6. Гихман И.И., Скороход А.В. Стохастические дифференциальные уравнения. – Киев: Наукова думка, 1968. – 354 с.
7. Далецкий Ю.Л., Крейн М.Г. Устойчивость решений дифференциальных уравнений в банаховом пространстве. – М.: Наука, 1970. – 536 с.
8. Данфорд Н., Шварц Дж.Т. Линейные операторы. 1. Общая теория. – М.: НЛ, 1962. – 895 с.
9. Дуб Дж.Л. Вероятностные процессы. – М.: НЛ, 1965. – 605 с.
10. Дынкин Е.Б. Марковские процессы. – М.: Физматгиз, 1963. – 859 с.
11. Жакод Ж., Ширяев А.Н. Предельные теоремы для случайных процессов. – Т.1. – М.: Наука, 1994. – 544 с.
12. Жакод Ж., Ширяев А.Н. Предельные теоремы для случайных процессов. – Т.2. – М.: Наука, 1996. – 628 с.
13. Кац И.Я. Метод функций Ляпунова в задачах устойчивости и стабилизации систем случайной структуры. – Екатеринбург: Изд-во Уральской госакадемии путей сообщения, 1998. – 222 с.
14. Колмановский В.Б., Носов В.Р. Устойчивость и периодические режимы регулируемых систем с последействием. – М. Наука, 1981. – 448 с.
15. Скороход А.В. Асимптотические методы теории стохастических дифференциальных уравнений. – Киев.: Наукова думка, 1987. – 328 с.
16. Хасьминский Р.З. Устойчивость систем дифференциальных уравнений при случайных возмущениях их параметров. – М.: Наука, 1969. – 367 с.
17. Хейл Дж . Теория функционально-дифференциальных уравнений. – М.: Мир, 1984. – 421 с.
18. Царьков Е.Ф. Случайные возмущения дифференциально-функциональных уравнений. – Рига: Зинатне, 1989. – 429 с.
19. Korolyuk V.S., Limnions W. Stochastic systems in merging Phase Space. – London: World Scientific, 2006. – 331 p.

Надійшла до редколегії 15.05.14

Никитин А. В. канд. физ.-мат. наук
Черновицкий национальный университет, Черновцы

МОМЕНТНЫЕ УРАВНЕНИЯ ДЛЯ ЛИНЕЙНЫХ СТОХАСТИЧЕСКИХ УРАВНЕНИЙ СО СЛУЧАЙНЫМИ КОЭФФИЦИЕНТАМИ В ГИЛЬБЕРТОВОМ ПРОСТРАНСТВЕ

Посвящена исследованию устойчивости решений линейных стохастических дифференциальных уравнений в гильбертовом пространстве с помощью моментных уравнений.
Ключевые слова: Гильбертовое пространство, устойчивость, дифференциальные уравнения

Nikitin A. V. Ph.D. Physics and Mathematics
Chernivtsi National University, Chernivtsi

MOMENT EQUATION FOR LINEAR STOCHASTIC DIFFERENTIAL EQUATIONS WITH RANDOM COEFFICIENTS IN A HILBERT SPACE

This article is devoted to research of stability of decisions of linear stochastic differential equations in Hilbert Space with the help of moment equations.
Keywords: Hilbert space, stability, differential equations

УДК 512.7+519.7+681.3

В. В. Скобелев, канд. физ.-мат. наук,
В. Г. Скобелев, д-р физ.-мат. наук, д-р техн. наук, проф.,
ИПММ НАН Украины, Донецк

МЕТОДЫ АНАЛИЗА АВТОМАТНО-АЛГЕБРАИЧЕСКИХ МОДЕЛЕЙ

В работе рассмотрены методы анализа автоматных моделей, определенных над конечными кольцами. Для управляемых логических операций исследована сложность обнаружения и локализации неисправностей в процессе off-line контроля их аппаратных реализаций, а также вычислительная стойкость семейств легко-вычислимых перестановок. Исследована задача построения имитационной модели для семейства автоматов, определенных системами уравнений над конечными кольцами, а также вычислительная стойкость семейства хэш-функций, определяемых автоматом без выхода. Исследованы автоматы, определенные на многообразии над конечным кольцом, в том числе, автоматы, определенные на эллиптической кривой над конечным полем.

Ключевые слова: конечные автоматы, конечные кольца, многообразия, эллиптические кривые.

Введение. Развитие информационных технологий на современном этапе, их проникновение практически во все сферы деятельности человечества выдвинули защиту информации в число одной из наиболее актуальных проблем. От ее успешного решения зависит не только благополучие индивидуумов, организаций и государств, но часто и их существование. Именно по этой причине в течение последних тридцати лет всем мире прилагаются значительные усилия в области разработки математических основ криптографии (достаточно полный анализ используемых в криптографии моделей и методов содержится в [1–3]). Последняя, в свою очередь, оказывает существенное влияние на переосмысление задач, решаемых в классических областях математики (теория чисел, теория конечных алгебраических систем, алгебраическая геометрия и т.д.) и компьютерных наук (теория булевых функций, теория автоматов, теория алгоритмов и т.д.). В частности, на первый план выходит анализ вычислительной стойкости алгоритмов преобразования информации [4].

Переход криптографии от комбинаторных моделей к комбинаторно-алгебраическим моделям стимулировал создание нового раздела алгебраической теории автоматов, объект исследования которого – автоматы, определенные на конечных алгебраических структурах, а предмет исследования – анализ вычислительной стойкости отображений, реализуемых исследуемыми инициальными автоматами. Отметим, что такой анализ включает в себя в качестве основных задачи идентификации начального состояния автомата и параметрической идентификации автомата, принадлежащего заданному семейству, а также исследование множества неподвижных точек автоматных отображений.

В настоящей работе дан обзор результатов исследований автоматно-алгебраических моделей, полученных в ИПММ НАН Украины.

1. Управляемые логические операции. Эти операции являются основой построения скоростных блочных шифров [5]. Формальная модель управляемой перестановочной (соответственно, подстановочной) операции – такое отображение $\mathbf{y}=\mathbf{f}(\mathbf{x},\mathbf{v})$, ($\mathbf{x}\in\mathbf{E}^n$, $\mathbf{v}\in\mathbf{E}^m$, $\mathbf{y}\in\mathbf{E}^l$, $\mathbf{E}=\{0,1\}$), что $n=l$ (соответственно, $n\le l$) и для каждого $\mathbf{v}_0\in\mathbf{E}^m$ отображение $\mathbf{g}_{\mathbf{v}_0}:\mathbf{E}^n\to\mathbf{E}^l$, где $\mathbf{g}_{\mathbf{v}_0}(\mathbf{x})=\mathbf{f}(\mathbf{x},\mathbf{v}_0)$ – перестановка компонент вектора $\mathbf{x}\in\mathbf{E}^n$ (соответственно, инъекция). Вектор $\mathbf{x}\in\mathbf{E}^n$ – информационный, а вектор $\mathbf{v}\in\mathbf{E}^m$ – управляющий.

Так как управляемые логические операции могут быть реализованы аппаратно, то естественно возникают задачи off-line обнаружения и локализации неисправностей комбинационной схемы C, реализующей ту или иную управляемую логическую операцию. Эти задачи исследованы в [6–12]. Основные результаты состоят в следующем.

