автомата.

Именно с позиции криптографии целесообразно рассматривать наиболее сильную атаку криптоаналитика. В терминах теории систем такие предположения состоят в том, что:

1) экспериментатор полностью управляет входом и полностью наблюдает выход исследуемой модели;

2) экспериментатор может осуществлять над исследуемой моделью кратный эксперимент любой кратности, причем под *кратным экспериментом* понимается возможность установки исследуемой модели в любое требуемое экспериментатору состояние.

В [1, 48, 49] показано, что:

1) для автомата $M_1 \in \mathsf{A}_{n,1}$:

а) каждая из матриц C и D идентифицируется в результате n-кратного эксперимента высоты 1;

б) если $C \in \mathtt{M}_n^{\text{inv}}$, то идентификация каждой из матриц A и B сводится к решению n систем линейных уравнений n-го порядка над кольцом $\boldsymbol{Z}_{p^k}$, построенных в результате n-кратного эксперимента высоты 2;

в) если $C \in \mathtt{M}_n^{\text{non-inv}}$, то идентификация матриц A и B сводится к решению высокостепенных систем уравнений

$$C \circ (A^i \circ \mathbf{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus \mathbf{x}_i) = \mathbf{y}_{i+1} \ominus D \circ \mathbf{x}_{i+1}$$

для всех $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и $\mathbf{x}_1 \dots \mathbf{x}_i \in \mathbb{Z}_{p^k}^{n \cdot i}$ $(i = 1, \dots, p^{n \cdot k} - 1)$;

2) для автомата $M_2 \in \mathsf{A}_{n,2}$ идентификация матриц A, B, C сводится к решению высокостепенных систем уравнений

$$C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \bigoplus_{j=0}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_{j+1} \oplus \mathbf{x}_{i+1}) = \mathbf{y}_{i+1}$$

для всех $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и $\mathbf{x}_1 \dots \mathbf{x}_i \in \mathbb{Z}_{p^k}^{n \cdot i}$ $(i = 1, \dots, p^{n \cdot k} - 1)$.

В [1, 52, 53] показано, что:

1) для автомата $M_1 \in \mathtt{A}_{n,1}^{\text{inv}}$:

а) каждая из матриц G и F идентифицируется в результате n-кратного эксперимента высоты 1;

б) идентификация вектора $\mathbf{d}$ с точностью, определяемой матрицей G, осуществляется простым экспериментом длины 2;

в) идентификация матрицы E с точностью, определяемой матрицей G, осуществляется n-кратным экспериментом высоты 2;

г) идентификация матриц A, C и вектора $\mathbf{b}$ сводится к поиску начального состояния $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и входного слова $\mathbf{x}_1 \dots \mathbf{x}_l \in \mathbb{Z}_{p^k}^{n \cdot l}$ с последующим решением нелинейной системы уравнений

$$G \circ (A \circ \mathbf{q}_{t-1} \circ \mathbf{q}_{t-1}^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_{t-1} \oplus \mathbf{d} \oplus E \circ \mathbf{x}_t) = \mathbf{y}_{t+1} \ominus F \circ \mathbf{x}_{t+1} \ (t = 1, \dots, l-1);$$

2) для автомата $M_2 \in \mathtt{A}_{n,2}^{\mathrm{inv}}$:

а) идентификация матрицы E осуществляется в результате n-кратного эксперимента высоты 1, причем множество возможных кандидатов на матрицу E определяется множеством решений $(G, \mathbf{d})$ уравнения

$$G \circ \mathbf{d} = \mathbf{y}_1;$$

б) идентификация матриц A, C и вектора $\mathbf{b}$ сводится к поиску начального состояния $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и входного слова $\mathbf{x}_1 \dots \mathbf{x}_l \in \mathbb{Z}_{p^k}^{n \cdot l}$ с последующим решением нелинейной системы уравнений

$$G \circ (A \circ \mathbf{q}_t \circ \mathbf{q}_t^T \circ \mathbf{b} \oplus C \circ \mathbf{q}_t \oplus \mathbf{d} \oplus E \circ \mathbf{x}_{t+1}) = \mathbf{y}_{t+1} \ \ (t = 0, 1, \dots, l-1).$$

Ясно, что дополнительный учет факторов, вытекающих из структуры уравнений, определяющих обратимый автомат, построенный на основе конкретной модельной хаотической динамической системы, дает возможность провести более тщательный анализ сложности решения задачи параметрической идентификации.

