Computer Science Journal of Moldova, vol.**26**, no.1(76), 2018

Finite automata over magmas: models and some applications in Cryptography

Volodymyr V. Skobelev, Volodymyr G. Skobelev

Abstract

In the paper the families of finite semi-automata and reversible finite Mealy and Moore automata over finite magmas are defined and analyzed in detail. On the base of these models it is established that the set of finite quasigroups is the most acceptable subset of the set of finite magmas at resolving model problems in Cryptography, such as design of iterated hash functions and stream ciphers. Defined families of finite semi-automata and reversible finite automata over finite T-quasigroups are investigated in detail. It is established that in this case models time and space complexity for simulation of the functioning during one instant of automaton time can be much lower than in general case.

Keywords: magmas, quasigroups, T-quasigroups, iterated hash functions, stream ciphers.

1 Introduction

Challenges of Modern Cryptography have stimulated the development of algebraic models for stream ciphers and computationally secure iterated hash function.

Many efforts have been devoted to the elaboration and analysis of these models, presented via finite, respectively, reversible automata and semi-automata over associative finite algebraic systems (short survey of these results is presented in [1], for example).

Much fewer success has been achieved for applications of finite non-associative algebraic systems at resolving model problems of Cryptography (it is worth to point that some interesting results, connected

with applications of finite quasigroups and rings in the coding and design of crypto-schemes are presented in [2]).

Possibly, this situation is justified by the fact that the classification of these algebraic systems is not complete at present, and their properties demand further deeper studying. Nevertheless the following question naturally arises:

Whether the set of finite quasigroups is the most acceptable subset of the set of finite magmas at resolving model problems in Cryptography, such as design of iterated hash functions and stream ciphers?

In the given paper we show that the answer to this question is YES.

Informally speaking, the expediency for applications of finite quasigroups at resolving model problems of Cryptography is caused by the following two factors.

Firstly, the binary operation in a quasigroup is reversible.

Secondly, the lack of requirements for associativity, commutativity, and existence of the unit element imply high complexity for resolving problems of identification formulated in terms of quasigroups.

A rather complete survey of applications of finite quasigroups for the design of authentication schemes, stream ciphers, and the unidirectional functions, is submitted in [3, 4].

In the present paper, the notions and definitions in Quasigroup Theory are the same as in [5, 6, 7]. The paper is organized as follows. In Section 2 necessary notions and definitions are introduced. In Section 3 models of families of finite semi-automata and automata over finite magmas are defined and analyzed. It is established that the set of finite quasigroups is the most acceptable subset of the set of finite magmas at resolving such model problems of Cryptography, as design of iterated hash functions and stream ciphers. In Section 4 defined models of families of finite semi-automata and automata are investigated over finite T-quasigroups. Section 5 consists of some conclusions.

2 Basic notions

By time and space complexity we mean the asymptotic worst-case complexity under logarithmic weight [8].

Let Q ($|Q| \geq 2$) be fixed finite set, and $\mathcal{S}_Q$ be the symmetric group over the set Q. It is well known that for any substitution $\xi \in \mathcal{S}_Q$ the upper bounds of time and space complexity for computing the value $\xi(a)$ ($\xi \in \mathcal{S}_Q, a \in Q$) are equal, correspondingly, to

$$T_\xi = O(|Q| \log |Q|) \ (|Q| \to \infty), \tag{1}$$

$$V_\xi = O(|Q| \log |Q|) \ (|Q| \to \infty). \tag{2}$$

Similarly, for any binary operation $\circ : Q \times Q \to Q$ the upper bounds of time and space complexity for computing the value $a \circ b$ ($a, b \in Q$) are equal, correspondingly, to

$$T_\circ = O(|Q| \log |Q|) \ (|Q| \to \infty), \tag{3}$$

$$V_\circ = O(|Q|^2 \log |Q|) \ (|Q| \to \infty). \tag{4}$$

Let $\mathfrak{M}_Q$ be the set of all magmas $\mathcal{M} = (Q, \circ)$, where $\circ : Q \times Q \to Q$, $\mathrm{Aut}(\mathcal{M})$ ($\mathcal{M} = (Q, \circ) \in \mathfrak{M}_Q$) be the set of all automorphisms of $\mathcal{M}$, i.e. the set of all bijections $\varphi : Q \to Q$, such that $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$ ($a, b \in Q$). The following subsets of the set $\mathfrak{M}_Q$ are considered, as a rule:

$\mathfrak{S}_Q$ – the set of all semigroups $\mathcal{S} = (Q, \circ)$, i.e. $\circ$ is some associative operation;

$\mathfrak{S}_Q^{(l)}$ – the set of all left-cancellative semigroups $\mathcal{S} = (Q, \circ)$, i.e. $\mathcal{S} \in \mathfrak{S}_Q$, and if $a \circ b = a \circ c$ ($a, b, c \in Q$), then $b = c$;

