Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations

D. Gligoroski[1,2]

[1] Centre for Quantifiable Quality of Service in Communication Systems, Norwegian University of Science and Technology, O.S.Bragstads plass 2E, N-7491 Trondheim, NORWAY

[2] University - "Ss Cyril and Methodius", Faculty of Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, 1000 Skopje, Republic of MACEDONIA

gligoroski@yahoo.com

Abstract. In this paper we propose a definition and construction of a new family of one-way candidate functions $\mathcal{R}_N : Q^N \to Q^N$, where $Q = \{0, 1, \ldots, s-1\}$ is an alphabet with s elements. Special instances of these functions can have the additional property to be permutations (i.e. one-way permutations). These one-way functions have the property that for achieving the security level of 2^n computations in order to invert them, only n bits of input are needed. The construction is based on quasigroup string transformations. Since quasigroups in general do not have algebraic properties such as associativity, commutativity, neutral elements, inverting these functions seems to require exponentially many readings from the lookup table that defines them (a Latin Square) in order to check the satisfiability for the initial conditions, thus making them natural candidates for one-way functions. [3]

Key words: one-way functions, one-way permutations, quasigroup string transformations

[3] This work was carried out during the tenure of an ERCIM fellowship of D. Gligoroski visiting the Centre Q2S - Centre for Quantifiable Quality of Service in Communication Systems at the Norwegian University of Science and Technology - Trondheim, Norway.

1 Introduction

Almost all known and well established one-way functions and one-way permutations in modern cryptography are based on intractable problems from number theory or closely related mathematical fields such as theory of finite fields, sphere packing or coding theory. For example, the discrete logarithm problem modulo a large randomly generated prime number is the Diffie-Helman proposal in [1] for one-way permutations, quadratic residuosity is Goldwasser and Micali proposal in [2] and RSA is an one-way permutation candidate based on the difficulty of factoring a number that is a product of two large prime numbers proposed by Rivest, Shamir and Adleman in [3]. There are also some one-way functions candidates based on sphere-packing problems and coding theory such as the proposals from Goldreich, Krawczyk and Luby in [4]. Constructing one-way functions based on the subset sum problem have been proposed by Impagliazzo and Naor in [5]. As far as we know, the only attempt to construct a one-way function that is completely defined by combinatorial elements is the proposal of Goldreich in [6]. The proposal is based on the combinatorial field of Expander Graphs.

In this paper we construct a new family of one-way functions and one-way permutations defined on a finite set $Q = \{0, 1, \ldots, s-1\}$ with s elements. The construction is based on the theory of quasigroups, and quasigroup string transformations. Our approach in opposite to other approaches, with an exception of [6] is completely based on a mathematical field not closely related to the field of number theory. By some of their properties (such as speed of computation, security level of inversion) quasigroup one-way functions outperform all currently known one-way candidate functions.

2 Preliminaries

Here we give a brief overview of quasigroups and quasigroup string transformations and more detailed explanation the reader can find in [7] and [8].

Definition 1. *A quasigroup $(Q, *)$ is a groupoid, i.e. a set Q with a binary operation $* : Q \times Q \to Q$, satisfying the law*

$$(\forall u, v \in Q)(\exists!\ x, y \in Q) \quad u * x = v \ \&\ y * u = v. \tag{1}$$

If Q is a finite set then the main body of the multiplication table of the quasigroup is a Latin Square over the set Q. A Latin Square over Q is a $|Q| \times |Q|$-matrix such that each row and column is a permutation of Q [7].

Next we define the basic quasigroup string transformation called e–transformation:

Definition 2. *A quasigroup e–transformation of a string $A = (a_0, a_1, \ldots, a_{N-1}) \in Q^N$ with a leader $l \in Q$ is the function $e_l : Q \times Q^N \to Q^N$ defined as $B = e_l(A)$ where $A = (a_0, a_1, \ldots, a_{N-1})$, $B = (b_0, b_1, \ldots, b_{N-1})$, $l \in Q$ and*

$$b_i := \begin{cases} l * a_0, & i = 0 \\ b_{i-1} * a_i, & 1 \le i \le N-1 \end{cases} \tag{2}$$

For better understanding the graphical representation of the e–transformation is shown on Fig. 1.

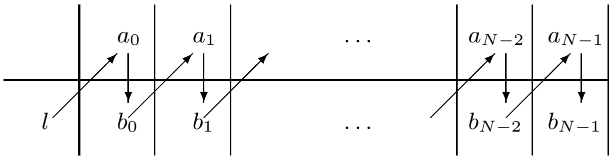


Fig. 1. Graphical representation of the e–transformation of a string $A = (a_0, a_1, \dots, a_{N-1})$.

Example 1. Let $Q = \{0, 1, 2, 3\}$ and let the quasigroup $(Q, *)$ be given by the multiplication scheme in Table 1.

