Generating huge quasigroups from small non-linear bijections via extended Feistel function

Smile Markovski and *Aleksandra Mileva*

Abstract. Quasigroups of huge order, like 2^{256}, 2^{512}, 2^{1024}, that can be effectively constructed, have important applications in designing several cryptographic primitives. We propose an effective method for construction of such huge quasigroups of order $r = 2^{s2^t}$ for small fixed values of s and arbitrary values of t; the complexity of computation of the quasigroup multiplication is $\mathcal{O}(\texttt{log}(\texttt{log}(r))) = \mathcal{O}(t)$. Besides the computational effectiveness, these quasigroups can be constructed in such a way to have other desirable cryptographic properties: do not satisfy the commutative law, the associative law, the idempotent law, to have no proper subquasigroups, to be non-linear, etc. These quasigroups are constructed by complete mappings generated by suitable bijections of order 2^s via extended Feistel network functions.

1. Introduction

The cryptographic community started dealing with quasigroups (or Latin squares, as their combinatorial counterpart) for producing different kinds of cryptographic primitives two decades ago. Authentication schemas have been proposed by J. Dènes and A.D. Keedwell (1992) [4], secret sharing schemes by J. Cooper et al. (1994) [3], a version of popular DES block cipher by using Latin squares by G. Carter et al. (1995) [2], different proposals for use in the design of cryptographic hash functions by several authors [10, 12, 20, 26], Latin squares in cipher systems (2003) [14], PRNG based on quasigroup string transformations by S. Markovski and al. (2005) [19], a hardware stream cipher by D. Gligoroski et al. (2005) [9], a public key cipher by D. Gligoroski, S. Markovski and S.J. Knapskog (2008) [11], and many others.

A *quasigroup* is a groupoid $(Q, *)$ that satisfies the property each one of the equations $a * x = b$ and $y * a = b$ to have a unique solution x, respectively

2000 Mathematics Subject Classification: Primary 20N05, Secondary 94A60
Keywords: huge quasigroup, complete mapping, Feistel network function.

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. In cryptographic applications the quasigroups are usually used in two different ways. If they are of relatively small order ($|Q| = 4, 8, 16, 32$), then the designers iteratively apply them many times (e.g., 80 times in EDON80 [9]). On the other side, for obtaining fast and secure cryptographic systems with a few iterations, finite quasigroups of huge order (called huge quasigroups) are needed. Here, by huge order we mean $|Q| = 2^n,\ n = 16, 32, 64, 128, \dots$.

Huge quasigroups can not be represented by Cayley tables and one should define them by using suitable functions. The cryptographic qualities of the huge quasigroups depend on the functions that are used for their definitions. By a quasigroup of a good cryptographic quality we mean a finite quasigroup that is non-commutative, non-associative, non-idempotent, without right or left units and without a proper subquasigroup. The algebraic degree of the quasigroup should be as high as possible, at least 2. Also, they should not satisfy identities of the kinds $\underbrace{x * (\dots * (x}_{l} * y)) = y$ and $y = ((y * \underbrace{x) * \dots) * x}_{l}$ for some $l < 2n$, where n is the order of the quasigroup.

Here we use modified Feistel networks [8], that we call extended Feistel networks, to define huge quasigroups. A Feistel network takes any function and transforms it into a bijection, so it is commonly used technique for creating a non-linear cryptographic function [6], [16]. Using a Feistel network for creating a huge quasigroup is not a novel approach. Kristen [21] presents several different constructions using one or two Feistel networks and isotopies of quasigroups. Complete mappings, introduced by Mann [17] (the equivalent concept of orthomorphism was introduced explicitly in [5]), are also useful for creation of huge quasigroups. In [21] complete mappings with non-affine functions represented by Cayley tables or with affine functions represented by binary transformations are used for that aim. The main disadvantages of the previously mentioned constructions is the lack of efficiency in one case and the lack of security in other case. Namely, the Cayley table representations need a lot of memory, and the affine functions have no good cryptographic properties.

In this paper we conjunct these two approaches. In fact, we use extended Feistel networks as complete mappings to generate huge quasigroups of order $r = 2^{s2^t}$. We only need to store small permutations of order $2^s,\ s = 4, 8, 16$. We show that the quasigroups obtained by our construction satisfy the security properties mentioned above (i.e., they are not: commutative, associative, idempotent, etc.).

The paper is organized as follows. Quasigroups obtained by complete mappings are considered in Section 2, where it is shown that such a quasigroup has a property that each of its parastrophes is defined by a complete mapping too. The extended Feistel networks are defined in Section 3, and in Section 4 their algebraic degree is counted. Huge quasigroups defined by extended Feistel networks are given in Section 5, where their cryptographic properties are considered too. Conclusion remarks are in Section 6.

2. Complete mappings

Our construction of huge quasigroups is based on quasigroups derived from groups by using complete mappings. Here we give the needed definitions and some properties.

Definition 2.1. A *complete mapping* of a group $(G,+)$ is a bijection $\theta : G \to G$ such that the mapping $\varphi : G \to G$ defined by $\varphi(x) = -x + \theta(x)$ ($\varphi = -I + \theta$, where I is the identity mapping) is again a bijection of G. The mapping φ is said to be the *orthomorphism* associated to the complete mapping θ. A group G is *admissible* if there is a complete mapping $\theta : G \to G$.

Question about whether or not a group G is admissible is a subject that has been extensively studied [13, 22, 23]. It is well-known fact that inverse of the complete mapping is also a complete mapping of Abelian group $(G,+)$ [7].