$\mathfrak{S}_Q^{(r)}$ – the set of all right-cancellative semigroups $\mathcal{S} = (Q, \circ)$, i.e. $\mathcal{S} \in \mathfrak{S}_Q$, and if $b \circ a = c \circ a$ ($a, b, c \in Q$), then $b = c$;

$\mathfrak{S}_Q^{(lr)} = \mathfrak{S}_Q^{(l)} \cap \mathfrak{S}_Q^{(r)}$ – the set of all cancellative semigroups;

$\mathfrak{S}_Q^{(m)}$ – the set of all monoids $\mathcal{S} = (Q, \circ)$, i.e. $\mathcal{S} \in \mathfrak{S}_Q$, and exists an identity element in Q;

$\mathfrak{G}_Q$ – the set of all groups $\mathcal{G} = (Q, \circ)$, i.e. $\circ$ is some invertible associative operation, and there exists an identity element in Q;

$\mathfrak{G}_Q^{(A)}$ – the set of all Abelian groups $\mathcal{G} = (Q, \circ)$, i.e. $\mathcal{G} \in \mathfrak{G}_Q$, and $\circ$ is commutative operation;

$\mathfrak{Q}_Q$ – the set of all quasigroups $\mathcal{Q} = (Q, \circ)$, i.e. $\circ$ is some invertible operation;

$\mathfrak{Q}_Q^{(T)}$ – the set of all T-quasigroups $\mathcal{Q} = (Q, \circ)$, i.e. $\mathcal{Q} \in \mathfrak{Q}_Q$, and there exist $\mathcal{G} = (Q, +) \in \mathfrak{G}_Q^{(A)}$, $(\varphi, \psi) \in \mathrm{Aut}(\mathcal{G}) \times \mathrm{Aut}(\mathcal{G})$, and an element $c \in Q$, such that $a \circ b = \varphi(a) + \psi(b) + c$ $(a, b \in Q)$.

It is well known that the following inclusions hold:

$$\begin{cases} \mathfrak{S}_Q \supseteq \mathfrak{S}_Q^{(l)} \supseteq \mathfrak{S}_Q^{(lr)}, \ \mathfrak{S}_Q \supseteq \mathfrak{S}_Q^{(r)} \supseteq \mathfrak{S}_Q^{(lr)}, \ \mathfrak{S}_Q^{(lr)} \supseteq \mathfrak{G}_Q \supseteq \mathfrak{G}_Q^{(A)}, \\ \mathfrak{S}_Q \supseteq \mathfrak{S}_Q^{(m)} \supseteq \mathfrak{G}_Q, \ \mathfrak{Q}_Q \supseteq \mathfrak{Q}_Q^{(T)}, \ \mathfrak{Q}_Q \supseteq \mathfrak{S}_Q^{(lr)}. \end{cases} \tag{5}$$

For any non-empty either finite, or infinite set Q in the set $\mathfrak{M}_Q$ there can be defined in the usual way the subset $\mathfrak{M}_Q^{(l)}$ of all left-cancellative magmas, the subset $\mathfrak{M}_Q^{(r)}$ of all right-cancellative magmas, and the subset $\mathfrak{M}_Q^{(lr)}$ of all cancellative magmas. It is evident that $\mathfrak{M}_Q^{(lr)} \supseteq \mathfrak{S}_Q^{(lr)}$, and the following proposition is true.

Proposition 1. *If the set Q is infinite, then $\mathfrak{Q}_Q \subset \mathfrak{M}_Q^{(lr)}$, while if the set Q is finite, then $\mathfrak{Q}_Q = \mathfrak{M}_Q^{(lr)}$.*

It has been assumed that only a finite set Q is considered. By this reason, each time when the set $\mathfrak{Q}_Q$ is considered, we deal in essence with the set $\mathfrak{M}_Q^{(lr)}$.

A finite automaton is a system $M = (S, X, Y, \delta, \lambda)$, where S, X and Y are respectively the finite set of states, the finite input alphabet and the finite output alphabet, $\delta : S \times X \to S$ is the transition mapping and $\lambda : S \times X \to Y$ is the output mapping. We remind that a system $M = (S, X, \delta)$ (i.e. the output alphabet Y and the output mapping λ are omitted) is called a semi-automaton. The mappings δ and λ can be extended on the set $S \times X^*$ by identities:

$$\begin{cases} \delta(s, \Lambda) = s, \ \ \delta(s, wx) = \delta(\delta(s, w), x) \\ \lambda(s, \Lambda) = \Lambda, \ \ \lambda(s, wx) = \lambda(s, w)\lambda(\delta(s, w), x) \end{cases} \tag{6}$$

for all $s \in S$, $w \in X^*$ and $x \in X$.

