GLASNIK MATEMATIČKI
Vol. 47(67)(2012), 333 – 349

SHAPELESS QUASIGROUPS DERIVED BY FEISTEL ORTHOMORPHISMS

Aleksandra Mileva and Smile Markovski
University "Goce Delčev" and University "Ss Cyril and Methodius",
Republic of Macedonia

Abstract. Shapeless quasigroups are needed for cryptography purposes. In this paper, we construct shapeless quasigroups by the diagonal method from orthomorphisms over abelian groups. We use generalizations of Feistel networks as orthomorphisms. We introduce parameters into several types of Extended Feistel networks and Generalized Feistel-non linear feedback shift registers and, by suitable choice of the parameter values, different shapeless quasigroup can be used in every application.

1. Introduction

A quasigroup is a groupoid $(Q, *)$ with the property that each of the equations $a * x = b$ and $y * a = b$ has a unique solution for x, respectively y. When Q is a finite set, the main body of the Cayley table of the quasigroup $(Q, *)$ represents a Latin square, i.e., a matrix with rows and columns that are permutations of Q.

Today, we can already speak about quasigroup based cryptography, because the number of new defined cryptographic primitives that use quasigroups is growing. There already exist stream ciphers like EDON-80 ([9]), hash functions like EDON-R ([10]) and NaSHA ([18]), digital signature scheme like MQQ-SIG ([8]), public key cryptosystem like LQLP-s (for $s \in \{104, 128, 160\}$) ([19]), etc.

In quasigroup based cryptography one can find that different authors seek quasigroups with different properties. Some need $CI-$quasigroups ([14]), some need multivariate quadratic quasigroups ([8]), other need orthogonal quasigroups ([24]), etc. There are also cryptosystems build on some particular

2010 *Mathematics Subject Classification.* 20N05, 94A60.
Key words and phrases. Shapeless quasigroup, extended Feistel network, orthomorphism, generalized Feistel-non linear feedback shift register.

subsets of quasigroups. In general, quasigroups that are suitable for cryptography need to be with as little structure as possible, like shapeless quasigroups, defined by Gligoroski et al. ([7]).

DEFINITION 1.1 ([7]). *A finite quasigroup $(Q, *)$ of order r is said to be* **shapeless** *iff it is non-idempotent, non-commutative, non-associative, it does not have neither left nor right unit, it does not contain proper sub-quasigroups, and there is no $k < 2r$ such that identities of the kinds*

$$\underbrace{x * (x \cdots * (x}_{k} * y)) = y, \ y = ((y * \underbrace{x) * \cdots x) * x}_{k} \tag{1.1}$$

are satisfied in $(Q, *)$.

Quasigroups in cryptography can be applied for quasigroup transformations, as non-linear building blocks in stream ciphers, block ciphers, and hash functions. For example, for $\mathcal{R}$ quasigroup transformation in Edon-$\mathcal{R}$ ([10]) a family of hash functions, and for $\mathcal{MT}$ quasigroup transformation in NaSHA-(m, k, r) ([18, 21]) a family of hash functions, used quasigroups should be at least shapeless.

Possible candidates for shapeless quasigroups are simple quasigroups without subquasigroups, that are studied in [2, 12, 15, 25]. In [2] simple quasigroups are constructed by fixing several elements in their Cayley schemes, and then completing the scheme arbitrarily. These constructions are not effective and hence they are not suitable for obtaining shapeless quasigroups of higher order. The simple linear quasigroups from [25] satisfy the identities (1.1) for $k \leq r$, so they are not shapeless.

In this paper we consider several ways for obtaining shapeless quasigroups of different orders. For that purpose, we investigate the constructions of Extended Fesitel Networks (EFN), that are originally defined for building block cipher's round functions. We show how shapeless quasigroups can be constructed by using EFN. Furthermore, we use parameters in our constructions, that provide us with a tool for using a set of different quasigroups, with similar properties, in the designs of cryptographic primitives.

In the sequel we suppose that all considered quasigroups are finite and non-trivial.

The paper is organized as follows. Section 2 recalls Sade's diagonal method for quasigroup construction and notions of orthomorphisms and complete mappings. Most important, sufficient conditions a quasigroup to be shapeless are established. Different generalizations of EFN are given in Section 3. Constructions of quasigroups by using the EFN of types PFN, *type-1* PEFN and GF-NLFSR are presented in the Sections 4, 5 and 6. Some conclusions are given in Section 7.

2. Diagonal method and orthomorphisms

Sade ([23]) proposed the following way of constructing quasigroups, now known as the *diagonal method*. Consider the group $(\mathbb{Z}_n, +)$ and let θ be a permutation of the set $\mathbb{Z}_n$, such that $\phi(x) = x - \theta(x)$ be also a permutation. Define an operation $\circ$ on $\mathbb{Z}_n$ by:

$$x \circ y = \theta(x - y) + y \tag{2.1}$$

where $x, y \in \mathbb{Z}_n$. Then $(\mathbb{Z}_n, \circ)$ is a quasigroup (and we say that $(\mathbb{Z}_n, \circ)$ is derived by θ).

Quasigroups that are constructed by the diagonal method possess a decomposition in disjoint transversals and therefore they posses an orthogonal mate. For these quasigroups, every translation $\sigma_h : x \to x + h$ is an automorphism. It can be shown that if θ works for the diagonal method, then each of the mappings $x \mapsto \theta^{-1}(x)$, $x \mapsto x - \theta(x)$, $x \mapsto -\theta(-x)$, $x \mapsto x + \theta(-x)$, $x \mapsto \theta(x) + h$ and $x \mapsto \theta(x + h)$, for any h, also works. Kristen ([20]) generalized this construction method for every group $(G, +)$. She incorrectly named those permutations as complete mappings. Complete mappings are first defined by Mann ([16]) and the name orthomorphism was first used by Johnson et al. ([13]).

Definition 2.1 ([3, 5]). *A* complete mapping *of a group $(G, +)$ is a permutation $\phi : G \to G$ such that the mapping $\theta : G \to G$ defined by $\theta(x) = x + \phi(x)$ ($\theta = I + \phi$, where I is the identity mapping) is again a permutation of G. The mapping θ is the* orthomorphism *associated with the complete mapping ϕ. A group G is* admissible *if there is a complete mapping $\phi : G \to G$.*

If θ is the orthomorphism associated with the complete mapping ϕ of a group $(G, +)$, then $-\phi$ is the orthomorphism associated with the complete mapping $-\theta$. We note that $-$ denotes the bijection $x \mapsto -x$.