Sade proposed the following method for creating a quasigroup from an admissible group [25]:

Proposition 2.1. *Let $(Q,+)$ be an admissible group with complete mapping θ. Define an operation $\bullet$ on Q by:*

$$x \bullet y = \theta(x - y) + y \tag{1}$$

where $x, y \in Q$. Then $(Q,\bullet)$ is a quasigroup. (*Then we say that $(Q,\bullet)$ is derived by θ.*) □

In the sequel, we will consider only complete mappings of the Abelian groups $(\mathbb{Z}_2^n, \oplus_n)$, where $\oplus_n$ denotes the operation bitwise XOR of words of length n bits. The results of Paige [22] implies that the groups $(\mathbb{Z}_2^n, \oplus_n)$ are admissible. Then the equation (1) get the form:

$$x \bullet y = \theta(x \oplus_n y) \oplus_n y. \tag{2}$$

Proposition 2.2. *If θ is a complete mapping of $(\mathbb{Z}_2^n, \oplus_n)$, then its orthomorphism $\varphi = I \oplus_n \theta$ is a complete mapping of $(\mathbb{Z}_2^n, \oplus_n)$ too, with orthomorphism $\theta = I \oplus_n \varphi$.* □

Example 2.1. Let $Q = \mathbb{Z}_2^2 = \{0,1,2,3\}$, where we use the integer notation $0 \equiv \langle 0,0\rangle, 1 \equiv \langle 0,1\rangle, 2 \equiv \langle 1,0\rangle, 3 \equiv \langle 1,1\rangle$. Define $\theta : Q \to Q$ by $\theta(\langle x_0, x_1\rangle) = \langle x_0 \oplus x_1, x_0 \oplus 1\rangle$, where x_1, x_0 are bits. Table 1 demonstrates that both θ and $I + \theta$ are bijections, and the quasigroup $(Q, \bullet)$ is defined by (2).

x	$\theta(x)$	$\varphi(x) = x \oplus_2 \theta(x)$
$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 0,1\rangle$
$\langle 0,1\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$
$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 0,0\rangle$
$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$

$\bullet$	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

Table 1: The complete mapping θ of the group $\mathbb{Z}_2^2$ and the derived quasigroup.

Given a quasigroup (Q, f), five new operations $f^{-1}, {}^{-1}f, {}^{-1}(f^{-1}), ({}^{-1}f)^{-1}$ and f^* on the set Q can be derived by as follows.

$$\begin{array}{rclcl}
{}^{-1}f(x,y) = z & \longleftrightarrow & f(z,y) = x, & & \\
f^{-1}(x,y) = z & \longleftrightarrow & f(x,z) = y, & & \\
{}^{-1}(f^{-1})(x,y) = z & \longleftrightarrow & f^{-1}(z,y) = x & \longleftrightarrow & f(z,x) = y, \\
({}^{-1}f)^{-1}(x,y) = z & \longleftrightarrow & ({}^{-1}f)(x,z) = y & \longleftrightarrow & f(y,z) = x, \\
f^*(x,y) = z & \longleftrightarrow & ({}^{-1}f)^{-1}(x,y) = yz & \longleftrightarrow & f(y,x) = z.
\end{array}$$

The set $Par(f) = \{f, f^{-1}, {}^{-1}f, {}^{-1}(f^{-1}), ({}^{-1}f)^{-1}, f^*\}$ is said to be the set of parastrophes of f. $|Par(f)| \leqslant 6$, i.e., some of parastrophes may coincides between themselves. For each $g \in Par(f)$, (Q, g) is a quasigroup too and $Par(f) = Par(g)$ (see [1], [4]). The parastrophes of a quasigroup determine some identities that can be used for cryptographic encoding and decoding functions to be defined. For example, by using the identities $f^{-1}(x, f(x,z)) = z$ and $f(x, f^{-1}(x,y)) = y$, f and f^{-1} can be taken as encoding and decoding functions.

The next theorem shows that if a quasigroup $(\mathbb{Z}_2^n, f)$ is derived by a complete mapping, then all of its parastrophes can be derived by complete mappings too. This fact can be especially useful for encoding and decoding purposes.

Theorem 2.1. *Let $\theta : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a complete mapping of the group $(\mathbb{Z}_2^n, \oplus_n)$ and let $(\mathbb{Z}_2^n, f)$ be the quasigroup derived by $f(x,y) = \theta(x \oplus_n y) \oplus_n y$. Then the following statements are true.*

a) $(Q, {}^{-1}f)$ *is derived by the complete mapping* $\delta = \theta^{-1}$.

b) (Q, f^{-1}) *is derived by the complete mapping* $\lambda = (I \oplus_n \theta^{-1})^{-1}$.

c) $(Q, ({}^{-1}(f^{-1})))$ *is derived by the complete mapping* $\rho = I \oplus_n \theta^{-1}$.

d) $(Q, ({}^{-1}f)^{-1})$ *is derived by the complete mapping* $\tau = (I \oplus_n \theta)^{-1}$.

e) (Q, f^*) *is derived by the complete mapping* $\varphi = I \oplus_n \theta$.

Proof. *a)* ${}^{-1}f(x,y) = z \longleftrightarrow f(z,y) = x \longleftrightarrow \theta(z \oplus_n y) \oplus_n y = x \longleftrightarrow$ $z \oplus_n y = \theta^{-1}(x \oplus_n y) \longleftrightarrow z = \theta^{-1}(x \oplus_n y) \oplus_n y,$ and that implies ${}^{-1}f(x,y) = \delta(x \oplus_n y) \oplus_n y$.

b) $f^{-1}(x,y) = z \longleftrightarrow f(x,z) = y \longleftrightarrow \theta(x \oplus_n z) \oplus_n z = y$ $\longleftrightarrow x \oplus_n z = \theta^{-1}(y \oplus_n z) \longleftrightarrow x = \theta^{-1}(y \oplus_n z) \oplus_n z \oplus_n y \oplus_n y$ $\longleftrightarrow x \oplus_n y = \theta^{-1}(y \oplus_n z) \oplus_n y \oplus_n z \longleftrightarrow x \oplus_n y = (I \oplus \theta^{-1})(y \oplus_n z)$ $\longleftrightarrow (I \oplus_n \theta^{-1})^{-1}(x \oplus_n y) = y \oplus_n z \longleftrightarrow (I \oplus_n \theta^{-1})^{-1}(x \oplus_n y) \oplus_n y = z,$ and that implies $f^{-1}(x,y) = \lambda(x \oplus_n y) \oplus_n y$.

c) $({}^{-1}(f^{-1}))(x,y) = z \longleftrightarrow f^{-1}(z,y) = x \longleftrightarrow f(z,x) = y$ $\longleftrightarrow \theta(z \oplus_n x) \oplus_n x = y \longleftrightarrow z \oplus_n x = \theta^{-1}(x \oplus_n y)$ $\longleftrightarrow z = \theta^{-1}(x \oplus_n y) \oplus_n x \oplus_n y \oplus_n y \longleftrightarrow z = (I \oplus_n \theta^{-1})(x \oplus_n y) \oplus_n y,$ and that implies $({}^{-1}(f^{-1}))(x,y) = \rho(x \oplus_n y) \oplus_n y$.

