M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 26, 2012, Fasc. 3–4

Analysis of Some Quasigroup Transformations as Boolean Functions

Aleksandra Mileva

Presented at MASSEE International Conference on Mathematics MICOM-2009

Two kind of attacks on cryptographic primitives - the linear and the differential cryptanalysis, have been occupied the attention of the cryptographic community since several years ago. Every cryptographic primitive can be examined as a vector valued Boolean function. The prop ratio tables and the correlation matrices are important tools for analyzing the resistance of any Boolean function to the linear and the differential cryptanalysis. There are several cryptographic primitives based on the so called quasigroup transformations, and in this paper we analyze these quasigroup transformations as Boolean functions. We examine correlation matrices, prop ratio tables and some other cryptographic properties.

MSC 2010: 94A60, 20N05, 11T71.

Key Words: vector valued Boolean function, prop ratio tables, correlation matrices, quasigroup transformations.

1. Introduction

Most of the known constructions of cryptographic primitives use structures from the associative algebras as groups, rings and fields. Two eminent specialists on quasigroups, J. Dénes and A. D. Keedwell [5], once proclaimed the advent of a new era in cryptology, consisting in the application of non-associative algebraic systems as quasigroups and neo-fields. In the past few years, cryptographic community have been introduced with several complete quasigroup based cryptographic primitives (complete in the sense of software and/or hardware implementations, security analysis and proofs and external cryptanalysis), as the binary additive stream cipher Edon80 [6], which is one of the few left unbroken eSTREAM finalists; two Round 1 candidate hash functions of NIST SHA-3 competition: Edon-$\mathcal{R}$ [7] and NaSHA [10]; etc. In these

examples, different quasigroup transformations are used, with quasigroup order that varies from 4 to 2^{512}.

Quasigroups and quasigroup transformations in cryptography have been used primarily as non-linear building blocks, so one have to examine confusion and diffusion they produce. Confusion corresponds to the nonlinearity, i.e., to the Hamming distances of the given function to the set of affine functions. The algebraic degree of the function is a first measure of nonlinearity. Another tool to measure of nonlinearity is the correlation matrix, introduced in [3]. The elements of the correlation matrices consist of the correlation coefficients associated with linear combinations of input bits and linear combinations of output bits. Linear cryptanalysis [12] can be seen as the exploitation of correlations between linear combinations of bits of different intermediate encryption values in a block cipher calculation, so correlation matrices are therefore the natural representation for the description and understanding of the mechanisms of linear cryptanalysis. Diffusion corresponds to the propagation characteristics of the given function, and can be estimated by several complementary measures ([17], [2]). One measure is connected with difference propagation, which is exploited by differential cryptanalysis [1] so the prop ratio tables [4] can be used as a tool.

In this paper we represent quasigroup transformations as vector valued Boolean functions and analyzed them in a term of correlation matrices and prop ratio tables.

2. Quasigroup string transformations

A *quasigroup* $(Q, *)$ is a groupoid with the property:

$$(\forall\ a, b \in Q)\ (\exists!\ x, y \in Q)\ (a * x = b\ \wedge\ y * a = b) \tag{2.1}$$

Let Q be an alphabet and let $*$ be a randomly chosen quasigroup operation on Q. Let denote by $Q^+ = \{x_1 x_2 \dots x_t \mid x_i \in Q, t \geq 1\}$ the set of all finite string over Q. For a fixed letter $l \in Q$ called leader, the quasigroup string transformations $e_l, d_l : Q^+ \to Q^+$ are defined in [13, 14] as:

$$e_l(x_1 \dots x_t) = (z_1 \dots z_t) \Leftrightarrow z_j = \begin{cases} l * x_1, & j = 1 \\ z_{j-1} * x_j, & 2 \leq j \leq t \end{cases}$$

$$d_l(z_1 \dots z_t) = (x_1 \dots x_t) \Leftrightarrow x_j = \begin{cases} l * z_1, & j = 1 \\ z_{j-1} * z_j, & 2 \leq j \leq t \end{cases}$$