A generalization of the diagonal method by using complete mappings and orthomorphisms is given by the following theorem.

Theorem 2.2. *Let ϕ be a complete mapping of the admissible group $(G, +)$ and let θ be an orthomorphism associated with ϕ. Define operations $\circ$ and $\bullet$ on G by*

$$x \circ y = \phi(y - x) + y = \theta(y - x) + x, \tag{2.2}$$

$$x \bullet y = \theta(x - y) + y = \phi(x - y) + x, \tag{2.3}$$

where $x, y \in G$. Then $(G, \circ)$ and $(G, \bullet)$ are quasigroups, opposite to each other, i.e., $x \circ y = y \bullet x$ for every $x, y \in G$.

An orthomorphism θ_2 of G is said to be orthogonal to an orthomorphism θ_1 if and only if $\theta_1\theta_2^{-1}$ is an orthomorphism of G as well. If G is an

abelian group and θ_2 is orthogonal to θ_1, then θ_1 is orthogonal to θ_2 too. This follows from the well-known fact that, for an abelian group $(G,+)$, the inverse of the complete mapping (orthomorphism) is also a complete mapping (orthomorphism) ([5, 13]). The orthomorphism θ^{-1} is associated with the complete mapping $-\phi\theta^{-1}$ and the orthomorphism $\theta\phi^{-1}$ is associated with the complete mapping ϕ^{-1}. Even more, each orthomorphism is orthogonal to I, and θ^{-1} is orthogonal to θ if and only if θ^2 is an orthomorphism ([13]).

If a quasigroup $(G,\bullet)$ is derived by an orthomorphism according to (2.3), then all of its parastrophes $/,\backslash,//,\backslash\backslash,\cdot$ can be also derived by an orthomorphisms (see [5] and [26]). This fact can be especially useful for designing cryptographic primitives, like encoding and decoding functions. The next theorem gives these orthomorphisms explicitly.

THEOREM 2.3. *Let $\phi : G \to G$ be a complete mapping of an abelian group $(G,+)$ with associated orthomorphism $\theta : G \to G$. Then all the parastrophies of the quasigroup $(G,\bullet)$ can be obtained by the equation (2.3) and the following statements are true.*

a) *The quasigroup $(G,/)$ is derived by the orthomorphism θ^{-1} associated with the complete mapping $-\phi\theta^{-1}$.*
b) *The quasigroup $(G,\backslash)$ is derived by the orthomorphism $-\theta(-\phi)^{-1}$ associated with the complete mapping $-(-\phi)^{-1}$.*
c) *The quasigroup $(G,//)$ is derived by the orthomorphism $-\phi(-\theta)^{-1}$ associated with the complete mapping $(-\theta)^{-1}$.*
d) *The quasigroup $(G,\backslash\backslash)$ is derived by the orthomorphism $-\phi^{-1}$ associated with the complete mapping $-\theta\phi^{-1}$.*
e) $(G,\cdot) = (G,\circ)$.

PROOF. a)

$$x/y = z \iff z \bullet y = x \iff \theta(z-y)+y = x$$
$$\iff z - y = \theta^{-1}(x-y) \iff z = \theta^{-1}(x-y)+y.$$

b)

$$x\backslash y = z \iff x \bullet z = y \iff \theta(x-z)+z = y$$
$$\iff x - z = \theta^{-1}(y-z) \iff x = \theta^{-1}(y-z)+z-y+y$$
$$\iff x - y = \theta^{-1}(y-z)-(y-z) \iff x-y = -(\phi\theta^{-1})(y-z)$$
$$\iff z = -(-(\phi\theta^{-1}))^{-1}(x-y)+y = -\theta(-\phi)^{-1}(x-y)+y.$$

c)

$$x//y = z \iff z \bullet x = y \iff \theta(z-x)+x = y$$
$$\iff -\theta(z-x) = x-y \iff z-x = (-\theta)^{-1}(x-y)$$
$$\iff z = (-\theta)^{-1}(x-y)+(x-y)+y$$
$$\iff z = -\phi(-\theta)^{-1}(x-y)+y.$$

d)

$$\begin{aligned} x\backslash\backslash y = z &\iff y \bullet z = x \iff \theta(y-z)+z = x \\ &\iff \theta(y-z)-(y-z) = x-y \iff \phi(y-z) = x-y \\ &\iff y-z = \phi^{-1}(x-y) \iff z = -\phi^{-1}(x-y)+y. \end{aligned}$$

e)

$$x \cdot y = y \bullet x = x \circ y.$$

□

Hsu and Keedwell ([11]) have introduced the notion of a strong complete mapping as a complete mapping that is also an orthomorphism. Every complete mapping of the abelian group $(\mathbb{Z}_2^n, \oplus)$ is a strong complete mapping, too.

Next we consider the algebraic properties of the quasigroup $(G, \bullet)$ derived by the orthomorphism θ as in the equation (2.3). Also, up to the end of this section, we suppose that G is an abelian group.

If $\theta(0) = 0$, $(G, \bullet)$ is idempotent and $(\theta, \theta(-x)+x)$ is a pair of orthogonal permutations [4].

PROPOSITION 2.4. *If $\theta(0) \neq 0$, then the quasigroup $(G, \bullet)$ has no idempotent elements, i.e., $x \bullet x \neq x$ for each $x \in G$.*

PROOF. Let $x \in G$ be an idempotent element. Then we have

$$x \bullet x = x \iff \theta(x-x)+x = x \iff \theta(0) = 0.$$ □

PROPOSITION 2.5. *The quasigroup $(G, \bullet)$ does not have a left unit and if θ is not the identity mapping it does not have a right unit either.*

PROOF. Let e be a left unit of $(G, \bullet)$. Then, for all $x \in G$, we have

$$e \bullet x = x \Longrightarrow \theta(e-x)+x = x \Longrightarrow \theta(e-x) = 0.$$

This contradicts the fact that θ is a bijection.

