УДК 512.552.37+519.115

В.В. СКОБЕЛЕВ

АНАЛИЗ СЕМЕЙСТВ ХЭШ-ФУНКЦИЙ, ОПРЕДЕЛЯЕМЫХ АВТОМАТАМИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Ключевые слова: *конечные кольца, автоматы без выхода, хэш-функции.*

ВВЕДЕНИЕ

Известно, что анализ автоматов над конечными кольцами является задачей алгебраической теории автоматов, имеющей многочисленные потенциальные приложения в области компьютерных наук. Одно из таких прикладных направлений состоит в исследовании возможности использования обратимых автоматов над конечными кольцами в качестве математических моделей поточных шифров [1–4], что актуально в связи с переходом к комбинаторно-алгебраическим моделям при решении задач современной криптографии [5, 6]. Другое направление связано с исследованием возможности применения автоматов над конечными кольцами при решении задач компактного представления информации. В этом случае определяющую роль играет процесс хеширования, суть которого состоит в преобразовании входного массива данных в выходную строку фиксированной длины. Такие преобразования называются хэш-функциями. С математической точки зрения, хэш-функции представляет собой отображение $H: X^+ \to Y$, где X и Y — такие непустые конечные множества, что $|X| \geq |Y|$.

Хэш-функции применяются в процессе решения многих задач, связанных с защитой информации [7, 8]. Формально требования, предъявляемые к такой хэш-функции $H: X^+ \to Y$, могут быть сформулированы следующим образом:

1) сложность вычисления значений функции H является полиномом от длины входа (H — легко вычислимая функция);

2) для любого фиксированного $y \in Y$ поиск такого $u \in X^+$, что $H(u) = y$, является трудной задачей (отсюда, в частности, вытекает, что для любого фиксированного $u \in X^+$ поиск такого $u' \in X^+$, что $H(u) = H(u')$ — трудная задача);

3) поиск двух таких случайных элементов $u, u' \in X^+$, что $H(u) = H(u')$, имеет, по крайней мере, субэкспоненциальную сложность.

Первые два требования означают, что H является однонаправленной функцией, а третье требование называется устойчивостью к коллизиям.

В настоящее время не известно ни одной функции, для которой доказано, что она удовлетворяет требованиям 1 и 2. Поэтому при решении прикладных задач под однонаправленной хэш-функцией понимают такую легко вычислимую функцию $H: X^+ \to Y$, что при любом фиксированном $y \in Y$ любой известный алгоритм решения уравнения $H(u) = y$ имеет субэкспоненциальную сложность. Исходя из этого, под криптостойкой хэш-функцией понимают однонаправленную функцию $H: X^+ \to Y$ (в указанном выше прикладном значении этого понятия), для которой любой известный алгоритм нахождения коллизий имеет субэкспоненциальную сложность.

Замечание 1. В криптографии (см., например, [8]) любая хэш-функция $H: (\mathbf{E}^m)^+ \to \mathbf{E}^k$ ($\mathbf{E} = \{0, 1\}$, а $k, m \in \mathbf{N}$ ($k \leq m$) — фиксированные числа) считается криптостойкой, если при любом фиксированном $\mathbf{y} \in \mathbf{E}^k$ асимптотическая сложность любого известного алгоритма поиска такого элемента $\mathbf{u} \in (\mathbf{E}^m)^n$, что $H(\mathbf{u}) = \mathbf{y}$, а также асимптотическая сложность любого известного алгоритма поиска двух таких случайных элементов $\mathbf{u}, \mathbf{u}' \in (\mathbf{E}^m)^n$, что $H(\mathbf{u}) = H(\mathbf{u}')$, равна $O(2^{0{,}5n})$ $(n \to \infty)$.

Цель настоящей работы — исследование свойств хэш-функций, определяемых автоматами без выхода над конечным кольцом $\mathsf{K} = (K, +, \cdot)$ ($|K| \geq 2$) (в дальнейшем кольцо K), являющихся естественным обобщением хэш-функций, указанных в замечании 1.

В разд. 1 семейства хеш-функций определены в терминах семейств отображений, реализуемых автоматами без выхода при всевозможных их инициализациях. В разд. 2 установлены основные свойства этих семейств хеш-функций. В разд. 3 охарактеризована вычислительная стойкость исследуемых семейств хэш-функций. Заключение содержит ряд выводов. Все неопределяемые в работе термины теории автоматов и теории графов такие же, как в [2, 4, 9, 10].

