Quasigroups and Related Systems **22** (2014), 267 − 276

Quasigroup representation of some lightweight block ciphers

Aleksandra Mileva and Smile Markovski

Abstract. Most of the lightweight block ciphers are build as S-P networks or Feistel networks, their generalization or variations. We represent the lightweight Feistel ciphers GOST and MIBS, and Generalized Feistel cipher Skipjack by quasigroup string transformations. For obtaining suitable representation we use the fact that Feistel round functions that are bijections can be considered as orthomorphisms of groups, and that give us a tool for creating wanted quasigroups.

1. Introduction

Over the past years, the lightweight cryptography has drawn considerable attention. Pervasive computing, presented with application of smart cards, RFID (Radio-frequency identification) tags and sensor nodes, is changing and improving everyday life and, at the same time, introducing many security issues and risks, in the same time. Many new cryptographic primitives have been proposed for use in resource-constrained environments, leaded by the lightweight block ciphers, which number increase constantly.

According to their design, there are two major classes of lightweight block ciphers: S-P type ciphers and Feistel-type ciphers. Examples of S-P type ciphers are PRESENT [2], KLEIN [10], etc. However, here we shall be more interested in the latter class of ciphers.

H. Feistel [8] invented a special transformation that takes any function f (known as round function) and produces a permutation. First, the input is split into two halves. The one half swaps with the result obtained from XOR-ing the output of the function f applied to this half, and the other half. This became a round of so called Feistel structure for construction of block ciphers, known as Feistel network or Feistel cipher. When two parts of the input in the Feistel round are with different lengths, we have Unbalanced Feistel networks (UFNs) [23]. There exist different generalizations of Feistel networks that split the input into $n > 2$ parts (cells), such as the *type-1*, *type-2* and *type-3* Extended Feistel networks from Zheng et al [30], the Generalized Feistel-Non Linear Feedback Shift Register (GF-NLFSR) from Choy et al [3], etc.

2010 Mathematics Subject Classification: 20N05, 14G50
Keywords: Feistel network, orthomorphism, quasigroup, MIBS, GOST, Skipjack.

Some lightweight Feistel ciphers are GOST 28147-89 [11], MIBS [13] and Kasumi [27]. There are block ciphers with variations of Feistel network, such as lightweight variants of DES, with names DESL/DESX/DESXL [14], then TEA [28], LBlock [29] and SEA [25]. Examples of Generalized Feistel ciphers that use *type-2* Extended Feistel networks are: HIGHT [12], TWINE [26], Piccolo [24]. Skipjack [21] is another Generalized Feistel cipher.

1.1 Previous work

Recent research activities show that possible quasigroup representations of some existing cryptographic primitives or their building blocks lead to finding weaknesses in their deployment or to improving their hardware implementations.

Paper [9] describes some block cipher's modes of operation as quasigroup string transformations, and with this methodology the authors showed that the OFB mode is a special case of the CBC mode of operation. Even more, they showed that in a cases of interchanged use of CBC and OFB modes, the plaintext can be obtained from the ciphertext, without the knowledge of the secret key.

Another paper [17] describes an algorithm for generating an optimal 4×4 S-boxes by quasigroup string transformations. Using this algorithm, the authors of [18] offer a methodology for more optimized hardware implementation of cryptographically strong 4×4 S-boxes, which not only iteratively reuse the same circuit to implement several different S-boxes, but it leads to bit level serialization and S-box implementation below 10 GEs.

The authors of paper [20] represent Feistel ciphers Misty1 [16] and Camellia [1], and Generalized Feistel ciphers Four-Cell^{+} [3, 4] and SMS4 [6] with quasigroup string transformations. For all of them, one feature is the same - they use bijections as round functions in their Feistel networks. This can be a promising methodology to analyze the block ciphers from totally new perspective.