Let e be a right unit of $(G, \bullet)$. Then, for all $x \in G$, we have

$$x \bullet e = x \Longrightarrow \theta(x-e)+e = x \Longrightarrow \theta(x-e) = x-e.$$

This means that $\theta = I$ is the identity mapping. □

PROPOSITION 2.6. *The quasigroup $(G, \bullet)$ is non-associative.*

PROOF. Let $(G, \bullet)$ be associative. Then $(G, \bullet)$ is a group and it possess a unit, a contradiction to Proposition 2.5. □

PROPOSITION 2.7. *Two elements x, y of a quasigroup $(G, \bullet)$ commute iff $\theta(x-y) = \phi(y-x)$.*

PROOF. We have

$$x \bullet y = y \bullet x \iff \theta(x-y)+y = \theta(y-x)+x$$
$$\iff \theta(x-y) = \theta(y-x)-(y-x) \iff \theta(x-y) = \phi(y-x).$$

□

COROLLARY 2.8. *The quasigroup $(G,\bullet)$ is non-commutative iff $\theta(z) - \theta(-z) \neq z$ for some $z \in G$.*

COROLLARY 2.9. *If θ is an orthomorphism of the abelian group $(\mathbb{Z}_2^n, \oplus)$, the quasigroup $(\mathbb{Z}_2^n, \bullet)$ is anti-commutative.*

Next, we have

$$y \bullet x = \theta(y-x)+x$$
$$(y \bullet x) \bullet x = \theta(\theta(y-x)+x-x)+x = \theta^2(y-x)+x$$

and, by induction,

$$((y \bullet \underbrace{x) \bullet \ldots) \bullet x}_{l} = \theta^l(y-x)+x. \tag{2.4}$$

We have also

$$x \bullet y = \theta(x-y)+y = \phi(x-y)+x,$$
$$x \bullet (x \bullet y) = \phi(x-\phi(x-y)-x)+x = -(-\phi(-\phi(x-y)))+x$$

and, by induction,

$$\underbrace{x \bullet (\cdots \bullet (x}_{l} \bullet y)) = \underbrace{-(-\phi(-\phi(\cdots - \phi(x-y)\ldots)))}_{l} + x. \tag{2.5}$$

These equations prove the following proposition.

PROPOSITION 2.10. *a) The identity*

$$y = ((y \bullet \underbrace{x) \bullet \ldots) \bullet x}_{l}$$

holds true in $(G,\bullet)$ iff $\theta^l = I$.

b) The identity

$$\underbrace{x \bullet (\cdots \bullet (x}_{l} \bullet y)) = y$$

holds true in $(G,\bullet)$ iff $(-\phi)^l = I = (I-\theta)^l$.

Since we are interested in shapeless quasigroups, we have also to consider the existence of subquasigroups of a quasigroup $(G,\bullet)$. Our first partial result is obtained by an exhaustive checking, and it is interesting only for small order quasigroups.

PROPOSITION 2.11. *Let θ be an orthomorphism of an abelian group $(G,+)$ and let $(G,\bullet)$ be a quasigroup obtained by the equation* (2.3)*. The following statements are true.*

(a) *If* $\theta(0) \neq 0$*, then the order of any subquasigroup of* $(G, \bullet)$ *is larger than* 2.
(b) *If* $\theta^2(0) \neq 0$*, then the order of any subquasigroup of* $(G, \bullet)$ *is larger than* 3.
(c) *If* $\theta^2(0) \neq 0$ *and* $\theta^3(0) \neq 0$*, then the order of any subquasigroup of* $(G, \bullet)$ *is larger than* 4.

Using identities (2.4) and (2.5) we have for any $x \in G$ the following equations, where ϕ is a complete mapping with an associated orthomorphism θ.

$$(2.6)\quad ((x \bullet \underbrace{x) \bullet \dots) \bullet x}_{l} = \theta^l(0) + x, \qquad \underbrace{x \bullet (\cdots \bullet (x}_{l} \bullet x)) = -(-\phi)^l(0) + x.$$

Having in mind Theorem 2.3, we have the following equations for the parastrophies as well.

$$(2.7)\quad ((x/\underbrace{x)/\dots)/x}_{l} = (\theta^{-1})^l(0) + x, \qquad \underbrace{x/(\dots(x}_{l}/x)) = -(\phi\theta^{-1})^l(0) + x,$$

(2.8)
$$((x\underbrace{\backslash x) \setminus \dots) \setminus x}_{l} = (-\theta(-\phi)^{-1})^l(0)+x,\ \underbrace{x \setminus (\cdots \setminus (x}_{l} \backslash x)) = -((-\phi)^{-1})^l(0)+x,$$

(2.9)
$$((x/\!\!/\underbrace{x)/\!\!/ \dots)/\!\!/x}_{l} = (-\phi(-\theta)^{-1})^l(0)+x,\ \underbrace{x/\!\!/(\dots/\!\!/(x}_{l}/\!\!/x)) = -(-(-\theta)^{-1})^l(0)+x,$$

(2.10)
$$((x \setminus\!\setminus \underbrace{x) \setminus\!\setminus \dots) \setminus\!\setminus x}_{l} = (-\phi^{-1})^l(0) + x,\ \underbrace{x \setminus\!\setminus (\cdots \setminus\!\setminus (x}_{l} \setminus\!\setminus x)) = -(\theta\phi^{-1})^l(0) + x.$$

Let $(S, \bullet)$ be a subquasigroup of the quasigroup $(G, \bullet)$. Then for each operation $* \in \{\bullet, /, \setminus, /\!\!/, \setminus\!\setminus\}$ and for every $x, y \in S$ we have $x * y \in S$. Let denote by $<x>$ the subquasigroup of $(G, \bullet)$ generated by an element $x \in G$. According to equations (2.6) – (2.10) we have that all of the elements

$$\begin{aligned} &x,\ \theta^l(0) + x,\ -(-\phi)^l(0) + x,\ (\theta^{-1})^l(0) + x,\ -(\phi\theta^{-1})^l(0) + x, \\ &(-\theta(-\phi)^{-1})^l(0) + x,\ -((-\phi)^{-1})^l(0) + x,\ (-\phi(-\theta)^{-1})^l(0) + x, \\ &-(-(-\theta)^{-1})^l(0) + x,\ (-\phi^{-1})^l(0) + x,\ -(\theta\phi^{-1})^l(0) + x \end{aligned} \tag{2.11}$$

belong to $<x>$ for each $l = 1, 2, 3, \dots$

Let us denote by

$$\begin{aligned} \pi = \{&\theta^l,\ -(-\phi)^l,\ (\theta^{-1})^l,\ -(\phi\theta^{-1})^l,\ (-\theta(-\phi)^{-1})^l, -((-\phi)^{-1})^l, \\ &(-\phi(-\theta)^{-1})^l,\ -(-(-\theta)^{-1})^l,\ (-\phi^{-1})^l,\ -(\theta\phi^{-1})^l \mid l = 1, 2, 3, \dots\}. \end{aligned}$$

The permutations from the set π are defined on a finite set G, so they are product of disjoint cycles. We conclude that the cardinality of $<x>$ depends on the length of the cycles containing the element 0 of the permutations from the set π.