1. ИССЛЕДУЕМАЯ МОДЕЛЬ

Зафиксируем числа $k, m \in \mathbf{N}$ ($k \leq m$). Обозначим $\mathsf{F}_{k,m}$ ($k, m \in \mathbf{N}$, $k \leq m$) множество всех отображений $\mathbf{f}: K^k \times K^m \to K^k$, удовлетворяющих следующим двум условиям:

1) для любых $\mathbf{q}, \mathbf{q}' \in K^k$ истинны равенства

$$|\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}'\}| = |K|^{m-k}; \tag{1}$$

2) для любых $\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k$ $(\mathbf{q} \neq \mathbf{q}')$ истинны равенства

$$\{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \varnothing. \tag{2}$$

Из (1) вытекает, что множество отображений $\mathsf{F}_{k,m}$ определяет над кольцом K множество $\mathsf{B}_{k,m}$ сильно связных автоматов без выхода:

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1}) \ (\mathbf{f} \in \mathsf{F}_{k,m},\ t \in \mathbf{Z}_+), \tag{3}$$

имеющих множество состояний K^k и входной алфавит K^m, т.е. $\mathbf{q}_t \in K^k$ и $\mathbf{x}_t \in K^m$ являются соответственно состоянием и входным символом в момент t.

Замечание 2. Любой автомат $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ характеризуется следующим образом. Рассмотрим автоматный граф $G_{\mathbf{f}}$ автомата $M_{\mathbf{f}}$. Удалим отметки всех дуг, и для каждой пары состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^k$ отождествим (иными словами, склеим) все дуги, идущие из вершины с отметкой $\mathbf{q}$ в вершину с отметкой $\widetilde{\mathbf{q}}$. Получим полный направленный граф G с петлями, имеющий $|K|^k$ вершин.

Следующий пример показывает, что множество отображений $\mathsf{F}_{k,m}$ $(k, m \in \mathbf{N}, k \leq m)$ определяет нетривиальное множество сильно связных автоматов без выхода над кольцом K.

Пример. Обозначим $\mathsf{F}_{k,m}^{(0)}$ $(k, m \in \mathbf{N}, k \leq m)$ множество всех отображений $\mathbf{f} : K^k \times K^m \to K^k$, имеющих вид

$$\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{g}(\mathbf{q}) + \mathbf{h}(\mathbf{x}),$$

где $\mathbf{h} : K^m \to K^k$ — такая сюръекция, что $|\mathbf{h}^{-1}(\mathbf{q})| = |K|^{m-k}$ для всех $\mathbf{q} \in K^k$, а $\mathbf{g} : K^k \to K^k$ — биекция. Так как для любого отображения $\mathbf{f} \in \mathsf{F}_{k,m}^{(0)}$ истинны равенства (1) и (2), то $\mathsf{F}_{k,m}^{(0)} \subseteq \mathsf{F}_{k,m}$. Следовательно, отображения, принадлежащие множеству $\mathsf{F}_{k,m}^{(0)}$, определяют множество $\mathsf{B}_{k,m}^{(0)}$ $(\mathsf{B}_{k,m}^{(0)} \subseteq \mathsf{B}_{k,m})$ сильно связных автоматов без выхода:

$$M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{g}(\mathbf{q}_t) + \mathbf{h}(\mathbf{x}_{t+1}) \ \ (\mathbf{f} \in \mathsf{F}_{k,m}^{(0)},\ t \in \mathbf{Z}_+). \tag{4}$$

Если $k = m$, то равенство (4) определяет функцию переходов некоторых нетривиальных подмножеств автоматов над кольцом K, исследованных в [2, 4], которым, в частности, принадлежат некоторые подмножества линейных автоматов, изученных в [1].

Как это обычно принято в теории автоматов, расширим отображение $\mathbf{f} \in \mathsf{F}_{k,m}$ на множество $K^k \times (K^m)^+$ равенством

$$\mathbf{f}(\mathbf{q}, \mathbf{x}_1 \ldots \mathbf{x}_{t+1}) = \mathbf{f}(\mathbf{f}(\ldots \mathbf{f}(\mathbf{f}(\mathbf{q}, \mathbf{x}_1), \mathbf{x}_2), \ldots, \mathbf{x}_t), \mathbf{x}_{t+1}) \tag{5}$$

и всюду в дальнейшем будем считать, что любое отображение $\mathbf{f} \in \mathsf{F}_{k,m}$ определено на множестве $K^k \times (K^m)^+$.