d) $({}^{-1}f)^{-1}(x,y) = z \longleftrightarrow^{-1} f(x,z) = y \longleftrightarrow f(y,z) = x$ $\longleftrightarrow \theta(y \oplus_n z) \oplus_n z = x \longleftrightarrow z \oplus_n y \oplus_n \theta(z \oplus_n y) = x \oplus_n y$ $\longleftrightarrow (I \oplus_n \theta)(z \oplus_n y) = x \oplus_n y \longleftrightarrow z \oplus_n y = (I \oplus_n \theta)^{-1}(x \oplus_n y) \longleftrightarrow$ $z = (I \oplus_n \theta)^{-1}(x \oplus_n y) \oplus_n y$, and that implies $({}^{-1}f)^{-1}(x,y) = \tau(x \oplus_n y) \oplus_n y$.

e) $f^*(x,y) = z \longleftrightarrow f(y,x) = z \longleftrightarrow \theta(y \oplus_n x) \oplus_n x = z \longleftrightarrow$ $\theta(x \oplus_n y) \oplus_n x \oplus_n y \oplus_n y = z \longleftrightarrow (I \oplus_n \theta)(x \oplus_n y) \oplus_n y = z$, and that implies $f^*(x,y) = \varphi(x \oplus_n y) \oplus_n y$. □

3. Extended Feistel networks

Generally, a group with affine complete mapping do not produces a quasigroup that satisfies the cryptography needs. Non-affine complete mappings are more promising. It is very easy to create a table-driven non-affine complete mapping as long as we don't care about the order of the quasigroup. Considering huge quasigroups, practically it is not possible to store table-driven bijections. It is much more difficult to create a non-affine bijection that is not table-driven and, additionally, that is a complete mapping. By using extended Feistel network, we create a huge non-affine complete mapping from a small table-driven non-affine bijection.

Definition 3.1. Let $(G,+)$ be an Abelian group, let $f : G \to G$ be a mapping and let $a,b,c \in G$ be constants. The *extended Feistel network* (shortly ExtFN), $F_{a,b,c} : G^2 \to G^2$ created by f is defined for every $l, r \in G$ by

$$F_{a,b,c}(l,r) = (r + a, l + b + f(r + c)).$$

The extended Feistel network $F_{a,b,c}$ is a bijection with inverse

$$F^{-1}_{a,b,c}(l,r) = (r - b - f(l + c - a), l - a).$$

A Feistel network can be obtained from an ExtFN if we take constants $a = b = c = 0$.

One of the main results of the paper, that we will use frequently, is the following.

Theorem 3.1. *Let $(G,+)$ be an arbitrary Abelian group and $a,b,c \in G$. If $F_{a,b,c} : G^2 \to G^2$ is an extended Feistel network created by a bijection $f : G \to G$, then $F_{a,b,c}$ is a complete mapping of the group $(G^2,+)$.*

Proof. Let $\varphi = -I + F_{a,b,c}$, i.e.,

$$\varphi(l,r) = -(l,r) + F(l,r) = (-l + r + a, -r + l + b + f(r + c))$$

for every $l, r \in G$. Define the function $\Omega : G^2 \to G^2$ by

$$\Omega(l,r) = (f^{-1}(l + r - a - b) - l + a - c, f^{-1}(l + r - a - b) - c).$$

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

In the sequel we will consider only ExtFN of the Abelian groups $(\mathbb{Z}_2^n, \oplus_n)$.

Definition 3.2. Let $(G,+)$ be a group and let $f : G \to G$ be a mapping. f is an *affine mapping* if $f(x + y) = f(x) + f(y) - f(0)$ for each $x, y \in G$, where $0 \in G$ is the identity element. A *linear mapping* is an affine mapping f with $f(0) = 0$.

Proposition 3.1. *Let $a,b,c \in \mathbb{Z}_2^k$ and let $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network created by a mapping $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$. Then $F_{a,b,c}$ is affine iff f is affine.*

Proof. Let $l_1, l_2, r_1, r_2 \in \mathbb{Z}_2^k$ and let f be affine. Then, since $f(r_1 \oplus_k r_2 \oplus_k c) = f(r_1 \oplus_k c) \oplus_k f(r_2 \oplus_k c) \oplus_k f(c)$, we have that $F_{a,b,c}$ is affine as well:

$$\begin{aligned}
&F_{a,b,c}((l_1, r_1) \oplus_{2k} (l_2, r_2))\\
&= ((r_1 \oplus_k r_2 \oplus_k a), (l_1 \oplus_k l_2 \oplus_k b \oplus_k f(r_1 \oplus_k r_2 \oplus_k c)))\\
&= [(r_1 \oplus_k a), (l_1 \oplus_k b \oplus_k f(r_1 \oplus_k c))] \oplus_{2k} [(r_2 \oplus_k a), (l_2 \oplus_k b \oplus_k f(r_2 \oplus_k c))] \oplus_{2k}\\
&\qquad [(0 \oplus_k a), (0 \oplus_k b \oplus_k f(0 \oplus_k c))]\\
&= F_{a,b,c}(l_1, r_1) \oplus_{2k} F_{a,b,c}(l_2, r_2) \oplus_{2k} F_{a,b,c}(0, 0),
\end{aligned}$$

Let now $F_{a,b,c}$ be an affine function. Then we have

$$F_{a,b,c}((l_1, r_1) \oplus_{2k} (l_2, r_2)) = F_{a,b,c}(l_1, r_1) \oplus_{2k} F_{a,b,c}(l_2, r_2) \oplus_{2k} F_{a,b,c}(0, 0)$$

and that implies

$$f(r_1 \oplus_k r_2 \oplus_k c) = f(r_1) \oplus_k f(r_2) \oplus_k f(c)$$

for each $r_1, r_2 \in \mathbb{Z}_2^k$. We infer from the last equality that f is affine too:
$f(r_1 \oplus_k r_2) = f(r_1 \oplus_k (r_2 \oplus_k c) \oplus_k c) = f(r_1) \oplus_k f(r_2 \oplus_k c) \oplus_k f(c) = f(r_1) \oplus_k f(0 \oplus_k r_2 \oplus_k c) \oplus_k f(c) = f(r_1) \oplus_k f(0) \oplus_k f(r_2) \oplus_k f(c) \oplus_k f(c) = f(r_1) \oplus_k f(r_2) \oplus_k f(0)$. □

So, if a non-affine ExtFN $F_{a,b,c}$ created by f is needed as a complete mapping, it is enough to take f to be a non-affine bijection.