Пример 15.

1. В [1, 55] показано, что:

1) для каждого из автоматов $M_{\mathrm{GH}} \in \mathsf{A}_{\mathrm{GH}}$ и $M_{\mathrm{FR}} \in \mathsf{A}_{\mathrm{FR}}$ идентификация параметров $\alpha_1, \alpha_2, \alpha_3$ осуществляется простым экспериментом длины 1;

2) для автомата $M_{\mathrm{GH}} \in \mathsf{A}_{\mathrm{GH}}$:

а) идентификация параметров b и c осуществляется кратным экспериментом кратности 2 и высоты 1;

б) для любого простого числа $p > 3$ идентификация параметров a и d сводится к решению системы двух линейных уравнений, сформированной в результате простого эксперимента длины 1;

3) для автомата $M_{\mathrm{FR}} \in \mathsf{A}_{\mathrm{FR}}$ для любого простого числа $p > 3$ идентификация параметров a и ζ сводится к решению системы двух уравнений, сформированной в результате простого эксперимента длины 1.

2. Для автомата $M_R \in \mathtt{A}_{3,4}$ задача параметрической идентификации решается следующим образом.

Подав на автомат $(M_R, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0, 1, 0)^T$, входной символ $x_1 = 0$, получим

$$h = \ominus y_1.$$

Подав на автомат $(M_R, \mathbf{0})$ входной символ $x_1 = 1$, получим

$$d = \ominus h^{-1} \circ y_1.$$

Подав на автомат $(M_R, \mathbf{0})$ входное слово $x_1 x_2 = 00$, получим

$$b = \ominus h^{-2} \circ y_2.$$

Подав на автомат $(M_R, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0, 0, 1)^T$, входное слово $x_1 x_2 = 00$, получим

$$r = \ominus h^{-2} \circ y_2 \oplus 2 \circ h^{-1} \ominus b.$$

Подав на автомат $(M_R, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0, 1, 0)^T$, входное слово $x_1 x_2 = 00$, получим

$$a = \ominus 2 \circ h^{-1} \ominus b \ominus h^{-2} \circ y_2.$$

3. Для автомата $M_S \in \mathtt{A}_{3,4}$ задача параметрической идентификации решается следующим образом.

Подав на автомат $(M_S, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0,1,0)^T$, входной символ $x_1 = 0$, получим

$$h = y_1.$$

Подав на автомат $(M_S, \mathbf{0})$ входной символ $x_1 = 1$, получим

$$a = \ominus h^{-1} \circ y_1.$$

4. Для автомата $M_L \in \mathtt{A}_{3,4}$ задача параметрической идентификации решается следующим образом.

Подав на автомат $(M_L, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0,1,0)^T$, входной символ $x_1 = 0$, получим

$$h = 1 \ominus y_1.$$

Подав на автомат $(M_L, \mathbf{0})$ входной символ $x_1 = 1$, получим

$$a = \ominus h^{-1} \circ y_1.$$

Подав на автомат $(M_L, \mathbf{q}_0)$, где $\mathbf{q}_0 = (1,0,0)^T$, входное слово $x_1x_2 = 00$, получим

$$a_2 = h^{-1} \circ y_1$$

и

$$y_2 = (1 \ominus h) \circ h \circ a_2 \oplus h \circ a_2 \circ (1 \ominus h \circ a_1).$$

Из этого уравнения определяется множество допустимых значений параметра a_1.

Подав на автомат $(M_L, \mathbf{q}_0)$, где $\mathbf{q}_0 = (1,0,1)^T$, входное слово $x_1x_2 = 00$, получим

$$y_2 = (1 \ominus h) \circ h \circ (a_2 \ominus 1) \oplus h \circ (1 \ominus h \circ a_1) \circ (a_2 \oplus h \circ a_3 \ominus 1).$$

Из этого уравнения определяется множество допустимых значений параметра a_3.

5. Для автомата $M_H \in \mathtt{A}_{2,4}$ задача параметрической идентификации решается следующим образом.

Подав на автомат $(M_H, \mathbf{0})$ входной символ $x_1 = 1$, получим

$$c = y_1 \ominus 1.$$

Подав на автомат $(M_H, \mathbf{q}_0)$, где $\mathbf{q}_0 = (0,1)^T$, входной символ $x_1 = 0$, получим

$$b = 1 \ominus y_1.$$

Подав на автомат $(M_H, \mathbf{q}_0)$, где $\mathbf{q}_0 = (1,0)^T$, входной символ $x_1 = 0$, получим

$$a = 1 \ominus y_1.$$

В заключение отметим, что полученные результаты дают возможность разбить на следующие два класса параметры, определяющие ключ средней длительности для поточного шифра, построенного на основе обратимого автомата над кольцом $\boldsymbol{Z}_{p^k}$.