Every quasigroup transformation that apply on the given string in one pass we will call *elementary quasigroup transformation.* e_l (used in Edon80) and d_l are elementary quasigroup transformations. Composition of elementary

quasigroup transformations we will call *composite quasigroup transformation.* Compositions of e_{l_i} or d_{l_i} transformations with fixed leaders $l_1, l_2, \ldots, l_s \in Q$ define new composite E and D transformations, which are permutations [14]:

$$E = e_{l_s} \circ e_{l_{s-1}} \circ \ldots \circ e_{l_1}, \quad D = d_{l_s} \circ d_{l_{s-1}} \circ \ldots \circ d_{l_1}.$$

Special kind of E transformation is the quasigroup reverse string transformation $\mathcal{R}$, first introduced in [8], where the leaders are the elements of the string, taken in reverse order. This transformation is used in Edon-$\mathcal{R}$.

There are extensive theoretical studies and numerical experiments of the sequences produced by E and D transformations [14, 15, 16].

Proposition 2.1 *The transformations e_l and d_l produced by a linear quasigroup are linear functions.*

P r o o f. Let $(Q, *)$ be a linear quasigroup [9] of order $r = 2^n$. Then for all $x, y, z \in Q$, with binary representations $(x_1, \ldots, x_n)$ of x and $(y_1, \ldots y_n)$ of y we have

$$z = x * y = (\sum \alpha_i^{(1)} x_i + \sum \beta_i^{(1)} y_i, \ldots, \sum \alpha_i^{(n)} x_i + \sum \beta_i^{(n)} y_i)$$

where $\alpha_i^{(k)}$ and $\beta_i^{(k)}$ are 1 or 0 for each $i, k \in \{1, 2, \ldots, n\}$. For $l, a^1, \ldots, a^s \in Q$ we have

$$e_l(a^1 \ldots a^s) = z^1 \ldots z^s, \quad d_l(a^1 \ldots a^s) = u^1 \ldots u^s.$$

Let $\alpha_{ri}^{(k)}$ $\beta_{ri}^{(k)}$, $\delta_{ri}^{(k)}$ and $\lambda_{ri}^{(k)}$ be 1 or 0 for each $i, k \in \{1, 2, \ldots, n\}$ and each $r \in \{1, 2, \ldots, s\}$. For each $j \in \{2, \ldots s\}$ we have

$$z^1 = l * a^1 = (\sum \alpha_{1i}^{(1)} l_i + \sum \beta_{1i}^{(1)} a_i^1, \ldots, \sum \alpha_{1i}^{(n)} l_i + \sum \beta_{1i}^{(n)} a_i^1) = (z_1^1, \ldots, z_n^1),$$

$$z^j = z^{j-1} * a^j = (\sum \alpha_{ji}^{(1)} z_i^{j-1} + \sum \beta_{ji}^{(1)} a_i^j, \ldots, \sum \alpha_{ji}^{(n)} z_i^{j-1} + \sum \beta_{ji}^{(n)} a_i^j) =$$

$$(z_1^j, \ldots, z_n^j),$$

$$u^1 = l * a^1 = (\sum \delta_{1i}^{(1)} l_i + \sum \lambda_{1i}^{(1)} a_i^1, \ldots, \sum \delta_{1i}^{(n)} l_i + \sum \lambda_{1i}^{(n)} a_i^1) = (u_1^1, \ldots, u_n^1),$$

$$u^j = a^{j-1} * a^j = (\sum \delta_{ji}^{(1)} a_i^{j-1} + \sum \lambda_{ji}^{(1)} a_i^j, \ldots, \sum \delta_{ji}^{(n)} a_i^{j-1} + \sum \lambda_{ji}^{(n)} a_i^j) =$$

$$(u_1^j, \ldots, u_n^j)$$

So, inductively we have that every bit in $e_l(a^1 \ldots a^s)$ and $d_l(a^1 \ldots a^s)$ is obtained by linear Boolean function, therefore e_l and d_l are linear vector valued Boolean functions. ∎

Composition of linear functions is also a linear function, so the following corollary is true.

