Quasigroups and Related Systems **28** (2020), 319 – 338

Families of semi-automata in finite quasigroups and iterated hash functions

Volodymyr G. Skobelev and Volodymyr V. Skobelev

Abstract. Families of semi-automata defined by a recurrence relation in a finite quasigroup are investigated. Initially, these families are defined in an abstract finite quasigroup, and their structure is studied. It is shown that from a probabilistic point of view these semi-automata are the best mathematical models for computationally secure families of iterated hash functions. Then families of semi-automata in T-quasigroups determined by a finite Abelian group are defined, and their structure is studied. Representation of these semi-automata by the parallel composition of the ones defined in T-quasigroups determined by cyclic groups of prime power order is considered. This decomposition results in speed up the functioning and reducing space complexity of a semi-automaton. In addition, families of semi-automata in the Abelian group of an elliptic curve over a finite field are investigated.

1. Introduction

Over the past two decades, intensive research of quasigroups has been largely caused by their successful applications in various fields, including cryptography. The significance of the latter is as follows.

Currently, the main approach to solving cryptography problems relies on algebraic models. Most of them are built in finite associative algebraic systems. However, for algebraic systems without the requirements "to be associative", "to be commutative", and "to be with unit", high complexity of solving identification problems is typical. Such algebraic systems include quasigroups [2, 18], i.e. magma with both left and right division. It seems promising to apply quasigroups to solving cryptography problems due to the following two circumstances, at least. Firstly, they have been applied successfully in the design of basic cryptography primitives including block and stream ciphers, public key crypto-schemes, signature schemes, codes, and hash functions [7, 10, 13, 14]. Secondly, a hardware implementation of encryption based on a finite quasigroup has been designed [15]. Some applications of quasigroups to solving cryptography problems have also been considered in [3, 4, 17].

Among the above pointed cryptography primitives, hash functions should be noted, since they are widely used for information protection. We remind, that any

2010 Mathematics Subject Classification: 20N05, 20K01, 68Q70, 94A60
Keywords: finite quasigroups, finite T-quasigroups, semi-automata, hash functions, computational security, elliptic curves

hash function is a mapping that transforms any binary string (a message) into a binary string of some fixed length (this string is the hash value or, simply, the hash). Informally, a cryptographic hash function (see [16], for example) satisfies the following four conditions:

1. The hash of any message can be computed sufficiently easy.
2. It is infeasible to reconstruct the original message via its hash.
3. It is infeasible to find two different messages with the same hash.
4. Small changes in a message lead to uncorrelated changes in its hash.

Numerous attempts for the design and implementation of cryptographic hash functions have led to the notion of an iterated hash function [16]. It can be characterized as follows. The original message is divided into the blocks of the equal length. If necessary, the last block is extended to the required length by its concatenation with some fixed string. Some fixed block is added as the initial fragment. Firstly, this block is hashed in accordance with a certain rule. Then the iterative process starts: the next hash is computed from the current hash and the current block of the message. The final hash is the hash of the original message.

It is evident that a mathematical model for iterated hash function is a semi-automaton, i.e. an automaton without output mapping. Hence, investigation of families of semi-automata defined by recurrence relations in a finite quasigroup due to their possible applications as mathematical models of iterated hash function is actual from both theoretic and applied point of view. Some attempts to solve this problem have been done in [19-21]. The main aim of the given paper is to generalize and to unify these results. By time and space complexity we mean asymptotic the worst-case complexity under logarithmic weight [1].

The rest of the paper is organized as follows. Section 2 contains mathematical notions and structures sufficient to present the results. In Section 3 basic families of semi-automata defined by a recurrence relation in a finite abstract quasigroup are investigated. In Section 4 these families of semi-automata are detailed for finite T-quasigroups. Section 5 is devoted to semi-automata defined by a recurrence relation in the Abelian group of an elliptic curve over a finite field. Section 6 is some discussion of obtained results. Section 7 contains concluding remarks.

2. Mathematical backgrounds

2.1. Abstract quaigroups and iterated hash functions

A semi-automaton (SA) is a triple $M = (Q, X, \delta)$, where Q ($|Q| \geqslant 2$) is a finite set of states, X is a finite input alphabet, and $\delta : Q \times X \to Q$ is the transition mapping. This mapping can be extended onto the set $Q \times X^+$ by the equality $\delta(q, wx) = \delta(\delta(q, w), x)$ $(w \in X^+, x \in X)$.

An initial SA is a pair (M, q) $(q \in Q)$, where q is the initial state. Any initial SA (M, q) implements the mapping $H_{(M,q)} : X^+ \to Q$ defined by the equality $H_{(M,q)}(w) = \delta(q, w)$ $(w \in X^+)$. This mapping can be interpreted as an iterated

hash function. Hence, any SA $M = (Q, X, \delta)$ implements the family of iterated hash functions $\mathfrak{H}_M = \{H_{(M,q)}\}_{q \in Q}$.

Let $\mathfrak{Q}_Q$ be the set of all quasigroups with the finite carrier Q ($|Q| \geqslant 2$).

Based on the Cayley table, we get for any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ that the upper bounds of time and space complexity for computation the element $a \circ b$ ($a, b \in Q$) are equal, correspondingly, to:

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

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

Besides, for any mapping $\chi : Q \to Q$ the upper bounds of time and space complexity for computation the value $\chi(a)$ ($a \in Q$) are equal, correspondingly, to:

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

$$V_\chi = O(|Q| \log |Q|) \quad (|Q| \to \infty). \tag{4}$$

Any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ can be presented by the labeled directed graph $\Gamma_\mathcal{Q}$ with the set of vertices Q such that for any $q_1, q_2, q \in Q$ there is an arc started in the vertex q_1, terminated in the vertex q_2, and labeled by the element q if and only if $q_1 \circ q = q_2$. It is evident that $\Gamma_\mathcal{Q}$ is completed labeled directed graph with a single loop in each vertex. Besides, for any vertex $q \in Q$, all $|Q|$ arcs started in q terminate in pair-wise different vertices, and exactly $|Q|$ arcs are terminated in q and labels of these arcs are pair-wise different. We can interpret $\Gamma_\mathcal{Q}$ as the SA $\Gamma_\mathcal{Q} = (Q, Q, \circ)$, where Q is both the set of the states and the input alphabet, and $\circ$ is the transition mapping. This SA implements the family of iterated hash functions $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)}\}_{q \in Q}$. Since elements of the family $\mathfrak{H}_{\Gamma_\mathcal{Q}}$ are pair-wise different hash functions, this family can be identified with the set $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)} | q \in Q\}$.