$*$	0	1	2	3
0	2	1	0	3
1	3	0	1	2
2	1	2	3	0
3	0	3	2	1

Table 1. Quasigroup $(Q, *)$

Consider the string $A = 1\ 0\ 2\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 2\ 1\ 0\ 2\ 2\ 0\ 1\ 0\ 1\ 0\ 3\ 0\ 0$ and let us choose the leader $l = 0$. Then by the e–transformation $e_0(A)$ we will obtain the following transformed string:

$e_0(A) = 1\ 3\ 2\ 2\ 1\ 3\ 0\ 2\ 1\ 3\ 0\ 2\ 1\ 0\ 1\ 1\ 2\ 1\ 1\ 1\ 3\ 3\ 0\ 1\ 3\ 1\ 3\ 0.$

The four consecutive applications of the e-transformation e_0 on A are represented in Table 2.

	$1\ 0\ 2\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 2\ 1\ 0\ 2\ 2\ 0\ 1\ 0\ 1\ 0\ 3\ 0\ 0 = A$
0	$1\ 3\ 2\ 2\ 1\ 3\ 0\ 2\ 1\ 3\ 0\ 2\ 1\ 0\ 1\ 1\ 2\ 1\ 1\ 1\ 3\ 3\ 0\ 1\ 3\ 1\ 3\ 0 = e_0(A)$
0	$1\ 2\ 3\ 2\ 2\ 0\ 2\ 3\ 3\ 1\ 3\ 2\ 2\ 1\ 0\ 1\ 1\ 2\ 2\ 2\ 0\ 3\ 0\ 1\ 2\ 2\ 0\ 2 = e_0(e_0(A))$
0	$1\ 1\ 2\ 3\ 2\ 1\ 1\ 2\ 0\ 1\ 2\ 3\ 2\ 2\ 1\ 0\ 1\ 1\ 1\ 1\ 3\ 1\ 3\ 3\ 2\ 3\ 0\ 0 = e_0(e_0(e_0(A)))$
0	$1\ 0\ 0\ 3\ 2\ 2\ 2\ 3\ 0\ 1\ 1\ 2\ 3\ 2\ 2\ 1\ 0\ 1\ 0\ 1\ 2\ 2\ 0\ 3\ 2\ 0\ 2\ 1 = e_0(e_0(e_0(e_0(A))))$

Table 2. Four consecutive e-transformations of A with leader 0.

If we have a string of leaders, we can apply consecutive e–transformations on a given string, as a composition of e–transformations. That is defined by the following definition:

Definition 3. *A quasigroup E–transformation of a string $A = (a_0, a_1, \dots, a_{N-1}) \in Q^N$ with a string of K leaders $\mathbf{L} = (l_0, l_1, \dots, l_{K-1}) \in Q^K$ is the function $E_{\mathbf{L},K} : Q^K \times Q^N \to Q^N$ defined as $B = E_{\mathbf{L},K}(A)$ where $A = (a_0, a_1, \dots, a_{N-1})$, $B = (b_0, b_1, \dots, b_{N-1})$ and*

$$B = e_{l_{K-1}}(\ e_{l_{K-2}}(\ \dots e_{l_1}(\ e_{l_0}(A)\ )\dots\ )\ ) \tag{3}$$

Definition 4. *Quasigroup single reverse string transformation is the function $\mathcal{R}_1 : Q^N \to Q^N$ defined as*

$$B = \mathcal{R}_1(A) = E_{\overline{A},N}(A) = e_{a_{N-1}}(\dots(e_{a_1}(e_{a_0}(A))))$$

where $A = (a_0, a_1, \dots, a_{N-1})$ and $B = (b_0, b_1, \dots, b_{N-1})$.

Definition 5. *Quasigroup double reverse transformation is the function $\mathcal{R}_2 : Q^N \to Q^N$ defined as*

$$B = \mathcal{R}_2(A) = E_{\overline{AA},2N}(A) = e_{a_{N-1}}(\dots(e_{a_1}(e_{a_0}(e_{a_{N-1}}(\dots(e_{a_1}(e_{a_0}(A))))$$

where $A = (a_0, a_1, \dots, a_{N-1})$ and $B = (b_0, b_1, \dots, b_{N-1})$.

Example 2. Let quasigroup $(Q, *)$ be given by the multiplication scheme in Table 1. Consider the string $A = 0\ 1\ 2\ 3\ 0$. Then by the transformation $\mathcal{R}_1(A) = E_{\overline{A},5}(A)$ we will obtain the following transformed string: $\mathcal{R}_1(A) = 0\ 0\ 1\ 0\ 3$ and by the transformation $\mathcal{R}_2(A) = E_{\overline{AA},10}(A)$ we will obtain the following transformed string: $\mathcal{R}_2(A) = 0\ 3\ 2\ 0\ 2$. The calculation's steps are given in Table 3.