Corollary 2.1 *The transformations E and D produced by a linear quasigroup are linear functions.*

If we allow $Q = Z_{2^n}$ to be with group operation addition modulo 2^n, for a fixed leader $l \in G$, the quasigroup additive string transformation $\mathcal{A}_l : Q^+ \to Q^+$ and the quasigroup reverse additive string transformation $\mathcal{RA}_l : Q^+ \to Q^+$ can be defined [11] as elementary quasigroup transformations:

$$\mathcal{A}_l(x_1 \dots x_t) = (z_1 \dots z_t) \Leftrightarrow z_j = \begin{cases} (l + x_1) * x_1, & j = 1 \\ (z_{j-1} + x_j) * x_j, & 2 \le j \le t \end{cases}$$

$$\mathcal{RA}_l(x_1 \dots x_t) = (z_1 \dots z_t) \Leftrightarrow z_j = \begin{cases} x_j * (x_j + z_{j+1}), & 1 \le j \le t-1 \\ x_t * (x_t + l), & j = t \end{cases}$$

These transformations are not bijective mappings. Special kind of composition of $\mathcal{A}$ and $\mathcal{RA}$ transformations applied consecutively, so called main transformation $\mathcal{MT}$, is used in NaSHA.

Let $QT_{L,s,t} : Q^t \to Q^t$ be a family of quasigroup transformations defined by the quasigroup $(Q, *)$, $|Q| = 2^n$, that are composition of s elementary quasigroup transformations, with leader string L of length s, $s \ge 1$. The transformation $QT_{L,s,t}$ can be represented as vector valued Boolean function $BQT_{L,s,t} : \{0,1\}^{tn} \to \{0,1\}^{tn}$.

Example 2.1. For the quasigroup of order 4 with lexicographic order 231 (Table 1), the elementary quasigroup transformations $e_1, d_1, \mathcal{A}_1$ and $\mathcal{RA}_1$ ($s = 1$ and $L = 1$) of strings of length $t = 2$, can be represented as vector valued Boolean functions $\{0,1\}^4 \to \{0,1\}^4$ (see Table 2), using integer representation.

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

Table 1: Quasigroup 231

We can take the leader string L to be consider as a string of variables and in such a way we obtain a family of transformations $QT_{s,t} : Q^s \times Q^t \to Q^t$, where the elements of Q^s are considered as leaders. Then, the transformation $QT_{s,t}$ can be represented as vector valued Boolean function $BQT_{s,t} : \{0,1\}^{sn} \times \{0,1\}^{tn} \to \{0,1\}^{tn}$.

Example 2.2. For the same quasigroup 231, the elementary quasigroup transformation e_l of strings of length 2, can be represented as vector

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$e_1(x)$	8	9	10	11	15	12	13	14	1	2	3	0	6	7	8	9
$d_1(x)$	9	10	11	8	14	15	12	13	0	1	2	3	7	4	5	6
$\mathcal{A}_1(x)$	8	8	11	9	6	5	5	4	6	5	5	4	1	3	2	2
$\mathcal{RA}_1(x)$	14	4	3	3	6	12	11	11	2	8	7	7	2	8	7	7

Table 2: Transformations $e_1, d_1, \mathcal{A}_1$ and $\mathcal{RA}_1$

valued Boolean functions $\{0,1\}^2 \times \{0,1\}^4 \to \{0,1\}^4$ (see Table 3), using integer representation.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$l=0$	6	7	4	5	8	9	10	11	15	12	13	14	1	2	3	0
$l=1$	8	9	10	11	15	12	13	14	1	2	3	0	6	7	4	5
$l=2$	1	2	3	0	6	7	4	5	8	9	10	11	15	12	13	14
$l=3$	15	12	13	14	1	2	3	0	6	7	4	5	8	9	10	11

Table 3: The transformation e_l as vector valued Boolean function

3. Correlation matrices and prop ratio tables of some quasigroup transformations

We investigated the behavior of transformations E, D, $\mathcal{A}_l$ and $\mathcal{RA}_l$ produced by all quasigroups of order 4, on strings of length $t = 2$ and $t = 3$. The transformations E and D are compositions of s elementary quasigroup transformations, where $1 \leq s \leq 100$. We use fixed leader l for all composite transformations, which is the worst case. All of these transformations can be represented as vector valued Boolean functions $\{0,1\}^4 \to \{0,1\}^4$ for $t = 2$ and $\{0,1\}^6 \to \{0,1\}^6$ for $t = 3$. We use the classification of quasigroups from [9].