Proposition 3.2. *Let $f, g : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be bijections, $a, b, c, a', b', c' \in \mathbb{Z}_2^k$ and let $F_{a,b,c}, F_{a',b',c'} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be extended Feistel networks created by f and g respectively. Then the composite function $F_{a,b,c} \circ F_{a',b',c'}$ is a complete mapping on $\mathbb{Z}_2^{2k}$ too.*

Proof. Let $\varphi = I \oplus_{2k} F_{a,b,c} \circ F_{a',b',c'}$. Then, for every $l, r \in \mathbb{Z}_2^k$, we have

$$\varphi(l, r) = ((g(r \oplus_k c') \oplus_k a \oplus_k b'), (a' \oplus_k b \oplus_k f(l \oplus_k b' \oplus_k g(r \oplus_k c') \oplus_k c))).$$

Define the function $\Omega : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ by

$$\Omega(l, r) = ((f^{-1}(r \oplus_k a' \oplus_k b) \oplus_k l \oplus_k a \oplus_k c), (g^{-1}(l \oplus_k a \oplus_k b') \oplus_k c')).$$

It can be checked that $\Omega \circ \varphi = \varphi \circ \Omega = I$, i.e., φ and $\Omega = \varphi^{-1}$ are bijections. □

Corollary 3.1. *If $F_{a,b,c}$ is an extended Feistel network created by bijection f, then $F_{a,b,c}^2$ is a complete mapping of $(\mathbb{Z}_2^{2k}, \oplus_{2k})$ too.* □

In general, if θ is a complete mapping on a group G, θ^2 may not be a complete mapping on G, as Example 3.1 shows.

Example 3.1. We have in Table 2 a complete mapping $\theta(x)$ on $(\mathbb{Z}_2^4, \oplus_4)$ (given in integer representation) such that $\theta^2(x)$ is not a complete mapping, as it is shown in Table 3.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\theta(x)$	12	6	3	14	2	13	5	9	8	11	15	1	7	4	10	0
$x \oplus_4 \theta(x)$	12	7	1	13	6	8	3	14	0	2	5	10	11	9	4	15

Table 2: Integer representation of a complete mapping $\theta(x)$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\theta^2(x)$	7	5	14	10	3	4	13	11	8	1	0	6	9	2	15	12
$x \oplus_4 \theta^2(x)$	7	4	12	9	7	1	11	12	0	8	10	13	5	15	1	3

Table 3: Integer representation of a non-complete mapping $\theta^2(x)$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	3	2	1	0												
$F(x)$	3	6	9	12	2	7	8	13	1	4	11	14	0	5	10	15
$x \oplus_4 F(x)$	3	7	11	15	6	2	14	10	9	13	1	5	12	8	4	0

Table 4: Integer representation of an extended Feistel network $F(x)$.

Example 3.2. In Table 4 we have an example of an ExtFN $F = F_{0,0,0}$ that is a complete mapping created by a bijection f such that F^3 is not a complete mapping. Namely, F^3 is the identical mapping, so $I \oplus_4 F^3 = I \oplus_4 I$ is the constant zero mapping, that maps each $x \in \mathbb{Z}_2^4$ into 0.

4. The algebraic degree of an ExtFN

A vector valued Boolean function (v.v.b.f.) is a mapping $B : {\mathbb{Z}_2}^s \to {\mathbb{Z}_2}^t$, where s and $t \geqslant 1$ are positive integers; we have a Boolean function for $t = 1$. Each v.v.b.f. B can be represented by t Boolean functions $b_i : {\mathbb{Z}_2}^s \to \mathbb{Z}_2$ as follows:

$$B(x_1, \dots, x_s) = (b_1(x_1, \dots, x_s), b_2(x_1, \dots x_s), \dots, b_t(x_1, \dots, x_s)),$$

where

$$b_1(x_1, \dots, x_s) = y_1, \dots, b_t(x_1, \dots, x_s) = y_t \quad \longleftrightarrow \quad B(x_1, \dots, x_s) = (y_1, \dots, y_t).$$

Each Boolean function b_i can be represented in Algebraic Normal Form as

$$b_i(x_1, x_2, \ldots, x_s) = \sum_{I \subseteq \{1,2,\ldots,s\}} \alpha_I (\prod_{i \in I} x_i) \tag{3}$$

where $\alpha_I \in \mathbb{Z}_2$, the sum is for the Boolean function XOR and the product is for the Boolean function conjunction. The right-hand side of (3) can be interpreted as a polynomial in the field $(\mathbb{Z}_2, +, \cdot)$ and the degree of b_i is taken to be the degree of the polynomial. The algebraic degree of a v.v.b.f. B is defined as the maximum of the degrees of its component polynomials $(b_1, b_2, \ldots, b_s)$:

$$deg(B) = \max\{deg(b_i) \mid i \in \{1, 2, \ldots, s\}\}.$$

Theorem 4.1. *Let the bijection $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be of algebraic degree $deg(f) \geqslant 1$ and let $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network created by f. Then $deg(F_{a,b,c}) = deg(f)$.*

Proof. Let $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_k)$ and $(c_1, \ldots, c_k)$ be the binary representations of the constants $a, b, c \in \mathbb{Z}_2^k$. The mappings $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ and $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ are v.v.b.f. and so there are Boolean polynomials $q_1, q_2, \ldots, q_k$ and $p_1, p_2, \ldots, p_{2k}$ such that

$$f(x_1, \ldots, x_k) = (q_1(x_1, \ldots, x_k), q_2(x_1, \ldots, x_k), \ldots, q_k(x_1, \ldots, x_k)),$$

$$F_{a,b,c}(x_1, \ldots, x_{2k}) = (p_1(x_1, \ldots, x_{2k}), p_2(x_1, \ldots, x_{2k}), \ldots, p_{2k}(x_1, \ldots, x_{2k})).$$

Let $deg(f) = \max\{deg(q_i) \mid i \in \{1, 2, \ldots, k\}\} \geqslant 1$. Then there is a $t \in \{1, 2, \ldots, k\}$ such that $deg(f) = deg(q_t)$.