Пусть C – комбинационная схема, реализующая управляемую логическую операцию. Сложность $\mu(\tilde{N})$ схемы C определим как общее число ножек всех ее элементов, неисправность схемы C – как одиночную константную неисправность ножки или как короткое замыкание двух соседних ножек элемента, сложность $\mu_a(C)$ теста, обнаруживающего $(a = dt)$, либо локализирующего $(a = lc)$ исследуемые неисправности – как количество элементов матрицы, строки которой – вход-выходные пары эталона, а относительную асимптотическую сложность теста по отношению к сложности схемы C – как величину $O(\mu_a(C)\cdot\mu^{-1}(\tilde{N}))$ при условии, что длина информационного вектора неограниченно возрастает.

Обозначим через $\mathbf{M}_{n,m}^{(1)}$ (соответственно, $\mathbf{M}_{n,m}^{(2)}$) блок управляемых перестановок (БУП) в котором элементы, реализующие перестановку, соединены последовательно (соответственно, параллельно), а через $\mathbf{M}_{n,m}^{(3)}$ – БУП, в котором отсутствует дешифратор, а управляющие символы подаются непосредственно на управляющие входы последовательно соединенных элементов, реализующих управляемые перестановки. Доказаны следующие теоремы.

Теорема 1. Для всех чисел $m,n \in \mathbf{N}$ $(m \le \lceil \log n! \rceil)$ истинны неравенства

$$\mu_{dt}(\mathbf{M}_{n,m}^{(1)}) \le (m+2n+2)(2^m + \lceil 0{,}5m \rceil + 1),$$

$$\mu_{lc}(\mathbf{M}_{n,m}^{(1)}) \le (m+2n+2)(2^m(n+1) + \lceil 0{,}5m \rceil - 2n + 1),$$

$$\mu_a(\mathbf{M}_{n,m}^{(2)}) \le (m+2n+2)(2^m(n+1) + \lceil 0{,}5m \rceil - 2n + 1) \quad (a \in \{dt, lc\}).$$

Теорема 2. Для всех чисел $m,n \in \mathbf{N}$ $(m \le \lceil \log n! \rceil)$ истинны неравенства

$$\mu_{dt}(\mathbf{M}_{n,m}^{(3)}) \le 2n(2n+m),\ \mu_{lc}(\mathbf{M}_{n,m}^{(3)}) \le (2n+m)(2n+m+nm).$$

Из этих теорем вытекает, что:

1. Если $2^m = O(n!)$ $(n \to \infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{M}_{n,m}^{(1)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(1)}$ не превосходит величины $O(\log n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{M}_{n,m}^{(1)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(1)}$, а также относительная асимптотическая сложность обнаружения либо локализации неисправностей БУП $\mathbf{M}_{n,m}^{(2)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(2)}$ не превосходит величины $O(n\log n)$ $(n \to \infty)$.

2. Если $m = O(n\log n)$ $(n \to \infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{M}_{n,m}^{(3)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(3)}$ не превосходит величины $O(\log n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{M}_{n,m}^{(3)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(3)}$ не превосходит величины $O(n\log n)$ $(n \to \infty)$.

Послойный БУП $\mathbf{P}_{n,m}$ содержит элементы, реализующие перестановки компонент n-битовой последовательности, которые последовательно соединены с помощью элементов $\mathbf{P}_{2,1}$, реализующих такое отображение $\mathbf{g}: \mathbf{E}^2 \times \mathbf{E} \to \mathbf{E}^2$, что

$$\mathbf{g}(\mathbf{x}, v) = \begin{cases} (x_2, x_1), \text{ åñëè } v = 1 \\ (x_1, x_2), \text{ åñëè } v = 0 \end{cases} \quad (\mathbf{x} = (x_1, x_2) \in \mathbf{E}^2).$$

Доказана следующая теорема.

Теорема 3. Для всех чисел $n,l \in \mathbf{N}$ (n – четное число) и $m = 0{,}5n(l-1)$ истинны неравенства $\mu_{dt}(\mathbf{P}_{n,m}) \le n^2(l+3)$ и $\mu_{lc}(\mathbf{P}_{n,m}) \le n^2(l+3)(l-1)$.

Из теоремы 3 вытекает, что если $n \to \infty$ и $l \to \infty$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{P}_{n,m}$ по отношению к сложности БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{P}_{n,m}$ по отношению к сложности БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(\mu^2(\mathbf{P}_{n,m}))$ $(n \to \infty)$.

Пусть $\mathbf{C}_{(r,s),m}$ и $\mathbf{C}_{(r,s,r),m}$ (где $rs = n$) – соответственно, 2-х и 3-х уровневая сеть Клоса.

Доказана следующая теорема.

Теорема 4. Для $a \in \{dt, lc\}$ истинны следующие неравенства

$$\mu_a(\mathbf{C}_{(r,s,r),m}) \le 2s(2r + 2m' + m'')(2s\mu_a(\mathbf{P}_{n,m'}) + r\mu_a(\mathbf{P}_{s,m''})),$$

$$\mu_a(\mathbf{C}_{(r,s),m}) \le 2s(2r + m' + m'')(s\mu_a(\mathbf{P}_{n,m'}) + r\mu_a(\mathbf{P}_{s,m''})).$$

На основе анализа сетей Клоса построена рекурсивная процедура построения тестов для рекурсивных БУП. Показано, что эта процедура применима также для достаточно широкого класса управляемых подстановочных операций.

В [13] исследована структура такого множества F_π семейств перестановок компонент n-битовых векторов $H(\mathbf{h}_1,\ldots,\mathbf{h}_k)=\{\mathbf{h}_1^{\alpha_1}\circ\ldots\circ\mathbf{h}_k^{\alpha_k}\mid\alpha_1,\ldots,\alpha_k\in\mathbf{E}\}$ (где $\circ$ – операция суперпозиции, а $\mathbf{h}_i^{\alpha_i}$ $(\alpha_i\in\mathbf{E})$ определено следующим образом: $\mathbf{h}_i^1=\mathbf{h}_i$, а $\mathbf{h}_i^0$ - тождественная перестановка), что для фиксированных чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ перестановка $\mathbf{h}_i$ $(i=1,\ldots,k)$ определена в терминах фиксированного разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$. Доказана следующая теорема.

Теорема 5. Для всех чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ элементы каждого семейства $H(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in F_\pi$ являются попарно различными перестановками множества n-битовых векторов.

Из теоремы 5 вытекает, что для всех чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=\prod_{i=1}^{k}(|B_i|-1)!$. Из этого равенства, в свою очередь, вытекает, что:

1) для каждого числа $n=kl$ $(k,l\in\mathbf{N},k\geq 2,l\geq 2)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|=l$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=((nk^{-1}-1)!)^k$;

2) для каждого числа $n=k^2$ $(k\in\mathbf{N},k\geq 2)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ (p_i $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=((\sqrt{n}-1)!)^k$.

Пусть $T_\pi=\{\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\mid\mathbf{h}_i\in S(B_i)\ (i=1,\ldots,k)\}$, где $S(U)$ – симметрическая группа на множестве U, а $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)=\{\mathbf{h}_1\}\cup\{\mathbf{h}_2^{\alpha_2}\circ\ldots\circ\mathbf{h}_k^{\alpha_k}\mid\alpha_2,\ldots,\alpha_k\in\mathbf{E},\ \sum_{i=2}^{k}\alpha_i\geq 1\}$. Обозначим через $S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k))$ множество всех неподвижных точек перестановок, принадлежащих семейству $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)$. Доказана следующая теорема.

Теорема 6. Если $n=\sum_{i=1}^{k}p_i$, где p_i $(i=1,\ldots,k)$ – простые числа, а $\pi=\{B_1,\ldots,B_k\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|=p_i$ $(i=1,\ldots,k)$, то для каждого семейства перестановок $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in T_\pi$ истинно равенство $|S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k))|=|\mathbf{E}^n|(1-\prod_{i=1}^{k}(1-2^{1-p_i}))$.