Example 3.1. The representation of the transformation $E_{L=22,s=5,t=2}$, produced by quasigroup 231, as vector valued Boolean function is given in Table 4, where integer representation is used.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$E_{L=22,s=5,t=2}(x)$	1	2	3	0	6	7	4	5	8	9	10	11	15	12	13	14

Table 4: Vector valued Boolean representation of $E_{L=22,s=5,t=2}$

The correlation matrix and the prop ratio table for this $E_{L=22,s=5,t=2}$ transformation are given in Table 5 and Table 6, respectfully.

One can see from the correlation matrix that there exist 7 nonzero output selection vectors that are correlated only to one input selection vector. Output selection vectors $0001 = 1$, $0100 = 4$ and $1000 = 8$ are correlated with input selection vectors 1101, 0100 and 1000, respectfully, with correlation coefficient

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	−1	0	0
2	0	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
3	0	0	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	0	0
4	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	−1	0	0	0	0	0	0
6	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{2}$
7	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$
8	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
9	0	0	0	0	0	−1	0	0	0	0	0	0	0	0	0	0
10	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$
11	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{2}$
12	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
13	0	−1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
15	0	0	0	0	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0

Table 5: Correlation matrix of transformation $E_{L=22,s=5,t=2}$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0
5	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0
7	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0
9	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0
11	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$
14	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$

Table 6: Prop ratio table of the transformation $E_{L=22,s=5,t=2}$

-1, 1 and 1. This means that this transformation has 2 linear and 1 affine component Boolean functions, i.e., $y_1 = x_1,\ y_0 = x_0$ and $y_3 = 1 \oplus x_0 \oplus x_1 \oplus x_3$.

We obtained several interesting results from our numerical experiments. Our experiments show us that all quasigroups of order 4 can produce linear $E_{l,s,2}$ and $E_{l,s,3}$ transformations, for some choices of the leader l. There are 48 quasigroups with a property to produce linear $E_{l,s,2}$ and $E_{l,s,3}$ transformations, independently from chosen leader and for every $s = 2k$ and $s = 4k$, respectfully

and another 16 quasigroups with the same property but for $s = 4k$ and $s = 8k$, respectfully. Another 80 quasigroups have a property to produce linear $E_{l,s,2}$ and $E_{l,s,3}$ transformations for at least one leader and for every $s = 2k$ and $s = 8k$, respectfully. The last class of 288 quasigroups have a property to produce linear $E_{l,s,2}$ and $E_{l,s,3}$ transformations, independently from chosen leader for $s = \{6k, 8k, 9k, 12k, 24k\}$ and $s = \{24k, 27k, 48k, 54k, 72k\}$, respectfully. This class is the only class that produce $E_{l,s,2}$ and $E_{l,s,3}$ transformations with maximal prop ratio not equal always to 1. The results about their least maximal absolute correlation coefficients and least maximal prop ratio are given in Table 7.

	$E_{l,s,2}$		$E_{l,s,3}$		$D_{l,s,2}$		$D_{l,s,3}$	
r	C	R_p	C	R_p	C	R_p	C	R_p
4	1	$\frac{1}{2}$	1	$\frac{3}{8}$	1	1	1	1
8	$\frac{1}{2}$	$\frac{7}{32}$			1	$\frac{5}{16}$		

Table 7: The least maximal absolute correlation coefficient C and the least maximal prop ratio R_p of E and D quasigroup transformations.

For $D_{l,s,2}$ and $D_{l,s,3}$ transformations, we do not obtain any linear transformation for any choice of the leader and any nonlinear quasigroups of order 4. They all produce correlation matrices with 7 ($t = 2$) and 15 ($t = 3$) nonzero output selection vectors that are correlated only to one input selection vector and prop ratio tables with maximal prop ratio of 1. All produced non-linear $D_{l,s,2}$, $D_{l,s,3}$, $E_{l,s,2}$ and $E_{l,s,3}$ transformations by quasigroups of order 4 have at least one linear component polynomial in their ANF.