We have $F_{a,b,c}(x_1, \ldots, x_{2k}) = (x_{k+1} \oplus a_1, \ldots, x_{2k} \oplus a_k, x_1 \oplus b_1 \oplus q_1(x_{k+1} \oplus c_1, \ldots, x_{2k} \oplus c_k), \ldots, x_k \oplus b_k \oplus q_k(x_{k+1} \oplus c_1, \ldots, x_{2k} \oplus c_k))$. This implies that $p_i(x_1, \ldots, x_{2k}) = x_{i+k} \oplus a_i$ and $p_{i+k}(x_1, \ldots, x_{2k}) = x_i \oplus b_i \oplus q_i(x_{k+1} \oplus c_1, \ldots, x_{2k} \oplus c_k)$ for each $i \in \{1, 2, \ldots, k\}$. Then, for each $i \in \{1, 2, \ldots, k\}$, $deg(p_i) = 1$ and

$$deg(p_{i+k}) = \begin{cases} 0, & \forall\, i\ (q_i(x_{k+1} \oplus c_1, \ldots, x_{2k} \oplus c_k) = x_i \oplus b_i) \\ deg(q_i), & \text{otherwise.} \end{cases} \tag{4}$$

So, $deg(F_{a,b,c}) = deg(f)$. □

Example 4.1. A bijection $f : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$ of $deg(f) = 3$ is given in Table 5. The representation of f as v.v.b.f. is $f(x_1, x_2, x_3, x_4) = (q_1, q_2, q_3, q_4)$, where

$q_1(x_1,x_2,x_3,x_4) = x_1 + x_3 + x_4 + x_1x_3 + x_1x_4 + x_2x_3 + x_1x_2x_4 + x_2x_3x_4,$
$q_2(x_1,x_2,x_3,x_4) = x_2 + x_3 + x_4 + x_1x_4 + x_3x_4 + x_1x_2x_3,$
$q_3(x_1,x_2,x_3,x_4) = x_1 + x_3 + x_1x_4 + x_1x_2x_3,$
$q_4(x_1,x_2,x_3,x_4) = 1+x_1+x_2+x_4+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_1x_2x_3+x_1x_2x_4.$

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

Table 5: A bijection f of $deg(f) = 3$.

The Theorem 4.1 implies that we can make non-affine complete mapping $F_{a,b,c}$ of different non-linearity. Namely, it is enough to choose a non-affine bijection f of desired degree. An effective construction of a bijection f of predefined higher degree is an open problem. Note that the maximum degree of a mapping $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ is less or equal than k.

The complete mapping $F_{a,b,c}$ has the property that the first k polynomials are of degree 1. On the other side, the complete mapping $F^2_{a,b,c}$ is with better performances, since $F^2_{a,b,c}(x_1,\dots,x_{2k}) = (A,B)$, where

$A = (x_1 \oplus b_1 \oplus q_1(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k),\dots,x_k \oplus b_k \oplus q_k(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k)),$

$B = (x_{k+1} \oplus a_1 \oplus q_1(x_1 \oplus b_1 \oplus q_1(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k),\dots,x_k \oplus b_k \oplus q_k(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k)),\dots,x_{2k} \oplus a_k \oplus q_k(x_1 \oplus b_1 \oplus q_1(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k),\dots,x_k \oplus b_k \oplus q_k(x_{k+1} \oplus c_1,\dots,x_{2k} \oplus c_k)).$

5. Huge quasigroups obtained by a chain of ExtFN

Recall that an ExtFN $F_{a,b,c}$ $(a,b,c \in {\mathbb{Z}_2}^s)$ created by a bijection $f : {\mathbb{Z}_2}^s \to {\mathbb{Z}_2}^s$ is a complete mapping, so $F_{a,b,c}$ is a bijection on ${\mathbb{Z}_2}^{2s}$ as well. Define $F^{(1)}_{a^{(1)},b^{(1)},c^{(1)}} = F_{a,b,c}$ and let ${F^{(n)}}_{a^{(n)},b^{(n)},c^{(n)}}$, $n \geqslant 1$, be defined. Then, for some $a^{(n+1)}, b^{(n+1)}, c^{(n+1)} \in {\mathbb{Z}_2}^{s2^{n+1}}$, define $F^{(n+1)}_{a^{(n+1)},b^{(n+1)},c^{(n+1)}}$ to be the ExtFN created by the bijection $F^{(n)}_{a^{(n)},b^{(n)},c^{(n)}}$. Note that $F^{(n)}_{a^{(n)},b^{(n)},c^{(n)}}$ is a complete mapping of the group ${\mathbb{Z}_2}^{s2^n}$ for each $n \geqslant 1$, hence we have defined inductively a chain of complete mappings $\{F^{(n)}_{a^{(n)},b^{(n)},c^{(n)}} \mid n = 1,2,3,\dots\}$ in the corresponding groups. Now, by using (1), one can define a quasigroup of order 2^{s2^n} on the set ${\mathbb{Z}_2}^{s2^n}$ for each $n \geqslant 1$.

In applications one needs effectively constructed quasigroups of order 2^{256}, 2^{512}, 2^{1024}, ... A huge quasigroup of order 2^{2^k} can now be designed as follows.

Take a suitable non-affine bijection of desired algebraic degree $f : {\mathbb{Z}_2}^{2^t} \to {\mathbb{Z}_2}^{2^t}$, where $t < k$ is a small positive integer ($t = 2, 3, 4$). Choose suitable constants $a^{(i)}, b^{(i)}, c^{(i)} \in {\mathbb{Z}_2}^{2^{t+i}}$, $1 \leqslant i \leqslant k-t$, and construct iteratively the complete mapping $F = F^{(k-t)}_{a^{(k-t)},b^{(k-t)},c^{(k-t)}} : {\mathbb{Z}_2}^{2^k} \to {\mathbb{Z}_2}^{2^k}$. Define a quasigroup operation $\bullet$ on the set ${\mathbb{Z}_2}^{2^k}$ by (1), i.e., $x \bullet y = F(x \oplus y) \oplus y$, for every $x, y \in {\mathbb{Z}_2}^{2^k}$.

Note that we need only $k - t$ iterations for getting F and a small amount of memory for storing the bijection f. Hence, the complexity of our algorithm for construction of quasigroups of order $n = 2^{2^k}$ is $\mathcal{O}(\texttt{log}(\texttt{log}\ n))$.