A finite quasigroup $(G, \bullet)$ cannot have a subquasigroup of order greater than $|G|/2$, so we have the following.

PROPOSITION 2.12. *If some of the permutations from the set π have a cycle containing 0 of length greater than $|G|/2$, then the quasigroup $(G, \bullet)$ cannot have a proper subquasigroup.*

We have from (2.11) that

$$\begin{aligned} y = \theta^l(0) + x \in <x> &\implies \theta^k(0) + y = \theta^k(0) + \theta^l(0) + x \in <x> \\ &\implies \theta^m(0) + \ldots + \theta^k(0) + \theta^l(0) + x \in <x> \end{aligned}$$

for any positive integers $m, \ldots, k, l$. In the same manner, for any $\lambda_1, \lambda_2, \ldots, \lambda_r \in \pi$, we have that $\lambda_1(0)+\lambda_2(0)+\cdots+\lambda_r(0)+x \in <x>$, where r is any positive integer. Let

$$\begin{aligned} S = \{&\theta^l(0),\ -(-\phi)^l(0),\ (\theta^{-1})^l(0),\ -(\phi\theta^{-1})^l(0),\ (-\theta(-\phi)^{-1})^l(0), \\ &-((-\phi)^{-1})^l(0), (-\phi(-\theta)^{-1})^l(0),\ -(-(-\theta)^{-1})^l(0),\ (-\phi^{-1})^l(0), \\ &-(\theta\phi^{-1})^l(0) \mid l = 1, 2, 3, \ldots\}, \end{aligned}$$

and let denote by LCS the set of all linear combinations of the elements in S. Then we have $|LCS| \leq |\ <x>\ |$, for each $x \in G$. Hence, the following property is true.

PROPOSITION 2.13. *The quasigroup $(G, \bullet)$ is without a proper subquasigroup if $|LCS| > |G|/2$.*

The next theorem, that gives sufficient conditions a quasigroup to be shapeless, follows from the Propositions 2.4-2.13.

THEOREM 2.14. *Let θ be an orthomorphism of the abelian group $(G, +)$, and let $(G, \bullet)$ be a quasigroup derived by θ by the equation (2.3). Then $(G, \bullet)$ is a shapeless quasigroup if the following conditions are satisfied:*

i) $\theta(0) \neq 0$,
ii) $\theta^k \neq I$ *for all* $k < 2|G|$,
iii) $(I - \theta)^k \neq I$ *for all* $k < 2|G|$,
iv) $\theta(z) - \theta(-z) \neq z$ *for some* $z \in G$,
v) $|LCS| > |G|/2$.

We can use Theorem 2.14 for practical generation of orthomorphisms that produce shapeless quasigroups and/or examination does given permutation is an orthomorphism that produce a shapeless quasigroup.

EXAMPLE 2.15. Let us examine the orthomorphism θ of the abelian group $(Z_2^4, \oplus)$ given on the Table 1. This orthomorphism satisfies all conditions from Theorem 2.14, so the quasigroup derived by θ is a shapeless quasigroup. It is presented on Table 2.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\theta(x)$	3	9	15	2	13	7	1	11	14	6	4	0	12	8	10	5
$x \oplus \theta(x)$	3	8	13	1	9	2	7	12	6	15	14	11	0	5	4	10

TABLE 1. An integer representation of an orthomorphism $\theta(x)$ of the group $(Z_2^4, \oplus)$

f	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	3	8	13	1	9	2	7	12	6	15	14	11	0	5	4	10
1	9	2	0	12	3	8	13	6	14	7	10	15	4	1	11	5
2	15	3	1	10	5	14	11	0	12	9	4	13	6	8	2	7
3	2	14	11	0	15	4	1	10	8	13	12	5	9	7	6	3
4	13	6	3	8	7	12	9	5	4	1	0	14	2	11	10	15
5	7	12	9	2	13	6	4	8	0	5	15	1	10	3	14	11
6	1	10	15	4	11	7	5	14	2	12	6	3	8	13	0	9
7	11	0	5	14	6	10	15	4	13	3	2	7	12	9	8	1
8	14	7	6	3	8	13	12	2	11	0	5	9	1	10	15	4
9	6	15	2	7	12	9	3	13	1	10	8	4	11	0	5	14
10	4	1	12	5	14	0	10	15	7	11	9	2	13	6	3	8
11	0	5	4	13	1	15	14	11	10	6	3	8	7	12	9	2
12	12	9	8	6	10	3	2	7	5	14	11	0	15	4	1	13
13	8	13	7	9	2	11	6	3	15	4	1	10	5	14	12	0
14	10	4	14	11	0	5	8	1	9	2	7	12	3	15	13	6
15	5	11	10	15	4	1	0	9	3	8	13	6	14	2	7	12

TABLE 2. The quasigroup derived by the orthomorphism θ

At the end of this section, we note that shapeless quasigroups produced by this method have some undesirable properties - they are diagonally cyclic quasigroups based on an abelian group $(G, +)$ (i.e., $(x + 1) \bullet (y + 1) = x \bullet y + 1$ for every $x, y \in G$) and if the group $(\mathbb{Z}_2^n, \oplus)$ is used, then Shroeder quasigroups are obtained [17] (i.e., $(x \bullet y) \bullet (y \bullet x) = x$ for every $x, y \in \mathbb{Z}_2^n$). This means that certain shapeless quasigroups have some structure undesirable for cryptographic applications, therefore a user has to be careful of the kind on shapeless quasigroup under consideration. The property of being a shapeless quasigroup is not a sufficient, but only a necessary condition, in order for a quasigroup to be good for cryptographic purposes. Still, we can use these particular constructions of the shapeless quasigroups in the cases when the diagonally cyclic property is not important.

3. Several generalizations of Feistel networks as orthomorphisms

H. Feistel ([6]) defined a special function, now known as Feistel network, that can be used for building cryptographic primitives (the block cipher DES, for example). In order to construct shapeless quasigroups, we consider several orthomorphisms obtained by generalizations of Feistel networks. We call these orthomorphisms, Feistel orthomorphisms.

We defined Extended Feistel network (EFN) in an earlier paper of ours [17]. Later, we understood that the same name has already been used by several authors for denoting the so called *type-1*, *type-2* and *type-3* Extended Feistel networks. Now we redefine EFN from [17] as Parameterized Feistel network (PFN).