Следствие 1. Пусть $n=\sum_{i=1}^{k}p_i$, где p_i $(i=1,\ldots,k)$ – простые числа, а $\pi=\{B_1,\ldots,B_k\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|=p_i$ $(i=1,\ldots,k)$. Если $p_i\to\infty$ для всех $i\in\mathbf{N}_k$, то для каждого семейства $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in T_\pi$ почти все векторы $\mathbf{x}\in\mathbf{E}^n$ не являются неподвижными точками.

В [14] исследован класс семейств легко вычислимых подстановок, определенных системой уравнений над кольцом вычетов $Z_{p^k}=(\mathbf{Z}_{p^k},\oplus,\circ)$, где p – простое число, а $k\in\mathbf{N}$. Такие семейства подстановок, управляемые изображением псевдофрактала, могут быть использованы в поточном шифре для преобразования информационных последовательностей. Основные результаты состоят в следующем.

Рассмотрим такие семейства подстановок $F^{(i)}=\{f_n^{(i)}:\mathbf{Z}_{p^k}\to\mathbf{Z}_{p^k}\mid n\in\mathbf{N}\}$ $(i\in\mathbf{N}_l)$, что $f_n^{(i)}(x)=\beta_i^n\circ x\oplus(n\ (\mathrm{mod}\ p^k))\circ A_i(n)$ $(x\in\mathbf{Z}_{p^k},n\in\mathbf{N})$, а $A_i(n)=\bigoplus_{j=1}^{l}a_j\circ\alpha_j^n\ominus 2\circ a_i\circ\alpha_i^n$ $(i\in\mathbf{N}_l;\ n\in\mathbf{N};\ \alpha_j,\beta_j,a_j\in\mathbf{Z}_{p^k}^{inv}\ (j\in\mathbf{N}_l))$. Доказаны следующие утверждения.

Утверждение 1. Если $\alpha_1=\ldots=\alpha_l=\alpha$ и $a_1=\ldots=a_l=a$, где $\alpha,a\in\mathbf{Z}_{p^k}^{inv}$, то:

1) $f_n^{(i)}=f_n^{(j)}$ $(i,j\in\mathbf{N}_l)$ тогда и только тогда, когда $\beta_i^n=\beta_j^n$;

2) для каждого $n\in\mathbf{N}$ множество неподвижных точек подстановки $f_n^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ совпадает с множеством решений уравнения $(1\ominus\beta_i^n)\circ x=(n\ (\mathrm{mod}\ p^k))\circ(l-2)\circ a\circ\alpha^n$.

Следствие 2. Пусть $\alpha_1=\ldots=\alpha_l=\alpha$ и $a_1=\ldots=a_l=a$, где $\alpha,a\in\mathbf{Z}_{p^k}^{inv}$, $1\ominus\beta_i^n\neq 0$, $n\ (\mathrm{mod}\ p^k)\neq 0$ и r_1,r_2 – такие максимальные натуральные числа, что $1\ominus\beta_i^n\equiv 0\ (\mathrm{mod}\ p^{r_1})$ и $(n\ (\mathrm{mod}\ p^k))\circ(l-2)\equiv 0\ (\mathrm{mod}\ p^{r_2})$. Если $r_1>r_2$, то подстановка $f_n^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ не имеет неподвижных точек.

Утверждение 2. Если $\alpha_1=\ldots=\alpha_l=\alpha$, то подстановка $f_{\phi(p^k)}^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ (где ϕ – функция Эйлера) имеет неподвижные точки тогда и только тогда, когда $l-2\equiv 0\ (\mathrm{mod}\ p)$.

Рассмотрим такое множество $\boldsymbol{K}$ семейств подстановок $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},h)=\{\mathbf{f}_n\mid n\in\mathbf{N}\}$, предназначенное для преобразования информационных векторов фиксированной длины l, что $h\in S(\mathbf{N}_l)$, $\mathbf{u}=(\alpha_1,\ldots,\alpha_l)\in(\mathbf{Z}_{p^k}^{inv})^l$,

$\mathbf{v} = (\beta_1,\ldots,\beta_l) \in (\mathbf{Z}_{p^k}^{inv})^l$, $\mathbf{a} = (a_1,\ldots,a_l) \in (\mathbf{Z}_{p^k}^{inv})^l$, а отображения $\mathbf{f}_n : (\mathbf{Z}_{p^k})^l \to (\mathbf{Z}_{p^k})^l$ определены равенством $\mathbf{f}_n(\mathbf{x}) = (f_n^{(1)}(x_{h^n(1)}),\ldots,f_n^{(l)}(x_{h^n(l)}))^{\mathrm{T}}$ $(\mathbf{x} = (x_1,\ldots,x_l) \in (\mathbf{Z}_{p^k})^l)$, где $f_n^{(i)} \in F^{(i)}$ $(i \in \mathbf{N}_l)$. Доказаны следующие теоремы.

Теорема 7. Пусть p – нечетное простое число. Тогда для всех $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},h) \in \boldsymbol{K}$ поиск семейства $\mathbf{F}_{n_0,n_1}(\mathbf{u},\mathbf{v},\mathbf{a},h) = \{\mathbf{f}_n\}_{n\in\mathbf{N}_{n_1}\setminus\mathbf{N}_{n_0}}$ $(n_0,n_1 \in \mathbf{N};\ n_1 > n_0)$, обладающего заданной неподвижной точкой $\mathbf{x}_0 \in (\mathbf{Z}_{p^k})^l$, при условии, что n_0 и n_1 не являются показателями (по модулю p^k) ни одного из чисел $\alpha_i,\beta_i \in \mathbf{Z}_{p^k}^{inv}$ $(i \in \mathbf{N}_l)$, сводится к решению системы многостепенных диофантовых уравнений с $2l$ неизвестными с последующей проверкой для каждого ее решения разрешимости $2l$ задач дискретного логарифмирования.

Теорема 8. Пусть $p = 2$, $\beta_i = 1$ $(i \in \mathbf{N}_l)$, l – нечетное число и $k \geq 3$. Тогда для любого семейства подстановок $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},e) \in \boldsymbol{K}$ (где $e \in S(\mathbf{N}_l)$ – тождественная подстановка) ни одно семейство подстановок $\mathbf{F}_{n_0,n_1}(\mathbf{u},\mathbf{v},\mathbf{a},e)$ $(1 \leq n_0 < n_1 < 2^k)$ не имеет неподвижных точек.

Теорема 9. Пусть известны значения векторов параметров $\mathbf{a}$ и $\mathbf{u}$. Если в момент $n_0 \in \mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим подстановку $\mathbf{f}_{n_0}$, и наблюдать соответствующий выход, то идентификация вектора параметров $\mathbf{v}$ сводится к независимому решению l задач дискретного логарифмирования.

Теорема 10. Пусть p – нечетное простое число и известны значения векторов параметров $\mathbf{a}$ и $\mathbf{v}$. Если в момент $n_0 \in \mathbf{N}$, где $(n_0 \pmod{p^k}) \in \mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего подстановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров $\mathbf{u}$ сводится к независимому решению l задач дискретного логарифмирования.