1.2 Our contribution

Using the same methodology from [20] we give the quasigroup representations of the lightweight Feistel ciphers: GOST and MIBS, and Generalized Feistel cipher Skipjack. Even more, we show that all three are the same from quasigroup point of view. With other words, all three are special instances of one block cipher obtained by generalized e-transformation of string that consists of 32 zeros $\mathbf{0}$ (each of length 64 bits), with 32 different quasigroups of order 2^{64}, with or without last swap.

To our knowledge, this is not a certificational weaknesses of the examined block ciphers, but only another view of them.

The following variations of the Feistel cipher, DESL/DESX/DESXL and TEA (and XTEA) **do not use** bijections as round functions. Kasumi is slightly modification of MISTY1 for optimized hardware implementations, so we are not looking at it.

2. Preliminaries

A quasigroup is a groupoid $(Q,*)$ with the property that for every $a,b\in Q$ there exist unique $x\in Q$ and $y\in Q$ such that the equations $a*x=b$ and $y*a=b$ are true. 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.

Given a quasigroup $(Q,*)$, define upon Q the operation of left division $\backslash$ by

$$x\backslash y = z \Longleftrightarrow x*z=y.$$

The quaisigroup string transformations are defined in [15]. Here we use their generalizations from [20], defined as follows. Consider the finite set Q as an alphabet with word set $Q^{+}=\{x_1x_2\dots x_t \mid x_i\in Q, t\geqslant 1\}$. Let $*_1,*_2,\dots,*_t$ be t (not necessarily distinct) quasigroup operations on Q and let $\backslash_i$ be the left division adjoint operation corresponding to $*_i$. Let $l\in Q$ be a fixed element, called a leader. Then the generalized quasigroup string transformations $e_{l,*_1,*_2,\dots,*_t}: Q^t\to Q^t$ and $d_{l,\backslash_1,\backslash_2,\dots,\backslash_t}: Q^t\to Q^t$ are defined as follows:

$$e_{l,*_1,*_2,\dots,*_t}(x_1\dots x_t)=(z_1\dots z_t)\Longleftrightarrow z_j=z_{j-1}*_j x_j,\ 1\leqslant j\leqslant t, \tag{1}$$

$$d_{l,\backslash_1,\backslash_2,\dots,\backslash_t}(z_1\dots z_t)=(x_1\dots x_t)\Longleftrightarrow x_j=z_{j-1}\backslash_{t-j+1} z_j,\ 1\leqslant j\leqslant t, \tag{2}$$

where $z_0=l$. It is easy to proof that following equation holds

$$e_{l,*_1,*_2,\dots,*_t}(d_{l,\backslash_t,\backslash_{t-1},\dots,\backslash_1}(x_1\dots x_t))=x_1\dots x_t=d_{l,\backslash_1,\backslash_2,\dots,\backslash_t}(e_{l,*_t,*_{t-1},\dots,*_1}(x_1\dots x_t)).$$

We need next the definition of complete mappings and orthomorphisms.

Definition 2.1. [5, 7] 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 to the complete mapping ϕ. A group G is *admissible* if there is a complete mapping $\phi: G\to G$.

One can notice that orthomorphisms and complete mappings coincide in the group $(\mathbb{Z}_2^n,\oplus)$. The generalization of Sade's [22] *diagonal method*, for construction of needed quasigroups, is presented in the following theorem.

Theorem 2.2. [19] *Let ϕ be a complete mapping of the admissible group $(G,+)$ and let θ be an orthomorphism associated to ϕ. Define operations $\circ$ and $*$ on G by*

$$x\circ y=\phi(y-x)+y=\theta(y-x)+x, \tag{3}$$

$$x*y=\theta(x-y)+y=\phi(x-y)+x, \tag{4}$$

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

Quasigroups produced by this method have the following properties [19]:

1. $(G, \circ)$ *and* $(G, *)$ *are non-associative quasigroups.*
2. *If the group* $(\mathbb{Z}_2^n, \oplus)$ *is used, then*
   2.1 $(\mathbb{Z}_2^n, \circ)$ *and* $(\mathbb{Z}_2^n, *)$ *are diagonally cyclic quasigroups, i.e.,* $(x \oplus 1) \circ (y \oplus 1) = x \circ y \oplus 1$ *and* $(x \oplus 1) * (y \oplus 1) = x * y \oplus 1$ *for* $x, y \in \mathbb{Z}_2^n$.
   2.2 $(\mathbb{Z}_2^n, \circ)$ *and* $(\mathbb{Z}_2^n, *)$ *are Schroeder quasigroups, i.e.,* $(x \circ y) \circ (y \circ x) = x$ *and* $(x * y) * (y * x) = x$ *for every* $x, y \in \mathbb{Z}_2^n$.
   2.3 $(\mathbb{Z}_2^n, \circ)$ *and* $(\mathbb{Z}_2^n, *)$ *are anti-commutative quasigroups.*

In [19] are defined and in [20] are redefined parameterized versions of the Feistel network, the *type-1* Extended Feistel network, and the Generalized Feistel-Non Linear Feedback Shift Register (GF-NLFSR), and has been proved that if a bijection f is used for their creation, then they are orthomorphisms of abelian groups. Another generalization of Feistel network is given in [20] as *type-4* PEFN (4-cell version was first presented in the SMS4 block cipher).

Definition 2.3. [20] Let $(G, +)$ be an abelian group, let $f_C : G \to G$ be a mapping, where C is an arbitrary constant and let $A, B, A_1, A_2, \dots, A_n \in G$.

- The *Parameterized Feistel Networks (PFN)* $F^d_{A,B,C}$ and $F^l_{A,B,C} : G^2 \to G^2$ created by f_C are defined for every $l, r \in G$ by
$$F^d_{A,B,C}(l, r) = (r + A, l + B + f_C(r)) \text{ and}$$
$$F^l_{A,B,C}(l, r) = (r + A + f_C(l), l + B).$$
- The *type-1 Parameterized Extended Feistel Network* $(PEFN)$ $F_{A_1,A_2,\dots,A_n,C} : G^n \to G^n$ created by f_C is defined for every $(x_1, x_2, \dots, x_n) \in G^n$ by
$$F_{A_1,A_2,\dots,A_n,C}(x_1, x_2, \dots, x_n) =$$
$$= (x_2 + f_C(x_1) + A_1, x_3 + A_2, \dots, x_n + A_{n-1}, x_1 + A_n).$$
- The *type-4 Parameterized Extended Feistel Network* $(PEFN)$ $F_{A_1,A_2,\dots,A_n,C} : G^n \to G^n$ created by f_C is defined for every $(x_1, x_2, \dots, x_n) \in G^n$ by
$$F_{A_1,A_2,\dots,A_n,C}(x_1, x_2, \dots, x_n) =$$
$$= (x_2 + A_1, x_3 + A_2, \dots, x_n + A_{n-1}, x_1 + A_n + f_C(x_2 + \dots + x_n)).$$
- The *PGF-NLFSR* (*Parameterized Generalized Feistel-Non Linear Feedback Shift Register*) $F_{A_1,A_2,\dots,A_n,C} : G^n \to G^n$ created by f_C is defined for every $(x_1, x_2, \dots, x_n) \in G^n$ by
$$F_{A_1,A_2,\dots,A_n,C}(x_1, x_2, \dots, x_n) =$$
$$= (x_2 + A_1, x_3 + A_2, \dots, x_n + A_{n-1}, x_2 + \dots + x_n + A_n + f_C(x_1)).$$

The last two generalizations are orthomorphisms only of the group $(\mathbb{Z}_2^m, \oplus)$ and even n. Note that, the PFN $F^l_{A,B,C}$ is in the same time a 2-cell *type-1* PEFN $F_{A,B,C}$, and the PFN $F^d_{A,B,C}$ is in the same time a 2-cell *type-4* PEFN $F_{A,B,C}$. *type-2* and *type-3* PEFN [19] are not orthomorphisms in general, thus, they are not subject of our interest. This means also, that the methodology used in this paper, can not be applied to HIGHT, TWINE and Piccolo.