Definition 3.1 ([17, 21]). *Let $(G,+)$ be an abelian group, let $f : G \to G$ be a mapping and let $A, B, C \in G$ be constants. The* **Parameterized Feistel network** *$F_{A,B,C} : G^2 \to G^2$ created by f is defined for every $l, r \in G$ by*

$$F_{A,B,C}(l,r) = (r + A, l + B + f(r + C)).$$

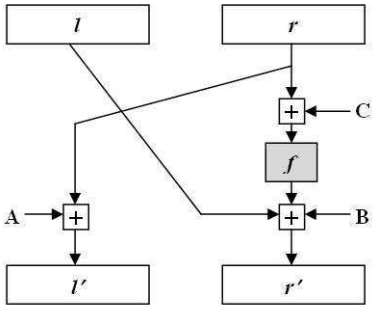

Figure 1. Parameterized Feistel network $F_{A,B,C}$

It was shown in [17, 21] that if the starting mapping f is a bijection, then the PFN $F_{A,B,C}$ and its square $F^2_{A,B,C}$ are orthomorphisms of the group $(G^2,+)$. Moreover, they are orthogonal orthomorphisms.

Type-1, *type-2* and *type-3* Extended Feistel networks, introduced by Zheng et al. ([27]), split the input blocks into $n > 2$ sub-blocks. We have redefined them with parameters and over abelian groups. We could prove that only *type-1* EFN is an orthomorphism.

Definition 3.2. *Let an abelian group $(G,+)$, a mapping $f : G \to G$, constants $A_1, A_2, \ldots, A_{n+1} \in G$ and an integer $n > 1$ be given. The* type-1

Parameterized Extended Feistel network (PEFN) $F_{A_1,A_2,\ldots,A_{n+1}} : G^n \to G^n$ *created by* f *is defined for every* $(x_1, x_2, \ldots, x_n) \in G^n$ *by*

$$F_{A_1,A_2,\ldots,A_{n+1}}(x_1, x_2, \ldots, x_n) = (x_2 + f(x_1 + A_1) + A_2, x_3 + A_3, \ldots, x_n + A_n, x_1 + A_{n+1}).$$

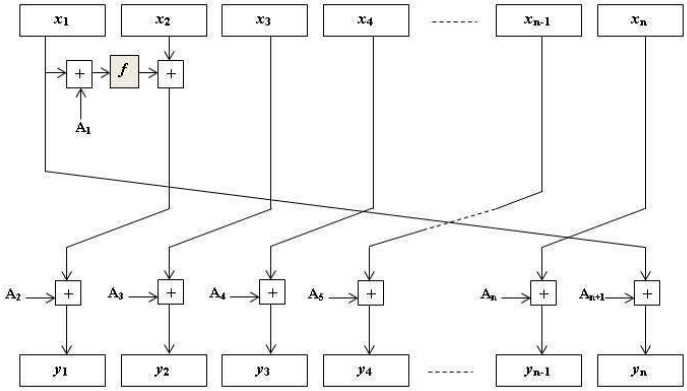

FIGURE 2. *Type-1* Parameterized Extended Feistel network (PEFN) $F_{A_1,A_2,\ldots,A_{n+1}}$

The *type-1* PEFN $F_{A_1,A_2,\ldots,A_{n+1}}$ is a bijection with inverse

$$F^{-1}_{A_1,A_2,\ldots,A_{n+1}}(y_1, y_2, \ldots, y_n) = (y_n - A_{n+1}, y_1 - f(y_n - A_{n+1} + A_1) - A_2, y_2 - A_3, y_3 - A_4, \ldots, y_{n-1} - A_n).$$

THEOREM 3.3. *If* $F_{A_1,A_2,\ldots,A_{n+1}} : G^n \to G^n$ *is a* type-1 *PEFN created by a bijection* $f : G \to G$*, then it is an orthomorphism of the group* $(G^n, +)$.

PROOF. Let $\Phi = F_{A_1,A_2,\ldots,A_{n+1}} - I$, i.e., $\Phi(x_1, x_2, \ldots, x_n) = (x_2 - x_1 + f(x_1 + A_1) + A_2, x_3 - x_2 + A_3, \ldots, x_n - x_{n-1} + A_n, x_1 - x_n + A_{n+1}) = (y_1, y_2, \ldots, y_n)$ for every $(x_1, x_2, \ldots, x_n) \in G^n$.

Define the function $\Omega : G^n \to G^n$ by $\Omega(y_1, y_2, \ldots, y_n) = (z, z - y_n - y_{n-1} - \ldots - y_2 + A_{n+1} + A_n + \ldots + A_3 - A_1, z - y_n - y_{n-1} - \ldots - y_3 + A_{n+1} + A_n + \ldots + A_4 - A_1, \ldots, z - y_n - y_{n-1} + A_{n+1} + A_n - A_1, z - y_n + A_{n+1} - A_1)$, where $z = f^{-1}(y_1 + y_2 + \ldots + y_n - A_2 - A_3 - \ldots - A_{n+1}) - A_1$.

We have $\Omega \circ \Phi = \Phi \circ \Omega = I$, i.e., Φ and $\Omega = \Phi^{-1}$ are bijections. □

We have defined *type-2* PEFN and *type-3* PEFN respectively, by the functions $G_{A_1,A_2,\ldots,A_{2n}}(x_1, x_2, \ldots, x_n) = (x_2 + f(x_1 + A_1) + A_2, x_3 + A_3, x_4 + f(x_3 + A_4) + A_5, x_5 + A_6, \ldots, x_n + f(x_{n-1} + A_{2n-2}) + A_{2n-1}, x_1 + A_{2n})$ and $H_{A_1,A_2,\ldots,A_{2n-1}}(x_1, x_2, \ldots, x_n) = (x_2 + f(x_1 + A_1) + A_2, x_3 + f(x_2 + A_3) +$

$A_4, \ldots, x_n + f(x_{n-1} + A_{2n-3}) + A_{2n-2}, x_1 + A_{2n-1})$. These functions are bijections, but they are not orthomorphisms in general. Thus, they are not subject of our interest.

Choy et al. ([1]) proposed a new structure called GF-NLFSR (Generalized Feistel-non linear feedback shift register). We will redefine it with parameters and over abelian groups.