Каждый инициальный автомат $(M_{\mathbf{f}}, \mathbf{q}_0)$ $(\mathbf{q}_0 \in K^k, \mathbf{f} \in \mathsf{F}_{k,m})$ определяет отображение $H_{\mathbf{f},\mathbf{q}_0} : (K^m)^+ \to K^k$ свободной входной полугруппы $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}}$, значения которого на входном слове

$\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^m)^t$ $(t \in \mathbf{N})$ вычисляются в соответствии с формулой

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_t). \tag{6}$$

Отметим, что из (5) и (6) вытекает, что для любых $\mathbf{f} \in \mathsf{F}_{k,m}$ и $\mathbf{q}_0 \in K^k$ равенство

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t \mathbf{x}_{t+1}) = H_{\mathbf{f}, H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t)}(\mathbf{x}_{t+1}) \tag{7}$$

истинно для всех входных слов $\mathbf{x}_1 \ldots \mathbf{x}_t \mathbf{x}_{t+1} \in (K^m)^{t+1}$ $(t \in \mathbf{N})$.

Таким образом, каждый автомат $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ определяет семейство хэш-функций $\mathsf{H}_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$, отображающих множество $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}}$.

2. АНАЛИЗ ИССЛЕДУЕМОЙ МОДЕЛИ

Основные свойства семейства хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ характеризуются следующим образом.

Теорема 1. Для любого отображения $\mathbf{f} \in \mathsf{F}_{k,m}$, если $\mathbf{q}_0 \neq \mathbf{q}'_0$ $(\mathbf{q}_0, \mathbf{q}'_0 \in K^k)$, то

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{u})$$

для любого входного слова $\mathbf{u} \in (K^m)^+$.

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathsf{F}_{k,m}$. Докажем теорему индукцией по длине t входного слова.

Пусть $t = 1$. Из (2) вытекает, что $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) \neq \mathbf{f}(\mathbf{q}'_0, \mathbf{x}_1)$ для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ $(\mathbf{q}_0 \neq \mathbf{q}'_0)$ автомата $M_{\mathbf{f}}$ и любого входного символа $\mathbf{x}_1 \in K^m$. Так как в силу равенства (6) $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1)$ и $H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1) = \mathbf{f}(\mathbf{q}'_0, \mathbf{x}_1)$, то $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1)$ для любых $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ $(\mathbf{q}_0 \neq \mathbf{q}'_0)$ автомата $M_{\mathbf{f}}$ и любого входного символа $\mathbf{x}_1 \in K^m$, что и требовалось доказать.

Предположим, что теорема истинна для $t = n$, т.е. если $\mathbf{q}_0 \neq \mathbf{q}'_0$ $(\mathbf{q}_0, \mathbf{q}'_0 \in K^k)$, то $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \ldots \mathbf{x}_n)$ для любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_n \in (K^m)^n$.

Докажем теорему для $t = n+1$. В силу (7) для любых состояний $\mathbf{q}_0, \mathbf{q}'_0 \in K^k$ $(\mathbf{q}_0 \neq \mathbf{q}'_0)$ автомата $M_{\mathbf{f}}$ и любого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_{n+1} \in (K^m)^{n+1}$ истинны равенства

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n \mathbf{x}_{n+1}) = H_{\mathbf{f}, H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n)}(\mathbf{x}_{nt+1}),$$
$$H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \ldots \mathbf{x}_n \mathbf{x}_{n+1}) = H_{\mathbf{f}, H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \ldots \mathbf{x}_n)}(\mathbf{x}_{n+1}).$$

По предположению индукции $\mathbf{q}_n = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n) \neq H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \ldots \mathbf{x}_n) = \mathbf{q}'_n$. А так как теорема истинна, если $t = 1$, то

$$H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n \mathbf{x}_{n+1}) = H_{\mathbf{f},\mathbf{q}_n}(\mathbf{x}_{n+1}) \neq H_{\mathbf{f},\mathbf{q}'_n}(\mathbf{x}_{n+1}) = H_{\mathbf{f},\mathbf{q}'_0}(\mathbf{x}_1 \ldots \mathbf{x}_n \mathbf{x}_{n+1}),$$

что и требовалось доказать.

Теорема доказана.

В силу теоремы 1 элементы каждого семейства хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ — отображения множества $(K^m)^+$ во множество K^k состояний автомата $M_{\mathbf{f}}$, значения которых попарно различны на любом входном слове $\mathbf{u} \in (K^m)^+$. Отсюда непосредственно вытекает, что истинно следующее следствие.

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

Теорема 2. Для любых $\mathbf{f} \in \mathsf{F}_{k,m}$ и $\mathbf{q}_0 \in K^k$ при всех $t \in \mathbf{N}$ истинны равенства

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k} \quad (\mathbf{q}_t \in K^k). \tag{8}$$

Доказательство. Зафиксируем отображение $\mathbf{f} \in \mathsf{F}_{k,m}$. Докажем теорему индукцией по длине t входного слова.