	0 1 2 3 0 $= A$
0	2 2 3 1 3
3	2 3 1 0 3
2	3 1 0 2 0
1	2 2 1 1 3
0	**0 0 1 0 3** $= \mathcal{R}_1(A)$

	0 1 2 3 0 $= A$
0	2 2 3 1 3
3	2 3 1 0 3
2	3 1 0 2 0
1	2 2 1 1 3
0	0 0 1 0 3
0	2 1 0 2 0
3	2 2 1 1 3
2	3 2 2 2 0
1	2 3 2 3 0
0	**0 3 2 0 2** $= \mathcal{R}_2(A)$

Table 3. $\mathcal{R}_1(A)$ and $\mathcal{R}_2(A)$ transformation of the string $A = 0\ 1\ 2\ 3\ 0$.

3 One-wayness from the lookup table point of view

Both $\mathcal{R}_1$ and $\mathcal{R}_2$ are serious candidates for one-way functions, with the difference that the number of computations to invert $\mathcal{R}_1$ is $O(s^{\lfloor \frac{N}{3} \rfloor})$ and to invert $\mathcal{R}_2$ it is $O(s^N)$. In the following two theorems we will prove these claims from a perspective of the lookup table (Latin Square) that defines the used quasigroup $(Q,*)$. We will discuss later in this section the reasons for this approach.

Theorem 1. *If the quasigroup $(Q,*)$ is non-associative and non-commutative, then the number of computations based only on the lookup table that defines the quasigroup $(Q,*)$ in order to find the preimage for the function $\mathcal{R}_1 : Q^N \to Q^N$ is $O(s^{\lfloor \frac{N}{3} \rfloor})$.*

Proof: Let $B = (b_0, b_1, \dots, b_{N-1})$ be given. The goal is to find a string $A = (a_0, a_1, \dots, a_{N-1})$ that satisfies the equality $B = E_{\overline{A},N}(A) = E_{(a_{N-1}, a_{N-2}, \dots, a_1, a_0),N}(A)$. Further, because the final values of the string B are obtained after N consecutive operations e_{a_j} we will use the following notation: $B^{(i)} = e_{a_{N-i}}(B^{(i-1)}) = (b_0^{(i)}, b_1^{(i)}, \dots, b_{N-2}^{(i)}, b_{N-1}^{(i)})$ for $i = \{1, \dots, N-1\}$, and $B^{(0)} = A$, $B^{(N)} \equiv B$.

	?	?	$\dots$	$\dots$	?
?	?	?	$\dots$	$\dots$	$b_{N-1}^{(1)}$
?	?	?	$\dots$	$\dots$	$b_{N-1}^{(2)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	.	$\vdots$
?	?	?	$b_2^{(N-2)}$	$\dots$	$b_{N-1}^{(N-2)}$
?	?	$b_1^{(N-1)}$	$\dots$	$\dots$	$b_{N-1}^{(N-1)}$
?	$b_0^{(N)}$	$b_1^{(N)}$	$\dots$	$\dots$	$b_{N-1}^{(N)}$

Table 4. Initial table obtained from the values of $B = (b_0, b_1, \dots, b_{N-1})$ before making any guess for the values of $A = (a_0, a_1, \dots, a_{N-1})$.

Since the quasigroup $(Q,*)$ is non-associative and non-commutative, the composition of e–transformations is fixed and it can not be changed (this is not the case if the quasigroup is commutative or associative). Thus, to solve the inverse task in fact we have to fill in the scheme in the Table 4, from bottom up using the properties of the quasigroup operation $*$. As a matter of fact due to the properties of quasigroup operation $*$ this scheme can be partially completed without guessing any value of A. Namely, from the equation $b_i^{(N)} * x = b_{i+1}^{(N)}$ we can calculate $x = b_{i+1}^{(N-1)}$ for $0 \le i \le N-1$, then from $b_i^{(N-1)} * y = b_{i+1}^{(N-1)}$ we

	a_0	$?$	$\dots$	$?$	a_{N-1}
a_{N-1}	$b_0^{(1)}$	$?$	$\dots$	$b_{N-2}^{(1)}$	$b_{N-1}^{(1)}$
$?$	$?$	$?$	$\dots$	$b_{N-2}^{(2)}$	$b_{N-1}^{(2)}$
$\vdots$	$\vdots$	$\vdots$	.	.	$\vdots$
$?$	$?$	$b_1^{(N-2)}$	$b_2^{(N-2)}$	$\dots$	$b_{N-1}^{(N-2)}$
$?$	$b_0^{(N-1)}$	$b_1^{(N-1)}$	$\dots$	$\dots$	$b_{N-1}^{(N-1)}$
a_0	$b_0^{(N)}$	$b_1^{(N)}$	$\dots$	$\dots$	$b_{N-1}^{(N)}$

a. Completing the table when the value of a_0 is guessed.