3. Quasigroup representation of GOST

The GOST is 64-bit block cipher, and the official encryption standard of the Russian Federation, known as “GOST 28147-89" [11] (Soviet “DES" from 1989). It uses key length of 256 bits.

GOST is a Feistel cipher with 32 rounds. The round functions $f_{sk_i} : \{0,1\}^{32} \to \{0,1\}^{32}$, $i \in \{1, 2, \dots, 32\}$, can be represented as $f_{sk_i}(x) = (S(x + sk_i))_{<<<11}$, where $+$ is addition modulo 2^{32}, S is permutation obtained by 8 4×4 S_j-boxes, $j \in \{1, 2, \dots, 8\}$, $(y)_{<<<11}$ is rotation of y to the left by 11 bits, and sk_i are subkeys generated from the secret key K. We leave the details how the subkeys are generated from the key.

Let the plaintext be denoted by $M = (l_0, r_0) = X_0 \in (\{0,1\}^{32})^2$. The GOST algorithm can be represented as follows:

1. For $i = 1$ to 32 do
   $X_i = (l_i, r_i) = (r_{i-1}, l_{i-1} \oplus f_{sk_i}(r_{i-1}))$
2. The ciphertext is $C = (r_{32}, l_{32})$.

The i-th round can be represented by the PFN $F^d_{0,0,sk_i}$, $i \in \{1, 2, \dots, 32\}$, as $X_i = F^d_{0,0,sk_i}(X_{i-1})$. Since its round function f_{sk_i} is a bijection for fixed sk_i, the PFN $F^d_{0,0,sk_i}$ is an orthomorphism of the group $((\mathbb{Z}_2^{32})^2, \oplus)$ (0 is the zero in $(\mathbb{Z}_2^{32}, \oplus)$ and $\mathbf{0} = (0,0)$). We can define 32 different quasigroups $((\mathbb{Z}_2^{32})^2, *_i)$ of order 2^{64} as

$$X *_i Y = F^d_{0,0,sk_i}(X \oplus Y) \oplus Y,$$

where $X, Y \in (\mathbb{Z}_2^{32})^2$.

So, we can write the output of the i-th round as

$$X_i = X_{i-1} *_i \mathbf{0}.$$

The output X_{32} of the final 32-th round can be written as

$$X_{32} = X_{31} *_{32} \mathbf{0} = (X_{30} *_{31} \mathbf{0}) *_{32} \mathbf{0} = ((\dots (X_0 *_1 \mathbf{0}) \dots) *_{31} \mathbf{0}) *_{32} \mathbf{0}.$$

Now we can represent the GOST algorithm by generalized $e_{l,*_1,*_2,\dots,*_{32}}$ quasigroup transformation on string of 32 zeros $\mathbf{0}$ with leader $l = X_0$ and 32 different quasigroups.

1. $X_{32} = (l_{32}, r_{32}) = e_{X_0,*_1,*_2,\dots,*_{32}}(\underbrace{\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}}_{32})$
2. The ciphertext is $C = (r_{32}, l_{32})$.

4. Quasigroup representation of MIBS

The MIBS is a lightweight 64-bit block cipher, with variable key length of 64 and 80 bits [13]. It is a Feistel cipher that uses 32 rounds. All internal operations in MIBS are nibble-wise.

The round functions $f_{K_i} : \{0,1\}^{32} \to \{0,1\}^{32}$, $i \in \{1, 2, \dots, 32\}$, have an SPN structure composed of round subkey addition, non-linear substitution layer with one 4×4 S-box applied 8 times in parallel and linear transformation layer. For our analysis, only important thing is that f_{K_i} are bijections for fixed round subkey K_i.

Let the plaintext be denoted by $M = (l_0, r_0) = X_0 \in (\{0,1\}^{32})^2$. The MIBS algorithm can be represented as follows:

1. For $i = 1$ to 32 do $X_i = (l_i, r_i) = (r_{i-1} \oplus f_{K_i}(l_{i-1}), l_{i-1})$.
2. The ciphertext is $C = X_{32}$.