Пусть $t=1$. Из определения отображения $H_{\mathbf{f},\mathbf{q}_0}$ $(\mathbf{q}_0 \in K^k,\ \mathbf{f} \in \mathsf{F}_{k,m})$ вытекает, что для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}}$ истинно равенство

$$H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_1) \cap K^m = \{\mathbf{x}_1 \in K^m \,|\, \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}_1\}. \tag{9}$$

В силу (1) для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}}$ истинно равенство

$$|\{\mathbf{x}_1 \in K^m \,|\, \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}_1\}| = |K|^{m-k}. \tag{10}$$

Из (9) и (10) вытекает, что если $t=1$, то равенство (8) истинно для любого состояния $\mathbf{q}_1 \in K^k$ автомата $M_{\mathbf{f}}$, что и требовалось доказать.

Предположим, что равенство (8) истинно, если $t=n$.

Докажем теорему для $t=n+1$. Из определения отображения $H_{\mathbf{f},\mathbf{q}_0}$ $(\mathbf{q}_0 \in K^k,\ \mathbf{f} \in \mathsf{F}_{k,m})$ и равенств (6) и (7) вытекает, что для любого состояния $\mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}}$

$$H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_{n+1}) \cap (K^m)^{n+1} = \{\mathbf{x}_1 \ldots \mathbf{x}_{n+1} \in (K^m)^{n+1} \,|\, \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_{n+1}) = \mathbf{q}_{n+1}\} =$$

$$= \bigcup_{\mathbf{q}_n \in K^k} \{\mathbf{x}_1 \ldots \mathbf{x}_n \mathbf{x}_{n+1} \in (K^m)^{n+1} \,|\, H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_n) = \mathbf{q}_n \,\&\, H_{\mathbf{f},\mathbf{q}_n}(\mathbf{x}_{n+1}) = \mathbf{q}_{n+1}\} =$$

$$= \bigcup_{\mathbf{q}_n \in K^k} (H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n) \times (H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m). \tag{11}$$

В силу равенства (2) для любого состояния $\mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}}$ множества $H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m$ $(\mathbf{q}_n \in K^k)$ попарно не пересекаются. Поэтому из (11) вытекает, что

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_{n+1}) \cap (K^m)^{n+1}| = \sum_{\mathbf{q}_n \in K^k} |H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n| \cdot |H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m|. \tag{12}$$

По предположению индукции для любых состояний $\mathbf{q}_0, \mathbf{q}_n \in K^k$ автомата $M_{\mathbf{f}}$ справедливо равенство $|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q}_n) \cap (K^m)^n| = |K|^{nm-k}$. А так как теорема истинна, если $t=1$, т.е. $|H^{-1}_{\mathbf{f},\mathbf{q}_n}(\mathbf{q}_{n+1}) \cap K^m| = |K|^{m-k}$ для любых состояний $\mathbf{q}_n, \mathbf{q}_{n+1} \in K^k$ автомата $M_{\mathbf{f}}$, то из (12) вытекает, что

$$|H^{-1}_{\mathbf{f},\mathbf{q}_0}(q_{n+1}) \cap (K^m)^{n+1}| = \sum_{\mathbf{q}_n \in K^k} |K|^{nm-k} \cdot |K|^{m-k} =$$

$$= |K|^{(n+1)m-2k} \left(\sum_{\mathbf{q}_n \in K^k} 1 \right) = |K|^{(n+1)m-2k} |K|^k = |K|^{(n+1)m-k},$$

что и требовалось доказать.

Теорема доказана.

Обозначим $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0,\mathbf{q}\in K^k$; $t\in\mathbf{N}$) вероятность того, что входное слово $\mathbf{u}$, случайно выбранное из множества $(K^m)^t$, является решением уравнения $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u})=\mathbf{q}$, а $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0\in K^k$; $t\in\mathbf{N}$) — вероятность того, что для двух различных входных слов: $\mathbf{u}$ и $\mathbf{u}'$, случайно выбранных из множества $(K^m)^t$, истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u})=H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}')$.

Следствие 2. Для любых $\mathbf{f}\in\mathsf{F}_{k,m}$ и $\mathbf{q}_0,\mathbf{q}\in K^k$ при всех $t\in\mathbf{N}$ истинны равенства

$$p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})=|K|^{-k}\quad (t\in\mathbf{N}). \tag{13}$$

Доказательство. Зафиксируем отображение $\mathbf{f}\in\mathsf{F}_{k,m}$, состояния $\mathbf{q}_0,\mathbf{q}\in K^k$ автомата $M_{\mathbf{f}}$ и число $t\in\mathbf{N}$. Учитывая равенство (8), получим, что для всех $t\in\mathbf{N}$

$$p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})=\frac{|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q})\cap(K^m)^t|}{|(K^m)^t|}=\frac{|K|^{mt-k}}{|K|^{mt}}=|K|^{-k}.$$

Следствие доказано.