Any initial automaton (M, s_{in}) (where $s_{in} \in S$ is some fixed initial state) implements the mapping $F_{(M,s_{in})} : X^* \to Y^*$ defined by identity

$$F_{(M,s_{in})}(w) = \lambda(s_{in}, w) \ \ (w \in X^*).$$

A finite automaton $M = (S, X, Y, \delta, \lambda)$ is reversible if and only if for each $s_{in} \in S$ the mapping $F_{(M,s_{in})}$ is a bijection. Let the mapping $\lambda_s : X \to Y$ $(s \in S)$ be defined by identity $\lambda_s(x) = \lambda(s, x)$ $(x \in X)$. It is evident that the following proposition is true.

Proposition 2. *A finite automaton $M = (S, X, Y, \delta, \lambda)$ is reversible if and only if for each its state $s \in S$ the mapping λ_s is a bijection.*

Thus, there exists an effective algorithm for checking whether the analyzed finite automaton $M = (S, X, Y, \delta, \lambda)$ is reversible.

The following two models are considered for a finite automaton $M = (S, X, Y, \delta, \lambda)$. as a rule:

1) a Mealy automaton if for the output mapping λ both variables $s \in S$ and $x \in X$ are essential;

2) a Moore automaton if for the output mapping λ the variable $x \in X$ is dummy (by this reason it is usually supposed that $\lambda : S \to Y$ for a Moore automaton).

If an automaton $M = (S, X, Y, \delta, \lambda)$ is considered as a dynamic system it is supposed that its functioning is carried out according to the following recurrence relations: $s_{t+1} = \delta(s_t, x_t)$, $y_{t+1} = \lambda(s_t, x_t)$ (for a Mealy automaton) and $y_{t+1} = \lambda(s_{t+1})$ (for a Moore automaton).

3 Analysis of models of finite semi-automata and automata over magmas

When defining a finite automaton over any magma it is convenient to assume that the basic set of the magma is the set of states, as well as the input and output alphabets of the automaton. Accepting this assumption the following finite automata models over the set $\mathfrak{M}_Q$ can be defined.

For any magma $\mathcal{M} \in \mathfrak{M}_Q$, where $\mathcal{M} = (Q, \circ)$, it can be defined the 2-elements family of semi-automata

$$\mathcal{F}_{\mathcal{M}} = \{M^{(i)} = (Q, Q, \delta^{(i)}_{\mathcal{M}})\}_{i \in \{l,r\}},$$

where the transition mappings $\delta^{(i)}_{\mathcal{M}}$ $(i = 1, 2)$ are defined as follows:

$$\delta^{(i)}_{\mathcal{M}}(q, x) = \begin{cases} x \circ q, & \text{if } i = l, \\ q \circ x, & \text{if } i = r. \end{cases} \tag{7}$$

Here and everywhere further the symbol q denotes a state and the symbol x denotes an input symbol.

Formula (7) implies that the upper bounds of time and space complexity for simulation of the functioning of any semi-automaton $M \in \mathcal{F}_{\mathcal{M}}$ during one instant of the semi-automaton time are defined according to formulae (3) and (4).

Let Γ_M be the transition diagram of a semi-automaton $M \in \mathcal{F}_{\mathcal{M}}$. It is evident that the following proposition is true.

Proposition 3. *The transition diagram Γ_M $(M \in \mathcal{F}_{\mathcal{M}})$ is the labelled directed complete $|Q|$-graph with the loop at each vertex, such that the labels of all arcs terminated in any vertex are pair-wise different if and only if $M \in \mathfrak{M}^{(lr)}_Q$, i.e. when $M \in \mathfrak{Q}_Q$.*

For any ordered pair of magmas $(\mathcal{M}_1, \mathcal{M}_2) \in \mathfrak{M}_Q \times \mathfrak{M}_Q$, where $\mathcal{M}_j = (Q, \circ_j)$ $(j = 1, 2)$, it can be defined the 4-elements family of Mealy automata

$$\mathcal{F}_{\mathcal{M}_1, \mathcal{M}_2} = \{M^{(i,j)} = (Q, Q, Q, \delta^{(i)}_{\mathcal{M}_1}, \lambda^{(j)}_{\mathcal{M}_2})\}_{i,j \in \{l,r\}},$$

where the transition mappings $\delta^{(i)}_{\mathcal{M}_1}$ $(i \in \{l, r\})$ are defined in accordance with formula (7) applied to the magma $\mathcal{M}_1$, and the output mappings $\lambda^{(j)}_{\mathcal{M}_2}$ $(j \in \{l, r\})$ are defined as follows:

$$\lambda^{(j)}_{\mathcal{M}_2}(q, x) = \begin{cases} x \circ_2 q, & \text{if } j = l, \\ q \circ_2 x, & \text{if } j = r. \end{cases} \tag{8}$$

Formulae (7) and (8) imply that the upper bounds of time and space complexity for computing each of the values $\delta^{(i)}_{\mathcal{M}_1}(q,x)$ $(i \in \{l,r\})$ and $\lambda^{(j)}_{\mathcal{M}_2}(q,x)$ $(j \in \{l,r\})$ are defined according to formulae (3) and (4).