These experiments and Proposition 1 are enough to conclude that E and D transformations preserve the linearity of used quasigroups. Even more, the E transformation increase the linearity in the sense that nonlinear quasigroup can produce linear transformations, sometimes. This is not the case with D transformation. We can conclude also that non-linear E transformations have better propagation characteristics (smaller maximal prop ratio), with less correlation between their input and output, then D transformations from the same quasigroups. Note that we have investigated the worst case - when the leader is fixed for all composite quasigroup transformations.

We also take the quasigroup of order 8 from [11] and investigate $E_{l,s,2}$ and $D_{l,s,2}$ transformations, for $s \leq 100$, on strings with length 2, for different choices of the fixed leader. In the set of $E_{l,s,2}$ and $D_{l,s,2}$ transformations, there are functions without any linear component polynomial in their ANF. Number of composite quasigroup transformations does not influence the correlation coefficients and the prop ratios in a sense that they do not decrease with it, but they vary in some range of values.

One can see, that even for smaller strings, taking quasigroups with higher order decrease the maximal absolute correlation coefficient and maximal prop ratio table of produced E transformation, regardless the number of composite quasigroup transformations. Length of the string additionally put bigger confusion and diffusion property on the same transformations. We made numerical experiments for $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, also. Because these transformations are not bijections, we investigated the case of producing constant functions. 24 quasigroups of order 4 produce constant functions with $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, independently from the chosen leader. These quasigroups have the structure - every next row is obtained from the previous one by rotating to the right by one position. In addition, it is not important quasigroup to be linear, with or without some component linear polynomial in its ANF (8 quasigroups are without any linear component polynomial). Additionally, we examined $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations with this group of quasigroups on bigger strings, with length up to 10, and we obtained constant functions again. We took several quasigroups of order 8 with this kind of structure and they produce constant $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations on strings of length 2 and 3. Another 88 quasigroups produce constant functions for some choice of the leader.

24 non-linear quasigroups produce linear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, independently from the chosen leader (again 8 quasigroups are without any linear component polynomial). They also have some structure - every next row is obtained from the previous one by rotating to the left by one position. We examined also $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations with this group of quasigroups on strings with length 3 and 4, and we obtained linear functions again. Another two sets of 86 quasigroups produce only linear $\mathcal{A}_l$ transformations or only linear $\mathcal{RA}_l$ transformations, independently from the chosen leader. Another 78 quasigroups produce linear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations for some choice of the leader.

	$\mathcal{A}_l$,	$t=2$	$\mathcal{A}_l$,	$t=3$	$\mathcal{RA}_l$,	$t=2$	$\mathcal{RA}_l$,	$t=3$
r	C	R_p	C	R_p	C	R_p	C	R_p
4	1	$\frac{1}{2}$	$\frac{1}{32}$	$\frac{3}{16}$	1	$\frac{1}{2}$	$\frac{1}{32}$	$\frac{3}{16}$
8	$\frac{1}{2}$	$\frac{9}{32}$			$\frac{1}{2}$	$\frac{1}{4}$		

Table 8: The least maximal absolute correlation coefficient and the least maximal prop ratio of $\mathcal{A}_l$ and $\mathcal{RA}_l$ quasigroup transformations.

At the end, 120 quasigroups produce nonlinear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, independently from the chosen leader, and here structure of quasigroups is different again (7 are linear and 38 quasigroups are without any linear component polynomial). All these transformations have maximal absolute value of the correlation coefficient of 1 and dependently of the leader, maximal prop ratio is 1 for the linear, and $\frac{1}{2}$ for nonlinear quasigroups (see Table 8).

4. Conclusion

Cryptographic properties of quasigroup transformations as vector valued Boolean functions depend mainly of the properties of used quasigroup and the string length. Linear quasigroups produce linear E and D transformations. From the numerical results we can conclude that nonlinear quasigroups can produce linear E transformations in some cases, but not linear D transformations. Non-linear E transformations have better propagation characteristics (smaller maximal prop ratio), with less correlation between their input and output, then D transformations from the same quasigroups.