Из (13) вытекает, что для вероятности $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0,\mathbf{q}\in K^k$; $t\in\mathbf{N}$) истинны следующие утверждения:

1) вероятность $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0,\mathbf{q}\in K^k$; $t\in\mathbf{N}$) не зависит от числа $m\in\mathbf{N}$ ($m\ge k$) (т.е. от мощности входного алфавита автомата $M_{\mathbf{f}}$), ни от длины $t\in\mathbf{N}$ $t\in\mathbf{N}$ входного слова;

2) вероятность $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0,\mathbf{q}\in K^k$; $t\in\mathbf{N}$) монотонно убывает при росте параметра $k\in\mathbf{N}$, причем $\lim\limits_{k\to\infty}p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}=0$ ($\mathbf{f}\in\mathsf{F}_{k,m}$; $\mathbf{q}_0\in K^k$; $t\in\mathbf{N}$).

Следствие 3. Для любых $\mathbf{f}\in\mathsf{F}_{k,m}$ и $\mathbf{q}_0\in K^k$ истинны равенства

$$p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})=|K|^{-k}\left(1-\frac{|K|^k-1}{|K|^{mt}-1}\right)\quad (t\in\mathbf{N}). \tag{14}$$

Доказательство. Зафиксируем отображение $\mathbf{f}\in\mathsf{F}_{k,m}$, состояние $\mathbf{q}_0\in K^k$ автомата $M_{\mathbf{f}}$ и число $t\in\mathbf{N}$. Так как множества входных слов $H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q})\cap(K^m)^t$ ($\mathbf{q}\in K^k$) попарно не пересекаются, то, учитывая равенства (8) и (9), получим, что для всех $t\in\mathbf{N}$ (через $\begin{pmatrix}a\\b\end{pmatrix}$ обозначено число сочетаний из a по b):

$$p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})=\frac{\sum\limits_{\mathbf{q}\in K^k}\begin{pmatrix}|H^{-1}_{\mathbf{f},\mathbf{q}_0}(\mathbf{q})\cap(K^m)^t|\\2\end{pmatrix}}{\begin{pmatrix}|(K^m)^t|\\2\end{pmatrix}}=\frac{\sum\limits_{\mathbf{q}\in K^k}0{,}5|K|^{mt-k}(|K|^{mt-k}-1)}{0{,}5|K|^{mt}(|K|^{mt}-1)}=$$

$$=\frac{0{,}5|K|^{mt-k}(|K|^{mt-k}-1)\left(\sum\limits_{\mathbf{q}\in K^k}1\right)}{0{,}5|K|^{mt}(|K|^{mt}-1)}=\frac{0{,}5|K|^{mt-k}(|K|^{mt-k}-1)|K|^k}{0{,}5|K|^{mt}(|K|^{mt}-1)}=$$

$$=\frac{|K|^{mt-k}-1}{|K|^{mt}-1}=|K|^{-k}\,\frac{|K|^{mt}-|K|^k}{|K|^{mt}-1}=$$

$$=|K|^{-k}\,\frac{|K|^{mt}-1+1-|K|^k}{|K|^{mt}-1}=|K|^{-k}\left(1-\frac{|K|^k-1}{|K|^{mt}-1}\right).$$

Следствие доказано.

Из (14) вытекает, для что вероятности $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$) истинны следующие утверждения:

1) вероятность $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$) монотонно возрастает при росте длины $t \in \mathbf{N}$ входного слова, причем $\lim\limits_{t\to\infty} p^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$);

2) вероятность $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$) монотонно возрастает при росте параметра $m \in \mathbf{N}$ $(m \ge k)$, причем $\lim\limits_{m\to\infty} p^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$);

3) число $|K|^{-k}$ является верхней границей для вероятности $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ ($\mathbf{f} \in \mathsf{F}_{k,m}$; $\mathbf{q}_0 \in K^k$; $t \in \mathbf{N}$) при любых значениях параметров $k, m \in \mathbf{N}$ $(k \le m)$ и при любой длине $t \in \mathbf{N}$ входного слова.

3. ВЫЧИСЛИТЕЛЬНАЯ СТОЙКОСТЬ ИССЛЕДУЕМОЙ МОДЕЛИ

Охарактеризуем вначале сложность поиска входного слова $\mathbf{u} \in (K^m)^t$, для которого при заданном значении $\mathbf{q} \in K^k$ истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, а также сложность поиска входных слов $\mathbf{u}, \tilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \ne \tilde{\mathbf{u}})$, для которых истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\tilde{\mathbf{u}})$ в предположении, что экспериментатору известно семейство хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$, т.е. известно отображение $\mathbf{f} \in \mathsf{F}_{k,m}$ для системы уравнений (3). Возможны следующие два случая.