Thus, the upper bounds of time and space complexity for simulation of the functioning of any automaton $M \in \mathcal{F}_{\mathcal{M}_1,\mathcal{M}_2}$ during one instant of the automaton time are also defined according to formulae (3) and (4).

For any ordered pair $(\mathcal{M},\xi) \in \mathfrak{M}_Q \times \mathcal{S}_Q$, where $\mathcal{M} = (Q,\circ)$, it can be defined the 2-elements family of Moore automata

$$\mathcal{F}_{\mathcal{M},\xi} = \{M^{(i)} = (Q,Q,Q,\delta^{(i)}_{\mathcal{M}},\xi\delta^{(i)}_{\mathcal{M}})\}_{i\in\{l,r\}},$$

where the transition mappings $\delta^{(i)}_{\mathcal{M}_1}$ $(i \in \{l,r\})$ are defined in accordance with formula (7), and the output mappings $\xi\delta^{(i)}_{\mathcal{M}}$ $(i \in \{l,r\})$ are defined as follows:

$$\xi\delta^{(i)}_{\mathcal{M}}(q,x) = \xi(\delta^{(i)}_{\mathcal{M}}(q,x)). \tag{9}$$

It has been established above that the upper bounds of time and space complexity for computing the value $\delta^{(i)}_{\mathcal{M}}(q,x)$ $(i \in \{l,r\})$ are defined according to formulae (3) and (4). Formula (9) implies that if the value $\delta^{(i)}_{\mathcal{M}}(q,x)$ $(i \in \{l,r\})$ has been computed previously, then the upper bounds of time and space complexity for computing the value $\xi\delta^{(i)}_{\mathcal{M}}(q,x)$ are defined according to formulae (1) and (2).

The comparison of formulae (1) and (2) according to formulae (3) and (4) implies that the upper bounds of time and space complexity for simulation of the functioning of any automaton $M \in \mathcal{F}_{\mathcal{M},\xi}$ during one instant of the automaton time are also defined by formulae (3) and (4).

Let's analyze what restrictions can be imposed on the structure of the models defined above in order to apply them successfully at resolving model problems of Cryptography.

It is evident that any iterated hash function is, in its essence, some finite semi-automaton. The structure of such semi-automaton has been investigated in [9] (and shortly presented in [1]) as follows.

Let K be some finite set, $k,m \in \mathbb{N}_+$ $(k \leq m)$ be fixed integers, and $\mathcal{F}_{k,m}$ be the set of all mappings $\mathbf{f} : K^k \times K^m \to K^k$, such that the

following two equalities:

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

$$\{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m | \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \emptyset \tag{11}$$

hold for all $\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k$ $(\mathbf{q} \neq \mathbf{q}')$.

Any mapping $\mathbf{f} \in \mathcal{F}_{k,m}$ defines the strongly connected semi-automaton $M_{\mathbf{f}} = (K^k, K^m, \mathbf{f})$, which, in its turn, defines the family of iterated hash functions $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$, where $H_{\mathbf{f},\mathbf{q}_0} : (K^m)^+ \to K^k$ is the mapping, such that $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{w}) = \mathbf{f}(\mathbf{q}_0, \mathbf{w})$ $(\mathbf{w} \in (K^m)^+)$.

Let $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q})$ $(\mathbf{f} \in \mathcal{F}_{k,m}; \mathbf{q}_0, \mathbf{q} \in K^k; t \in \mathbb{N}_+)$ be probability that an input string $\mathbf{u}$ randomly selected in the set $(K^m)^t$ is some solution of the equation $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, and $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t}$ $(\mathbf{f} \in \mathcal{F}_{k,m}, \mathbf{q}_0 \in K^k, t \in \mathbb{N}_+)$ be probability that for two different input strings $\mathbf{u}$ and $\mathbf{u}'$ randomly selected in the set $(K^m)^t$ the equality $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}')$ holds. The following two theorems are true:

Theorem 1. [9]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ *and any* $\mathbf{q}_0, \mathbf{q} \in K^k$ *equality* $p^{(1)}_{\mathbf{f},\mathbf{q}_0,t}(\mathbf{q}) = |K|^{-k}$ *holds for all* $t \in \mathbb{N}_+$.

Theorem 2. [9]. *For any mapping* $\mathbf{f} \in \mathcal{F}_{k,m}$ *and any* $\mathbf{q}_0 \in K^k$ *equality* $p^{(2)}_{\mathbf{f},\mathbf{q}_0,t} = |K|^{-k}(1 - (|K|^{mt} - 1)^{-1}(|K|^k - 1)$ *holds for all* $t \in \mathbb{N}_+$.

Theorems 1 and 2 characterize computational security for any family $\{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0 \in K^k}$ $(\mathbf{f} \in \mathcal{F}_{k,m})$ of iterated hash functions. It is evident that these values of probabilities are the best least estimations that can be established theoretically on the base of probabilistic approach.