Example 5.1. As starting bijection we can use the bijection $f : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$ from Example 4.1. So, $t = 2$. We choose constants $(a^{(i)}, b^{(i)}, c^{(i)}) = (i, 0, 0) \in {\mathbb{Z}_2}^{2^{t+i}}$, $i = 1, 2, \ldots, 7$. Now we can construct the following complete mappings, where $l_i, r_i \in \mathbb{Z}_2^i$, $i = 4, 8, 16, \ldots$:

$$F^{(1)}_{1,0,0} : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8 \text{ as } F^{(1)}_{1,0,0}(l_4, r_4) = ((r_4 \oplus_4 1), (l_4 \oplus_4 f(r_4))),$$
$$F^{(2)}_{2,0,0} : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16} \text{ as } F^{(2)}_{2,0,0}(l_8, r_8) = ((r_8 \oplus_8 2), (l_8 \oplus_8 F^{(1)}_{1,0,0}(r_8))),$$
$$F^{(3)}_{3,0,0} : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32} \text{ as } F^{(3)}_{3,0,0}(l_{16}, r_{16}) = ((r_{16} \oplus_{16} 3), (l_{16} \oplus_{16} F^{(2)}_{2,0,0}(r_{16}))),$$
$$F^{(4)}_{4,0,0} : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64} \text{ as } F^{(4)}_{4,0,0}(l_{32}, r_{32}) = ((r_{32} \oplus_{32} 4), (l_{32} \oplus_{32} F^{(3)}_{3,0,0}(r_{32}))),$$
$$F^{(5)}_{5,0,0} : \mathbb{Z}_2^{128} \to \mathbb{Z}_2^{128} \text{ as } F^{(5)}_{5,0,0}(l_{64}, r_{64}) = ((r_{64} \oplus_{64} 5), (l_{64} \oplus_{64} F^{(4)}_{4,0,0}(r_{64}))),$$
$$F^{(6)}_{6,0,0} : \mathbb{Z}_2^{256} \to \mathbb{Z}_2^{256} \text{ as } F^{(6)}_{6,0,0}(l_{128}, r_{128}) = ((r_{128} \oplus_{128} 6), (l_{128} \oplus_{128} F^{(5)}_{5,0,0}(r_{128}))),$$
$$F^{(7)}_{7,0,0} : \mathbb{Z}_2^{512} \to \mathbb{Z}_2^{512} \text{ as } F^{(7)}_{7,0,0}(l_{256}, r_{256}) = ((r_{256} \oplus_{256} 7), (l_{256} \oplus_{256} F^{(6)}_{6,0,0}(r_{256}))).$$

We need only $7 = 9 - 2$ iterations for getting $F^{(7)}_{7,0,0} : \mathbb{Z}_2^{512} \to \mathbb{Z}_2^{512}$.

Further on in this section we consider the algebraic properties of the quasigroups obtained by the above algorithm. For that aim we take a somewhat simplified situation when $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ is a bijection and $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ is an ExtFN created by f. We denote by $(Q, \bullet)$ the quasigroup on the set $Q = \mathbb{Z}_2^{2k}$ derived by the complete mapping $F_{a,b,c}$.

Proposition 5.1. *The quasigroup $(Q, \bullet)$ is non-idempotent iff $f(c) \neq b$ or $a \neq 0$.*

Proof. Let $(Q, \bullet)$ be idempotent. Then, for all $x \in Q$ we have

$$x \bullet x = x \longleftrightarrow F_{a,b,c}(x \oplus_{2k} x) \oplus_{2k} x = x \longleftrightarrow F_{a,b,c}(0, 0) = (0, 0)$$
$$\longleftrightarrow F_{a,b,c}(a, b \oplus_k f(c)) = (0, 0) \longleftrightarrow a = 0 \wedge f(c) = b. \qquad \square$$

Proposition 5.2. *The quasigroup $(Q, \bullet)$ does have neither left nor right unit.*

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

$$x \bullet e = x \longrightarrow F_{a,b,c}(x \oplus_{2k} e) \oplus_{2k} e = x \longrightarrow F_{a,b,c}(x \oplus_{2k} e) = x \oplus_{2k} e.$$

This means that $F_{a,b,c} = I$ is the identity mapping. We have now, for every $l, r \in Q$, that $(r \oplus_k a, l \oplus_k b \oplus_k f(r \oplus_k c)) = (l, r)$ and this implies that $f(r \oplus_k c) = a \oplus_k b$ for each r. The last equality contradicts the bijectivity of f.

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

$$e \bullet x = x \longrightarrow F_{a,b,c}(e \oplus_{2k} x) \oplus_{2k} x = x \longrightarrow F_{a,b,c}(e \oplus_{2k} x) = 0.$$

This contradicts the fact that $F_{a,b,c}$ is a bijection. □

Proposition 5.3. *The equality*

$$(x \bullet y) \bullet (y \bullet x) = x \tag{5}$$

is an identity in $(Q, \bullet)$.

Proof. $(x \bullet y) \bullet (y \bullet x) = F_{a,b,c}((x \bullet y) \oplus_n (y \bullet x)) \oplus_n (y \bullet x)) =$
$F_{a,b,c}(F_{a,b,c}(x \oplus_n y) \oplus_n y \oplus_n F_{a,b,c}(y \oplus_n x) \oplus_n x) \oplus_n F_{a,b,c}(y \oplus_n x) \oplus_n x = x.$ □

The quasigroups that satisfy the identity (5) are known as *Schroeder quasigroups* (see [15]).

Corollary 5.1. *The quasigroup $(Q, \bullet)$ is anti-commutative, i.e., no different elements of Q commutes.*

Proof. Let $x, y \in Q$ and let $x \bullet y = y \bullet x$. By (5), we have $x = (x \bullet y) \bullet (y \bullet x) = (y \bullet x) \bullet (x \bullet y) = y$. □

Lemma 5.1. *Let $\varphi = I \oplus_{2k} F_{a,b,c}$. Then $\varphi \circ F_{a,b,c} = F_{a,b,c} \circ \varphi$ iff $a = 0$ and $f(r \oplus_k c) \oplus_k f(l \oplus_k b \oplus_k c \oplus_k f(r \oplus_k c)) = b \oplus_k f(l \oplus_k r \oplus_k b \oplus_k c \oplus_k f(r \oplus_k c))$ for each $l, r \in Q$.*