The i-th round can be represented by the PFN $F^l_{0,0,K_i}$, $i \in \{1, 2, \dots, 32\}$, as $X_i = F^l_{0,0,K_i}(X_{i-1})$. Since its round function f_{K_i} is a bijection for fixed K_i, the PFN $F^l_{0,0,K_i}$ is an orthomorphism of the group $((\mathbb{Z}_2^{32})^2, \oplus)$. We can define 32 different quasigroups $((\mathbb{Z}_2^{32})^2, *_i)$ of order 2^{64} as

$$X *_i Y = F^l_{0,0,K_i}(X \oplus Y) \oplus Y,$$

where $X, Y \in (\mathbb{Z}_2^{32})^2$.

Like GOST, MIBS algorithm can be represented by generalized $e_{l,*_1,*_2,\dots,*_{32}}$ quasigroup transformation on string of 32 zeros $\mathbf{0}$ with leader $l = X_0$ and 32 different quasigroups, but with one difference, without final swap.

$$C = X_{32} = e_{X_0,*_1,*_2,\dots,*_{32}}(\underbrace{\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}}_{32}).$$

5. Quasigroup representation of Skipjack

Skipjack [21] is a Generalized Feistel cipher with 64-bit block, 80-bit key and 32 rounds. It is designed by NSA and it is one of the three approved encryption algorithm by NIST. It uses two different types of generalized Feistel rounds, referred as A-round and B-round.

Let the plaintext be denoted by $M = (x_0, x_1, x_2, x_3) = X_0 \in (\{0,1\}^{16})^4$. Skipjack consists of 8 A-rounds, followed by 8 B-rounds, and once again 8 A-rounds followed by 8 B-rounds, and can be represented as follows:

1. For $i = 1$ to 8 do
$X_i = (x_i, x_{i+1}, x_{i+2}, x_{i+3}) = (x_{i+3} \oplus G_{K_i}(x_{i-1}) \oplus counter, G_{K_i}(x_{i-1}), x_{i+1}, x_{i+2})$.
2. For $i = 1$ to 8 do
$X_{8+i} = (x_{8+i}, x_{8+i+1}, x_{8+i+2}, x_{8+i+3}) =$
$(x_{8+i+3}, G_{K_{8+i}}(x_{8+i-1}), x_{8+i-1} \oplus x_{8+i} \oplus counter, x_{8+i+2})$

3. For $i = 1$ to 8 do
$X_{16+i} = (x_{16+i}, x_{16+i+1}, x_{16+i+2}, x_{16+i+3}) =$
$(x_{16+i+3} \oplus G_{K_{16+i}}(x_{16+i-1}) \oplus counter, G_{K_{16+i}}(x_{16+i-1}), x_{16+i+1}, x_{16+i+2})$.
4. For $i = 1$ to 8 do
$X_{24+i} = (x_{24+i}, x_{24+i+1}, x_{24+i+2}, x_{24+i+3}) =$
$(x_{24+i+3}, G_{K_{24+i}}(x_{24+i-1}), x_{24+i-1} \oplus x_{24+i} \oplus counter, x_{24+i+2})$.
5. The ciphertext is $C = X_{32}$.

The functions G_{K_i}, $1 \leqslant i \leqslant 32$, have four-round Feistel structure, so, they are bijections for fixed K_i, where K_i is 32-bit round subkey. We can proof the following two propositions.

Proposition 5.1. *The A-round of Skipjack* $A_{K,C} : (\mathbb{Z}_2^{16})^4 \to (\mathbb{Z}_2^{16})^4$ *given by*

$$A_{K,C}(x_0, x_1, x_2, x_3) = (x_3 \oplus G_K(x_0) \oplus C, G_K(x_0), x_1, x_2)$$

for fixed K *and* C*, and created by a bijection* $G_K : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$ *is an orthomorphism of the group* $((\mathbb{Z}_2^{16})^4, \oplus)$.