Remark 1. It is known, that the set of string transformations [8, 9, 11, 12] of any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ contains the set of bijections $e_{q,\circ} : Q^+ \to Q^+$ ($q \in Q$), where $e_{q,\circ}(q_1 q_2 \dots q_m) = q'_1 q'_2 \dots q'_m$ ($q_1 q_2 \dots q_m \in Q^+$; $m = 1, 2, \dots$) if and only if $q'_1 = q \circ q_1$ and $q'_i = q'_{i-1} \circ q_i$ ($i = 2, \dots m$). Relationship between the sets of mappings $\{e_{q,\circ} | q \in Q\}$ and $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)} | q \in Q\}$ is that the equality $e_{q,\circ}(q_1 q_2 \dots q_m) = q'_1 q'_2 \dots q'_m$ implies the equality $H_{(\Gamma_\mathcal{Q},q)}(q_1 q_2 \dots q_m) = q'_m$.

Proposition 1. *Let $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ be any quasigroup. Then:*

1. *For any elements $q, q' \in Q$ holds the equality*

$$|\{x \in Q^m | H_{(\Gamma_\mathcal{Q},q)}(x) = q'\}| = |Q|^{m-1} \quad (m = 1, 2, \dots). \tag{5}$$

2. *For any elements $q, q', q'' \in Q$ ($q \neq q'$) holds the equality*

$$\{x \in Q^+ | H_{(\Gamma_\mathcal{Q},q)}(x) = q''\} \cap \{x \in Q^+ | H_{(\Gamma_\mathcal{Q},q')}(x) = q''\} = \emptyset. \tag{6}$$

Proof. By induction on the length of an input string. □

Since $H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q') = \{x \in Q^+ | H_{(\Gamma_{\mathcal{Q}},q)}(x) = q'\}$ $(q, q' \in Q)$, we can present (5) and (6) as follows:

$$|H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q') \cap Q^m| = |Q|^{m-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{7}$$

$$H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q'') \cap H^{-1}_{(\Gamma_{\mathcal{Q}},q')}(q'') = \emptyset \quad (q, q', q'' \in Q;\ q \neq q'). \tag{8}$$

Let $\mathsf{P}^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q')$ $(q, q' \in Q;\ m = 1, 2, \dots)$ be the probability that uniformly randomly chosen input string $x \in Q^m$ is a solution of equation $H_{(\Gamma_{\mathcal{Q}},q)}(x) = q'$, and $\mathsf{P}^{(2)}_{\Gamma_{\mathcal{Q}},q,m}$ $(q \in Q;\ m = 1, 2, \dots)$ be the probability that for two uniformly randomly chosen input strings $x, x' \in Q^m$ $(x \neq x')$ the equality $H_{(\Gamma_{\mathcal{Q}},q)}(x) = H_{(\Gamma_{\mathcal{Q}},q)}(x')$ holds. Applying (7) and (8), it is not difficult to prove the following theorem.

Theorem 1. *Let $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ be any quasigroup. Then:*

$$P^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q') = |Q|^{-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{9}$$

$$P^{(2)}_{\Gamma_{\mathcal{Q}},q,m} = |Q|^{-1}(1 - (|Q| - 1)(|Q|^m - 1)^{-1}) \quad (q \in Q;\ m = 1, 2, \dots). \tag{10}$$

It follows directly from (9) and (10) that $\lim\limits_{|Q|\to\infty} \mathsf{P}^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q') = 0$ $(q, q' \in Q)$ and $\lim\limits_{m\to\infty} \mathsf{P}^{(2)}_{\Gamma_{\mathcal{Q}},q,m} = |Q|^{-1}$. This is a significant argument to use finite quasigroups in mathematical models of cryptographic iterated hash functions.

2.2. T-quaigroups

A quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ is a T-quasigroup [6] if there exist an Abelian group $\mathcal{G} = (Q, +)$, some ordered pair $(\xi, \zeta) \in \mathrm{Aut}(\mathcal{G}) \times \mathrm{Aut}(\mathcal{G})$, and an element $c \in Q$ such that holds the equality

$$a \circ b = \xi(a) + \zeta(b) + c \quad (a, b \in Q). \tag{11}$$

It follows from this definition that any finite Abelian group $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ determines the family of T-quasigroups $\mathfrak{F}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c)\}_{\xi,\zeta\in\mathrm{Aut}(\mathcal{G});c\in Q}$, where $(Q, +, \xi, \zeta, c)$ is the T-quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ such that the operation $\circ$ is defined by the equality (11). Since elements of the family $\mathfrak{F}_{\mathcal{G}}$ are pair-wise different T-quasigroups (see Theorem 1 in [20]), this family can be identified with the set $\mathfrak{F}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c) | \xi, \zeta \in \mathrm{Aut}(\mathcal{G}); c \in Q\}$.

Let $\varepsilon_Q : Q \to Q$ be the identity mapping. It is not difficult to prove that for any finite Abelian group $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$:

1. There exists the left unit e_l in a T-quasigroup $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ if and only if $\zeta = \varepsilon_Q$. In this case, $e_l = -\xi^{-1}(c)$.

2. There exists the right unit e_r in a T-quasigroup $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ if and only if $\xi = \varepsilon_Q$. In this case, $e_l = -\zeta^{-1}(c)$.

3. $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ is a loop if and only if $\xi = \zeta = \varepsilon_Q$. In this case, $e = -c$.

4. $(Q,+,\xi,\zeta,c)\in\mathfrak{F}_{\mathcal{G}}$ is a commutative T-quasigroup if and only if $\xi=\zeta$ (see Theorem 2 in [20]).

5. $(Q,+,\xi,\zeta,c)\in\mathfrak{F}_{\mathcal{G}}$ is an associative T-quasigroup if and only if $\xi=\zeta=\varepsilon_Q$ (see Theorem 3 in [20]).

Remark 2. Therefore, for T-quasigroups the statements "a loop", "to be associative", and "to be associative-commutative" are the same.

Due to Fundamental Theorem, any Abelian group can be presented uniquely as a direct product of cyclic groups of prime-power order. More precisely, let $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) be any Abelian group, such that $|Q|=p_1^{r_1}\dots p_m^{r_m}$ ($m\geqslant 1$), where $r_i\geqslant 1$ ($i=1,\dots,m$) and p_i ($i=1,\dots,m$) are pair-wise different prime integers. Then