	a_0	a_1	$\dots$	a_{N-2}	a_{N-1}
a_{N-1}	$b_0^{(1)}$	$b_1^{(1)}$	$\dots$	$b_{N-2}^{(1)}$	$b_{N-1}^{(1)}$
a_{N-2}	$b_0^{(2)}$	$b_1^{(2)}$	$\dots$	$b_{N-2}^{(2)}$	$b_{N-1}^{(2)}$
$\vdots$	$\vdots$	$\vdots$	.	.	$\vdots$
$?$	$?$	$b_1^{(N-3)}$	$b_2^{(N-3)}$	$\dots$	$b_{N-1}^{(N-3)}$
$?$	$b_0^{(N-2)}$	$b_1^{(N-2)}$	$b_2^{(N-2)}$	$\dots$	$b_{N-1}^{(N-2)}$
a_1	$b_0^{(N-1)}$	$b_1^{(N-1)}$	$\dots$	$\dots$	$b_{N-1}^{(N-1)}$
a_0	$b_0^{(N)}$	$b_1^{(N)}$	$\dots$	$\dots$	$b_{N-1}^{(N)}$

b. Completing the table when the values of a_0 and a_1 are guessed.

Table 5.

can calculate $y = b_{i+1}^{(N-2)}$ for $1 \leq i \leq N-1$, and so on up to the first row of the table, where we can calculate the value of $b_{N-1}^{(1)}$.

Now, by knowing (or by guessing) the value of a_0 that range among s possible values we can find value $b_0^{(N-1)}$, from which we can find the other values in the scheme of Table 5a, together with the value of a_{N-1}.

If we continue with choosing a_1 from all possible s values we will obtain a new value for a_{N-2}. Next, with every choice of a_i, $2 \leq i \leq \frac{N}{2}$ we will obtain also the values for a_{N-i-1}, and by knowing that we will be in a position to complete the upper left corner of the scheme (see Table 5b). The intersection of the lower completed and the upper completed part is for $\lfloor \frac{N}{3} \rfloor$. So by choosing $\lfloor \frac{N}{3} \rfloor$ values we will obtain other values of the string A. Now, we can check whether we have made the right choice for a_0, $a_1, \dots, a_{\lfloor \frac{N}{3} \rfloor}$ or not. Therefore, the complexity of inversion of $\mathcal{R}_1$ only by using the lookup definition of the quasigroup $(Q, *)$ is $O(s^{\lfloor \frac{N}{3} \rfloor})$. $\Box$

Theorem 2. *If the quasigroup $(Q, *)$ is non-associative and non-commutative, then the number of computations based only on the lookup table that defines the quasigroup $(Q, *)$ in order to find the preimage for the function $\mathcal{R}_2 : Q^N \to Q^N$ is $O(s^N)$.*

Proof: The proof is similar to the proof for the function $\mathcal{R}_1$ except that now there is no intersection in the process of completing the scheme until the last guess for a_{N-1} is made. Therefore we have to make a guess for all N values $a_0, a_1, \dots, a_{N-1}$ and thus the complexity of inverting the function $\mathcal{R}_2$ only by using the lookup definition of the quasigroup $(Q, *)$ is $O(s^N)$. $\Box$

From previous two theorems we can make the following conjecture:

Conjecture 1. $\mathcal{R}_1$ and $\mathcal{R}_2$ are one-way functions.

To support Conjecture 1 we would like to stress that the used quasigroup $(Q, *)$ in general will not have any algebraic property such as commutativity, associativity, neutral elements etc. Thus, the only possible way to deal with the problem of inversion of these functions is to look at the lookup table (or Latin Square) that defines the quasigroup $(Q, *)$.

	$\mathcal{R}_N(A)$	a_0	a_1	$\dots$	a_{N-2}	a_{N-1}
$\mathbf{L}$	l_0	$\cdot$	$\cdot$		$\cdot$	$\cdot$
	l_1	$\cdot$	$\cdot$		$\cdot$	$\cdot$
	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$l_{P(N)}$	$\cdot$	$\cdot$		$\cdot$	$\cdot$
$\overline{A}$	a_{N-1}	$\cdot$	$\cdot$		$\cdot$	$\cdot$
	a_{N-2}	$\cdot$	$\cdot$		$\cdot$	$\cdot$
	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	a_0	$\cdot$	$\cdot$		$\cdot$	$\cdot$
$\overline{A}$	a_{N-1}	$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$
	a_{N-2}	$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	a_0	b_0	b_1	$\dots$	b_{N-2}	b_{N-1}

Table 6. Schematic representation of the process of computation of the function $\mathcal{R}_N$.