К 1-му классу относятся параметры, идентификация которых не составляет большого труда. Для обеспечения секретности значений этих параметров бесполезно применять существенные меры.

Ко 2-му классу относятся параметры, идентификация которых является трудной задачей. Именно на обеспечение секретности значений этих параметров и следует направить все усилия.

3.5. Идентификация начального состояния исследуемых моделей

Задача идентификации начального состояния конечного автомата — одна из модельных задач теории экспериментов с конечными автоматами (см., напр., [59]). В [60] показано, что с позиции теории систем эта задача представляет собой анализ *наблюдаемости* динамической системы. В [61] показано, что даже для слабоинициальных абстрактных автоматов с двухбуквенным входным алфавитом длина минимального диагностического слова может являться субэкспонентой от размера автоматной таблицы. Отсюда вытекает (см., напр., [62]), что заведомо имеет субэкспоненциальную временную сложность любой алгоритм поиска минимального диагностического слова, который за единицу времени восстанавливает фрагмент диагностического слова, длина которого — полином от размера автоматной таблицы.

С позиции криптографии сложность решения задачи идентификации начального состояния автомата характеризует сложность атаки криптоаналитика на сеансовый ключ поточного шифра, построенного на основе соответствующего обратимого автомата.

Охарактеризуем сложность решения задачи идентификации начального состояния посредством простого диагностического эксперимента для поточного шифра, построенного на основе обратимого автомата над кольцом $\boldsymbol{Z}_{p^k}$. При этом естественно предположить, что *криптоаналитику известны параметры исследуемого автомата, но он не может управлять этими параметрами.*

Замечание 5. Такие предположения характеризуют внутреннюю сложность задачи идентификации начального состояния автомата. При их ослаблении сложность решения рассматриваемой задачи существенно возрастает, так как возникает тот или иной вариант задачи построения контрольного эксперимента с автоматом. Если же предположить, что экспериментатор может управлять параметрами, то возникает совершенно иная новая задача, а именно: идентификация начального состояния автомата посредством кратного эксперимента на основе вариации его параметров.

Исследование этой задачи, по своей сути, представляет собой разработку методов дифференциального и интегрального анализа для словарных функций, реализуемых инициальными обратимыми автоматами. Насколько известно автору, решение этой задачи отсутствует в настоящее время.

В [1, 48, 49] показано, что:

1) для автомата $M_1 \in \mathsf{A}_{n,1}$:

а) если $C \in \mathtt{M}_n^{\text{inv}}$, то идентификация начального состояния сводится к решению системы линейных уравнений над кольцом $\boldsymbol{Z}_{p^k}$, полученной в результате простого эксперимента длины 1;

б) если $C \in \mathtt{M}_n^{\text{non-inv}}$, то идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к решению при известных матрицах A, B, C, D систем линейных уравнений

$$C \circ (A^i \circ \mathbf{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus \mathbf{x}_i) = \mathbf{y}_{i+1} \ominus D \circ \mathbf{x}_{i+1}$$

для всех $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbb{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$;

2) для автомата $M_2 \in \mathsf{A}_{n,2}$:

а) если $C \in \mathtt{M}_n^{\mathrm{inv}}$, то идентификация начального состояния сводится к решению системы линейных уравнений над кольцом $\boldsymbol{Z}_{p^k}$, полученной в результате простого эксперимента длины 1;

б) если $A, C \in \mathtt{M}_n^{\text{non-inv}}$, то идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к решению при известных матрицах A, B, C систем линейных уравнений

$$C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \bigoplus_{j=0}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_{j+1} \oplus \mathbf{x}_{i+1}) = \mathbf{y}_{i+1}$$

для всех $\mathbf{q}_0 \in \mathbb{Z}_{p^k}^n$ и $\mathbf{x}_1 \ldots \mathbf{x}_i \in \mathbb{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

В [1, 52, 53] показано, что для автомата $M_1 \in \mathtt{A}_{n,1}^{\mathrm{inv}} \cup \mathtt{A}_{n,2}^{\mathrm{inv}} \cup \mathtt{A}_{n,3} \cup \mathtt{A}_{n,4}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску входного слова заранее неизвестной длины и решению высокостепенных систем нелинейных уравнений над кольцом $\boldsymbol{Z}_{p^k}$, полученных в результате подачи этого слова на исследуемый автомат.