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

where $\cong$ is the isomorphism relation, d_{ij} ($i=1,\dots,m;j=1,\dots,k_i$) are fixed positive integers such that $1\leqslant d_{i1}\leqslant\dots\leqslant d_{ik_i}$ ($i=1,\dots,m$), $r_i=\sum\limits_{j=1}^{k_i}d_{ij}$ ($i=1,\dots,m$), $\mathbb{Z}_{p_j^{d_{ij}}}=\{0,1,\dots,p_j^{d_{ij}}-1\}$ ($i=1,\dots,m;j=1,\dots,k_i$), and $+_{ij}$ ($i=1,\dots,m;j=1,\dots,k_i$) is the module $p_j^{d_{ij}}$ addition. Due to (12), any element $z\in Q$ can be identified with a vector $z=(z_{11},\dots,z_{1k_1},\dots,z_{m1},\dots,z_{mk_m})$, where $z_{ij}\in\mathbb{Z}_{p_j^{d_{ij}}}$ ($i=1,\dots,m;j=1,\dots,k_i$). Hence, computation the sum $x+y$ ($x,y\in Q$) can be reduced to independent additions of corresponding components of vectors x and y. From here it follows that for any Abelian group $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) that satisfies to (12), time and space complexity for computation the element $x+y$ ($x,y\in Q$) are equal, correspondingly, to:

$$T_+=O(\sum_{i=1}^{m}\sum_{j=1}^{k_i}d_{ij}\log p_i)\quad(|Q|\to\infty), \tag{13}$$

$$V_+=O(\sum_{i=1}^{m}\sum_{j=1}^{k_i}d_{ij}\log p_i)\quad(|Q|\to\infty). \tag{14}$$

Remark 3. If additions of the corresponding components of vectors x and y can be implemented in parallel then time complexity for computation the element $x+y$ can be reduced to

$$T_+=O(\max_{i=1,\dots m}\max_{j=1,\dots k_i}d_{ij}\log p_i)\quad(|Q|\to\infty). \tag{15}$$

If an Abelian group $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) satisfies to (12) then

$$\mathrm{Aut}(\mathcal{G})\cong\bigotimes_{i=1}^{m}\mathrm{Aut}(\bigotimes_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}},+_{ij})). \tag{16}$$

Besides, for any $i = 1, \dots, m$ (see Theorem 4.1 in [5]) holds the equality

$$|\mathrm{Aut}(\bigotimes_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = \prod_{j=1}^{k_i}(p_i^{\alpha_{ij}} - p_i^{j-1}) \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\alpha_{ij}} \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\beta_{ij}+1}, \quad (17)$$

where $\alpha_{ij} = \max\{h | d_{ih} = d_{ij}\}$ and $\beta_{ij} = \min\{h | d_{ih} = d_{ij}\}$ for all $i = 1, \dots, m$ and $j = 1, \dots k_i$. Due to (16) and (17), for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12) holds the equality

$$|\mathrm{Aut}(\mathcal{G})| = \prod_{i=1}^{m}\prod_{j=1}^{k_i}(p_i^{\alpha_{ij}} - p_i^{j-1}) \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\alpha_{ij}} \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\beta_{ij}+1}. \quad (18)$$

Since $\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a subgroup of the group $\mathrm{Aut}(\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$, then $\bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a subgroup of the group $\bigotimes\limits_{i=1}^{m} \mathrm{Aut}(\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$. Besides, $|\mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = p_i^{d_{ij}}(1 - p_i^{-1})$ $(i = 1, \dots, m;\ \ j = 1, \dots, k_i)$. Hence

$$|\bigotimes_{i=1}^{m}\bigotimes_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = |Q| \prod_{i=1}^{m}(1 - p_i^{-1}). \quad (19)$$

By comparing (18) and (19), we conclude that $\bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a non-trivial subset of the set $\mathrm{Aut}(\mathcal{G})$.

For any $\chi = (\chi_{11}, \dots, \chi_{1k_1}, \dots, \chi_{m1}, \dots, \chi_{mk_m}) \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ and $z = (z_{11}, \dots, z_{1k_1}, \dots, z_{m1}, \dots, z_{mk_m}) \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij})$ we get

$$\chi(z) = (\chi_{11}(z_{11}), \dots, \chi_{1k_1}(z_{1k_1}), \dots, \chi_{m1}(z_{m1}), \dots, \chi_{mk_m}(z_{mk_m})),$$

i.e. computation the vector $\chi(z)$ can be reduced to independent computations of its components. From here it follows that for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12), time and space complexity for computation the element $\chi(z)$ ($z \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}), \chi \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$) are equal, correspondingly, to

$$T_\chi = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty), \quad (20)$$

$$V_\chi = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty). \quad (21)$$

Remark 4. If computations of components can be implemented in parallel then time complexity for computation the element $\chi(z)$ can be reduced to

$$T_\chi = O(\max_{i=1,\dots m} \max_{j=1,\dots k_i} d_{ij} \log p_i) \quad (|Q| \to \infty). \tag{22}$$

Comparing (13), (14) with (1), (2), and (20), (21) with (3), (4), we conclude that for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12) it is reasonable to consider the set of T-quasigroups

$$\widetilde{\mathfrak{F}}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c) | \xi, \zeta \in \bigotimes_{i=1}^{m} \bigotimes_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij})); c \in Q\}.$$

Due to (18) and (19), $\widetilde{\mathfrak{F}}_{\mathcal{G}}$ is a non-trivial subset of the set $\mathfrak{F}_{\mathcal{G}}$ for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12).

2.3. Elliptic curves over finite fields

At present, Abelian groups associated with elliptic curves over finite fields are widely used for solving information protection problems. This is due to the high complexity of identification the elements of these groups. So, it is it is reasonable to consider the sets of T-quasigroups defined by Abelian groups associated with elliptic curves over finite fields.

We remind, that an elliptic curve γ over any field $\mathbb{F} = (F, +, \cdot)$ can be defined as the set of all solutions of an equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in F),$$

such that $\Delta = d_2^2 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \neq 0$, where $d_2 = a_1^2 + 4a_2$, $d_4 = 2a_4 + a_1 a_3$, $d_6 = a_3^2 + 4a_6$, and $d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$. With this elliptic curve can be associated the Abelian group $\mathcal{G}_\gamma = (\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma})$, where $\mathbf{0} +_{\mathcal{G}_\gamma} \mathbf{0} = \mathbf{0}$, $\mathbf{0} +_{\mathcal{G}_\gamma} P = P +_{\mathcal{G}_\gamma} \mathbf{0} = P$ ($P \in \gamma$), and $P = (x, y) \in \gamma \Rightarrow -_{\mathcal{G}_\gamma} P = (x, -y - a_1 x - a_3)$. For any two points $P_i = (x_i, y_i) \in \gamma$ ($i = 1, 2$), such that $P_1 \neq -_{\mathcal{G}_\gamma} P_2$, the point $P_3 = P_1 +_{\mathcal{G}_\gamma} P_2$ can be computed as follows

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha a_1 - a_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + a_1 x_3 - a_3 \end{cases},$$

where

$$\alpha = \begin{cases} (3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1)(2y_1 + a_1 x_1 + a_3)^{-1}, & if \;\; x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & if \;\; x_1 \neq x_2 \end{cases}.$$

For any non-negative integer m and any element $P \in \gamma \cup \{\mathbf{0}\}$ we set

$$mP = \begin{cases} \mathbf{0}, & if \;\; m = 0 \\ \underbrace{P +_{\mathcal{G}_\gamma} \cdots +_{\mathcal{G}_\gamma} P}_{m \;\; times}, & if \;\; m = 1, 2, \dots \end{cases}.$$

Let γ be an elliptic curve over any finite field $\mathbb{F} = (F, +, \cdot)$.