Next we will use the function $\mathcal{R}_2$ as a core for defining a family of one-way function candidates. The idea is that before applying the function $\mathcal{R}_2$ on some string A of length N, we would like to apply a certain number (polynomial on N) of e–transformations with leaders that are some constants from Q or they are fixed indexes that address certain letters of the string A. For that purpose we will need the following definition:

Definition 6. *Preprocessing string of leaders* $\mathbf{L} = \mathbf{L}_{Q,I_N,P(N)} = (l_0, l_1, \dots, l_{P(N)})$ *is a string of length that is polynomial of* N *and where* $l_i \in Q \cup I_N$, $Q = \{0, 1, \dots, s-1\}$ *and* $I_N = \{i_0, i_1, \dots, i_{N-1}\}$ *in an index set. By convention,* $\mathbf{L}$ *can be also an empty string.*

Definition 7. *The family* $\mathcal{Q}_N$ *of quasigroup one-way functions of strings of length* N *consists of functions* $\mathcal{R}_N : Q^N \to Q^N$ *such that*

$$B = \mathcal{R}_N(A) = E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$$

where $\mathbf{L}$ *is defined in Deffinition 6, and* $A, B \in Q^N$*. By convention, when applying the* e*–transformations with index leader i.e.* $l_j \in I_N$*, then* e*–transformation have to be applied with the leader* a_{l_j}*.*

For better understanding, a schematic representation of the process of computation of the function $\mathcal{R}_N$ is given in Table 6.

Conjecture 2. The family $\mathcal{Q}_N$ is a family of one-way functions.

Example 3. Let chose $N = 2$ and $(Q, *)$ be as in Table 1. If we interpret the elements of $Q = \{0, 1, 2, 3\}$ as two-bit letters $\{00, 01, 10, 11\}$ then by having $N = 2$ we will define function $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ from $\{0, 1, \ldots, 15\}$ into itself. If we chose $\mathbf{L} = (3, 3, i_1, i_0)$, then $E_{(3,3,i_1,i_0)\overline{AA},8}(A)$ is represented in Figure 2a. Notice that the function is permutation. On the other hand if we choose $\mathbf{L} = (3, 3, i_0, i_1)$ then we will get a function that is not a permutation. That is represented in Figure 2b. Particular computations for the string $01 \equiv 1$ in both cases is shown in Table 7.

	$0\ 1 \equiv 0001 \equiv 1$
3	0 1
3	0 1
1	3 3
0	3 1
1	2 2
0	0 0
1	3 0
0	**3 0** $\equiv 1100 \equiv 12$

	$0\ 1 \equiv 0001 \equiv 1$
3	0 1
3	0 1
0	2 2
1	1 1
1	0 1
0	2 2
1	1 1
0	**1 0** $\equiv 0100 \equiv 4$

Table 7. Transformation of the string $A = 0\ 1$ when $\mathbf{L} = (3, 3, i_1, i_0)$ (on the left) and $\mathbf{L} = (3, 3, i_0, i_1)$ (on the right).

4 One-way functions v.s. one-way permutations – non-fractal v.s. fractal quasigroups

Having defined families of one-way candidate functions, we are interested in which case functions $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ are permutations, and when they are not. In this section we will describe our experimental findings that give some directions for possible mathematical answers to these questions. We hope that this paper and the findings presented here will be sufficiently provocative for some readers to investigate them further and possibly give some solid mathematical explanations.

There are a lot of classifications of quasigroups of a specific order. Two main classifications are obtained by using the algebraic properties of the quasigroups: (1) classes of isotopic quasigroups, which are known only for quasigroups of orders up to 10 [9] and (2) classes of isomorphic quasigroups [7]. The importance of quasigroup classification is noted in many papers that deal with these algebraic structures (for example see [10], [11]).