Proof. Let $l, r \in Q$. Then

$$\begin{aligned}
\varphi(l,r) &= ((l \oplus_k r \oplus_k a), (l \oplus_k r \oplus_k b \oplus_k f(r \oplus_k c))),\\
(\varphi \circ F_{a,b,c})(l,r) &= ((r \oplus_k l \oplus_k b \oplus_k f(r \oplus_k c)), (r \oplus_k a \oplus_k l \oplus_k f(r \oplus_k c) \oplus_k \\
&\qquad f(l \oplus_k b \oplus_k f(r \oplus_k c) \oplus_k c))),\\
(F_{a,b,c} \circ \varphi)(l,r) &= ((l \oplus_k r \oplus_k b \oplus_k f(r \oplus_k c) \oplus_k a), (l \oplus_k r \oplus_k a \oplus_k b \oplus_k \\
&\qquad f(l \oplus_k r \oplus_k b \oplus_k f(r \oplus_k c) \oplus_k c))).
\end{aligned}$$

Hence, we have:

$(\varphi \circ F_{a,b,c})(l,r) = (F_{a,b,c} \circ \varphi)(l,r) \longleftrightarrow a = 0 \ \wedge \ f(r \oplus_k c) \oplus_k f(l \oplus_k b \oplus_k c \oplus_k f(r \oplus_k c)) = b \oplus_k f(l \oplus_k r \oplus_k b \oplus_k c \oplus_k f(r \oplus_k c))$. □

Lemma 5.2. *For the quasigroup $(Q, \bullet)$ we have*

$$x \bullet (y \bullet x) = (x \bullet y) \bullet x \longleftrightarrow (\varphi \circ F_{a,b,c})(x \oplus_{2k} y) = (F_{a,b,c} \circ \varphi)(x \oplus_{2k} y)$$

for any $x, y \in Q$, $x \neq y$, where $\varphi = I \oplus_{2k} F_{a,b,c}$.

Proof. $x \bullet (y \bullet x) = (x \bullet y) \bullet x \longleftrightarrow F_{a,b,c}(x \oplus_{2k} F_{a,b,c}(y \oplus_{2k} x) \oplus_{2k} x) \oplus_{2k} F_{a,b,c}(y \oplus_{2k} x) \oplus_{2k} x = F_{a,b,c}(F_{a,b,c}(x \oplus_{2k} y) \oplus_{2k} y \oplus_{2k} x) \oplus_{2k} x \longleftrightarrow$
$F_{a,b,c}(F_{a,b,c}(y \oplus_{2k} x)) \oplus_{2k} F_{a,b,c}(y \oplus_{2k} x) = F_{a,b,c}(F_{a,b,c}(x \oplus_{2k} y) \oplus_{2k} x \oplus_{2k} y)$
$\longleftrightarrow \varphi(F_{a,b,c}(x \oplus_{2k} y)) = F_{a,b,c}(\varphi(x \oplus_{2k} y))$. □

An immediate consequence of Lemma 5.1 and Lemma 5.2 is that

$$x \bullet (x \bullet x) = (x \bullet x) \bullet x \longleftrightarrow a = 0 \ \wedge \ f(c) = b.$$

Now we have the following sufficient conditions for non-associativity of the quasigroup $(Q, \bullet)$.

Proposition 5.4. *If $a \neq 0$, or $f(c) \neq b$, or $\varphi \circ F_{a,b,c}(x) \neq F_{a,b,c} \circ \varphi(x)$ for some $x \neq 0 \in Q$, then the quasigroup $(Q, \bullet)$ is non-associative.* □

It can be checked that the quasigroup $(Q, \bullet)$ is associative iff the following equalities are identities in $(\mathbb{Z}_2^k, \oplus_k)$, where $t, x_l, x_r, y_l, y_r, z_l, z_r$ are variables:

$$\left.\begin{array}{l} t = x_l \oplus_k x_r \oplus_k z_l \oplus_k z_r \oplus_k f(y_r \oplus_k z_r \oplus_k c), \\ t = a \oplus_k f(x_r \oplus_k y_r \oplus_k c), \\ t = b \oplus_k f(x_l \oplus_k y_l \oplus_k y_r \oplus_k z_r \oplus_k a \oplus_k b \oplus_k c \oplus_k t) \oplus_k \\ \qquad \oplus_k f(x_l \oplus_k y_l \oplus_k b \oplus_k c \oplus_k t). \end{array}\right\} \tag{6}$$

Namely, we can represent $x, y, z \in Q$ by $x = (x_l, x_r)$, $y = (y_l, y_r)$, $z = (z_l, z_r)$, where $x_l, x_r, y_l, y_r, z_l, z_r \in \mathbb{Z}_2^k$, and then $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ iff (6) holds true. This shows that the quasigroup $(Q, \bullet)$ is highly non-associative, since a bijection f can hardly satisfies the equations (6) for given elements $x, y, z \in Q$.

Note that if θ is a complete mapping of a group $(\mathbb{Z}_2^n, \oplus_n)$, we have

$$y \bullet x = \theta(y \oplus_n x) \oplus_n x$$

$$(y \bullet x) \bullet x = \theta(\theta(y \oplus_n x) \oplus_n x \oplus_n x) \oplus_n x = \theta^2(y \oplus_n x) \oplus_n x$$

and, by induction, $((y \bullet \underbrace{x) \bullet \dots) \bullet x}_{l} = \theta^l(y \oplus_n x) \oplus_n x$.

We have also

$$x \bullet y = \theta(x \oplus_n y) \oplus_n y \oplus_n x \oplus_n x = \varphi(x \oplus_n y) \oplus_n x,$$

$$x \bullet (x \bullet y) = \theta(x \oplus_n \varphi(x \oplus_n y) \oplus_n x) \oplus_n \varphi(x \oplus_n y) \oplus_n x = \varphi^2(x \oplus_n y) \oplus_n x$$

and, by induction, $\underbrace{x \bullet (\cdots \bullet (x}_{l} \bullet y)) = \varphi^l(x \oplus_n y) \oplus_n x$.

Proposition 5.5.

a) The identity $y = ((y \bullet \underbrace{x) \bullet \dots) \bullet x}_{l}$ *holds true in* $(Q, \bullet)$ *iff* $F^l_{a,b,c} = I$.

b) The identity $\underbrace{x \bullet (\cdots \bullet (x}_{l} \bullet y)) = y$ *holds true in* $(Q, \bullet)$ *iff* $\varphi^l = I$,

where $\varphi = I \oplus_{2k} F_{a,b,c}$. □

Regarding the subquasigroups of the quasigroup $(Q, \bullet)$, we notice the following property, where $< A >$ denotes the subquasigroup generated by the subset A of Q.