Proof. The function $A_{K,C}$ is a bijection, with the inverse

$$A_{K,C}^{-1}(x_0, x_1, x_2, x_3) = (G_K^{-1}(x_1), x_2, x_3, x_0 \oplus x_1 \oplus C).$$

Let $\Phi = A_{K,C} \oplus I$, i.e., $\Phi(x_0, x_1, x_2, x_3) = (x_3 \oplus G_K(x_0) \oplus C \oplus x_0, G_K(x_0) \oplus x_1, x_1 \oplus x_2, x_2 \oplus x_3) = (y_0, y_1, y_2, y_3)$ for every $(x_0, x_1, x_2, x_3) \in (\mathbb{Z}_2^{16})^4$.

Define the function $\Omega : (\mathbb{Z}_2^{16})^4 \to (\mathbb{Z}_2^{16})^4$ by $\Omega(y_0, y_1, y_2, y_3) = (z, y_1 \oplus G_K(z), y_1 \oplus y_2 \oplus G_K(z), y_1 \oplus y_2 \oplus y_3 \oplus G_K(z))$ where $z = y_0 \oplus y_1 \oplus y_2 \oplus y_3 \oplus C$.

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

Proposition 5.2. *The B-round of Skipjack* $B_{K,C} : (\mathbb{Z}_2^{16})^4 \to (\mathbb{Z}_2^{16})^4$ *given by*

$$B_{K,C}(x_0, x_1, x_2, x_3) = (x_3, G_K(x_0), x_0 \oplus x_1 \oplus C, x_2)$$

for fixed K *and* C*, and created by a bijection* $G_K : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$ *is an orthomorphism of the group* $((\mathbb{Z}_2^{16})^4, \oplus)$.

Proof. The function $B_{K,C}$ is a bijection, with the inverse

$$B_{K,C}^{-1}(x_0, x_1, x_2, x_3) = (G_K^{-1}(x_1), x_2 \oplus G_K^{-1}(x_1) \oplus C, x_3, x_0).$$

Let $\Phi = B_{K,C} \oplus I$, i.e., $\Phi(x_0, x_1, x_2, x_3) = (x_0 \oplus x_3, G_K(x_0) \oplus x_1, x_0 \oplus x_1 \oplus x_2 \oplus C, x_2 \oplus x_3) = (y_0, y_1, y_2, y_3)$ for every $(x_0, x_1, x_2, x_3) \in (\mathbb{Z}_2^{16})^4$.

Define the function $\Omega : (\mathbb{Z}_2^{16})^4 \to (\mathbb{Z}_2^{16})^4$ by $\Omega(y_0, y_1, y_2, y_3) = (G_K^{-1}(z), y_0 \oplus y_2 \oplus y_3 \oplus C, y_0 \oplus y_3 \oplus G_K^{-1}(z), y_0 \oplus G_K^{-1}(z))$ where $z = y_0 \oplus y_1 \oplus y_2 \oplus y_3 \oplus C$.

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

Let $A_{K_i,counter} : (\{0,1\}^{16})^4 \to (\{0,1\}^{16})^4$, $i = 1, 2, \ldots, 8, 17, 18, \ldots, 24$, be orthomorphisms created by the bijections G_{K_i}, respectfully. The quasigroup operations are defined by

$$X *_i Y = A_{K_i,counter}(X \oplus Y) \oplus Y,$$

where $X, Y \in (\{0,1\}^{16})^4$.

Let $B_{K_i,counter} : (\{0,1\}^{16})^4 \to (\{0,1\}^{16})^4$, $i = 9, 10, \ldots, 16, 25, 26, \ldots, 32$, be orthomorphisms created by the bijections G_{K_i}, respectfully. The quasigroup operations are defined by

$$X *_i Y = B_{K_i,counter}(X \oplus Y) \oplus Y,$$

where $X, Y \in (\{0,1\}^{16})^4$.