Formulae (10) and (11) imply that if $K = Q$ and $k = m = 1$, then $\mathcal{F}_{1,1}$ is the set of all invertible binary operations on the set Q. Hence, if $K = Q$ and $k = m = 1$, then $\{M_{\mathbf{f}}\}_{\mathbf{f} \in \mathcal{F}_{1,1}}$ is the set of all semi-automata on the set $\mathfrak{Q}_Q$ with the transition mapping defined by formula (7). Thus, the following theorem is proved.

Theorem 3. *For any quasigroup* $\mathcal{Q} \in \mathfrak{Q}_Q$ *each semi-automaton* $M^{(i)} = (Q, Q, \delta^{(i)}_{\mathcal{Q}}) \in \mathcal{F}_{\mathcal{Q}}$ $(i \in \{l, r\})$ *defines the family* $\{H_{\delta^{(i)}_{\mathcal{Q}},q_0}\}_{q_0 \in Q}$

of iterated hash functions, such that equalities

$$p^{(1)}_{\delta^{(i)}_{\mathcal{Q}},q_0,t}(q) = |Q|^{-1} \ \ (q_0, q \in Q)$$

and

$$p^{(2)}_{\delta^{(i)}_{\mathcal{Q}},q_0,t} = |Q|^{-1}(1 - (|Q|^t - 1)^{-1}(|Q| - 1) \ \ (q_0 \in Q)$$

hold for all $t \in \mathbb{N}_+$.

Summing up, we conclude that if the transition mapping can be defined only by formula (7) then for the design of families of Cryptographic iterated hash functions the set of semi-automata defined on the set $\mathfrak{Q}_Q$ is the most acceptable subset of the set of all semi-automata defined on the set $\mathfrak{M}_Q$.

Taking this factor into account, we can restrict ourselves to consider the families of finite Mealy automata

$$\mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} = \{M^{(i,j)} = (Q, Q, Q, \delta^{(i)}_{\mathcal{Q}_1}, \lambda^{(j)}_{\mathcal{Q}_2})\}_{i,j\in\{l,r\}} \ \ (\mathcal{Q}_1, \mathcal{Q}_2 \in \mathfrak{Q}_Q)$$

and the families of finite Moore automata

$$\mathcal{F}_{\mathcal{Q},\xi} = \{M^{(i)} = (Q, Q, Q, \delta^{(i)}_{\mathcal{Q}}, \xi\delta^{(i)}_{\mathcal{Q}})\}_{i\in\{l,r\}} \ \ (\mathcal{Q} \in \mathfrak{Q}_Q, \xi \in \mathcal{S}_Q).$$

Since the binary operation in any quasigroup is invertible and any $\xi \in \mathcal{S}_Q$ is a bijection, then formulae (8), (9) and Proposition 2 imply that the following proposition is true.

Proposition 4. *Any family* $\mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2}$ $(\mathcal{Q}_1, \mathcal{Q}_2 \in \mathfrak{Q}_Q)$ *of finite Mealy automata and any family* $\mathcal{F}_{\mathcal{Q},\xi}$ $(\mathcal{Q} \in \mathfrak{Q}_Q, \xi \in \mathcal{S}_Q)$ *of finite Moore automata consists of reversible automata.*

Propositions 1 and 4 imply that if the transition mapping can be defined only by formula (7) and the output mapping can be defined only by formula (8) (correspondingly, by formula (9)), then at the resolving the problem of the design of stream ciphers the set of all finite Mealy (correspondingly, Moore) automata defined on the set $\mathfrak{Q}_Q$ is the maximal admissible subset of the set of all Mealy (correspondingly, Moore) automata defined on the set $\mathfrak{M}_Q$.

Let us analyze computational security of a stream cipher presented by some finite automaton $M \in \mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} \cup \mathcal{F}_{\mathcal{Q},\xi}$ $(\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q} \in \mathfrak{Q}_Q; \xi \in \mathcal{S}_Q)$.

It is evident that the initial state of the automaton M can be some fragment of the session key. By induction on the length of an input sequence it can be proved that the following theorem is true.

Theorem 4. *For any finite automaton*

$$M \in \mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} \cup \mathcal{F}_{\mathcal{Q},\xi} \ (\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q} \in \mathfrak{Q}_Q; \xi \in \mathcal{S}_Q)$$

the number of pre-images for each output string of the length $l \in \mathbb{N}_+$ *equals to* $|Q|$.

The established estimation does not depend on the length of the output sequence. By this reason, any stream cipher presented by the single automaton $M \in \mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} \cup \mathcal{F}_{\mathcal{Q},\xi}$ $(\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q} \in \mathfrak{Q}_Q; \xi \in \mathcal{S}_Q)$ with the initial state being the secret session key is not computationally secure. It is possible to eliminate this situation as follows.

Let G_1 and G_2 be some pseudo random generators that generate integers, correspondingly, $1, \ldots, |Q|$, and $1, \ldots, k$. The stream cipher can be defined as the system $\mathbf{C} = (M, \mathrm{G}_1, \mathrm{G}_2)$ with the initializations of pseudo-random generators G_1 and G_2 being the secret session key. The stream cipher $\mathbf{C}$ is functioning as follows.