We define the mappings $\chi_m : \gamma \cup \{\mathbf{0}\} \to \gamma \cup \{\mathbf{0}\}$ $(m = 0, 1, \ldots, |\gamma|)$ by the equality $\chi_m(P) = mP$ $(P \in \gamma \cup \{\mathbf{0}\})$.

It is evident that $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$ $(m = 1, \ldots, |\gamma|)$ if and only if the integer m is not a multiple of the order of any element $P \in \gamma$. Hence, we can define the set of T-quasigroups $\mathfrak{F}_{\mathcal{G}_\gamma} = \{(\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \xi, \zeta, P) | \xi, \zeta \in \mathrm{Aut}(\mathcal{G}_\gamma), P \in \gamma \cup \{\mathbf{0}\}\}$, and apply to it all results obtained in Subsection 2.2.

3. Families of SA in finite abstract quasigroups

For any abstract finite quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ the following families of SA $\mathfrak{A}_\mathcal{Q}^{(i)}$ $(i = 1, \ldots, 22)$ can be defined, at least:

$$\mathfrak{A}_\mathcal{Q}^{(1)} = \{M_{a,b}^{(1)} = (Q, Q, \delta_{a,b}^{(1)}) | \delta_{a,b}^{(1)}(q, x) = (a \circ q) \circ (b \circ x) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(2)} = \{M_{a,b}^{(2)} = (Q, Q, \delta_{a,b}^{(2)}) | \delta_{a,b}^{(2)}(q, x) = (b \circ x) \circ (a \circ q) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(3)} = \{M_{a,b}^{(3)} = (Q, Q, \delta_{a,b}^{(3)}) | \delta_{a,b}^{(3)}(q, x) = (q \circ a) \circ (b \circ x) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(4)} = \{M_{a,b}^{(4)} = (Q, Q, \delta_{a,b}^{(4)}) | \delta_{a,b}^{(4)}(q, x) = (b \circ x) \circ (q \circ a) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(5)} = \{M_{a,b}^{(5)} = (Q, Q, \delta_{a,b}^{(5)}) | \delta_{a,b}^{(5)}(q, x) = (a \circ q) \circ (x \circ b) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(6)} = \{M_{a,b}^{(6)} = (Q, Q, \delta_{a,b}^{(6)}) | \delta_{a,b}^{(6)}(q, x) = (x \circ b) \circ (a \circ q) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(7)} = \{M_{a,b}^{(7)} = (Q, Q, \delta_{a,b}^{(7)}) | \delta_{a,b}^{(7)}(q, x) = (q \circ a) \circ (x \circ b) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(8)} = \{M_{a,b}^{(8)} = (Q, Q, \delta_{a,b}^{(8)}) | \delta_{a,b}^{(8)}(q, x) = (x \circ b) \circ (q \circ a) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(9)} = \{M_{a}^{(9)} = (Q, Q, \delta_{a}^{(9)}) | \delta_{a}^{(9)}(q, x) = (a \circ q) \circ x \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(10)} = \{M_{a}^{(10)} = (Q, Q, \delta_{a}^{(10)}) | \delta_{a}^{(10)}(q, x) = x \circ (a \circ q) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(11)} = \{M_{a}^{(11)} = (Q, Q, \delta_{a}^{(11)}) | \delta_{a}^{(11)}(q, x) = (q \circ a) \circ x \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(12)} = \{M_{a}^{(12)} = (Q, Q, \delta_{a}^{(12)}) | \delta_{a}^{(12)}(q, x) = x \circ (q \circ a) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(13)} = \{M_{a}^{(13)} = (Q, Q, \delta_{a}^{(13)}) | \delta_{a}^{(13)}(q, x) = q \circ (a \circ x) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(14)} = \{M_{a,b}^{(14)} = (Q, Q, \delta_{a,b}^{(14)}) | \delta_{a}^{(14)}(q, x) = (a \circ x) \circ q \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(15)} = \{M_{a}^{(15)} = (Q, Q, \delta_{a}^{(15)}) | \delta_{a}^{(15)}(q, x) = q \circ (x \circ a) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(16)} = \{M_{a}^{(16)} = (Q, Q, \delta_{a}^{(16)}) | \delta_{a}^{(15)}(q, x) = (x \circ a) \circ q \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(17)} = \{M_{a}^{(17)} = (Q, Q, \delta_{a}^{(17)}) | \delta_{a}^{(17)}(q, x) = a \circ (q \circ x) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(18)} = \{M_a^{(18)} = (Q, Q, \delta_a^{(17)}) | \delta_a^{(18)}(q, x) = (q \circ x) \circ a \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(19)} = \{M_a^{(19)} = (Q, Q, \delta_a^{(19)}) | \delta_a^{(19)}(q, x) = a \circ (x \circ q) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(20)} = \{M_a^{(20)} = (Q, Q, \delta_a^{(20)}) | \delta_a^{(20)}(q, x) = (x \circ q) \circ a \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(21)} = \{M_a^{(21)} = (Q, Q, \delta_a^{(21)}) | \delta_a^{(21)}(q, x) = q \circ x \ \ (q, x \in Q)\},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(22)} = \{M_a^{(22)} = (Q, Q, \delta_a^{(22)}) | \delta_a^{(22)}(q, x) = x \circ q \ \ (q, x \in Q)\}.$$

It is evident that any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 8)$ consists of $|Q|^2$ elements, any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ consists of $|Q|$ elements, and any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$ consists of a single element.

Let $Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 1, \ldots, 22)$ be the set of all SA that are elements of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$. Then $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| = 1$ $(i = 21, 22)$. Besides, since $\mathcal{Q} \in \mathfrak{Q}_Q$ is a cancellative magma, it is not difficult to prove that $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| \geqslant |Q|$ $(i = 1, \ldots, 8)$, and $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| = |Q|$ $(i = 9, \ldots, 20)$, i.e. elements of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ are pair-wise different SA.

It follows from definition of the families $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ that the following proposition is true.

Proposition 2. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup. Then any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 8)$ is functioning by 1.5 times more slowly than any SA $M' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$, and three times more slowly than the SA $M'' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$. Besides, any SA $M' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ is functioning twice more slowly than the SA $M'' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$.*

Applying (1) and (2) it is not difficult to prove the following theorem.