В [1, 55] показано, что:

1) для автомата $M_{\mathrm{GH}} \in \mathsf{A}_{\mathrm{GH}}$ идентификация начального состояния сводится к последовательности решений систем трех кубических уравнений над кольцом $\boldsymbol{Z}_{p^k}$;

2) для автомата $M_{\mathrm{FR}} \in \mathsf{A}_{\mathrm{FR}}$ идентификация начального состояния сводится к последовательности решений задач дискретного логарифмирования над кольцом $\boldsymbol{Z}_{p^k}$.

В заключение отметим, что высокая сложность решения задачи идентификации начального состояния обратимых автоматов над кольцом $\boldsymbol{Z}_{p^k}$ свидетельствует о том, что криптоаналитик столкнется с высокой сложностью идентификации секретного сеансового ключа при атаке на шифры, построенные на основе таких автоматов.

3.6. Вариация поведения исследуемых моделей

В замечании 5 было отмечено, что с позиции криптографии исследование вариации поведения словарной функции, реализуемой инициальным обратимым автоматом, является актуальной при разработке методов дифференциального и интегрального анализа, предназначенных для исследования сложности атаки криптоаналитика на секретный ключ поточного шифра, построенного на основе соответствующего обратимого автомата.

Проиллюстрируем некоторые особенности решения этой задачи на примере автомата $M_1 \in \mathsf{A}_{n,1}$ (см., напр., [1, 48, 49]).

Пусть

$$(M_1, \mathbf{q}_0) : \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+), \tag{37}$$

$$(\widehat{M}_1, \widehat{\mathbf{q}}_0) : \begin{cases} \widehat{\mathbf{q}}_{t+1} = \widehat{A} \circ \widehat{\mathbf{q}}_t \oplus \widehat{B} \circ \widehat{\mathbf{x}}_{t+1}, \\ \widehat{\mathbf{y}}_{t+1} = \widehat{C} \circ \widehat{\mathbf{q}}_t \oplus \widehat{D} \circ \widehat{\mathbf{x}}_{t+1}, \end{cases} \quad (t \in \mathbb{Z}_+). \tag{38}$$

Положим

$$\widehat{A} = A \oplus \Delta A, \ \widehat{B} = B \oplus \Delta B, \ \widehat{C} = C \oplus \Delta C, \ \widehat{D} = D \oplus \Delta D,$$

$$\widehat{\mathbf{q}}_{t+1} = \mathbf{q}_{t+1} \oplus \Delta\mathbf{q}_{t+1}, \ \widehat{\mathbf{q}}_t = \mathbf{q}_t \oplus \Delta\mathbf{q}_t, \ \widehat{\mathbf{x}}_{t+1} = \mathbf{x}_{t+1} \oplus \Delta\mathbf{x}_{t+1}, \ \widehat{\mathbf{y}}_{t+1} = \mathbf{y}_{t+1} \oplus \Delta\mathbf{y}_{t+1}$$

и вычтем из уравнений системы (38) уравнения системы (37). Получим

$$\begin{cases} \Delta\mathbf{q}_{t+1} = (A \circ \Delta\mathbf{q}_t \oplus B \circ \Delta\mathbf{x}_{t+1}) \oplus (\Delta A \circ \mathbf{q}_t \oplus \Delta B \circ \mathbf{x}_{t+1}) \oplus \\ \qquad\qquad \oplus (\Delta A \circ \Delta\mathbf{q}_t \oplus \Delta B \circ \Delta\mathbf{x}_{t+1}), \\ \Delta\mathbf{y}_{t+1} = (C \circ \Delta\mathbf{q}_t \oplus D \circ \Delta\mathbf{x}_{t+1}) \oplus (\Delta C \circ \mathbf{q}_t \oplus \Delta D \circ \mathbf{x}_{t+1}) \oplus \\ \qquad\qquad \oplus (\Delta C \circ \Delta\mathbf{q}_t \oplus \Delta D \circ \Delta\mathbf{x}_{t+1}), \end{cases} \quad (t \in \mathbb{Z}_+). \qquad (39)$$

Таким образом, анализ вариации поведения словарной функции, реализуемой инициальным автоматом $M_1 \in \mathsf{A}_{n,1}$, сводится к совместному исследованию систем уравнений (37)–(39).