The generators G_1 and G_2 generate some integers i_1 and i_2. The finite automaton M is initialized at its i_1-th state and the current input sequence fragment of the length i_2 is transformed. These actions are repeated until all input sequence would be processed.

Theorem 4 implies that the following theorem is true.

Theorem 5. *Let* $M \in \mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} \cup \mathcal{F}_{\mathcal{Q},\xi}$ $(\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q} \in \mathfrak{Q}_Q; \xi \in \mathcal{S}_Q)$ *and the pseudo random generators* G_1 *and* G_2 *generate integers, correspondingly,* $1, \ldots, |Q|$ *and* $1, \ldots, k$. *Then for the stream cipher* $\mathbf{C} = (M, \mathrm{G}_1, \mathrm{G}_2)$ *with the initializations of pseudo-random generators* G_1 *and* G_2 *being the secret session key the number of pre-images for each output string of the length* $l \in \mathbb{N}_+$ *is not less than* $|Q|^{k^{-1}l}$.

Since $k > 0$ is some fixed integer, then $|Q|^{k^{-1}l} \to \infty$ when $l \to \infty$. Thus, any stream cipher $\mathbf{C} = (M, \mathrm{G}_1, \mathrm{G}_2)$ with the initializations of

pseudo-random generators G_1 and G_2 being the secret session key can be considered as computationally secure stream cipher.

Computational security of stream ciphers defined by the considered finite automata can be significantly increased if instead of the single automaton $M \in \mathcal{F}_{\mathcal{Q}_1,\mathcal{Q}_2} \cup \mathcal{F}_{\mathcal{Q},\xi}$ $(\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q} \in \mathfrak{Q}_Q; \xi \in \mathcal{S}_Q)$ to deal with the set $\mathrm{S} = \{M_1, \ldots, M_n\}$ $(n \geq 2)$ of finite automata, where $M_j \in \mathcal{F}_{\mathcal{Q}_1^{(j)},\mathcal{Q}_2^{(j)}} \cup \mathcal{F}_{\mathcal{Q}^{(j)},\xi^{(j)}}$ $(\mathcal{Q}_1^{(j)}, \mathcal{Q}_2^{(j)}, \mathcal{Q}^{(j)} \in \mathfrak{Q}_Q; \xi^{(j)} \in \mathcal{S}_Q)$.

Indeed, let G_3 be some pseudo random generator that generates integers $1, \ldots, n$. This generator selects the automaton $M \in \mathrm{S}$ for transformation of the current input sequence fragment. Then the stream cipher $\mathbf{C} = (\mathrm{S}, \mathrm{G}_1, \mathrm{G}_2, \mathrm{G}_3)$ with the initializations of pseudo-random generators G_1, G_2 and G_3 being the secret session key can be designed. It is evident that for this stream cipher the number of pre-images for each output string of the length $l \in \mathbb{N}_+$ is some integer from the interval $[|Q|^{k^{-1}l}, |Q|^{k^{-1}nl}]$.

It is worth to note that even for the fixed integer n $(n \geq 2)$ searching of the sets S that maximize the number of pre-images for each output string is a hard problem.

Summing up, we conclude that if the transition mapping can be defined only by formula (7) and the output mapping can be defined only either by formula (8) or by formula (9), then at the resolving the problem of the design of stream ciphers the set of all finite Mealy and Moore automata defined on the set $\mathfrak{Q}_Q$ is the most acceptable subset of the set of all finite automata defined on the set $\mathfrak{M}_Q$.

4 Finite semi-automata and automata over quasigroups

Families of finite semi-automata and automata, defined on abstract finite quasigroups, have been investigated in detail in [10]. The most important of these results have been presented in Section 3 from a little different point of view.

In [11] families of finite semi-automata and automata defined on finite T-quasigroups have been investigated in detail. In this case the

basic idea has been as follows.

Any Abelian group $\mathcal{G} = (Q, +) \in \mathfrak{G}_Q^{(A)}$ generates 3-parametric family of T-quasigroups

$$\mathrm{F}_{\mathcal{G}} = \{(Q, +, \varphi, \psi, c)\}_{\varphi,\psi \in \mathrm{Aut}(\mathcal{G}), c \in Q},$$

where $(Q, +, \varphi, \psi, c)$ denotes the T-quasigroup $(Q, \circ) \in \mathfrak{Q}_Q^{(T)}$, such that $a \circ b = \varphi(a) + \psi(b) + c$. The following theorem is true.