DEFINITION 3.4. *Let an abelian group $(G, +)$, a mapping $f : G \to G$, constants $A_1, A_2, \ldots, A_{n+1} \in G$ and an integer $n > 1$ be given. The* **PGF-NLFSR (Parameterized Generalized Feistel-non linear feedback shift register)** *$F_{A_1,A_2,\ldots,A_{n+1}} : G^n \to G^n$ created by f is defined for every $(x_1, x_2, \ldots, x_n) \in G^n$ by*

$$F_{A_1,A_2,\ldots,A_{n+1}}(x_1, x_2, \ldots, x_n) = (x_2 + A_1, x_3 + A_2, \ldots, x_n + A_{n-1}, x_2 + \ldots + x_n + A_n + f(x_1 + A_{n+1})).$$

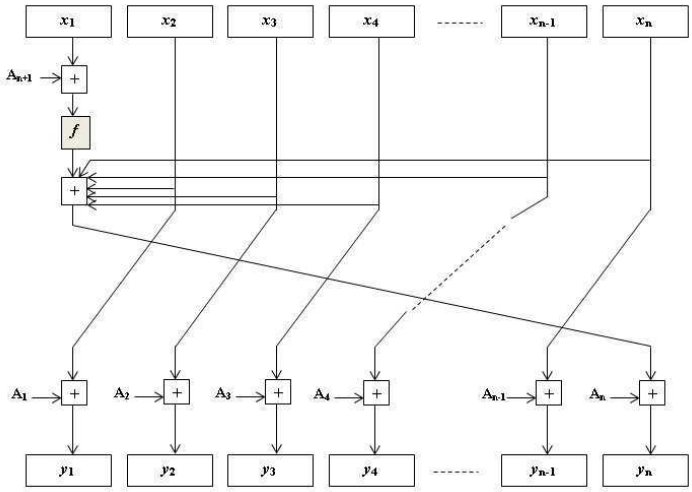

FIGURE 3. PGF-NLFSR $F_{A_1,A_2,\ldots,A_{n+1}}$

If f is a bijection, then PGF-NLFSR $F_{A_1,A_2,\ldots,A_{n+1}}$ is a bijection with inverse $F^{-1}_{A_1,A_2,\ldots,A_{n+1}}(y_1, y_2, \ldots, y_n) = (f^{-1}(y_n - y_1 - y_2 - \ldots - y_{n-1} - A_n + A_1 + A_2 + \ldots + A_{n-1}) - A_{n+1}, y_1 - A_1, y_2 - A_2, \ldots, y_{n-1} - A_{n-1})$.

We note that when the group $(\mathbb{Z}_2^m, \oplus)$ is used and $A_1 = A_2 = \ldots = A_{n+1} = 0$, then we obtain the GF-NLFSR according to Choy et al. ([1]).

THEOREM 3.5. *For the abelian group $(\mathbb{Z}_2^m, \oplus)$ and for every positive even integer n, any PGF-NLFSR $F_{A_1,A_2,\ldots,A_{n+1}} : (\mathbb{Z}_2^m)^n \to (\mathbb{Z}_2^m)^n$ created by a bijection $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ is an orthomorphism of the group $((\mathbb{Z}_2^m)^n, \oplus)$.*

PROOF. Let $\Phi = F_{A_1,A_2,\ldots,A_{n+1}} - I$, i.e., $\Phi(x_1, x_2, \ldots, x_n) = F_{A_1,A_2,\ldots,A_{n+1}}(x_1, x_2, \ldots, x_n) \oplus (x_1, x_2, \ldots, x_n) = (x_2 \oplus A_1 \oplus x_1, x_3 \oplus A_2 \oplus x_2, \ldots, x_n \oplus A_{n-1} \oplus x_{n-1}, x_2 \oplus \ldots \oplus x_{n-1} \oplus A_n \oplus f(x_1 \oplus A_{n+1})) = (y_1, y_2, \ldots, y_n)$ for every $(x_1, x_2, \ldots, x_n) \in (\mathbb{Z}_2^m)^n$.

First we observe that

$$\begin{aligned} &y_1 = x_2 \oplus x_1 \oplus A_1, \\ &y_1 \oplus y_2 = x_3 \oplus x_1 \oplus A_1 \oplus A_2, \\ &\vdots \\ &y_1 \oplus y_2 \oplus \ldots \oplus y_{n-2} = x_{n-1} \oplus x_1 \oplus A_1 \oplus A_2 \oplus \ldots \oplus A_{n-2}. \end{aligned}$$

The sum of the right-hand sides of the previous equality, when $n = 2k$, is $x_2 \oplus x_3 \oplus \ldots \oplus x_{n-1} \oplus A_2 \oplus A_4 \oplus \ldots \oplus A_{n-2}$.

Define the function $\Omega : (\mathbb{Z}_2^m)^n \to (\mathbb{Z}_2^m)^n$ by

$$\begin{aligned} \Omega(y_1, y_2, \ldots, y_n) = (&z, z \oplus y_1 \oplus A_1, z \oplus y_1 \oplus y_2 \oplus A_1 \oplus A_2, \ldots, \\ &z \oplus y_1 \oplus \ldots \oplus y_{n-1} \oplus A_1 \oplus \ldots \oplus A_{n-1}). \end{aligned}$$

where $z = f^{-1}(y_n \oplus y_1 \oplus (y_1 \oplus y_2) \oplus \ldots \oplus (y_1 \oplus y_2 \ldots \oplus y_{n-2}) \oplus A_2 \oplus A_4 \oplus \ldots \oplus A_{n-2} \oplus A_n) \oplus A_{n+1}$.

We have $\Omega \circ \Phi = \Phi \circ \Omega = I$, i.e., Φ and $\Omega = \Phi^{-1}$ are bijections. □

Additionally orthomorphisms, by themselves can have applications in cryptography ([22]).

4. Quasigroups derived by Feistel orthomorphisms

We use the results from Section 2 in order to construct shapeless quasigroups derived by Feistel orthomorphisms F, where F is a PFN orthomorpism, a *type-1* PEFN orthomorphism or a GF-NLFSR orthomorphism. Given an orthomorphism F over an abelian group G, the quasigroup $(G, \bullet)$ derived by F is defined according to (4), i.e.,

$$x \bullet y = F(x - y) + y,$$

where $x, y \in G^2$. Theorem 2.14 gives sufficient conditions needed for a given quasigroup $(G, \bullet)$ to be shapeless.

For our effective constructions of shapeless quasigroups we used a personal computer with Intel Core 2 Duo Processor, 2, 33GHz clock speed, 2GB RAM, running Windows 7 Enterprise (32-bit) with SP1.

4.1. *PFN orthomorphisms.* Given an abelian group $(G, +)$, a PFN orthomorphism $F_{A,B,C}$ is defined over the group $(G^2, +)$, and the quasigroup $(G^2, \bullet)$ is derived by $F_{A,B,C}$ as $x \bullet y = F_{A,B,C}(x - y) + y$, where $x, y \in G^2$.