Нетрудно убедиться в том, что для нелинейных автоматов над кольцом $\boldsymbol{Z}_{p^k}$ аналог системы уравнений (39) является значительно более громоздким.

Отсюда вытекает, что, по всей видимости, единственным способом анализа вариации поведения словарной функции, реализуемой инициальным автоматом над кольцом $\boldsymbol{Z}_{p^k}$, является компьютерное моделирование с использованием той или иной системы символьных вычислений.

3.7. Множество неподвижных точек исследуемых моделей

Неподвижной точкой словарной функции

$$f : X^+ \to X^+$$

называется такое слово $u \in X^+$, что

$$f(u) = u.$$

С позиции криптографии актуальность исследования структуры множеств неподвижных точек словарных функций, реализуемых обратимыми автоматами над кольцом $\boldsymbol{Z}_{p^k}$, обусловлена тем, что учет этой структуры дает возможность разработать меры по предотвращению ситуации, когда критический фрагмент открытого текста преобразуется в себя поточным шифром, построенным на основе такого автомата.

Рассмотрим результаты исследования структуры множеств неподвижных точек словарных функций, представленные в [1, 55, 63].

Обозначим через $S_{fxd}(M, \mathbf{q}_0)$ $(M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2} \cup \mathsf{A}_{\mathrm{GH}} \cup \mathsf{A}_{\mathrm{FR}})$ множество всех неподвижных точек словарной функции, реализуемой инициальным автоматом $(M, \mathbf{q}_0)$. Положим

$$S^{(t)}_{fxd}(M, \mathbf{q}_0) = S_{fxd}(M, \mathbf{q}_0) \cap (\mathbb{Z}^n_{p^k})^t \ \ (t \in \mathbb{N}).$$

Так как

$$S^{(t+1)}_{fxd}(M, \mathbf{q}_0) \subseteq \{\mathbf{ux} | \mathbf{u} \in S^{(t)}_{fxd}(M, \mathbf{q}_0), \mathbf{x} \in \mathbb{Z}^n_{p^k}\} \ \ (t \in \mathbb{N}),$$

то достаточно исследовать структуру множества $S^{(1)}_{fxd}(M, \mathbf{q}_0)$.

В [1, 63] показано, что:

1) если $M \in \mathsf{A}_{n,1}$, то $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ тогда и только тогда, когда $\mathbf{x}$ — решение уравнения

$$(I \ominus D) \circ \mathbf{x} = C \circ \mathbf{q}_0;$$

2) если $M \in \mathsf{A}_{n,2}$, то $\mathbf{x} \in S^{(1)}_{fxd}(M, \mathbf{q}_0)$ тогда и только тогда, когда $\mathbf{x}$ — решение уравнения

$$(I \ominus C \circ B) \circ \mathbf{x} = C \circ A \circ \mathbf{q}_0.$$

Отсюда вытекает, что:

1) для любого автомата $M \in \mathsf{A}_{n,1} \cup \mathsf{A}_{n,2}$ множество $S_{fxd}(M, \mathbf{0})$ непусто;

2) для любого автомата $M \in \mathsf{A}_{n,1}$, если $I \ominus D \in \mathtt{M}_n^{\mathrm{inv}}$, то $S_{fxd}(M, \mathbf{q}_0)$ — бесконечное множество, причем $S_{fxd}^{(t)}(M, \mathbf{q}_0)$ — одноэлементное множество для всех $t \in \mathbb{N}$;

3) для любого автомата $M \in \mathsf{A}_{n,2}$, если $I \ominus C \circ B \in \mathtt{M}_n^{\mathrm{inv}}$, то $S_{fxd}(M, \mathbf{q}_0)$ — бесконечное множество, причем $S_{fxd}^{(t)}(M, \mathbf{q}_0)$ — одноэлементное множество для всех $t \in \mathbb{N}$.