Now we can rewrite Skipjack with quasigroups as generalized $e_{l,*_1,*_2,\ldots,*_{32}}$ transformation of string that consists of 32 zeros $\mathbf{0}$ (in the group $((\{0,1\}^{16})^4, \oplus)))$ and $l = X_0$, with 32 different quasigroups of order 2^{64}:

$$C = e_{X_0,*_1,*_2,\ldots,*_{32}}(\underbrace{\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}}_{32}).$$

The round function $G_K : \{0,1\}^{16} \to \{0,1\}^{16}$, where $K = (k_1, k_2, k_3, k_4)$ ($k_j \in \{0,1\}^8$, for $j \in \{1,2,3,4\}$) can be represent by quasigroup transformations in similar manner. It has a four-round Feistel structure, with round function f_{k_j}, which is permutation on $\{0,1\}^8$, for fixed k_j. For a given $x_0 = (l_0, r_0)$, $G_K(x_0) = x_4$ can be represented as:

For $j = 1$ to 4 do $x_j = (r_{j-1}, l_{j-1} \oplus f_{k_j}(r_{j-1})) = F^d_{0,0,k_j}(l_j, r_j)$.

We have that $F^d_{0,0,k_j}$ are orthomorphisms of the group $(\{0,1\}^{16}, \oplus)$, and the quasigroup operations are defined by $x \star_j y = F^d_{0,0,k_j}(x \oplus y) \oplus y$, where $x, y \in \{0,1\}^{16}$. So, G_K can be represented as generalized $e_{x_0,\star_1,\star_2,\star_3,\star_4}$ transformation of 4 zeros $\mathbf{0}$ (length of 16 bits), with 4 different quasigroups of order 2^{16}, or

$$G_K(x_0) = e_{x_0,\star_1,\star_2,\star_3,\star_4}(\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}).$$

6. Conclusions

In this paper we give a quasigroup representation of lightweight block ciphers GOST, MIBS and Skipjack. One can see, that all three block ciphers are similar in their quasigroup representations. All three can be seen as special instances of one block cipher obtained by generalized e-transformation of string that consists of 32 zeros $\mathbf{0}$, with 32 different quasigroups of order 2^{64}, with or without last swap. This methodology offer a new way to analyze existing block ciphers, and how this can be deployed, remains as an open problem.

References

[1] **K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita**, *Camellia: a 128-bit block cipher suitable for multiple platforms – design and analysis*, Lecture Notes Computer Sci. **2012** (2001), 39 – 56.

[2] **A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe**, *Present: An ultra-lightweight block cipher*, Lecture Notes Computer Sci. **4727**, (2007), 450 – 466.

[3] **J. Choy, G. Chew, K. Khoo and H. Yap**, *Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure*, Lecture Notes Computer Sci. **5594**, (2009), 73 – 89.

[4] **J. Choy, G. Chew, K. Khoo and H. Yap**, *Cryptographic Properties and Applications of a Generalized Unbalanced Feistel Network Structure* (*Revised Version*), Cryptography and Communications **3(3)** (2011), 141 – 164.

[5] **J. Dénes and A. D. Keedwell**, *Latin squares: New developments in the theory and applications*, Elsevier, (1991).

[6] **W. Diffie and G. Ledin (translators)**, *SMS4 encryption algorithm for wireless networks*, Cryptology ePrint Archive, Report 2008/329, (2008), http://eprint.iacr.org/2008/329.

[7] **A. B. Evans**, *Orthomorphism Graphs of Groups*, J. Geometry, **35** (1989), 66 – 74.

[8] **H. Feistel**, *Cryptography and computer privacy*, Scientific American, **228(5)**, (1973), 15 – 23.

[9] **D. Gligoroski, S. Andova and S. J. Knapskog**, *On the importance of the key separation principle for different modes of operation*, ISPEC 2008, (2008), 404 – 418.

[10] **Z. Gong, S. Nikova and Y.W. Law**, *KLEIN: A New Family of Lightweight Block Ciphers*, RFIDSec 2011, (2011), 1 – 18.