Theorem 2. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup. Then for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ time and space complexity for computing the value of the transition mapping are equal, correspondingly, to*

$$T_M = O(|Q| \log |Q|) \ \ (|Q| \to \infty), \tag{23}$$

$$V_M = O(|Q|^2 \log |Q|) \ \ (|Q| \to \infty). \tag{24}$$

Any abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is a cancellative magma. Hence, the diagram of any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ is completed labeled directed graph with a single loop in each vertex, such that for any vertex $q \in Q$, all $|Q|$ arcs started in q terminate in pair-wise different vertices, and exactly $|Q|$ arcs are terminated in q and labels of these arcs are pair-wise different. From here we get that Theorem 1 is true for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$, and it can be reformulated as follows.

Theorem 3. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any be any abstract finite quasigroup. Then for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ hold equalities:*

$$P_{M,q,m}^{(1)}(q') = |Q|^{-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{25}$$

$$P_{M,q,m}^{(2)} = |Q|^{-1}(1 - (|Q| - 1)(|Q|^m - 1)^{-1}) \quad (q \in Q;\ m = 1, 2, \dots). \tag{26}$$

Due to Theorems 2 and 3, we can consider $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ as basic families of SA defined by a recurrence relation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$.

Let us characterize the structure of the families $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ with additional restrictions on the operation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$.

Based on the definition of the left unit, the right unit and the unit in a quasigroup, it is not difficult to prove the following three propositions.

Proposition 3. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the left unit. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(1)})\ (i = 9, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(2)})\ (i = 10, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(11)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(12)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(15)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(16)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 9, 13, 17),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 10, 14, 19).$$

Proposition 4. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the right unit. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(7)})\ (i = 11, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(8)})\ (i = 12, 16, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(13)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(14)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(9)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(10)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 11, 15, 18),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 12, 16, 20).$$

Proposition 5. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite loop. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(1)})\ (i = 9, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(2)})\ (i = 10, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)})\ (i = 11, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)})\ (i = 12, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)})\ (i = 9, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)})\ (i = 12, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(7)})\ (i = 11, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(8)})\ (i = 12, 16, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 9, 11, 13, 15, 17, 18),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 10, 12, 14, 16, 19, 20).$$

Proceeding from definitions of associative and/or commutative magma, it is not difficult to prove the following three propositions.

Proposition 6. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite associative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(9)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(17)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(10)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(16)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(11)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(13)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(12)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(20)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(14)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(19)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(15)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(18)}).$$

Proposition 7. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite commutative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 1,\dots,8), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 9,\dots,12),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 13,\dots,16), \ Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 17,\dots,20),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 21,22).$$

Proposition 8. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite associative-commutative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(17)}) \ (i = 1,\dots,16,18,19,20).$$

It should be noted, that if $\mathcal{Q} \in \mathfrak{Q}_Q$ is a finite associative-commutative quasigroup, then for all elements $a,b \in Q$ any SA $M_{a,b}^{(i)} \in Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 1,\dots,8)$ appears as an element of the family $Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 9,\dots,20)$ exactly $|Q|$ times.

4. Families of SA in finite T-quasigroups

Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be given Abelian group.

For any T-quasigroup $\mathcal{Q} = (Q,\circ) = (Q,+,\xi,\zeta,c) \in \mathfrak{F}_{\mathcal{G}}$, applying (11), we can redefine the families of SA $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1,\dots,22)$ as follows:

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(1)} = \{M_{a,b,c,\xi,\zeta}^{(1)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(1)}) | \delta_{a,b,c,\xi,\zeta}^{(1)}(q,x) =$$

$$= \xi\zeta(q) + \zeta^2(x) + \xi^2(a) + \zeta\xi(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(2)} = \{M_{a,b,c,\xi,\zeta}^{(2)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(2)}) | \delta_{a,b,c,\xi,\zeta}^{(2)}(q,x) =$$

$$= \zeta^2(q) + \xi\zeta(x) + \zeta\xi(a) + \xi^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(3)} = \{M_{a,b,c,\xi,\zeta}^{(3)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(3)}) | \delta_{a,b,c,\xi,\zeta}^{(3)}(q,x) =$$

$$= \xi^2(q) + \zeta^2(x) + \xi\zeta(a) + \zeta\xi(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}^{(4)}_{(Q,+,\xi,\zeta,c)} = \{M^{(4)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(4)}_{a,b,c,\xi,\zeta})|\delta^{(4)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi\zeta(x) + \zeta^2(a) + \xi^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(5)}_{(Q,+,\xi,\zeta,c)} = \{M^{(5)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(5)}_{a,b,c,\xi,\zeta})|\delta^{(5)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \zeta\xi(x) + \xi^2(a) + \zeta^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(6)}_{(Q,+,\xi,\zeta,c)} = \{M^{(6)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(6)}_{a,b,c,\xi,\zeta})|\delta^{(6)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \xi^2(x) + \zeta\xi(a) + \xi\zeta(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(7)}_{(Q,+,\xi,\zeta,c)} = \{M^{(7)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(7)}_{a,b,c,\xi,\zeta})|\delta^{(7)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \zeta\xi(x) + \xi\zeta(a) + \zeta^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(8)}_{(Q,+,\xi,\zeta,c)} = \{M^{(8)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(8)}_{a,b,c,\xi,\zeta})|\delta^{(8)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi^2(x) + \zeta^2(a) + \xi\zeta(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(9)}_{(Q,+,\xi,\zeta,c)} = \{M^{(9)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(9)}_{a,c,\xi,\zeta})|\delta^{(9)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \zeta(x) + \xi^2(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(10)}_{(Q,+,\xi,\zeta,c)} = \{M^{(10)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(10)}_{a,c,\xi,\zeta})|\delta^{(10)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \xi(x) + \zeta\xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(11)}_{(Q,+,\xi,\zeta,c)} = \{M^{(11)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(11)}_{a,c,\xi,\zeta})|\delta^{(11)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \zeta(x) + \xi\zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(12)}_{(Q,+,\xi,\zeta,c)} = \{M^{(12)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(12)}_{a,c,\xi,\zeta})|\delta^{(12)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi(x) + \zeta^2(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(13)}_{(Q,+,\xi,\zeta,c)} = \{M^{(13)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(13)}_{a,c,\xi,\zeta})|\delta^{(13)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi(q) + \zeta^2(x) + \zeta\xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(14)}_{(Q,+,\xi,\zeta,c)} = \{M^{(14)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(14)}_{a,c,\xi,\zeta})|\delta^{(14)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta(q) + \xi\zeta(x) + \xi^2(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(15)}_{(Q,+,\xi,\zeta,c)} = \{M^{(15)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(15)}_{a,c,\xi,\zeta})|\delta^{(15)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi(q) + \zeta\xi(x) + \zeta^2(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(16)}_{(Q,+,\xi,\zeta,c)} = \{M^{(16)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(16)}_{a,c,\xi,\zeta})|\delta^{(16)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta(q) + \xi^2(x) + \xi\zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$