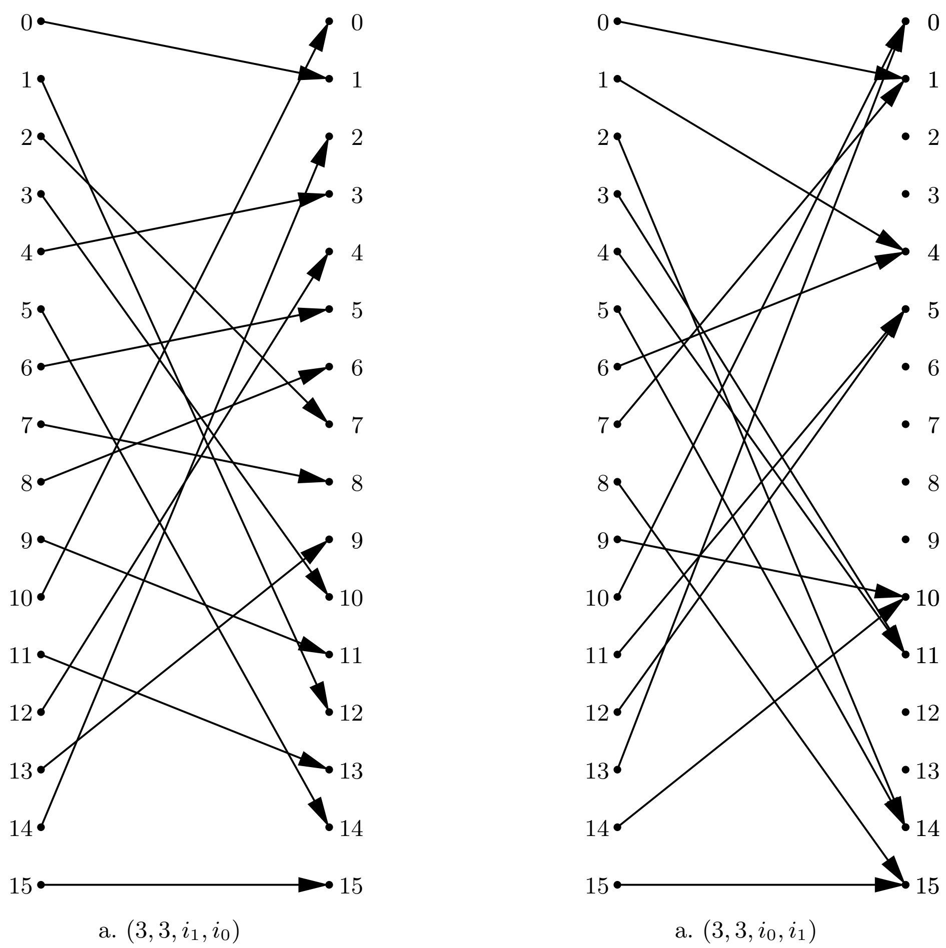


Fig. 2. Functions obtained by $\mathbf{L}$ being a. $(3, 3, i_1, i_0)$ and b. $(3, 3, i_0, i_1)$

From the point of view of this paper, classification of quasigroups can be done according to the nature of the one-way functions obtained by each quasigroup.

Since the number of quasigroups increases exponentially by the order of the quasigroup, we have made our experiments mainly for order 4 and some of our conjectures we have tested also on quasigroups of order 5. The total number of quasigroups of order 4 is 576. Our experiments have shown that the set of all 576 quasigroups of order 4 can be divided into two classes. One class $\mathcal{F}$ contains 192 quasigroups and the other class $\mathcal{NF}$ contains 384 quasigroups. If we order all quasigroups lexicographically from 1 to 576, then the class $\mathcal{F}$ contains the following quasigroups: $\mathcal{F} =\{$ 1, 2, 3, 4, 5, 7, 9, 11, 14, 18, 21, 24, 25, 26, 27, 28, 37, 40, 43, 46, 49, 51, 54, 57, 60, 63, 70, 71, 77, 80, 82, 83, 92, 93, 100, 101, 110, 111, 113, 116, 121, 126, 127, 132, 133, 138, 139, 144, 145, 146, 147, 148, 157, 160, 163, 166, 169, 170, 171, 172, 174, 176, 178, 179, 182, 185, 189, 192, 196, 197, 203, 206, 212, 213, 218, 222, 223, 228, 229, 232, 234, 235, 242, 243, 246, 252, 253, 259, 262, 263, 269, 272, 274, 275, 284, 285, 292, 293, 302, 303, 305, 308, 314, 315, 318, 324, 325, 331, 334, 335, 342, 343, 345, 348, 349, 354, 355, 359, 364, 365, 371, 374, 380, 381, 385, 388, 392, 395, 398, 399, 401, 403, 405, 406, 407, 408, 411, 414, 417, 420, 429, 430, 431, 432, 433, 438, 439, 444, 445, 450, 451, 456, 461, 464, 466, 467, 476, 477, 484, 485, 494, 495, 497, 500, 506, 507, 514, 517, 520, 523, 526, 528, 531, 534, 537, 540, 549, 550, 551, 552, 553, 556, 559, 563, 566, 568, 570, 572, 573, 574, 575, 576$\}$. (By the way, the quasigroup defined in Table 1 by which we have performed examples in this paper has the lexicographic number 355.)

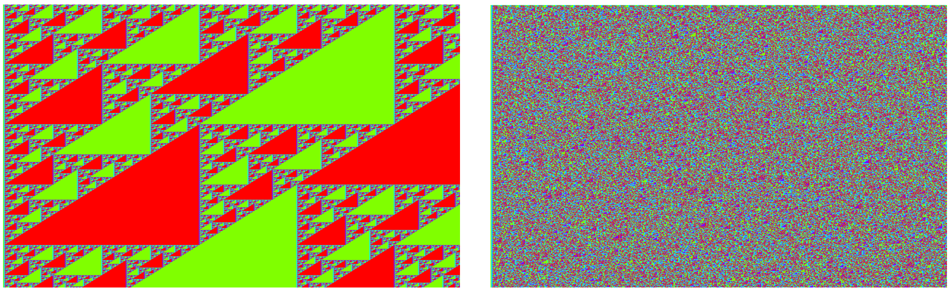
From numerous experiments that we have performed, we can post the following conjectures:

Conjecture 3. For any quasigroup $(Q, *) \in \mathcal{F}$ and for every natural number N there exists at least one string $\mathbf{L}$ such that the function $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ is a permutation in the set $\{0, 1, \ldots, 2^{2N} - 1\}$.