2. Автоматы над конечными кольцами. Исследования поточных шифров, построенных на аддитивном внесении информационной переменной в хаотическую динамическую систему, показывают, что возникают ошибки из-за погрешностей округления. Для того чтобы нивелировать эти ошибки естественно перейти к вычислениям в конечной алгебраической системе. В качестве такой алгебраической системы целесообразно выбрать конечное кольцо, так как при наличии делителей нуля в кольце существенно возрастает сложность действий криптоаналитика в процессе его атаки на соответствующий шифр. Исходя из этого, были исследованы над кольцом Z_{p^k} (p – простое число, $k \in \mathbf{N}$) автоматы, построенные как аналоги хаотических динамических систем Эно [15], Спротта [16], Лоренца [17], free-running system и Guckenheimer and Holmes cycle [18]. Развитые при этом методы послужили основой для системного анализа над кольцом Z_{p^k} множества линейных автоматов [11,19,20], и множества нелинейных автоматов, определенных системами уравнений 2-й степени от состояния автомата [11]. В [21] эти результаты были следующим образом обобщены для автоматов над произвольным конечным ассоциативно-коммутативным кольцом $K = (K,+,\cdot)$ с единицей.

Пусть $A_{n,1}$ – множество автоматов Мили M_1, а $A_{n,2}$ – множество автоматов Мура M_2, определенных, соответственно, системами уравнений

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{f}_i : K^n \to K^n$ $(i = 1,\ldots,4)$, а $\mathbf{q}_t,\mathbf{x}_t,\mathbf{y}_t \in K^n$ – соответственно, состояние автомата, входной и выходной символ в момент $t \in \mathbf{Z}_+$. Следующим образом охарактеризованы подмножества $A_{n,1}^{inv}$ и $A_{n,2}^{inv}$ обратимых автоматов.

Теорема 11. Равенство $A_{n,1}^{inv} = \{M_1 \in A_{n,1} \mid \mathbf{f}_4 : K^n \to K^n$ – áèåêöèÿ$\}$ истинно для любых отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 1,2,3)$.

Теорема 12. Равенство $A_{n,2}^{inv} = \{M_2 \in A_{n,2} \mid \mathbf{f}_2 : K^n \to K^n, \mathbf{f}_3 : K^n \to K^n -$ áèåêöèè$\}$ истинно для любого отображения $\mathbf{f}_1 : K^n \to K^n$.

Из этих теорем вытекает, что истинны следующие три следствия.

Следствие 3. Для любого поточного шифра $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M \in A_{n,1}^{inv} \cup A_{n,2}^{inv})$ в процессе "шифрование-расшифрование" автоматы M и M^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Следствие 4. Для любого автомата $M_1 \in A_{n,1}^{inv}$ функции переходов и выходов автомата M_1^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимы отображения $\mathbf{g}_1(\mathbf{q},\mathbf{x}) = \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x} - \mathbf{f}_2(\mathbf{q})))$ и $\mathbf{g}_2(\mathbf{q},\mathbf{x}) = \mathbf{f}_4^{-1}(\mathbf{x} - \mathbf{f}_2(\mathbf{q}))$.

Следствие 5. Для любого автомата $M_2 \in A_{n,2}^{inv}$ функции переходов и выходов автомата M_2^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимо отображение $\mathbf{g}_3(\mathbf{q},\mathbf{x}) = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}) - \mathbf{f}_1(\mathbf{q}))$.

Построена общая схема анализа конечно-автоматных характеристик исследуемых моделей. В рамках этой схемы охарактеризованы качественные и количественные характеристики основных нетривиальных подмножеств исследуемых автоматов. В частности доказаны следующие утверждения.

Утверждение 3. Автомат $M \in A_{n,1} \cup A_{n,2}$ – сильно-связный автомат с диаметром графа переходов равным 1 тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ биекция.

Следствие 6. Автомат $M \in A_{n,1} \cup A_{n,2}$ – перестановочный автомат тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ – биекция.

Следствие 7. Если отображение $\mathbf{f}_3 : K^n \to K^n$ не является биекцией, то диаметр графа переходов автомата $M \in A_{n,1} \cup A_{n,2}$ больше, чем 1.

Утверждение 4. Если $\mathbf{f}_2 : K^n \to K^n$ - биекция, то $M \in A_{n,1}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Утверждение 5. Если $\mathbf{f}_1 : K^n \to K^n$ и $\mathbf{f}_2 : K^n \to K^n$ – биекции, то $M \in A_{n,2}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Утверждение 6. Состояния $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \tilde{\mathbf{q}})$ автомата $M \in A_{n,1} \cup A_{n,2}$ являются близнецами тогда и только тогда, когда они принадлежат одному и тому же классу разбиения K^n / ε, где $\varepsilon = \ker \mathbf{f}_1 \cap \ker \mathbf{f}_2$, если $M \in A_{n,1}$ и $\varepsilon = \ker \mathbf{f}_1$, если $M \in A_{n,2}$.

На основании этих и аналогичных утверждений оценены мощности подмножеств обратимых автоматов, сильно связных автоматов, перестановочных и приведенных автоматов, а также автоматов, имеющих состояния-близнецы. Кроме того, оценены вероятности того, что при равномерном распределении параметров случайно выбранный автомат принадлежит указанным подмножествам.

Пусть $\tilde{A}_{n,1}$ и $\tilde{A}_{n,2}$ – подмножества множеств $A_{n,1}$ и $A_{n,2}$, состоящие из автоматов, имеющих, соответственно, вид

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

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

где $\mathbf{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^{\mathrm{T}}$, $\mathbf{x}_t = (x_t^{(1)}, \ldots, x_t^{(n)})^{\mathrm{T}}$ и $\mathbf{y}_t = (y_t^{(1)}, \ldots, y_t^{(n)})^{\mathrm{T}}$ – соответственно, состояние автомата, входной и выходной символ в момент t, $A, C, E, G, F \in M_n$ – фиксированные матрицы (M_n – множество всех $n \times n$-матриц над кольцом K), а $\mathbf{b} = (b^{(1)}, \ldots, b^{(n)})^{\mathrm{T}} \in K^n$ и $\mathbf{d} = (d^{(1)}, \ldots, d^{(n)})^{\mathrm{T}} \in K^n$ – фиксированные векторы.

В [22,23] для автомата $M \in \tilde{A}_{n,1} \cup \tilde{A}_{n,2}$ решены задачи параметрической идентификации и идентификации начального состояния. Получены следующие результаты.

Доказано, что для любого автомата $M_1 \in \tilde{A}_{n,1}$ идентификация матриц G и F осуществляется достаточно легко. Сложность идентификации вектора $\mathbf{d}$ и матрицы E существенно зависит от того, является ли матрица G обратимой матрицей. При положительном ответе идентификация вектора $\mathbf{d}$ и матрицы E также осуществляется достаточно легко. Однако если матрица G не является обратимой, то приходится осуществлять перебор по множествам решений систем уравнений. Для идентификации матриц A, C и вектора $\mathbf{b}$ приходится формировать и решать системы нелинейных уравнений над кольцом K (известно, что даже над полями Галуа $GF(2^k)$ решение системы уравнений 2-й степени от многих переменных – NP-полная задача). Показано, что, для любого автомата $M_2 \in \tilde{A}_{n,2}$ идентификация вектора $G\mathbf{d}$ и матрицы GE осуществляется достаточно легко. Однако трудной задачей является идентификация матриц GA, GC и вектора $\mathbf{b}$. Отсюда вытекает, что переход к обратимым автоматам не упрощает решение задачи параметрической идентификации для исследуемых моделей. Поэтому при использовании автомата $M \in \tilde{A}_{n,1}^{inv} \cup \tilde{A}_{n,2}^{inv}$ в качестве поточного шифра (в этом случае параметры играют роль долговременного секретного ключа) особое внимание следует уделить обеспечению секретности параметров A, C и $\mathbf{b}$. Показано, что идентификация начального состояния автомата $M_1 \in \tilde{A}_{n,1}$ (при условии, что $G \in M_n^{non-inv}$) и идентификация начального состояния автомата $M_2 \in \tilde{A}_{n,2}$ сводится к решению системы нелинейных уравнений над кольцом K. Отсюда вытекает, что переход к обратимым автоматам не упрощает решение задачи идентификация начального состояния исследуемых моделей. Это обосновывает целесообразность выбора начального состояния автомата $M \in \tilde{A}_{n,1}^{inv} \cup \tilde{A}_{n,2}^{inv}$ в качестве секретного сеансового ключа соответствующего поточного шифра.