Proposition 5.6. $< 0 >=< \{F^i_{a,b,c}(0) \,|\, i = 1, 2, \dots \} >$.

Proof. $0 \bullet 0 = F_{a,b,c}(0)$, $F_{a,b,c}(0) \bullet 0 = F^2_{a,b,c}(0)$, $F^2_{a,b,c}(0) \bullet 0 = F^3_{a,b,c}(0), \dots .$ □

6. Conclusions

In this paper we have defined a generalization of a Feistel network so called extended Feistel network, and then we conjuncted two very familiar approaches of Feistel networks and complete mappings in one novel way for creating quasigroups of huge order 2^{s2^t}. The starting function f, needed a Feistel network to be defined, is of small order 2^s and it can be chosen in such a way the created quasigroup to be non-idempotent, non-commutative, non-associative, without left or right unit, nonlinear,... Although of huge order, the multiplication in the created quasigroup is highly effective, its complexity is $\mathcal{O}(t)$.

The quasigroups of huge orders defined in this paper are suitable for applications in cryptography. The fact that the constructed extended Feistel networks are complete mappings θ, such that the mappings θ^{-1} and $I \oplus_k \theta$ are also complete, can be used parastrophes to be defined in a suitable way. So, these quasigroups can be used for encoding and decoding purposes.

References

[1] **V. D. Belousov**, *Osnovi teorii kvazigrup i lup*, "Nauka", Moskva, 1967.

[2] **G. Carter, E. Dawson, and L. Nielsen**, *A latin square version of DES*, Proc. Workshop of Selected Areas in Cryptography, Ottawa, Canada, 1995.

[3] **J. Cooper, D. Donovan and J. Seberry**, *Secret sharing schemes arising from Latin Squares*, Bull. Inst. Combin. Appl. **4** (1994), 33 – 43.

[4] **J. Dénes and A. D. Keedwell**, *A new authentication scheme based on latin squares*, Discrete Math. **106-107** (1992), 157 – 161.

[5] **A. L. Dulmage, N. S. Mendelsohn, and D. M. Johnson**, *Orthomorphisms of groups and orthogonal latin squares I*, Canad. J. Math. **13** (1961), 356 – 372.

[6] Federal Information New York Data Encryption Standard, Processing Standards Publication **No. 46** (1977), National Bureau of Standards.

[7] **A. B. Evans**, *Orthomorphism Graphs of Groups*, J. Geometry **32** (1989), 66−74.

[8] **H. Feistel**, *Cryptography and computer privacy*, Scientific American **228** (1973), no. 5, 15 – 23.

[9] **D. Gligoroski, S. Markovski, L. Kocarev, and M. Gusev**, *Edon80 - Hardware Synchronous stream cipher*, SKEW 2005 - Symmetric Key Encryption Workshop, Aarhus, Denmark, 2005.

[10] **D. Gligoroski, S. Markovski, S.J. Knapskog**, *A Fix of the MD4 Family of Hash Functions - Quasigroup Fold*, NIST Cryptographic Hash Workshop, NIST in Gaithersburg, Maryland, USA, 2005.

[11] **D. Gligoroski, S. Markovski, S.J. Knapskog**, *Multivariate Quadratic Trapdoor Functions Based on Multivariate Quadratic Quasigroups*, Recent Advances Appl. Math., Proc. Amer. Conf. Appl. Math. (MATH'08), Cambridge, Massachusetts, 2008, 44 – 49.

[12] **D. Gligoroski, S. Markovski, L. Kocarev**, *Edon-R Family of Cryptographic Hash Functions*, The Second NIST Cryptographic Hash Workshop, UCSB, Santa Barbara, 2006.

[13] **M. Hall and L. J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541 – 549.

[14] **J. Kong**, *The role of Latin square in cipher systems: a matrix approach to model encryption modes of operation*, UCLA Comp. Science Depart. technical report CSD-TR0038, July, 2003.

[15] **C. C. Lindner, N. S. Mendelsohn and S. R. Sun**, *On the construction of Schroeder quasigroups*, Discrete Math. **32**(1980), 271 – 280.

[16] **M. Luby and C. Rackoff**, *How to Construct Pseudorandom Permutations and Pseudorandom Functions*, SIAM J. Comput. **17**(1988), 373 – 386.

[17] **H. B. Mann**, *The construction of orthogonal Latin squares*, Annals Math. Statistics **13** (1942), 418 – 423.

[18] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup string transformations, Part 1* Contributions, Sec. math. Tech. Sci., MANU, XX, 1 – 2 (1999) 13 – 28.

[19] **S. Markovski, D. Gligoroski and Lj. Kocarev**, *Unbiased Random Sequenses from Quasigroup String Transformations*, H. Gilbert and H. Handschuh (Eds.), FSE 2005, LNCS 3557 (2005), 163 – 180.

[20] **S. Markovski and A. Mileva**, *The NaSHA family of cryptographic hash functions*, NIST SHA-3 call for hush functions,

http://inf.ugd.edu.mk/images/stories/file/Mileva/nasha_hf.html

[21] **K. A. Meyer**, *A new message authentication code based on the non-associativity of quasigroups*, Ph.D. thesis, Iowa State Univ. 2006.

[22] **L. J. Paige**, *A note on finite abelian groups*, Bull. Amer. Math. Soc. **53** (1947), 590 – 593.

[23] **L. J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111 – 116.

[24] **K. Pommerening**, *Fourier Analysis of Boolean Maps*, A Tutorial 2005, J. Gutenberg University.

[25] **A. Sade**, *Quasigroups automorphes par le groupe cyclique*, Canadian J. Math. **9** (1957), 321 – 335.

[26] **C. P. Schnorr and S. Vaudenay**, *Black Box Cryptanalysis of hash networks based on multipermutations*, Advances of Cryptology - EUROCRYPT'94, Springer, Berlin, 1995, 447 – 57.

[27] http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/program.html

Received March 24, 2009

S. Markovski:
Institute of Informatics, Faculty of Natural Science, “Ss Cyril and Methodious” University,
Bul. Aleksandar Makedonski bb, pf. 162, Skopje, Republic of Macedonia
E-mail: smile@ii.edu.mk

A. Mileva:
Faculty of Informatics, University “Goce Delčev”, “Krste Misirkov” bb, Štip, Republic of Macedonia
E-mail: saskamileva@yahoo.com