Conjecture 4. For any quasigroup $(Q, *) \in \mathcal{NF}$ and for every natural number N there is no string $\mathbf{L}$ such that the function $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ is a permutation in the set $\{0, 1, \ldots, 2^{2N} - 1\}$.

The classes $\mathcal{F}$ and $\mathcal{NF}$ have another interesting "graphical" property. Namely, if we take the periodic string $01230123\ldots$, and treat every letter as a pixel with the corresponding color, then by consecutive application of e–transformations with any constant leader l the set of 576 quasigroups can be divided into two classes: A class of quasigroups that give self-similar i.e. fractal images, and the class of quasigroups that give non self-similar images. As an example on Figure 8a we show the image obtained by the quasigroup number 46, and on Figure 8b the image obtained by the quasigroup number 47.

In [12] one can find the same classification but instead of terms "fractal" and "non-fractal" classes of quasigroups they are named by an other property of them - a class of linear and a class of exponential quasigroups. In the same paper it is mentioned that when the order of quasigroup increases, the number of fractal (linear) quasigroups decreases exponentially compared to the number of



a. b.

Table 8. The images obtained by consecutive e–transformations with the quasigroups of order 4 with lexicographic numbers 46 and 47. The transformations are done on a periodic string $01230123\ldots0123$ with the length 600 and with the leader 0.

non-fractal quasigroups. An additional classification that is close to the fractal – non-fractal classification can be found in [11] and an excellent survey for many types of classifications of quasigroups is done in [13].

It is really amazing how our experimental findings about the fractal – non-fractal classification of quasigroups comply with the classification of quasigroups that give one-way permutations and one-way functions. An open problem is to investigate the relation between these two classifications. Here even without precise definition of what "fractal" quasigroup would mean, we just give the following conjecture:

Conjecture 5. The classes of fractal quasigroups and quasigroups for which there is a permutation $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ coincide.

5 Some comparative analysis for the quasigroup one-way functions

In this section we would like to set the following convention: For a random oracle in the sense of Rudich and Impagliazzo works on one-way functions ([14], [16]), we will take any quasigroup $(Q,*)$ of order s together with the family $\mathcal{Q}_N$ of one-way functions that can be defined by that quasigroup.

Rudich in his PhD thesis [14], based on a combinatorial conjecture (which was proved in 2000 by Kahn, Saks and Smith in [15]) concluded that there exist oracles for which there exist one-way functions, but there are no one-way permutations. That is in perfect compliance with our case of quasigroup one-way functions. If the oracle (quasigroup) is non-fractal, our Conjecture 4 says that there are no strings $\mathbf{L}_{Q,I_N,P(N)}$ such that the function $E_{\mathbf{L}\overline{AA},P(N)+2N}(A)$ is a permutation.

Impaliazzo and Rudich in [16] showed that "There exist an oracle relative to which a strongly one-way permutation exists, but secure secret-key agreement is impossible." That is again in compliance with quasigroup one-way functions. Namely, since quasigroup one-way functions rely on combinatorial characteristics of the quasigroups, in general there are no evident "shortcuts" and properties that will define a trapdoor function, that will enable secure secret-key agreement.

Quasigroup one-way functions are strong one-way functions i.e. there is only a small set of values on which they can be inverted in polynomial time. Thus, security amplification of a weak one-way function by an iterative process, that was established as a very useful technique in the work of Yao in 1982 [17] is not necessary for quasigroup one-way functions. This means that the speed of computation of quasigroup one-way functions can be very high. Additionally, since the computations are done consecutively, they can be parallelized in a pipeline, and then the computation of the function can be done in time $O(P(N))$. Some initial applications of quasigroup one-way functions and their properties to be easily parallelized are already done in definition of the stream cipher Edon80 [18]. In that stream cipher the IVSetup procedure is in fact a sort of quasigroup one-way function.

From Theorem 2 it follows that quasigroup one-way functions can achieve the level of security of 2^n attempts to invert the function with the length of the input being n bits. That is most efficient construction as far as we know compared to other candidate one-way functions that require from $2n$ to $10n$ input bits to reach the security level of 2^n.