В [24,25] следующим образом решена задача построения имитационной модели для семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a} \in \mathbf{A}}$ $(\varnothing \neq \mathbf{A} \subseteq K^l)$, заданного над конечным кольцом $K = (K, +, \cdot)$ системой рекуррентных соотношений с параметрами

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_3}$, либо

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_1(\mathbf{q}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times \mathbf{A} \to K^{n_3}$. Зафиксируем числа $r, l_1 \in \mathbf{N}$, множество $\mathbf{B}$ $(\varnothing \neq \mathbf{B} \subseteq K^{l_1})$ и семейства $\{\phi_{\mathbf{b}}^{(1)} : K^{n_1} \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$, $\{\phi_{\mathbf{b}}^{(2)} : K^{n_1} \times \bigcup_{j=1}^{r-1} (K^{n_3})^j \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$ и $\{\phi_{\mathbf{b}}^{(3)} : K^{n_1} \times (K^{n_3})^r \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$. Пусть $G_{\mathbf{B}} = \{G_{\mathbf{b}} : K^{n_1} \times (K^{n_2})^+ \to (K^{n_3})^+\}_{\mathbf{b}\in\mathbf{B}}$ – такое семейство, что $G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ $(\mathbf{b} \in \mathbf{B}, m \in \mathbf{N})$, где

$$\mathbf{y}_i = \begin{cases} \phi_{\mathbf{b}}^{(1)}(\mathbf{q}_0, \mathbf{x}_1), \text{ åñëè } i = 1 \\ \phi_{\mathbf{b}}^{(2)}(\mathbf{q}_0, \mathbf{y}_1 \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ åñëè } i = 2, \dots, r \\ \phi_{\mathbf{b}}^{(3)}(\mathbf{q}_0, \mathbf{y}_{i-r} \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ åñëè } r < i \le m \end{cases}.$$

Определим отображение $H_{\mathbf{b},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ равенством $H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m)$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ и зафиксируем такую сюръекцию $h : \mathbf{B} \to \mathbf{A}$, что $H_{h(\mathbf{a}),\mathbf{q}_0}|_{\bigcup_{i=1}^{r}(K^{n_2})^i} = F_{\mathbf{a},\mathbf{q}_0}|_{\bigcup_{i=1}^{r}(K^{n_2})^i}$ $(\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$, где $F_{\mathbf{a},\mathbf{q}_0}$ – о.-д.- функция, реализуемая инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$.

Упорядоченную пару $(G_{\mathbf{B}}, h)$ назовем имитационной моделью семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$. На основе стандартного подхода теории алгоритмов формально определено понятие ν -точная $(\nu \in \{\nu_1, \dots, \nu_4\})$ имитационная модель $(G_{\mathbf{B}}, h)$, где числа $\nu_1, \dots, \nu_4 \in [0,1]$ охватывают все комбинации понятий "в наихудшем случае" и "в среднем". ν -точная имитационная модель определяется как асимптотически точная, если $\nu = 1$. Доказана следующая теорема ($\gamma_{\mathbf{a},\mathbf{q}_0,m}$ – среднее количество букв в выходных словах, приходящихся на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины, не превосходящей число m).

Теорема 13. Пусть $(G_{\mathbf{B}}, h)$ – такая имитационная модель семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ $(\mathbf{A} \subseteq K^l, |\mathbf{A}| \ge 1)$ над кольцом K, что: 1) существует предел $\gamma_{\mathbf{a},\mathbf{q}_0} = \lim_{m\to\infty} \gamma_{\mathbf{a},\mathbf{q}_0,m}$; 2) существует такое число $r_0 \in \mathbf{N}$ $(r_0 \ge r)$, что при всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m$ $(m > r_0)$ для выходных слов $F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ и $H_{h(\mathbf{a}),\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \tilde{\mathbf{y}}_1 \dots \tilde{\mathbf{y}}_m$ равенства $\mathbf{y}_i = \tilde{\mathbf{y}}_i$ имеют место для всех $i = r_0 + 1, \dots, m$. Тогда $\nu_1 = \nu_2 = \nu_3 = \nu_4 = 1$, т.е. $(G_{\mathbf{B}}, h)$ - асимптотически точная имитационная модель семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ для всех $\nu \in \{\nu_1, \dots, \nu_4\}$.

В [25,26] исследуется задача использования в качестве семейства хеш-функций семейства автоматов без выхода, заданного системой рекуррентных соотношений с параметрами над конечным кольцом $K = (K, +, \cdot)$. Получены следующие результаты.

Пусть $F_{k,m}$ $(k, m \in \mathbf{N}, k \le m)$ – множество всех таких отображений $\mathbf{f} : K^k \times K^m \to K^k$, что $|\{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}'\}| = |K|^{m-k}$ $(\mathbf{q}, \mathbf{q}' \in K^k)$ и $\{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \varnothing$ $(\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k; \mathbf{q} \neq \mathbf{q}')$. Рассмотрим семейство $M_{F_{k,m}} = \{M_{\mathbf{f}}\}_{\mathbf{f}\in F_{k,m}}$ сильно связных автоматов без выхода $M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1})$ $(t \in \mathbf{Z}_+)$. Каждый автомат $M_{\mathbf{f}}$ определяет семейство хэш-функций $H_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^k}$, где $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_t)$. Доказаны следующие теоремы.

Теорема 14. Для каждого отображения $\mathbf{f} \in F_{k,m}$ при любых таких состояниях $\mathbf{q}_0, \mathbf{q}_0' \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$, что $\mathbf{q}_0 \neq \mathbf{q}_0'$ неравенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}_0'}(\mathbf{u})$ истинно для каждого входного слова $\mathbf{u} \in (K^m)^+$.

Следствие 8. Для каждого отображения $\mathbf{f} \in F_{k,m}$, если $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, то $H_{\mathbf{f},\mathbf{q}_0}^{-1}(\mathbf{q}) \cap H_{\mathbf{f},\mathbf{q}_0'}^{-1}(\mathbf{q}) = \varnothing$ для любого состояния $\mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$.

Теорема 15. Для каждого отображения $\mathbf{f} \in F_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $|H_{\mathbf{f},\mathbf{q}_0}^{-1}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k}$ $(\mathbf{q}_t \in K^k)$ истинно для всех чисел $t \in \mathbf{N}$.

Пусть $P_{\mathbf{f},\mathbf{q}_0,t}^{(1)}(\mathbf{q})$ $(\mathbf{f} \in F_{k,m}; \mathbf{q}_0, \mathbf{q} \in K^k, t \in \mathbf{N})$ – вероятность того, что случайно выбранное из множества $(K^m)^t$ входное слово $\mathbf{u}$ является решением уравнения $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, а $P_{\mathbf{f},\mathbf{q}_0,t}^{(2)}$ $(\mathbf{f} \in F_{k,m}; \mathbf{q}_0 \in K^k, t \in \mathbf{N})$ – вероятность того, что для двух различных входных слов $\mathbf{u}$ и $\mathbf{u}'$, случайно выбранных из множества $(K^m)^t$, истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}')$. Из теоремы 15 вытекает, что истинны следующие два следствия.