It is trivial to check that the condition $i)$ of Theorem 2.14 (i.e., $F_{A,B,C}(0) \neq 0$) is satisfied iff $A \neq 0$ or $B \neq -f(C)$.

PROPOSITION 4.1. *$F_{A,B,C}$ satisfies the condition $iv)$ of Theorem 2.14.*

PROOF. Let $x \neq 0 \in G$. We have

$$F_{A,B,C}(x,x) - F_{A,B,C}(-(x,x)) = F_{A,B,C}(x,x) - F_{A,B,C}(-x,-x)$$
$$= (2x, 2x + f(x+C) - f(-x+C)) \neq (x,x).$$

□

We have made an m-file in MatLab that produces a starting bijection $f : \mathbb{Z}_2^b \to \mathbb{Z}_2^b$ and parameters A, B and C for obtaining an orthomorphism $F_{A,B,C}$ over the group $(\mathbb{Z}_2^{2b}, \oplus)$ that satisfies all conditions of Theorem 2.14. The execution time is less than half a second for $b \in \{3,4,5\}$, less than 5 seconds for $b = 6$, less than two minutes for $b = 7$, about 45 minutes for $b = 8$ and less than 10 hours for $b = 9$. Thus, we could effectively construct shapeless quasigroups of order $2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}$ and 2^{18}. As an example, you can obtain a shapeless quasigroup of order 2^{12} by taking parameters $A = 49$, $B = 54$ and $C = 59$ and a bijection $f = (0\ 9\ 11\ 41\ 20\ 15\ 36\ 16\ 28\ 2\ 53\ 37\ 18\ 8\ 34\ 41\ 46\ 27\ 19\ 24\ 62\ 17\ 39\ 54\ 6\ 57\ 14\ 10\ 23\ 60\ 42\ 55\ 22\ 38\ 52\ 48\ 7\ 47\ 59\ 31\ 56)(1\ 58\ 51\ 63\ 5\ 49\ 61\ 4\ 25)(3\ 30\ 29)(12\ 32\ 26)(13\ 45\ 44\ 35\ 21\ 50\ 33\ 40)$, given by its cycles. Even more, $F_{A,B,C}$ and $F_{A,B,C}^2$ are orthogonal orthomorphisms.

4.2. Type-1 *PEFN orthomorphisms.* Let $(G,+)$ be an abelian group. A *type-1* PEFN orthomorphism $F_{A_1,A_2,\ldots,A_{n+1}}$ is defined over the group $(G^n,+)$, and the quasigroup $(G^n,\bullet)$ is defined by $x \bullet y = F_{A_1,A_2,\ldots,A_{n+1}}(x-y)+y$, where $x, y \in G^n$.

It is trivial to check that the condition i) of Theorem 2.14 is satisfied iff $A_i \neq 0$ for some $i \in \{3,4,\ldots,n+1\}$ or $A_2 \neq -f(A_1)$.

PROPOSITION 4.2. *The orthomorphism $F_{A_1,A_2,\ldots,A_{n+1}}$ satisfies the condition iv) of Theorem 2.14.*

PROOF. Let $x \neq 0 \in G$. We have

$$F_{A_1,\ldots,A_{n+1}}(x,x,\ldots,x) - F_{A_1,\ldots,A_{n+1}}(-(x,x,\ldots,x))$$
$$= F_{A_1,\ldots,A_{n+1}}(x,x,\ldots,x) - F_{A_1,\ldots,A_{n+1}}(-x-,x,\ldots,-x)$$
$$= (2x + f(x+A_1) - f(-x+A_1), 2x, \ldots, 2x) \neq (x,x,\ldots,x).$$

□

We have made an m-file in MatLab that produces a starting bijection $f : \mathbb{Z}_2^b \to \mathbb{Z}_2^b$ and parameters $A_1, A_2, \ldots, A_{n+1}$ for obtaining an orthomorphism $F_{A_1,\ldots,A_{n+1}}$ over the group $(\mathbb{Z}_2^{nb}, \oplus)$, which produces a shapeless quasigroup. When we use $b = 3$, the execution time is about two seconds for $n = 3$, less than 5 seconds for $n = 4$, less than 7 minutes for $n = 5$ and less than 11 hours for $n = 6$. These results correspond to shapeless quasigroups of orders $2^9, 2^{12}, 2^{15}$ and 2^{18}. For $b = 4$, the execution time in the best case is less than 5 seconds for $n = 3$ and less than half an hour for $n = 4$. These results correspond to shapeless quasigroups of orders 2^{12} and 2^{16}. For $b = 5$, the

execution time is about 5 minutes for $n = 3$ and corresponding shapeless quasigroup is of order 2^{15}. For example, a shapeless quasigroup of order 2^{16} is obtained when the bijection f and the parameters A_1, A_2, A_3, A_4, A_5 are taken as follows: $f = (0\ 7\ 9\ 14\ 3)(1\ 6\ 4\ 10\ 8\ 5\ 15\ 12)(2\ 13\ 11)$ and $(A_1, A_2, A_3, A_4, A_5) = (3, 12, 10, 14, 6)$.

4.3. *GF-NLFSR orthomorphisms.* Here we use the abelian group $(\mathbb{Z}_2^b, \oplus)$ and we take that n is an even integer and $A_1, A_2, \ldots, A_{n+1} \in \mathbb{Z}_2^b$. A GF-NLFSR orthomorphism $F_{A_1,A_2,\ldots,A_{n+1}}$ is defined over the group $((\mathbb{Z}_2^b)^n, \oplus)$ and by $x \bullet y = F_{A_1,A_2,\ldots,A_{n+1}}(x - y) + y$ the derived quasigroup $(\mathbb{Z}_2^b, \bullet)$ is obtained, where $x, y \in (\mathbb{Z}_2^b)^n$.

Again, it is trivial to check that the condition $i)$ of Theorem 2.14 is satisfied iff $A_i \neq 0$ for some $i \in \{1, 2, \ldots, n-1\}$ or $A_n \neq -f(A_{n+1})$. By Corollary 2.9 we have that $F_{A_1,A_2,\ldots,A_{n+1}}$ satisfies the condition $iv)$ of Theorem 2.14.