The last property of quasigroup one-way functions that we want to mention in this paper, and that is similar to the properties that have been already found in other one-way functions is the property of a one-way function to be regular i.e. that have equal number of inversions on every point of their codomain. Namely, in [19] and [20] techniques for obtaining 1–1 one-way functions are proposed if the one-way function is regular. In our numerous experiments, every time when we have used fractal quasigroup, the obtained one-way functions were either permutations or regular ones. The example that we show on Figure 2b. is an example of a regular function, where every point of its codomain has exactly two inversions. It would be a challenging task to apply the same techniques to quasigroup one-way functions.

6 Conclusions and further directions

In this paper we have given a formal definition and construction of a new family of one-way functions and one-way permutations. They are based on quasigroup string transformations, and have numerous interesting properties. By some of those properties (such as speed of computation, security level of inversion) they outperform all currently known candidate one-way functions.

Many of our results concerning these functions are still experimental, and thus we have set up several conjectures about them. We hope that the intriguing experimental results mentioned in this paper about the new family of one-way functions will be interesting enough to attract attention of other researchers.

References

1. W. Diffie and M. Helman, New directions in cryptography, *IEEE Trans. Inform. Theory*, Vol. 22, 1976, pp. 644–654.
2. S. Goldwasser and S. Micali, Probabilistic Encryption, *JCSS*, Vol 28, No. 2, April 1984, pp. 270–299.
3. R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. of the ACM*, Vol. 21, 1978, pp. 120–126.
4. O. Goldreich, H. Krawczyk and M. Luby, On the existance of Pseudorandom Generators, *SIAM J. on Computing*, Vol. 22, No. 6, December, 1993, pp. 1163–1175.
5. R. Impagliazzo and M. Naor, Efficient Cryptographic Schemes Provably as Secure as Subset Sum, In *Proc.* 30^{th} *FOCS*, 1989, pp. 236 – 241.
6. O. Goldreich, Candidate One-Way Functions Based on Expander Graphs, 2000, Manuscript, `http://www.wisdom.weizmann.ac.il/õded/ow-candid.html`
7. J. Dénes, A.D. Keedwell, *Latin Squares and their Applications*, English Univer. Press Ltd., 1974.
8. S. Markovski, D. Gligoroski, and V. Bakeva, Quasigroup String Processing: Part 1, *Contributions, Sec. Math. Tech. Sci., MANU*, XX 1-2(1999) 13-28.
9. McKay, B.D., Rogoyski, E.:Latin squares of order 10. *Electronic J. Comb.* Vol. **2** (1995) `http://ejc.math.gatech.edu:8080/Journal/journalhome.html`
10. R. L. McCasland and V. Sorge, Automating Algebra's Tedious Tasks: Computerised Classification, In *Proc. First Workshop on Challenges and Novel Applications for Automated Reasoning*, Miami, 2003 (http://www.uclic.ucl.ac.uk/usr/jgow/cnaar.pdf) 37 – 40.
11. S. Markovski, D. Gligoroski and J. Markovski, Classification of Quasigroups by Random Walk on Torus, *J.Appl. Math. & Computing* Vol. 19(2005), No. 1 – 2, pp. 57 – 75.
12. S. Markovski, D. Gligoroski and L. Kocarev, Unbiased Random Sequences from Quasigroup String Transformations, In *Proc. Fast Software Encryption: 12th International Workshop, FSE 2005*, Paris, France, February 21-23, 2005, LNCS, Vol. 3557, 2005, pp. 163.
13. V. Dimitrova, *Quasigroup Transformations and Their Applications*, MS Thesis, 2005, Institute of Informatics, Faculty of Natural Sciences, Skopje, Macedonia `vesnap@ii.edu.mk`.
14. S. Rudich, *Limits on the provable consequences of one-way functions*, Ph.D Thesis, University of California at Berkeley, 1988, `http://www.cs.cmu.edu/řudich/`
15. J. Kahn, M. Saks and C. Smyth, A dual version of Reimer's inequality adn a proof of Rudich's conjecture. In *Proceedings of the 15th IEEE Conference on Computational Complexity*, 2000.
16. R. Impagliazzo and S. Rudich, Limits on the provable consequences of one-way permutations. In *Proc. of the 21st ACM Symposium on Theory of Computing*, pp. 44–61, 1989.
17. A.C. Yao, Theory and Application of Trapdoor Functions, In *Proc. of 23th IEEE Symposium on Foundations of Computer Science*, pp. 80–91, 1982.
18. D. Gligoroski, S. Markovski, L. Kocarev, and M. Gušev, Edon80 - Hardware synchoronous stream cipher. In *Proc. Symmetric Key Encryption Workshop*, Århus, Denmark, May, 2005.
19. O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan, and D. Zuckerman. Security preserving amplification of hardness. In *Proc. 31st Annual Symposium on Foundations of Computer Science*, pp. 318– 326. IEEE, 1990.

20. O. Goldreich, L. A. Levin and N. Nisan, On Constructing 1-1 One-Way Functions, *Electronic Colloquium on Computational Complexity (ECCC)*, Vol. 2, Nr. 029, 1995.