Следствие 9. Для каждого отображения $\mathbf{f} \in F_{k,m}$ при любых состояниях $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $|P_{\mathbf{f},\mathbf{q}_0,t}^{(1)}(\mathbf{q})| = |K|^{-k}$ истинно для всех $t \in \mathbf{N}$.

Следствие 10. Для каждого отображения $\mathbf{f} \in F_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $P_{\mathbf{f},\mathbf{q}_0,t}^{(2)} = |K|^{-k}\left(1 - \frac{|K|^k - 1}{|K|^{mt} - 1}\right)$ истинно для всех $t \in \mathbf{N}$.

На основе полученных результатов охарактеризована сложность решения задач идентификации для семейства хэш-функций $H_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^k}$.

3. Автоматы на многообразиях над конечными кольцами. Успешное применение эллиптических кривых при решении задач защиты информации [27,28] обосновывают актуальность исследования автоматов, определенных на многообразиях (так как эллиптическая кривая, как и любая алгебраическая кривая, представляет собой специальный случай многообразия). Исследованию семейств автоматов, определенных на многообразиях над конечными кольцами, посвящены работы [25,29–34]. Основные результаты состоят в следующем.

Выделены следующие 2 множества многообразий над кольцом $K=(K,+,\cdot)$:

1) множество $V_{1,n}(K)$ $(n\in\mathbf{N})$ всех таких многообразий $\mathbf{V}\subseteq K^n$, что задана алгебра $A_{\mathbf{V}}=(\mathbf{V},F_{1,\mathbf{V}},F_{2,\mathbf{V}})$, где $F_{1,\mathbf{V}}=\{\alpha_0,\alpha_1,\ldots,\alpha_{k_1}\}$ $(k_1\in\mathbf{Z}_+)$ и $F_{2,\mathbf{V}}=\{\beta_1,\ldots,\beta_{k_2}\}$ $(k_2\in\mathbf{N})$ есть множество, соответственно, унарных и бинарных операций, определенных на множестве $\mathbf{V}$;

2) множество $V_{2,n}(K)$ $(n\in\mathbf{N})$ всех многообразий $\mathbf{V}\subseteq K^n$ $(n\in\mathbf{N})$, для которых существует параметризация $\mathbf{v}=\mathbf{h}(\mathbf{t})$, где $\mathbf{t}\in K^m$ $(m<n)$, а $\mathbf{h}$ – набор из n многочленов от m переменных, а также задано семейство отображений $\Theta=\{\theta_i\}_{i\in\mathbf{N}_k}$, где $\theta_i:K^m\to K^m$ $(i\in\mathbf{N}_k)$ (отображение θ_i $(i\in\mathbf{N}_k)$ и параметризация $\mathbf{v}=\mathbf{h}(\mathbf{t})$ определяют на многообразии $\mathbf{V}\in V_{2,n}(K)$ множество траекторий $\mathbf{h}(\mathbf{t}),\mathbf{h}(\theta_i(\mathbf{t})),\mathbf{h}(\theta_i^2(\mathbf{t})),\ldots$ $(\mathbf{t}\in K^m)$).

Многообразие $\mathbf{V}_2\in V_{1,n_2}(K_2)$ назовем гомоморфным образом многообразия $\mathbf{V}_1\in V_{1,n_1}(K_1)$, если алгебра $A_{\mathbf{V}_2}$ – гомоморфный образ алгебры $A_{\mathbf{V}_1}$ (соответственно, многообразия $\mathbf{V}_1\in V_{1,n_1}(K_1)$ и $\mathbf{V}_2\in V_{1,n_2}(K_2)$ изоморфны, если алгебры $A_{\mathbf{V}_1}$ и $A_{\mathbf{V}_2}$ изоморфны). Если $\mathbf{V}_j\in V_{2,n_j}(K_j)$ $(j=1,2)$ и существует такая пара сюръекций $\phi_1:\mathbf{V}_1\to\mathbf{V}_2$ и $\phi_2:K^{m_1}\to K^{m_2}$, что равенства $\phi_1(\mathbf{h}_1(\mathbf{t}))=\mathbf{h}_2(\phi_2(\mathbf{t}))$ и $\phi_2(\theta_i^{(1)}(\mathbf{t}))=\theta_i^{(2)}(\phi_2(\mathbf{t}))$ истинны для всех $\mathbf{t}\in K^{m_1}$ и $i\in\mathbf{N}_k$, то будем говорить, что: 1) упорядоченная пара $(\mathbf{V}_2,\Theta_2)$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1,\Theta_1)$; 2) упорядоченные пары $(\mathbf{V}_1,\Theta_1)$ и $(\mathbf{V}_2,\Theta_2)$ изоморфны, если ϕ_1 и ϕ_2 – биекции.

Упорядоченная пара $(\mathbf{V},A_{\mathbf{V}})$ (где $\mathbf{V}\in V_{1,n}(K)$ и $A_{\mathbf{V}}=(\mathbf{V},F_{1,\mathbf{V}},F_{2,\mathbf{V}})$) дает возможность определить семейство $M^{(1)}(\mathbf{V},A_{\mathbf{V}})$ автоматов Мили

$$\begin{cases}\mathbf{q}_{t+1}=\beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_1))\\ \mathbf{y}_{t+1}=\beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_2))\end{cases}\quad(t\in\mathbf{Z}_+)$$

и семейство $M^{(2)}(\mathbf{V},A_{\mathbf{V}})$ автоматов Мура

$$\begin{cases}\mathbf{q}_{t+1}=\beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_1))\\ \mathbf{y}_{t+1}=\beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}),\mathbf{v}_2)\end{cases}\quad(t\in\mathbf{Z}_+).$$

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство автоматов с состояниями-источниками, семейство автоматов с состояниями-стоками, семейство явно-приведенных автоматов). Доказана следующая теорема о гомоморфизмах.

Теорема 16. Если упорядоченная пара $(\mathbf{V}_2,A_{\mathbf{V}_2})$ $(\mathbf{V}_2\in V_{1,n_2}(K_2))$ - гомоморфный образ упорядоченной пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{1,n_1}(K_1))$, то существуют такие отображения

$$\Psi_r:M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})\to M^{(r)}(\mathbf{V}_2,A_{\mathbf{V}_2})\quad(r=1,2),$$

что автомат $\Psi_r(M_r)$ $(M_r\in M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1}))$ является гомоморфным образом автомата M_r.

Следствие 11. Если упорядоченные пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{1,n_1}(K_1))$ и $(\mathbf{V}_2,A_{\mathbf{V}_2})$ $(\mathbf{V}_2\in V_{1,n_2}(K_2))$ изоморфны, то существуют такие отображения

$$\Psi_r:M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})\to M^{(r)}(\mathbf{V}_2,A_{\mathbf{V}_2})\quad(r=1,2),$$

что автоматы $M_r\in M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})$ и $\Psi_r(M_r)$ изоморфны.