В [55] показано, что:

1) если $M \in \mathsf{A}_{\mathrm{GH}}$, то $x \in S_{fxd}^{(1)}(M, \mathbf{q}_0)$ тогда и только тогда, когда x — решение системы уравнений

$$\begin{cases} (1 \ominus \alpha_1) \circ x = q_0^{(1)} \circ (d \oplus a \circ (q_0^{(1)})^2 \oplus b \circ (q_0^{(2)})^2 \oplus c \circ (q_0^{(3)})^2, \\ (1 \ominus \alpha_2) \circ x = q_0^{(2)} \circ (d \oplus c \circ (q_0^{(1)})^2 \oplus a \circ (q_0^{(2)})^2 \oplus b \circ (q_0^{(3)})^2, \\ (1 \ominus \alpha_3) \circ x = q_0^{(3)} \circ (d \oplus b \circ (q_0^{(1)})^2 \oplus c \circ (q_0^{(2)})^2 \oplus a \circ (q_0^{(3)})^2; \end{cases}$$

2) если $M \in \mathsf{A}_{\mathrm{FR}}$, то $x \in S_{fxd}^{(1)}(M, \mathbf{q}_0)$ тогда и только тогда, когда x — решение системы уравнений

$$\begin{cases} (1 \ominus \alpha_1) \circ x = f(q_0^{(1)}) \circ \zeta^{q_0^{(3)}}, \\ (1 \ominus \alpha_2) \circ x = f(q_0^{(2)}) \circ \zeta^{q_0^{(1)}}, \\ (1 \ominus \alpha_3) \circ x = f(q_0^{(3)}) \circ \zeta^{q_0^{(2)}}. \end{cases}$$

Из этих уравнений несложно получить критерии непустоты множества $S_{fxd}(M, \mathbf{q}_0)$ ($M \in \mathsf{A}_{\mathrm{GH}} \cup \mathsf{A}_{\mathrm{FR}}$) в случае, когда все элементы $1 \ominus \alpha_i$ ($i = 1, 2, 3$) являются обратимыми элементами кольца $\boldsymbol{Z}_{p^k}$.

В заключение отметим, что хотя учет структуры множества неподвижных точек словарных функций, реализуемых обратимыми автоматами над кольцом $\boldsymbol{Z}_{p^k}$, дает возможность разработать меры по предотвращению ситуации, когда критический фрагмент открытого текста преобразуется в себя поточным шифром, построенным на основе такого автомата, сама разработка этих мер является достаточно сложной задачей.

Выше был рассмотрен фрагмент теории автоматов над конечным кольцом с позиции их возможного использования при построениии поточных шифров. Некоторые задачи, требующие дополнительного анализа, были охарактеризованы выше.

Если в качестве элементов секретного ключа кроме параметров автомата и начального состояния автомата использовать также числа p и k, то при атаке, направленной на идентификацию секретного ключа, криптоаналитик столкнется, по-видимому, с необходимостью решения варианта проблемы тождества слов в свободных полугруппах. Ясно, что вычислительная стойкость таких поточных шифров существенно возрастет. Однако при этом возникает следующая проблема.

Специального исследования требует сравнительный анализ скорости поточных шифров, построенных на основе обратимых автоматов над кольцом $\boldsymbol{Z}_{p^k}$, со скоростью существующих поточных шифров. Результаты компьютерного моделирования с использованием стандартных программ, реализующих операции в конечном кольце, показывают, что скорость шифров, построенных на основе обратимых автоматов над кольцом $\boldsymbol{Z}_{p^k}$, существенно падает с ростом значений p и k.

Поэтому при использовании обратимых автоматов над кольцом $\boldsymbol{Z}_{p^k}$ для построения поточных шифров, по-видимому, придется существенно использовать аппаратно-программные реализации операций над фиксированным конечным кольцом, либо выделять мнотонно возрастающую подпоследовательность k_i ($i \in \mathbb{N}$) значений числа k

и разрабатывать быстрые алгоритмы реализации операций над последовательностью колец $\boldsymbol{Z}_{p^{k_i}}$ $(i \in \mathbb{N})$.