For the nonlinearity of $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, nonlinearity of quasigroup is not important, but some other structural properties of quasigroups must be investigated. Linear quasigroups can produce nonlinear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations, and vice versa, linear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations can be produced by nonlinear quasigroups. Secondly, we can make a hypothesis that quasigroups with structure - next row to be the previous one, rotated to the right by one position, produce constant functions, independently of the choice of the leader, length of the string or order of the quasigroup. Also, we can make a hypothesis that quasigroups of order 4 with structure - next row to be the previous one, rotated to the left by one position produce linear $\mathcal{A}_l$ and $\mathcal{RA}_l$ transformations.

The order of the used quasigroup and the length of the string have influence on decreasing the maximal absolute correlation coefficient and maximal prop ratio table of the produced quasigroup transformations, regardless the number of composite quasigroup transformations.

References

[1] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. // *Journal of Cryptology* **4(1)**, 1991, 3–72.

[2] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine. Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. // *Advances in Cryptology – Eurocrypt 2000, LNCS* **1807**, 2000, 507–522.

[3] J. Daemen, R. Govaerts, J. Vandewalle. Correlation matrices. // *Fast Software Encryption 1994, LNCS* **1008**, 1995, 275–285.

[4] J. Daemen. *Cipher and Hash Function Design. Strategies based on Linear and Differential Cryptanalysis.* PhD Thesis, Katholieke Universiteit Leuven, 1995.

[5] J. Dénes, A. D. Keedwell. Some applications of non-associative algebraic systems in cryptology. // *Pure Math. and Applications*, **12(2)**, 2001, 147–195.

[6] D. Gligoroski, S. Markovski, S. J. Knapskog. *The Stream Cipher Edon80*, New Stream Cipher Designs: The eSTREAM Finalists. Springer-Verlag, 2008, 152–169.

[7] D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drápal, V. Klima. Cryptographic Hash Function EDON–R. Submited to NIST, 2008.

[8] D. Gligoroski. Candidate one-way functions and one-way permutations based on quasigroup string transformations. // *Cryptology ePrint Archive*, Report 2005/352, 2005.

[9] D. Gligoroski, V. Dimitrova, S. Markovski. Classification of Quasigroups as Boolean Functions, their Algebraic Complexity and Application of Gröbner Bases in Solving Systems of Quasigroup Equations // M. Sala (ed.), *Groebner, Coding, and Cryptography*, Springer, 2007.

[10] S. Markovski, A. Mileva. NaSHA Cryptographic Hash Function. Submited to NIST, 2008.

[11] A. Mileva, S. Markovski. Correlation Matrices and Prop Ratio Tables for Quasigroups of order 4. // *The* 6^{th} *International Conference for Informatics and Information Technology, CIIT*, 2008, 17–22.

[12] M. Matsui. Linear Cryptanalysis Method for DES Cipher. // *Advances in Cryptology, EUROCRYPT 1993, LNCS* **765**, 1993, 386–397.

[13] S. Markovski, D. Gligoroski, S. Andova. Using quasigroups for one-one secure encoding. // *Proc. VIII Conf. Logic and Computer Science LIRA97*, Novi Sad, 1997, 157–162.

[14] S. Markovski, D. Gligoroski, V. Bakeva. Quasigroup String Processing – Part 1. // *Contributions, Sec. Math. Tech. Sci.*, MANU, **XX, 1–2**, 1999, 13–28.

[15] S. Markovski, V. Kusakatov. Quasigroup String Processing – Part 2. // *Contributions, Sec. Math. Tech. Sci.*, MANU, **XXI, 1–2**, 2000, 15–32.

[16] S. Markovski, V. Kusakatov. Quasigroup String Processing – Part 3. // *Contributions, Sec. Math. Tech. Sci.*, MANU, **XXIII–XXIV, 1–2**, 2002–2003, 7–27.

[17] K. Pommerening. *Fourier Analysis of Boolean Maps, A tutorial.* 2005.

Faculty of Informatics
University Goce Delčev
Štip 2000, REPUBLIC OF MACEDONIA
E-MAIL: aleksandra.mileva@ugd.edu.mk

Received 04.02.2010