Упорядоченная пара $(\mathbf{V},\Theta)$ (где $\mathbf{V}\in V_{2,n}(K)$ и $\Theta=\{\theta_i\}_{i\in\mathbf{N}_k}$) дает возможность определить семейство $M^{(1)}_{n,k,l}(\mathbf{V},\Theta)$ автоматов Мили

$$\begin{cases}\mathbf{q}_{t+1}=\mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t))\\ \mathbf{y}_{t+1}=\mathbf{g}_{x_{t+1}}(\mathbf{q}_t)\end{cases}\quad(t\in\mathbf{Z}_+)$$

и семейство $M^{(2)}_{n,k,l}(\mathbf{V},\Theta)$ автоматов Мура

$$\begin{cases}\mathbf{q}_{t+1}=\mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t))\\ \mathbf{y}_{t+1}=\mathbf{g}(\mathbf{q}_{t+1})\end{cases}\quad(t\in\mathbf{Z}_+),$$

где $\mathbf{t}_0\in K^m$, $\mathbf{q}_0=\mathbf{h}(\mathbf{t}_0)$, $\mathbf{t}_{t+1}=\theta_{x_{t+1}}(\mathbf{t}_t)$ $(t\in\mathbf{Z}_+)$, $\mathbf{g}_i:K^n\to K^l$ $(i\in\mathbf{N}_k)$, $\mathbf{g}:K^n\to K^l$ и $x_{t+1}\in\mathbf{N}_k$.

Пусть $M^{(r)}_{n,k}(\mathbf{V},\Theta)=\bigcup_{l=1}^{\infty}M^{(r)}_{n,k,l}(\mathbf{V},\Theta)$ $(r=1,2)$, $F_m(K)$ – множество всех отображений $f:K^m\to K^m$, $T_{\mathbf{V},f}$ $(f\in F_m(K))$ – множество всех траекторий $\mathbf{h}(\mathbf{t}_0),\mathbf{h}(\mathbf{t}_1),\ldots\mathbf{h}(\mathbf{t}_j),\ldots$ $(\mathbf{t}_0\in K^m)$, а $F_{m,\mathbf{h}}(K)$ – множество всех отображений $f\in F_m(K)$, удовлетворяющих условию $(\forall\mathbf{t},\mathbf{t}'\in K^m)(\mathbf{t}\equiv\mathbf{t}'(\ker\mathbf{h})\Rightarrow\mathbf{t}\equiv\mathbf{t}'(\ker(\mathbf{h}\circ f)))$. Доказана следующая теорема.

Теорема 17. Пусть $\mathbf{v}=\mathbf{h}(\mathbf{t})$ $(\mathbf{t}\in K^m)$ – параметризация многообразия $\mathbf{V}\in V_{2,n}(K)$, а $f\in F_m(K)$. Любые две различные траектории, принадлежащие множеству $T_{\mathbf{V},f}$, исходят из различных точек многообразия $\mathbf{V}$ тогда и только тогда, когда не существуют такие точки $\mathbf{t}_0^{(1)},\mathbf{t}_0^{(2)}\in K^m$, что $\mathbf{t}_0^{(1)}\equiv\mathbf{t}_0^{(2)}(\ker\mathbf{h})$ и $\mathbf{t}_0^{(1)}\not\equiv\mathbf{t}_0^{(2)}(\ker(\mathbf{h}\circ f))$.

Следствие 12. Пусть $\mathbf{v}=\mathbf{h}(\mathbf{t})$ $(\mathbf{t}\in K^m)$ – параметризация многообразия $\mathbf{V}\in V_{2,n}(K)$. Тогда:

1) семейство $M_{n,k}^{(r)}(\mathbf{V},\Theta)$ $(r=1,2)$ состоит из детерминированных автоматов тогда и только тогда, когда Θ состоит только из элементов, принадлежащих множеству $F_{m,\mathbf{h}}(K)$;

2) семейство $M_{n,k}^{(r)}(\mathbf{V},\Theta)$ $(r=1,2)$ состоит из недетерминированных автоматов тогда и только тогда, когда Θ содержит хотя бы один элемент из множества $F_m(K)\setminus F_{m,\mathbf{h}}(K)$.

В дальнейшем рассматриваются только семейства детерминированных автоматов.

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство автоматов с состояниями-источниками, семейство автоматов с состояниями-стоками, семейство явно-приведенных автоматов). Доказана следующая теорема о гомоморфизмах.

Теорема 18. Если упорядоченная пара $(\mathbf{V}_2,\Theta_2)$ $(\mathbf{V}_2\in V_{2,n_2}(K_2))$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{2,n_1}(K_1))$, то существуют такие отображения

$$\Psi_r: M_{n_1,k}^{(r)}(\mathbf{V}_1,\Theta_1)\to M_{n_2,k}^{(r)}(\mathbf{V}_2,\Theta_2)\quad (r=1,2),$$

что автомат $\Psi_r(M_r)$ $(M_r\in M_{n_1,k}^{(r)}(\mathbf{V}_1,\Theta_1))$ является гомоморфным образом автомата M_r.

Пусть Γ_{F} – множество всех эллиптических кривых над полем $\mathrm{F}=\mathbf{GF}(q)$ (где $q=p^k$ (p – простое число, $k\in\mathbf{N}$)), G_γ – множество всех точек (включая бесконечно удаленную точку O) эллиптической кривой $\gamma\in\Gamma_{\mathrm{F}}$, а $G_\gamma=(G_\gamma,+_\gamma)$ – абелева группа, определяемая эллиптической кривой γ. Для точки $P\in G_\gamma$ и числа $a\in\mathbf{N}$ положим $aP=\underbrace{P+\ldots+P}_{a\ \text{ðàç}}$.

Для любой эллиптической кривой $\gamma\in\Gamma_{\mathrm{F}}$, любых фиксированных чисел $n,m,l\in\mathbf{N}_{|G_\gamma|}$ и любых фиксированных точек $P_1,P_2\in G_\gamma$ рекуррентные соотношения

$$\begin{cases} q_{t+1}=nq_t+_\gamma x_{t+1}P_1 \\ y_{t+1}=mq_t+_\gamma x_{t+1}P_2 \end{cases}\quad (t\in\mathbf{Z}_+)$$

и

$$\begin{cases} q_{t+1}=nq_t+_\gamma x_{t+1}P_1 \\ y_{t+1}=mq_{t+1} \end{cases}\quad (t\in\mathbf{Z}_+),$$

где $x_{t+1}\in\mathbf{N}_l$, определяют семейство, соответственно, автоматов Мили $M_{1,\gamma,l}$ и автоматов Мура $M_{2,\gamma,l}$.

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство приведенных автоматов, семейство автоматов с состояниями-близнецами, семейство не сильно связанных автоматов). Решена задача идентификации начального состояния и задача построения асимптотически точной имитационной модели для исследуемых семейств автоматов в предположении, что $n,m\in\mathbf{N}_{|G_\gamma|-1}$ и $P_1,P_2\in G_\gamma\setminus\{O\}$. Доказаны следующие теоремы.

Теорема 19. Для каждого автомата $M_1\in M_{1,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $v\in G_\gamma$ уравнения $mu=a_0$, где элемент $a_0\in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_1.

Теорема 20. Для каждого автомата $M_2\in M_{2,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $u\in G_\gamma$ уравнения $mnv=b_0$, где элемент $b_0\in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_2.

Теорема 21. Построение точной имитационной модели для семейства автоматов $M_{1,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 3, а высота которого не превосходит число $|G_\gamma|+1$. При этом суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента, не превосходит число $|G_\gamma|+1+0.5|G_\gamma|(|G_\gamma|+3)$.

Теорема 22. Построение точной имитационной модели для семейства автоматов $M_{2,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 2, а высота которого не превосходит число $|G_\gamma|$. При этом суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента, не превосходит число $|G_\gamma|+0.5|G_\gamma|(|G_\gamma|+1)$.