ЛИТЕРАТУРА

1. *Скобелев В. В., Скобелев В. Г.* Анализ шифрсистем. Донецк: ИПММ НАН Украины, 2009. 479 с.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
3. *Скобелев В. Г., Сперанский Д. В.* Идентификация булевых функций методами линейной алгебры // Украинский математический журнал. 1995. Т. 47. № 2. С. 260–268.
4. *Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В.* Криптография. Скоростные шифры. СПб: БХВ-Петербург, 2002. 496 с.
5. *Huffman D. A.* Canonical forms for information-lossless finite state logical machines // IRE Transactions Circuit Theory. Special Supplment. 1959. V. CT-6. P. 41–59.
6. *Even S.* On information-lossless automata of finite order // IEEE Transactions on Electronic Computers. 1965. V. C-14. No. 4. P. 561–569.
7. *Курмит А. А.* Автоматы без потери информации конечного порядка. Рига: Зинатне, 1972. 266 с.
8. *Гилл А.* Линейные последовательностные машины. М.: Наука, 1974. 298 с.
9. *Фараджев Р. Г.* Линейные последовательностные машины. М.: Сов. радио, 1975. 248 с.
10. *Агибалов Г. П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Изв. АН СССР. Техническая кибернетика. 1970. № 3. С. 99–108.
11. *Агибалов Г. П., Юфит Я. Г.* О простых экспериментах для линейных инициальных автоматов // Автоматика и вычислительная техника. 1972. № 2. С. 17–19.
12. *Сперанский Д. В.* Эксперименты с линейными и билинейными конечными автоматами. Саратов: СГУ, 2004. 144 с.
13. *Глушков В. М.* Синтез цифровых автоматов. М.: Физматлит, 1962. 476 с.
14. *Бабаш А. В.* Приближенные модели конечных автоматов // Обозрение прикладной и промышленной математики. 2005. Т. 12. Вып. 2. С. 108–117.
15. *Скобелев В. В.* Построение стойких к частотному анализу криптосистем на основе регулярных комбинаторных структур // Искусственный интеллект. 2004. № 1. С. 88–96.
16. *Скобелев В. В.* Разрушение частот букв на основе регулярных комбинаторных структур // Труды ИПММ НАНУ. 2008. Т. 17. С. 185–193.
17. *Скобелев В. Г., Зайцева Э. Е.* Шифры на основе фракталов // Труды ИПММ НАНУ. 2006. Т. 12. С. 63–68.
18. *Зайцева Э. Е., Скобелев В. Г.* Шифр на основе отображения Мандельброта // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 107–113.
19. *Шнайер Б.* Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке СИ. М.: Триумф, 2003. 816 с.
20. *Скобелев В. Г.* Локальные алгоритмы на графах. Донецк: ИПММ НАН Украины, 2003. 217 с.
21. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982. 384 с.
22. *Стенли Р.* Перечислительная комбинаторика. М.: Мир, 1990. 440 с.
23. *Скобелев В. В.* Точная формула для числа обратимых матриц над конечным кольцом // Труды ИПММ НАНУ. 2009. Т. 18. С. 63–68.
24. *Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В.* Математические и компьютерные основы криптологии. Минск: Новое знание, 2003. 382 с.

25. *Скобелев В. Г., Зайцева Э. Е.* Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. 2008. № 5. С. 12–24.
26. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы. М.: Мир, 1988. 316 с.
27. *Коблиц Н.* Курс теории чисел и криптография. М.: Научное изд-во ТВП, 2001. 262 с.
28. *Горчинский В. Г.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. Т. 1. М.: Научное изд-во ТВП, 1997. С. 67–84.
29. *Lynch N.* I/O automaton models for proofs for shared-key communication systems // Proceedings of the 12th IEEE Computer Security Foundations Workshop (CSFW'99). Mordana, Italy, 1999. 16 p.
30. *Девянин П. Н.* Модели безопасности компьютерных систем. М.: Издательский центр «Академия», 2005. 144 с.
31. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
32. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2006. 824 с.
33. *Шустер Г.* Детерминированный хаос. М.: Мир, 1985. 255 с.
34. *Кузнецов С. П.* Динамический хаос. М.: Физматлит, 2001. 296 с.
35. *Дмитриев А. С.* Запись и восстановление информации в одномерных динамических системах // Радиотехника и радиоэлектроника. 1991. Т. 36. № 1. С. 101–108.
36. *Дмитриев А. С.* Хаос и обработка информации в одномерных динамических системах // Радиотехника и радиоэлектроника. 1993. Т. 38. № 1. С. 1–24.
37. *Андреев Ю. В., Бельский Ю. Л., Дмитриев А. С.* Запись и восстановление информации с использованием устойчивых циклов двумерных и многомерных отображений // Радиотехника и радиоэлектроника. 1994. Т. 39. № 4. С. 114–123.
38. *Дмитриев А. С., Старков С. О.* Передача сообщений с использованием хаоса и классическая теория информации // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1998. № 11. С. 4–32.
39. *Андреев Ю. В., Дмитриев А. С., Куминов Д. А.* Хаотические процессоры // Радиотехника и радиоэлектроника. 1997. Т. 42. № 10. С. 50–79.
40. *Костенко П. Ю., Сиващенко С. И., Антонов А. В., Костенко Т. П.* Применение методов хаотической динамики для обеспечения информационной скрытности в коммуникационных системах и сетях // Изв. вузов. Радиоэлектроника. 2006. Т. 49. № 3. С. 63–70.
41. *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.
42. *Костенко П. Ю., Антонов А. В., Костенко Т. П.* Развитие концепции односторонних функций для систем криптографической защиты информации с использованием достижений хаотической динамики // Кибернетика и системный анализ. 2006. № 6. С. 136–146.
43. *Grassi G., Mascolo S.* Hyperchaos-based secure communications by observer design // Proceedings of the 7th International Workshop on Nonlinear Dynamics of Electronic Systems, Ronne, Denmark, July 15–17, 1999. P. 157–160.
44. Proceedings of the 7th International Workshop on Nonlinear Dynamics of Electronic Systems, Ronne, Denmark, July 15–17, 1999. Technical University of Denmark, Technical University of Dresden, 1999. 294 p.
45. Synchronization: Theory and applications, Yalta, Crimea, Ukraine, May 19 – June 1, 2002. NATO Science Series: II. Mathematics, Physics and Chemistry. V. 109. Kluver Academic Publishers, 2002. 258 p.