Случай 1. Экспериментатору известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$, т.е. иными словами, известна хэш-функция $H_{\mathbf{f},\mathbf{q}_0}$.

Охарактеризуем сложность поиска такого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^m)^t$ $(t \in \mathbf{N})$, что $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t) = \mathbf{q}$, где $\mathbf{q} \in K^k$ — фиксированное состояние автомата $M_{\mathbf{f}}$.

Если $t = 1$, то эта сложность совпадает со сложностью поиска одного (не важно, какого именно) решения $\mathbf{x}_1 \in K^m$ уравнения $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1) = \mathbf{q}$ или, иными словами, уравнения $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}$.

Если же $t > 1$, то в качестве $\mathbf{x}_1 \ldots \mathbf{x}_{t-1}$ достаточно выбрать любое входное слово, а в качестве входного символа $\mathbf{x}_t$ — любое решение уравнения $\mathbf{f}(H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{q}$.

Таким образом, если известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$, то при любом $t \in \mathbf{N}$ сложность поиска такого входного слова $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^m)^t$ $(t \in \mathbf{N})$, что $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t) = \mathbf{q}$, совпадает со сложностью поиска одного (не важно, какого именно) решения $\mathbf{x} \in K^m$ уравнения $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \tilde{\mathbf{q}}$ при известных значениях $\mathbf{q}, \tilde{\mathbf{q}} \in K^k$.

Охарактеризуем теперь сложность поиска двух различных таких входных слов: $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^m)^t$ и $\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_t \in (K^m)^t$, что $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t) = H_{\mathbf{f},\mathbf{q}_0}(\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_t)$.

Пусть $t = 1$. Если $k = m$, то в силу (1) не существует двух различных входных символов: $\mathbf{x}_1$ и $\tilde{\mathbf{x}}_1$, для которых истинно равенство $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1)$. Если же $k < m$, то эта сложность совпадает со сложностью поиска одного (не важно, какого именно) решения $(\mathbf{x}_1, \tilde{\mathbf{x}}_1) \in K^m \times K^m$ $(\mathbf{x}_1 \ne \tilde{\mathbf{x}}_1)$ уравнения $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1)$.

Пусть $t > 1$. Если $k < m$, то в качестве $\mathbf{x}_1 \ldots \mathbf{x}_{t-1}$ достаточно выбрать любое входное слово, положить $\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_{t-1} = \mathbf{x}_1 \ldots \mathbf{x}_{t-1}$, а в качестве $\mathbf{x}_t$ и $\tilde{\mathbf{x}}_t$ выбрать любые два такие различные входные символы, что $\mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_{t-1}), \tilde{\mathbf{x}}_t)$.

Если же $k = m$, то в качестве $\mathbf{x}_1 \ldots \mathbf{x}_{t-1}$ и $\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_{t-1}$ достаточно выбрать любые два такие входные слова, что $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_{t-1}) \neq \mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_{t-1})$, а качестве $\mathbf{x}_t$ и $\tilde{\mathbf{x}}_t$ — любые такие входные символы, что $\mathbf{f}(\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \ldots \mathbf{x}_{t-1}), \mathbf{x}_t) = \mathbf{f}(\mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_{t-1}), \tilde{\mathbf{x}}_t)$. При этом допускается равенство $\mathbf{x}_t = \tilde{\mathbf{x}}_t$, так как $\mathbf{x}_1 \ldots \mathbf{x}_{t-1} \neq \tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_{t-1}$.

Таким образом, если известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$, то при любом $t \in \mathbf{N}$ сложность поиска двух различных входных слов: $\mathbf{x}_1 \ldots \mathbf{x}_t \in (K^m)^t$ и $\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_t \in (K^m)^t$, для которых истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \ldots \mathbf{x}_t) = H_{\mathbf{f},\mathbf{q}_0}(\tilde{\mathbf{x}}_1 \ldots \tilde{\mathbf{x}}_t)$, определяется сложностью поиска одного (не важно, какого именно) решения $(\mathbf{x}, \tilde{\mathbf{x}}) \in K^m \times K^m$ (возможно, при дополнительном условии $\mathbf{x} \neq \tilde{\mathbf{x}}$) уравнения $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{f}(\tilde{\mathbf{q}}, \tilde{\mathbf{x}})$ при известных значениях $\mathbf{q}, \tilde{\mathbf{q}} \in K^k$.

Отметим, что если $m > k$, то число скалярных уравнений, определяемых как векторным уравнением $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \tilde{\mathbf{q}}$, так и векторным уравнением $\mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{f}(\tilde{\mathbf{q}}, \tilde{\mathbf{x}})$, меньше числа неизвестных. Это обстоятельство существенно усложняет перебор в процессе поиска решений уравнений над конечным кольцом с делителями нуля (см., например, [4]).