$$\mathfrak{A}^{(17)}_{(Q,+,\xi,\zeta,c)} = \{M^{(17)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(17)}_{a,c,\xi,\zeta}) | \delta^{(17)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \zeta^2(x) + \xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(18)}_{(Q,+,\xi,\zeta,c)} = \{M^{(18)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(18)}_{a,c,\xi,\zeta}) | \delta^{(18)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \xi\zeta(x) + \zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(19)}_{(Q,+,\xi,\zeta,c)} = \{M^{(19)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(19)}_{a,c,\xi,\zeta}) | \delta^{(19)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \zeta\xi(x) + \xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(20)}_{(Q,+,\xi,\zeta,c)} = \{M^{(20)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(20)}_{a,c,\xi,\zeta}) | \delta^{(20)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \xi^2(x) + \zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(21)}_{(Q,+,\xi,\zeta,c)} = \{M^{(21)}_{c,\xi,\zeta} = (Q,Q,\delta^{(21)}_{c,\xi,\zeta}) | \delta^{(21)}_{c,\xi,\zeta}(q,x) = \xi(q) + \zeta(x) + c \ \ (q,x \in Q)\},$$
$$\mathfrak{A}^{(22)}_{(Q,+,\xi,\zeta,c)} = \{M^{(22)}_{c,\xi,\zeta} = (Q,Q,\delta^{(22)}_{c,\xi,\zeta}) | \delta^{(22)}_{c,\xi,\zeta}(q,x) = \zeta(q) + \xi(x) + c \ \ (q,x \in Q)\}.$$

It is evident that for any family of SA $\mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ all results obtained in Section 3 are true. Moreover, due to Remark 2, for T-quasigroups, Proposition 8 is the strongest one among Propositions 5, 6, and 8. Therefore, for a T-quasigroup $(Q,+,\xi,\zeta,c) \in \mathfrak{F}_{\mathcal{G}}$ with additional restrictions on the operation in it (see subsection 2.2), Propositions 3, 4, 7, and 8 can be reformulated as follows:

In Proposition 3, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the left unit" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any T-quasigroup with the left unit". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 4, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the right unit" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any T-quasigroup with the right unit". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 7, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite commutative quasigroup" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any commutative T-quasigroup". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 8, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite loop" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any loop". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

Fundamental theorem for finite Abelian groups (see Subsection 2.2) makes it possible to represent SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ by the parallel composition of SA over T-quasigroups determined by cyclic groups of prime-power order.

Remark 5. The parallel composition of SA $M_i = (Q_i, X_i, \delta_i)$ $(i = 1, \ldots, n)$ is the SA $\bigotimes\limits_{i=1}^{n} M_i = (\bigotimes\limits_{i=1}^{n} Q_i, \bigotimes\limits_{i=1}^{n} X_i, \delta)$, where

$$\delta((q_1, \ldots, q_n), (x_1, \ldots, x_n)) = (\delta_1(q_1, x_1), \ldots, \delta_n(q_n, x_n))$$

for all $(q_1, \ldots, q_n) \in \bigotimes\limits_{i=1}^{n} Q_i$ and $(x_1, \ldots, x_n) \in \bigotimes\limits_{i=1}^{n} X_i$.

Indeed, let $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ be an Abelian group that satisfies to (12), and $(Q, +, \xi, \zeta, c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$. Setting

$$a = (a_{11}, \ldots, a_{1k_1}, \ldots, a_{m1}, \ldots, a_{mk_m}), \quad b = (b_{11}, \ldots, b_{1k_1}, \ldots, b_{m1}, \ldots, b_{mk_m}),$$

$$\xi = (\xi_{11}, \ldots, \xi_{1k_1}, \ldots, \xi_{m1}, \ldots, \xi_{mk_m}), \quad \zeta = (\zeta_{11}, \ldots, \zeta_{1k_1}, \ldots, \zeta_{m1}, \ldots, \zeta_{mk_m}),$$

$$c = (c_{11}, \ldots, c_{1k_1}, \ldots, c_{m1}, \ldots, c_{mk_m}),$$

we get the following representations of SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 22)$ by the parallel composition of SA over cyclic groups of prime-power order:

1. If $M^{(i)}_{a,b,c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 8)$ then

$$M^{(i)}_{a,b,c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{a_{jh},b_{jh},c_{jh},\xi_{jh},\zeta_{jh}}. \tag{27}$$

2. If $M^{(i)}_{a,c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 9, \ldots, 20)$ then

$$M^{(i)}_{a,c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{a_{jh},c_{jh},\xi_{jh},\zeta_{jh}}. \tag{28}$$

3. If $M^{(i)}_{c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 21, 22)$ then

$$M^{(i)}_{c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{c_{jh},\xi_{jh},\zeta_{jh}}. \tag{29}$$

Applying (13), (14), (20) and (21) to the representations (27)-(29), the following theorem can be proved.

Theorem 4. *Let $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ be an Abelian group that satisfies to (12), and $(Q, +, \xi, \zeta, c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$. Then for any SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 22)$ time and space complexity for computation the value of the transition mapping are equal, correspondingly, to*

$$T_M = O(\sum_{i=1}^{m} \sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty), \tag{30}$$

$$V_M = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij}\log p_i) \quad (|Q|\to\infty). \tag{31}$$

Remark 6. If computations of transition mappings for components in the parallel composition of SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ can be implemented in parallel, then, due to (15) and (22), for SA M time complexity for computation the value of the transition mapping can be reduced to

$$T_M = O(\max_{i=1,\dots m}\max_{j=1,\dots k_i} d_{ij}\log p_i) \quad (|Q|\to\infty). \tag{32}$$

By comparing (30), (31) with (23), (24), we conclude that for any T-quasigroup $(Q,+,\xi,\zeta,c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$ it is reasonable to use SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ as mathematical models for the families of fast iterated hash functions.

5. Families of SA in elliptic curves over finite fields

Let γ be any elliptic curve over a finite field, and $(\gamma\cup\{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \chi_{m_1}, \chi_{m_2}, P) \in \mathfrak{F}_{\mathcal{G}_\gamma}$ be any T-quasigroup. To transform the families $\mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ into the families $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ it is sufficient to substitute:

1) $\gamma\cup\{\mathbf{0}\}$ instead of Q;
2) $P_1, P_2, P \in \gamma$, correspondingly, instead of $a, b, c \in Q$;
3) $\chi_{m_1}, \chi_{m_2} \in \mathrm{Aut}(\mathcal{G}_\gamma)$, correspondingly, instead of $\xi, \zeta \in \mathrm{Aut}(\mathcal{G})$;
4) $+_{\mathcal{G}_\gamma}$ instead of $+$.