Theorem 6. [11]. *Any Abelian group $\mathcal{G} = (Q, +) \in \mathfrak{G}_Q^{(A)}$ generates 3-parametric family $\mathrm{F}_G = \{(Q, +, \varphi, \psi, c)\}_{\varphi,\psi \in Aut(\mathcal{G}), c \in Q}$ of pair-wise different T-quasigroups.*

Thus, the family $\mathrm{F}_{\mathcal{G}}$ ($\mathcal{G} \in \mathfrak{G}_Q^{(A)}$) can be considered as the set of all T-quasigroups generated by the Abelian group $\mathcal{G}$.

It is evident that any set $\mathrm{F}_{\mathcal{G}}$ ($\mathcal{G} \in \mathfrak{G}_Q^{(A)}$) can be used as some base for designing families of finite semi-automata, and families of finite Mealy and Moore automata, such that the transition mapping is defined by formula (7) and the output mapping is defined, correspondingly, by formula (8) or by formula (9).

For finite semi-automata and automata designed in a such way the upper bounds of time and space complexity for simulation of the functioning during one instant of automaton time can be lowered (in comparison with formulae (3) and (4)) as follows.

Let $|Q| = p_1^{r_1} \dots p_m^{r_m}$, where $m \geq 1$, $r_i \geq 1$ $(i = 1, \dots, m)$, and p_i $(i = 1, \dots, m)$ be pair-wise different prime integers. Then any Abelian group $\mathcal{G} = (Q, +) \in \mathfrak{G}_Q^{(A)}$ can be uniquely presented as the direct sum of cyclic subgroups of prime-power order

$$\mathcal{G} \cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i} (\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}) \right), \tag{12}$$

where d_{ij} $(i = 1, \dots, m; j = 1, \dots, k_i)$ are fixed positive integers, such that $1 \leq d_{i1} \leq \dots \leq d_{ik_i}$ and $r_i = d_{i1} + \dots + d_{ik_i}$ for all $i = 1, \dots, m$; $\mathbb{Z}_{p_j^{d_{ij}}} = \{0, 1, \dots, p_j^{d_{ij}} - 1\}$, and by $+_{ij}$ it is denoted a module $p_j^{d_{ij}}$

addition for all $i = 1, \ldots, m$ and $j = 1, \ldots, k_i$. The following theorem is true.

Theorem 7. [11]. *Let $\mathcal{G} = (Q, +) \in \mathfrak{G}_Q^{(A)}$, where $|Q| = p_1^{r_1} \ldots p_m^{r_m}$, $m \geq 1$, $r_i \geq 1$ $(i = 1, \ldots, m)$, and p_i $(i = 1, \ldots, m)$ are pair-wise different prime integers. For any T-quasigroup $(Q, \circ) = (Q, +, \varphi, \psi, c) \in \mathrm{F}_{\mathcal{G}}$ time and space complexity for computing the value $a \circ b$ $(a, b \in Q)$ are equal, correspondingly, to*

$$T_\circ = O(\max\{p_i^{d_{ij}} d_{ij} \log p_i | i = 1, \ldots, m \wedge$$

$$\wedge\, j = 1, \ldots, k_i\})\ (\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty), \tag{13}$$

$$V_\circ = O(m \cdot \max\{d_{ij} \log p_i | i = 1, \ldots, m \wedge$$

$$\wedge\, j = 1, \ldots, k_i\})\ (\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty). \tag{14}$$

Comparing formulae (13) and (14) according to formulae (3) and (4) we conclude that for finite semi-automata and automata designed on T-quasigroups $(Q, \circ) = (Q, +, \varphi, \psi, c) \in \mathrm{F}_{\mathcal{G}}$ time and space complexity for simulation of the functioning during one instant of automaton time can be much lower than in general case.

Considering finite semi-automata and automata on T-quasigroups $(Q, \circ) = (Q, +, \varphi, \psi, c) \in \mathrm{F}_{\mathcal{G}}$ it is necessary to mark the following circumstance especially.

It is well known that any elliptic curve γ over any finite field defines the Abelian group $\mathcal{G}_\gamma = (G_\gamma, +_\gamma)$, where G_γ is the set of all points of γ including specified point $\mathcal{O}$ that serves as the neutral element of the group $\mathcal{G}_\gamma$. Families of finite Mealy and Moore automata defined by recurrence relations on the group $\mathcal{G}_\gamma$ have been considered in [1]. It has been established that identification for these automata is a hard problem. Thus, these finite automata can be used at resolving information protection problems.

Proceeding from the Abelian group G_γ the set $\mathrm{F}_{\mathcal{G}_\gamma}$ of T-quasigroups can be constructed. On the base of this set, families of finite semi-automata, and families of finite Mealy and Moore automata, such that the transition mapping is defined by formula (7) and the output mapping is defined by formula (8) or by formula (9), can be designed.

These generalizations of families of finite Mealy and Moore automata that have been considered in [1] imply the feasibility for using finite T-quasigroups at resolving information protection problems.

5 Conclusions

In the given paper families of finite semi-automata and reversible finite Mealy and Moore automata have been defined and analyzed. These models have been applied to establish that the set of finite quasigroups (i.e. the maximal subset of cancellative finite magmas) is the most acceptable subset of the set of finite magmas at resolving model problems in Cryptography, such as design of iterated hash functions and stream ciphers.