Случай 2. Экспериментатору не известно начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ (при этом, как обычно, предполагается, что любое состояние $\mathbf{q}_0 \in K^k$ может быть выбрано в качестве начального состояния автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ с одной и той же вероятностью), т.е. иными словами, известно семейство $\mathsf{H}_{\mathbf{f}}$ хэш-функций, но не известна хэш-функция $H_{\mathbf{f},\mathbf{q}_0} \in \mathsf{H}_{\mathbf{f}}$.

Пусть $t = 1$. Тогда единственным способом поиска входного символа $\mathbf{x}_1 \in K^m$, для которого истинно равенство $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}$ при фиксированных значениях $\mathbf{q}_0, \mathbf{q} \in K^k$, а также (при условии, что $k < m$) поиска входных символов $\mathbf{x}_1, \tilde{\mathbf{x}}_1 \in K^m$ ($\mathbf{x}_1 \neq \tilde{\mathbf{x}}_1$), для которых истинно равенство $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1)$ при фиксированном значении $\mathbf{q}_0 \in K^k$, является случайный выбор входных символов.

Из (13) вытекает, что вероятность того, что при случайном выборе входного символа $\mathbf{x}_1 \in K^m$ истинно равенство $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{q}$, равна $p^{(1)}_{\mathbf{f},\mathbf{q}_0,1}(\mathbf{q}) = |K|^{-k}$. Аналогичным образом из (14) вытекает, что вероятность того, что при случайном выборе двух различных входных символов $\mathbf{x}_1 \in K^m$ и $\tilde{\mathbf{x}}_1 \in K^m$ истинно равенство $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1) = \mathbf{f}(\mathbf{q}_0, \tilde{\mathbf{x}}_1)$, равна

$$p^{(2)}_{\mathbf{f},\mathbf{q}_0,1}(\mathbf{q}) = |K|^{-k} \left(1 - \frac{|K|^k - 1}{|K|^m - 1}\right).$$

Пусть $t > 1$. Возможны следующие две ситуации.

Ситуация 1. Экспериментатор имеет возможность наблюдать состояние исследуемого автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ на промежуточных вычислениях. Тогда, выбрав произвольный входной символ $\mathbf{x}_1 \in K^m$, экспериментатор определяет текущее состояние $\mathbf{f}(\mathbf{q}_0, \mathbf{x}_1)$ исследуемого автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$, и ситуация сводится к рассмотренному выше случаю 1.

Ситуация 2. Экспериментатор не имеет возможности наблюдать состояние исследуемого автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ на промежуточных вычислениях. Тогда единственным способом поиска входного слова $\mathbf{u} \in (K^m)^t$, для которого истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, а также поиска входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$, для которых истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\widetilde{\mathbf{u}})$, является случайный выбор входных слов. Вероятность того, что при случайном выборе входного слова $\mathbf{u} \in (K^m)^t$ истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, определяется формулой (13), а вероятность того, что при случайном выборе входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$ истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\widetilde{\mathbf{u}})$, определяется формулой (14).

Высокая сложность поиска входного слова $\mathbf{u} \in (K^m)^t$, для которого истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, а также поиска входных слов $\mathbf{u}, \widetilde{\mathbf{u}} \in (K^m)^t$ $(\mathbf{u} \neq \widetilde{\mathbf{u}})$, для которых истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\widetilde{\mathbf{u}})$, обосновывают возможность использования семейства хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ в алгоритмах защиты информации. При этом начальное состояние $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ целесообразно использовать в качестве секретного сеансового ключа используемой хэш-функции.

Рассмотрим теперь задачу параметрической идентификации семейства хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$.

Пусть (3) — система уравнений с параметрами над кольцом K, т.е.

$$\mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1}) = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_t, \mathbf{x}_{t+1}) \ \ (t \in \mathbf{Z}_+),$$

где $a_1, \ldots, a_r \in K$ — параметры. Таким образом, система уравнений (3) имеет вид

$$\mathbf{q}_{t+1} = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_t, \mathbf{x}_{t+1}) \ \ (t \in \mathbf{Z}_+), \tag{15}$$

где отображение $\mathbf{F}$ известно экспериментатору.

Предположим, что экспериментатору не известны значения параметров системы уравнений (15), но он имеет возможность в каждый момент наблюдать состояние исследуемого автомата. Тогда идентификация семейства хэш-функций (15) является задачей параметрической идентификации автомата, принадлежащего заданному множеству автоматов над кольцом K.