Заключение. Приведенные в настоящей работе результаты были получены на основе синтеза моделей и методов современной алгебры, теории систем, теории алгоритмов, теории автоматов и алгебраической геометрии. Новым моментом явилась необходимость разработки методов решения над конечными кольцами систем уравнений с параметрами и разработки методов анализа выполнимости формул над конечными кольцами. В [35] разработана

схема представления в виде теоретико – множественной формулы множества решений над конечным ассоциативным кольцом (с односторонними единицами, либо с двусторонней единицей) систем уравнений с параметрами. Эта схема основана на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) классов ассоциированных элементов. В [36] построена схема решателя, предназначенного для проверки выполнимости формул линейной арифметики над любым конечным ассоциативным кольцом с ненулевым умножением. Эта схема основана на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) классов ассоциированных элементов, а также на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) делителей нуля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Menezis A., van Oorschot P., Vanstone S. Handbook of applied cryptography. − CRC Press, 1997. − 780 p.
2. Шнайер Б. Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2003. – 816 с.
3. Харин Ю. С., Берник В.И., Матвеев Г.В., Агиевич С.Г. Математические и компьютерные основы криптологии: – Минск: Новое знание, 2003. – 382 с.
4. Диффи У., Хеллмен М.Е. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. – 1979. – Т.67. – № 3. – С. 71–109.
5. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.
6. Анисимова Е.Н., Скобелев В.Г. Сложность идентификации неисправностей блоков управляемых перестановок // Искусственный интеллект. – 2004. – № 4. – С. 794–803.
7. Анисимова Е.Н., Скобелев В.Г. Анализ послойных блоков управляемых перестановок // Искусственный интеллект. – 2005. – № 1. – С. 146–152.
8. Анисимова Е.Н., Скобелев В.Г. Сложность тестирования матричных и послойных БУП // Вестник Томского государственного университета. Приложение. – 2005. – № 14. – С. 139–143.
9. Анисимова Е.Н., Скобелев В.Г. Сложность идентификации неисправностей блока управляемых перестановок // Труды V международной конференции "Идентификация систем и задачи управления (SICPRO 06)". – М.: ИПУ РАН, 2006. – С. 1241–1258.
10. Скобелев В.Г. Контроль неисправностей блоков управляемых перестановок // Надежность. – 2006. – № 4. – С. 41–45.
11. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. – Донецк: ИПММ НАН Украины, 2009. – 479 с.
12. Скобелев В.Г. Оценки сложности экспериментов с блоками управляемых перестановок // Доповіді НАНУ. – 2011. – № 4. – С. 41–43.
13. Скобелев В.Г. Об одном семействе суперпозиций подстановок // Компьютерная математика. – 2011. – № 1. – С. 116–121.
14. Скобелев В.Г., Зайцева Э.Е. Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. – 2008. – № 5. – С. 12–24.
15. Скобелев В.Г., Тубольцева О.В. Шифр на основе отображения Эно // Вестник Томского государственного университета. Приложение. − 2004. − № 9(1). − С. 77–82.
16. Скобелев В.Г., Сухинин В.А. Шифры на основе систем Спротта // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 122–126.
17. Скобелев В.Г. Анализ системы Лоренца над кольцом Z_{p^k} // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 134–139.
18. Скобелев В.В. Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Труды ИПММ НАНУ. − Т.10. − 2005. − С. 184–189.
19. Скобелев В.В. Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Доповіді НАНУ. − 2007. − № 10. − С. 44–49.
20. Скобелев В.В. Анализ структуры класса линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Кибернетика и системный анализ. − 2008. − № 3. − С. 60–74.
21. Скобелев В.В., Глазунов Н.М., Скобелев В.Г. Многообразия над кольцами. Теория и приложения. − Донецк: ИПММ НАНУ. − 2011. − 323 с.
22. Скобелев В.Г. Анализ задачи параметрической идентификации нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 5. – С. 37–41.
23. Скобелев В.Г. Восстановление вектора начального состояния нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 6. – С. 31–34.
24. Скобелев В.В. Моделирование автоматов над кольцом автоматами с конечной памятью // Проблемы управления и информатики. – 2012. – № 3. – С. 114–122.
25. Скобелев В.В. Автоматы на алгебраических структурах. Модели и методы их исследования. – Донецк: ИПММ НАНУ, 2013. – 307 с.
26. Скобелев В.В. Анализ семейств хэш-функций, определяемых автоматами над конечным кольцом // Кибернетика и системный анализ. – 2013. – № 2. – С. 46–55.
27. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.
28. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. − 326 с.
29. Скобелєв В.В. Аналіз автоматів, які визначено на еліптичних кривих // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 1. – С. 223–230.
30. Скобелев В.В. Об автоматах на многообразиях над кольцом // Труды ИПММ НАНУ. – 2012. – Т. 24. – С. 190–201.
31. Скобелєв В.В. Автомати на многовидах з алгеброю // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 2. – С. 234–238.
32. Скобелев В.В. Об автоматах на полиномиально параметризованном многообразии над конечным кольцом // Труды ИПММ НАНУ. – 2012. – Т. 25. – С. 185–195.
33. Skobelev V.V. Analysis of automata determined over parametric varieties over an associative ring // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 3. – С. 239–244.
34. Скобелев В.В. О гомоморфизмах автоматов на многообразиях над кольцом // Доповіді НАНУ. – 2013. – № 1. – С. 42–46.
35. Skobelev V.V. On systems of polynomial equations over finite rings // Наукові записки НаУКМА. Серія: Комп'ютерні науки. – 2012. – Т. 138. – С. 15–19.
36. Skobelev V.V. Satisfiability modulo linear arithmetic over a finite ring // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2013. – Вип. 2. – С. 95–106.

Надійшла до редколегії 15.09.14

Скобелєв В. В., канд. фіз.-мат. наук,
Скобелєв В. Г., д-р фіз.-мат. наук, д-р техн. наук, проф.
ІПММ НАН України, Донецьк

МЕТОДИ АНАЛІЗУ АВТОМАТНО-АЛГЕБРАЇЧНИХ МОДЕЛЕЙ

В роботі розглянуто методи аналізу автоматних моделей, які визначено над скінченними кільцями. Для керованих логічних операцій досліджено складність виявлення та локалізації дефектів у процесі off-line контролю їх апаратних реалізацій, а також обчислювальна стійкість сімей легко-обчислюваних переставлень. Досліджено задачу побудови імітаційної моделі для сім'ї автоматів, які визначено системами рівнянь над скінченними кільцями, а також обчислювальну стійкість сім'ї гэш-функцій, які визначено автоматом без вихідної функції. Досліджено автомати, які визначено на многовиді над скінченним кільцем, у тому числі, автомати, які визначено на еліптичній кривій над скінченним полем.

Ключові слова: скінченні автомати, скінченні кільця, многовиди, еліптичні криві.

Skobelev V. V., PHD, Phys.-math. Sci.
Skobelev V. G., Dr. Phys. Math. Sci., Dr. Tech. Sci., Professor
IAMM of NAS of Ukraine, Donetsk

METHODS FOR ANALYSIS OF AUTOMATA-ALGEBRAIC MODELS

In the given paper there are presented methods for analysis of automata models defined over finite rings. For controlled logic operations there are investigated complexity of checking and localization of faults in the process off-line analysis of their hardware realizations, and computational security of families of easy-computable permutations. There are investigated the problem of design of simulation model for a family of automata defined via a system of equations over a finite ring, and computational security of a family of hash-functions determined by an automaton without output function. There are investigated automata defined on a variety over a finite ring, and automata defined on elliptic curve over a finite field.

Keywords: finite automata, finite rings, varieties, elliptic curves.