46. *Alia M. A., Samsudin A. B.* New key exchange protocol based on Mandelbrot and Julia fractal sets // IJCSNS International Journal of Computer Science and Network Security. 2007. V. 7. No. 2. P. 302–307.
47. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. Т. 1. М.: Научное изд-во ТВП, 1997. С. 139–202.
48. *Скобелев В. В.* Исследование структуры множества линейных БПИ-автоматов над кольцом $\boldsymbol{Z}_{p^k}$ // Доповіді НАНУ. 2007. №10. С. 44–49.
49. *Скобелев В. В.* Анализ структуры класса линейных автоматов над кольцом $\boldsymbol{Z}_{p^k}$ // Кибернетика и системный анализ. 2008. №3. С. 60–74.
50. *Скобелев В. В.* Характеристики линейных одномерных автоматов с лагом l над конечным кольцом // Труды ИПММ НАНУ. 2008. Т. 16. С. 190–196.
51. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) // Труды по дискретной математике. Т. 2. М.: Научное изд-во ТВП, 1998. С. 191–222.
52. *Скобелев В. Г.* Нелинейные автоматы над конечным кольцом $\boldsymbol{Z}_{p^k}$ // Кибернетика и системный анализ. 2006. №6. С. 29–42.
53. *Скобелев В. Г.* О некоторых свойствах нелинейных БПИ-автоматов над кольцом $\boldsymbol{Z}_{p^k}$ // Прикладная радиоэлектроника. 2007. Т. 6. №2. С. 288–299.
54. *Скобелев В. В.* Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Труды ИПММ НАНУ. 2005. Т. 10. С. 184–189.
55. *Скобелев В. В.* О двух типах нелинейных автоматов над конечным кольцом $\boldsymbol{Z}_{p^k}$ // Кибернетика и системный анализ. 2009. №4. С. 57–68.
56. *Ashwin P., Ruclidge A. M., Sturman R.* Cyclic attractors of coupled cell systems and dynamics with symmetry // Synchronization: Theory and applications, Yalta, Crimea, Ukraine, May 19 – June 1, 2002. NATO Science Series: II. Mathematics, Physics and Chemistry. V. 109. Kluver Academic Publishers, 2002. P. 5–23.
57. *Голод П. И., Климык А. У.* Математические основы теории симметрий. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 528 с.
58. *Скобелев В. В.* Анализ комбинаторно-алгебраических моделей инъективных дискретных преобразователей информации: дис. ... канд. физ.-мат. наук. 01.05.01 — теоретические основы информатики и кибернетики. Донецк: ИПММ НАН Украины. 2009. 128 с.
59. *Гилл А.* Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.
60. *Горяшко А. П.* Проектирование легко тестируемых дискретных устройств // Автоматика и телемеханика. 1984. №7. С. 5–35.
61. *Скобелев В. Г.* Об оценках длин диагностических и возвратных слов для автоматов // Кибернетика. 1987. №4. С. 114–116.
62. *Скобелев В. Г.* Анализ дискретных систем. Донецк: ИПММ НАН Украины, 2002. 172 с.
63. *Скобелев В. В.* Характеристика неподвижных точек линейных автоматов над конечным кольцом // Прикладная дискретная математика. 2008. №1(1). С. 126–130.