We have made an m-file in MatLab that produces a starting bijection $f : \mathbb{Z}_2^b \to \mathbb{Z}_2^b$ and parameters $A_1, A_2, \ldots, A_{n+1}$ for obtaining an orthomorphism $F_{A_1,\ldots,A_{n+1}}$ over the group $(\mathbb{Z}_2^{nb}, \oplus)$. When we use $b = 3$ and $n = 4$, the execution time for producing a shapeless quasigroup of order 2^{12} is less than 5 seconds. For $b = 4$ and $n = 4$, the execution time for producing a shapeless quasigroup of order 2^{16} is less than two hours. As an example of a shapeless quasigroup of order 2^{16}, produced as in this subsection, one can take the bijection $f = (0\ 2\ 9\ 3\ 13\ 8\ 11\ 7\ 14\ 4\ 15\ 6\ 1\ 10)(5)(12)$ and parameters $(A_1, A_2, A_3, A_4, A_5) = (13, 9, 0, 11, 15)$.

5. Conclusions

The shapeless quasigroups are important because of their applications for building cryptographic primitives. We are using Feistel orthomorphisms in order to effectively construct shapeless quasigroups of order up to 2^{18}. The constructions are based on the sufficient conditions we have examined. For practical implementations, quasigroups of order 2^{16} would be more useful. It is an open problem whether more efficient algorithms for obtaining shapeless quasigroups of higher order, like 2^{32} or even 2^{64}, can be defined. If so, more efficient cryptographic primitives based on shapeless quasigroups could also be designed.

References

[1] J. Choy, G. Chew, K. Khoo, and H. Yap, *Cryptographic properties and application of a generalized unbalanced Feistel network structure*, in: ACISP 2009 (ed. C. Boyd, J. González Nieto), LNCS **5594** (2009), Springer Berlin Heidelberg, 73–89.

[2] T. P. Cowhig, Constructing monogenic quasigroups with specified properties, PhD thesis, University of London, 2009.

[3] J. Dénes and A. D. Keedwell, Latin squares. New developments in the theory and applications, North-Holland Publishing Co., Amsterdam, 1991.

[4] A. Drápal and T. Kepka, *Parity of orthogonal automorphisms*, Comment. Math. Univ. Carolin. **28** (1987), 251–259.
[5] A. B. Evans, *Orthomorphism Graphs of Groups*, J. of Geom. **35** (1989), 66–74.
[6] H. Feistel, *Cryptography and computer privacy*, Sci. Amer. **228** (1973), 15–23.
[7] D. Gligoroski, S. Markovski and L. Kocarev, *Edon-$\mathcal{R}$, an infinite family of cryptographic hash functions*, The Second NIST Cryptographic Hash Workshop, UCSB, Santa Barbara, CA, 2006. `http://www.csrc.nist.gov/pki/HashWorkshop/2006/Papers/GLIGOROSKI\_EdonR-ver06.pdf`. Accessed 16 June 2009.
[8] D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugère, S. J. Knapskog and S. Markovski, The digital signature scheme MQQ-SIG, Report 527, Cryptology ePrint Archive, 2010.
[9] D. Gligoroski, S. Markovski and S.J. Knapskog, *The stream cipher edon80*, in: New stream cipher designs: The eSTREAM finalists, Springer-Verlag, 2008, 152–169.
[10] D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, L. Kocarev, and A. Drápal, *Cryptographic hash function EDON-R. Submission to NIST as first round candidate*, `http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions\_rnd1.html`, 2008. Accessed 16 June 2009.
[11] D. F. Hsu, and A. D. Keedwell, *Generalized complete mappings, neofields, sequenceable groups and block designs II*, Pac. J. Math. **117** (1985), 291–312.
[12] V. I. Izbash, *Monoquasigroups without congruences and automorphisms*, Bul. Acad. Stiinte Repub. Mold. Mat. **(4)** (1992), 66–76.
[13] D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn, *Orthomorphisms of groups and orthogonal latin squares, I*, Can. J. Math. **13** (1961), 356–372.
[14] A. D. Keedwell, *Crossed inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. **20** (1999), 241–250.
[15] T. Kepka, *A note on simple quasigroups*, Acta Univ. Carolin.—Math. Phys. **19** (1978), 59–60.
[16] H. B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Statistics **13** (1942), 418–423.
[17] S. Markovski and A. Mileva, *Generating huge quasigroups from small non-linear bijections via extended Feistel function*, Quasigroups Related Systems **17** (2009), 91–106.
[18] S. Markovski and A. Mileva, *NaSHA*, Submission to NIST as first round candidate, `http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions\_rnd1.html`, 2008. Accessed 16 June 2009.
[19] S. Markovski, S. Samardziska, D. Gligoroski and S. J. Knapskog, *Multivariate trapdoor functions based on multivariate left quasigroups and left polynomial quasigroups*, in: Proc. of The 2^{nd} international conference on symbolic computation and cryptography (ed. C. Cid and J.-C. Faugère), 2010, Royal Halloway, Egham, UK, 237–251.
[20] K. A. Meyer, *A new message authentication code based on the non-associativity of quasigroups*, PhD thesis, Iowa State University, 2006.
[21] A. Mileva, *Cryptographic primitives with quasigroup string transformations*, PhD thesis, University "Ss Cyril and Methodious" - Skopje, 2010.
[22] L. Mittenthal, *Block substitutions using orthomorphic mappings*, Adv. in Appl. Math. **16** (1995), 59–71.
[23] A. Sade, *Groupoïdes automorphes par le groupe cyclique*, Can. J. Math. **9** (1957), 321–335.
[24] D. G. Sarvate and J. Seberry, *Encryption methods based on combinatorial designs*, Ars Combinatoria **21A** (1986), 237–246.

[25] V. A. Shcherbacov, *On linear quasigroups and their automorphism groups*, Mat. Issled. **120** (1991), 104–113 (in Russian).
[26] I. M. Wanless, *Diagonally cyclic latin squares*, European J. Combin. **25** (2004), 393–413.
[27] Y. Zheng, T. Matsumoto and H. Imai, *On the construction of block provably secure and not relying on any unproved hypotheses*, in: Advances in Cryptology - CRYPTO '89 (ed. G. Brassard) , LNCS **435** (1990), Springer Berlin Heidelberg, 461–480.

A. Mileva
Faculty of Computer Science
University "Goce Delčev"
2000 Štip
Republic of Macedonia
E-mail: aleksandra.mileva@ugd.edu.mk

S. Markovski
Faculty of Computer Science and Engineering
University "Ss Cyril and Methodius"
1000 Skopje
Republic of Macedonia
E-mail: smile.markovski@finki.ukim.mk

Received: 18.11.2011.
Revised: 26.1.2012. & 23.5.2012.