При возможности экспериментатора проводить только простой эксперимент решение задачи параметрической идентификации автомата сводится к поиску входного слова $\mathbf{x}_1 \ldots \mathbf{x}_n \in (K^m)^n$ заранее неизвестной длины $n \geq r$ в целях формирования и решения над кольцом K системы уравнений

$$\mathbf{q}_i = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_{i-1}, \mathbf{x}_i) \ \ (i = 1, \ldots, n) \tag{16}$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

При возможности экспериментатора проводить l-кратный эксперимент (где $l \geq 2$ — фиксированное число) решение задачи параметрической идентификации автомата сводится к поиску l-элементного множества входных слов $\mathbf{x}_1^{(i)} \ldots \mathbf{x}_{n_i}^{(i)} \in (K^m)^{n_i}$ $(i = 1, \ldots, l)$, длины n_i которых заранее неизвестны, в целях формирования и решения над кольцом K системы уравнений

$$\mathbf{q}_j^{(i)} = \mathbf{F}(a_1, \ldots, a_r, \mathbf{q}_0, \mathbf{x}_1^{(i)} \ldots \mathbf{x}_j^{(i)}) \ \ (i = 1, \ldots, l;\ j = 1, \ldots, n_i) \tag{17}$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

Ситуация несколько отличается, если экспериментатор может сколько угодно раз устанавливать исследуемый автомат в любое требуемое начальное состояние и при каждой установке начального состояния проводить с исследуемым автоматом кратный эксперимент любой кратности. В этом случае для решения задачи параметрической идентификации автомата достаточно сформировать и решить над кольцом K систему уравнений

$$\widetilde{\mathbf{q}} = F(a_1, \ldots, a_r, \mathbf{q}, \mathbf{x}) \ \ (\mathbf{q} \in K^k, \ \ \mathbf{x} \in K^m) \qquad (18)$$

относительно неизвестных $a_1, \ldots, a_r \in K$.

Отметим, что в кольце с делителями нуля при достаточно большом значении k решение любой из систем уравнений (16)–(18) является сложной задачей из-за перебора, обусловленного именно наличием делителей нуля.

Таким образом, при использовании семейства хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ в алгоритмах защиты информации целесообразно использовать параметры, входящие в уравнение (15), в качестве долговременного секретного ключа.

ЗАКЛЮЧЕНИЕ

В настоящей работе исследованы семейства хэш-функций, определяемые сильно связанными автоматами без выхода над произвольным конечным кольцом $\mathsf{K} = (K, +, \cdot)$ $(|K| \geq 2)$. Анализ вычислительной стойкости показывает, что при нелинейном отображении $\mathbf{f} \in \mathsf{F}_{k,m}$ эти хеш-функции могут использоваться в процессе решения задач защиты информации. При этом параметры, присутствующие в отображении $\mathbf{f} \in \mathsf{F}_{k,m}$, могут использоваться в качестве долговременного секретного ключа, что дает дополнительную возможность центру распределения ключей независимо варьировать распределение семейств хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ между отдельными группами пользователей. Кроме того, в результате использования начального состояния автомата $M_{\mathbf{f}} \in \mathsf{B}_{k,m}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$ в качестве секретного сеансового ключа отдельные пользователи (или их группы) независимо от центра распределения ключей могут варьировать хеш-функции в различных сеансах связи.

Детальный анализ семейств хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$, определяемых полиномами того или иного вида над ассоциативно-коммутативным кольцом K с единицей, представляет дальнейшее направление исследований. Анализ семейств хэш-функций $\mathsf{H}_{\mathbf{f}}$ $(\mathbf{f} \in \mathsf{F}_{k,m})$, определяемых над ассоциативными некоммутативными кольцами с единицей (в частности, над кольцами квадратных матриц того или иного вида над конечными полями), является другим направлением исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Скобелев В.В. Анализ структуры класса линейных автоматов над кольцом Z_{p^k} // Кибернетика и системный анализ. — 2008. — № 3. — С. 60–74.

2. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. — Донецк: ИПММ НАН Украины, 2009. — 479 с.

3. Скобелев В.В., Скобелев В.Г. О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. — 2010. — № 4. — С. 17–30.

4. Скобелев В.В., Глазунов Н.М., Скобелев В.Г.. Многообразия над кольцами. Теория и приложения. — Донецк: ИПММ НАН Украины, 2011. — 323 с.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др. Основы криптографии. — М.: Гелиос АРВ, 2002. — 480 с.

6. Харин Ю.С., Берник В.И., Матвеев Г.В. и др. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 382 с.

7. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001. — 368 с.

8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — М.: Триумф, 2003. — 816 с.

9. Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы (поведение и синтез). — М.: Наука, 1970. — 400 с.

10. Bollobás B. Modern graph theory. — N.Y.: Springer-Verlag, 1998. — 394 p.

Поступила 30.01.2012