It is evident that for the families of SA $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ $(i = 1,\dots,22)$ all results obtained in Section 4 are true. Hence, $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ $(i = 1,\dots,22)$ can be considered as basic families of SA defined by a recurrence relation in a T-quasigroup $(\gamma\cup\{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \chi_{m_1}, \chi_{m_2}, P) \in \mathfrak{F}_{\mathcal{G}_\gamma}$.

The following another approach to definition families of SA in an elliptic curve γ over a finite field has been proposed in [22].

Let $\mathcal{F}_\gamma = \{\chi_m | m = 1,\dots,|\gamma|\}$. For any fixed integer $l \in \{1,\dots,|\gamma|\}$ we can define the family of SA

$$\mathfrak{A}_{\gamma,l} = \{M_{\chi_m,P} = (\gamma\cup\{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P})\}_{\chi_m\in\mathcal{F}_\gamma, P\in\gamma},$$

where

$$\delta_{\chi_m,P}(q,x) = \chi_m(q) +_{\mathcal{G}_\gamma} \chi_x(P) \quad (q \in \gamma\cup\{\mathbf{0}\}, x \in \mathbb{Z}_{l+1}). \tag{33}$$

Let $Ordr(P)$ be the order of the element P in the Abelian group $\mathcal{G}_\gamma$.

Theorem 5. *Let γ be any elliptic curve over a finite field, $l \in \{1,\dots,|\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma\cup\{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA. Then for any state $q \in \gamma\cup\{\boldsymbol{0}\}$ and any two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q,x_1) \neq \delta_{\chi_m,P}(q,x_2)$ holds if and only if $Ordr(P) > l$.*

Proof. Suppose that there exists an SA $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ such that $Ordr(P) > l$, and for some state $q \in \gamma \cup \{\mathbf{0}\}$ and some two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)$.

Due to (33), we get

$$(\exists q \in \gamma \cup \{\mathbf{0}\})(\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q \in \gamma \cup \{\mathbf{0}\})(\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \chi_m(q) +_{\mathcal{G}_\gamma} \chi_{x_1}(P) =$$

$$= \chi_m(q) +_{\mathcal{G}_\gamma} \chi_{x_2}(P)) \Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \chi_{x_1}(P) = \chi_{x_2}(P)) \Leftrightarrow$$

$$\Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& x_1 P = x_2 P) \Leftrightarrow$$

$$\Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& (\max\{x_1, x_2\} - \min\{x_1, x_2\})P = \mathbf{0}) \Leftrightarrow$$

$$\Leftrightarrow (\exists x \in \{1, \ldots, l\})(xP = \mathbf{0}) \Leftrightarrow Ordr(P) \leqslant l.$$

We get a contradiction, since, by supposition, $Ordr(P) > l$.

Therefore, $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ is an SA such that for any state $q \in \gamma \cup \{\mathbf{0}\}$ and any two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q, x_1) \neq \delta_{\chi_m,P}(q, x_2)$ holds if and only if $Ordr(P) > l$. □

From proof of Theorem 5 we get that the following corollary is true.

Corollary 1. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA such that $Ordr(P) \leqslant l$. Then for any state $q \in \gamma \cup \{\boldsymbol{0}\}$ and for all two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ such that the integer $\max\{x_1, x_2\} - \min\{x_1, x_2\}$ is some multiple of the integer $Ordr(P)$ holds the equality $\delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)$.*

Theorem 6. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA. Then for any two different states $q_1, q_2 \in \gamma \cup \{\boldsymbol{0}\}$ and any input symbol $x \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q_1, x) \neq \delta_{\chi_m,P}(q_2, x)$ holds if and only if $\chi_m \in Aut(\mathcal{G}_\gamma)$.*

Proof. Suppose that there exists an SA $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ such that $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$, and for some two different states $q_1, q_2 \in \gamma \cup \{\mathbf{0}\}$ and some input symbol $x \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)$.

Due to (33), we get

$$(\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(\exists x \in \mathbb{Z}_{l+1})(q_1 \neq q_2 \& \delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(\exists x \in \mathbb{Z}_{l+1})(q_1 \neq q_2 \& \chi_m(q_1) +_{\mathcal{G}_\gamma} \chi_x(P) =$$

$$= \chi_m(q_2) +_{\mathcal{G}_\gamma} \chi_x(P)) \Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& \chi_m(q_1) = \chi_m(q_2)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& mq_1 = mq_2 P) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& m(q_1 -_{\mathcal{G}_\gamma} q_2) = \mathbf{0}) \Leftrightarrow$$

$$\Leftrightarrow (\exists q \in \gamma)(mq = \mathbf{0}) \Leftrightarrow (\exists q \in \gamma)(\chi_m(q) = \mathbf{0}) \Leftrightarrow \chi_m \notin \mathrm{Aut}(\mathcal{G}_\gamma).$$

We get a contradiction, since, by supposition, $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$.

Therefore, $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ is an SA such that for any two different states $q_1, q_2 \in \gamma \cup \{\mathbf{0}\}$ and any input symbol $x \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q_1, x) \neq \delta_{\chi_m,P}(q_2, x)$ holds if and only if $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$. □

From proof of Theorem 6 we get that the following corollary is true.

Corollary 2. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA such that $\chi_m \in \mathcal{F}_\gamma \backslash Aut(\mathcal{G}_\gamma)$. Then for all two different states $q_1, q_2 \in \gamma \cup \{\boldsymbol{0}\}$ such that the integer m is some multiple of the integer $Order(q_1 -_{\mathcal{G}_\gamma} q_2)$ any for any input symbol $x \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)$.*

Due to Theorems 5 and 6, and Corollaries 1 and 2, it seems promising to use SA $M_{\chi_m,P} \in \mathfrak{A}_{\gamma,l}$ ($\chi_m \in \mathcal{F}_\gamma, P \in \gamma, Ordr(P) > l$) and SA $M_{\chi_m,P} \in \mathfrak{A}_{\gamma,l}$ ($\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma), P \in \gamma$) as mathematical models for the design and implementation of computationally secured families of iterated hash functions.

6. Discussion

The main aim of the given paper was to explore the feasibility to use SA defined by a reccurence relation in a finite quasigroup as mathematical models for computationally secure families of iterated hash functions.

Basic families of SA defined by a recurrence relation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ have been introduced and examined in Section 3. The main results of these studies are presented in Theorem 1. Their significance is that from a probabilistic point of view SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 22$) are the best in the class of SA mathematical models for computationally secure sets $\mathfrak{H}_M = \{H_{(M,q)} | q \in Q\}$ of iterated hash functions.