It has been also established that the set of finite T-quasigroups can be applied for designing families of finite semi-automata and reversible finite Mealy and Moore automata, such that, both, time and space complexity for simulation of the functioning during one instant of automaton time is much lower than in general case.

The following further research can be pointed.

Firstly, it is the investigation in detail of the sets of families of finite semi-automata and reversible finite Mealy and Moore automata generated by the sets $\mathrm{F}_{\mathcal{G}}$ ($\mathcal{G} \in \mathfrak{G}_Q^{(A)}$) under the supposition that in the decomposition (12) the integers $p_j^{d_{ij}}$ ($i = 1, \ldots, m; j = 1, \ldots, k_i$) differ a little from each other.

The significance of this case consists in the fact that for such semi-automata and reversible finite Mealy and Moore automata, both, time and space complexity for simulation of the functioning during one instant of automaton time are very close to the minimal possible simulation time.

Secondly, it is important to define and to investigate in detail sufficiently narrow non-trivial subsets S of the set $\mathfrak{Q}_Q$ that differ from the subset $\mathfrak{Q}_Q^{(T)}$ and satisfy exactly to one of the following two excluding each other conditions.

The first condition consists that for any quasigroup $\mathcal{G} \in \mathrm{S}$ time and space complexity of computing $a \circ b$ $(a, b \in Q)$ is close to estimations established by formulae (3) and (4).

In this case for semi-automata and reversible finite Mealy and Moore automata defined on the set S, both, time and space complexity for simulation of the functioning during one instant of automaton time are very close to estimations established by formulae (3) and (4).

The second condition consists in the fact that for any set Q there exists some positive integer m such that $m = o(|Q|)$ $(|Q| \to \infty)$, and for any quasigroup $\mathcal{G} \in \mathrm{S}$ time and space complexity of computing $a \circ b$ $(a, b \in Q)$ are defined by formulae

$$T_\circ = O(m^{-1}|Q| \log m^{-1}|Q|) \ \ (|Q| \to \infty), \tag{15}$$

$$V_\circ = O(m \log m^{-1}|Q|) \ \ (|Q| \to \infty), \tag{16}$$

In this case for semi-automata and reversible finite Mealy and Moore automata defined on the set S, both, time and space complexity for simulation of the functioning during one instant of automaton time are very close to estimations established by formulae (15) and (16).

References

[1] V.V. Skobelev, and V.G. Skobelev, "Finite automata over algebraic structures: models and some methods of analysis," *Computer Science Journal of Moldova*, vol. 23, no. 2, pp. 165–188, 2015.

[2] V.T. Markov, A.V. Michajlev, A.V. Gribov, P.A. Zolotykh, and S.S. Skazenik, "Quasigroups and rings in coding and design of crypto-schemes," *Prikladnaya Diskretnaya Matematika*, no. 4, pp. 31–52, 2012. ISSN:2071-0410. (in Russian)

[3] M.M. Glukhov, "On applications of quasigroups in Cryptography," *Prikladnaya Diskretnaya Matematika*, no. 2, pp. 28–32, 2008. ISSN:2071-0410. (in Russian)

[4] V.A. Shcherbacov, "Quasigroups in Cryptology," *Computer Science Journal of Moldova*, vol. 17, no. 2, pp. 193–228, 2009.

[5] V.D. Belousov, *Backgrounds of quasigroups and loops theory*, Moscow, USSR: Nauka, 1967. (in Russian)

[6] V.A. Shcherbacov, *Elements of quasigroup theory and applications*, Boca Raton, Florida, USA: CRC Press, 2017, 576p.

[7] T. Kepka, and P. Nemec, "T-quasigroups. I," *Acta Univ. Carolin. Math. Phys.*, vol. 12, no. 1, pp. 39–49, 1971.

[8] A.V. Aho, J.E. Hopcroft, and J.D. Ullman, *The design and analysis of computer algorithms*, Boston, MA, USA: Addison-Wesley, 1975.

[9] V.V. Skobelev, "Analysis of families of hash functions defined by automata over a finite ring," *Cybernetics and Systems Analysis*, vol. 49, no. 2, pp. 209–216, 2013.

[10] V.V. Skobelev, and V.G. Skobelev, "Automata over abstract finite quasigroups," *Cybernetics and Systems Analysis*, vol. 53, no. 5, pp. 669–674, 2017.

[11] V.V. Skobelev, and V.G. Skobelev, "Automata over finite T-quasigroups," *Cybernetics and Systems Analysis*, vol. 54, no. 3, pp. 345–356, 2018.

Volodymyr V. Skobelev, Volodymyr G. Skobelev Received April 11, 2018

Volodymyr V. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 066 276 85 72
E–mail: volodimirvskobelev@gmail.com

Volodymyr G. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 063 431 86 05
E–mail: skobelevvg@gmail.com