[11] **GOST, Gosudarstvennyi Standard 28147-89**, *Cryptographic Protection for Data Processing Systems*, Government Committee of the USSR for Standards, (1989).

[12] **D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim and S. Chee**, *HIGHT: A New Block Cipher Suitable for Low-Resource Device*, Lecture Notes Computer Sci. **4249** (2006), 46–59.

[13] **M.I. Izadi, B. Sadeghiyan, S. S. Sadeghian and H. A. Khanooki**, *MIBS: a new lightweight Block Cipher.* Lecture Notes Computer Sci. **5888** (2009), 334 – 348.

[14] **G. Leander, C. Paar, A. Poschmann and K. Schramm**, *New lighweight DES variants*, Lecture Notes Computer Sci. **4593**, (2007), 196 – 210.

[15] **S. Markovski, D. Gligoroski and S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. VIII Conf. Logic and Computer Science LIRA'97, Novi Sad, Serbia, (1997), 157 – 162.

[16] **M. Matsui**, *New block encryption algorithm MISTY*, Lecture Notes Computer Sci. **1267** (1997), 5468.

[17] **H. Mihajloska and D. Gligoroski**, *Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4*, Proc. SECURWARE 2012, Rome, Italy, 163 – 168.

[18] **H. Mihajloska, T. Yalcin and D. Gligoroski**, *How Lightweight is the Hardware Implementation of Quasigroup S-boxes*, Advances in Intelligent Systems and Computing - ICT Innovations 2012, **207**, Springer Berlin Heidelberg (2013), 121 – 128.

[19] **A. Mileva, S. Markovski**, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glasnik Matematicki **47(2)**, (2012), 333 – 349.

[20] **A. Mileva, S. Markovski**, *Quasigroup representation of some Feistel and Generalized Feistel ciphers*, Advances in Intelligent Systems and Computing - ICT Innovations 2012, **207**, Springer Berlin Heidelberg (2013), 161 – 171.

[21] **National Security Agency**, *Skipjack and KEA algorithm specifications*, May 1998, Available at http://csrc.ncsl.nist.gov/encryption/skipjack-1.pdf

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

[23] **B. Schneier and J. Kelsey**, *Unbalanced Feistel Networks and Block-Cipher Design*, 3rd International Workshop on Fast Software Encryption - FSE '96, (1996), Springer-Verlag, 121 – 144.

[24] **K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita and T. Shirai**, *Piccolo: An Ultra-Lightweight Blockcipher*, CHES 2011, Lecture Notes Computer Sci. **6917** (2011), 342 – 357.

[25] **F.-X. Standaert, G. Piret, N. Gershenfeld and J.-J. Quisquater**, *SEA: A Scalable Encryption Algorithm for Small Embedded Applications*, Lecture Notes Computer Sci. **3928** (2006), 222 – 236.

[26] **T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi**, *TWINE : A Lightweight Block Cipher for Multiple Platforms*, In Proceedings of Selected Areas in Cryptography 2012, (2012), 339 – 354.

[27] **3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms**, *Document 2: KASUMI Specification, V3.1.1* (2001).

[28] **D. J. Wheeler and R. Needham**, *TEA, a Tiny Encryption Algorithm*, Lecture Notes Computer Sci. **1008** (1994), 363 – 366.

[29] **W. Wu and L. Zhang**, *LBlock: A Lightweight Block Cipher*, Lecture Notes Computer Sci. **6715** (2011), 327 – 344.

[30] **Y. Zheng, T. Matsumoto, and H. Imai**, *On the construction of block ciphers provably secure and not relying on any unproved hypotheses*, Lecture Notes Computer Sci. **435**, (1990), 461 – 480.

Received February 26, 2014

A.Mileva
Faculty of Computer Science, University "Goce Delčev". "Krste Misirkov" bb, 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"
P.O.Box 393, 1000 Skopje, Republic of Macedonia
E-mail: smile.markovski@finki.ukim.mk