It is known that solving equations in a quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is a hard Problem when $|Q|$ is sufficiently large integer. Let the initial state $q \in Q$ of a SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 22$) and the length l of the hashed input string $w \in Q^l$ be some part of the short-term secret key. Suppose that an intruder have intercepted the hash q', and his aim is to find the hashed input string $w \in Q^l$. Therefore, he is faced with the family of equations $H_{(M,q)}(w) = q'$ in a situation, when the integer l is unknown to him. In the absence of additional information this Problem cannot be solved at all. Even if the integer l is known to an intruder, then, due to Theorem 1, any searching based either on deterministic or probabilistic approach does not guarantee identification of the hashed input string w in the admissible time. Due to Theorem 1, the similar situation arises if an intruder tries to change the hashed message. The values of the parameters of SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 20$) can be considered as some part of the medium-term secret key. In this case, when an intruder tries to find the hashed input string, he must additionally identify the

SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$. Besides, some algorithm that determines the selection of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ can be designed as the long-term secret key.

Any abstract quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is specified by the Cayley table, as a rule. Hence, any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ has a sufficiently high time and space complexity (see Theorem 2). It seems promising to define similar families of SA for some set of quasigroups that can be specified compactly and operations in which are fast. The set of all T-quasigroups defined by a given finite Abelian group $\mathcal{G} = (Q, +)$ meets these conditions. In Sections 4 the families of SA $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ defined in these T-quasigroups have been investigated. The representation of SA $M \in \mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ by the parallel composition of SA over T-quasigroups determined by cyclic groups of prime-power order reduces its time and space complexity (see Theorem 4 and Remark 6). Investigation of the families $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ for specific Abelian groups $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ can help to find the most suitable families of SA for mathematical models of fast computationally secure families of iterated hash functions.

It is known, that elliptic curves over finite fields can be successfully used for solving information protection problems. In Section 5 it has been shown how the families $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ can be transformed into the families $\mathfrak{A}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}^{(i)}$, where γ is an elliptic curve over a finite field, and $\mathcal{G}_\gamma = (\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma})$ is the Abelian group associated with it. Besides, the families of SA $\mathfrak{A}_{\gamma,l} = \{M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P})\}_{\chi_m \in \mathcal{F}_\gamma, P \in \gamma}$ $(l \in \{1, \ldots, |\gamma|\})$ have been analyzed. Obtained results justify that it is reasonable to use families of SA in elliptic curves over finite fields as mathematical models for computationally secure families of iterated hash functions.

7. Conclusion

In the given paper, some fragment of the Algebraic Theory of SA in finite quasigroups has been developed. The main aim of these studies was to elaborate some theoretic backgrounds for possible using these SA as mathematical models for the design and implementation of computationally secure families of iterated hash functions. To achieve this aim, basic families of SA in abstract finite quasigrops, in finite T-quasigroups, and in elliptic curves over finite fields have been defined and investigated. Obtained results form some base for developing similar fragment of the Algebraic Theory of Automata in finite quasigroups with the aim to use them as mathematical models for families of stream ciphers. This is the main area of our future research.

References

[1] **A.V. Aho, J.E. Hopcroft, J.D. Ullman**, *The design and analysis of computer*

algorithms, Boston, MA, USA, Addison-Wesley Longman Publishing Co., Inc. 1974.

[2] **V.D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Moscow, Nauka, 1967.

[3] **D. Chauhan, I. Gupta, R. Verma**, *Quasigroups and their applications in cryptography*, Cryptologia, Taylor & Francis Online, Published online: 01 May 2020, 1 – 39, https://doi.org/10.1080/01611194.2020.1721615

[4] **M.M. Glukhov**, *Some applications of quasigroups in cryptography*, (Russian), Prikl. Diskr. Mat. **2** (2008), no. 2, 28 – 32.

[5] **C.D. Hillar, D.L. Rhea**, *Automorphisms of finite Abelian groups*, Amer. Math. Monthly, **115** (2007), no. 11, 17 – 23.

[6] **T. Kepka, P. Nemec**, *T-quasigroups. I*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 1, 39 – 49.

[7] **V.T. Markov, A.V. Michajlev, A.V. Gribov, P.A. Zolotykh, S.S. Skazenik**, *Quasigroups and rings in coding and design of cryptoschemes*, (Russian), Prikl. Diskr. Mat. **6** (2012), no. 4, 31 – 52.

[8] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigrouop string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **20** (1999), no. 1 – 2, 13 – 28.

[9] **S. Markovski, V. Kusakatov**, *Quasigroup String Processing: Part 2*, Contributions, Sec. Math. Tech. Sci., MANU, **21** (2000), no. 1 – 2, 15 – 32.

[10] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup and hash functions*, Proc. of the 6$^{\text{th}}$ ICDMA, Bansko, 2001, 43 – 50

[11] **S. Markovski, V. Kusakatov**, *Quasigroup String Processing: Part 3*, Contributions, Sec. Math. Tech.Sci., MANU, **23-24** (2002-2003), no. 1 – 2, 7 – 27.

[12] **S. Markovski, V. Bakeva**, *Quasigroup string processing: Part 4*, Contributions, Sec. Math. Tech. Sci., MANU, **27** (2006), no. 1 – 2, 41 – 53.

[13] **S. Markovski**, *Design of crypto primitives based on quasigroups*, Quasigroups and Related Systems, **23** (2015), 41 – 90.

[14] **A. Mileva, S. Markovski**, *Quasigroup string transformations and hash function design*, Proc. of Int. Conf. ICT Innovations 2009. Springer, Berlin, Heidelberg. 2010. 367 – 376.

[15] **N. A. Nikhil, D.S. Harish Ram**, *Hardware implementation of quasigroup based encryption*, Int. J. of Scientific & Engineering Research, **5** (2014), no. 5, 159 – 162.

[16] **B. Schneier**, *Applied cryptography, protocols, algorithms, and source code in C. Second Edition*, Wiley Computer Publishing, John Wiley & Sons, Inc., 1995.

[17] **V.A. Shcherbacov**, *Quasigroups in cryptology*, Comput. Sci. J. Moldova, **17** (2009), no. 2, 193 – 228.

[18] **V.A. Shcherbacov**, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, London, New York. 2017.

[19] **V.V. Skobelev, V.G. Skobelev**, *Automata over abstract finite quasigroups*, Cybern. Syst. Anal., **53** (2017), no. 5, 669 – 674.

[20] **V.V. Skobelev, V.G. Skobelev**, *Automata over finite T-quasigroups*, Cybern. Syst. Anal., **54** (2018), no. 3, 345 – 356.

[21] **V.V. Skobelev, V.G. Skobelev**, *Finite automata over magmas: models and some applications in cryptography*, Comput. Sci. J. Moldova. **26** (2018), no. 1, 77 − 92.

[22] **V.V. Skobelev**, *Automata in algebraic structures. Models and methods of their analysis*, (Russian), Donetsk, Ukraine, IAMM of NAS of Ukraine. 2013.

Received June 20, 2020

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
Glushkova ave., 40
Kyiv, 03187
Ukraine
E-mails: skobelevvg@gmail.com, volodimirvskobelev@gmail.com