Math. Maced.
Vol. 8 (2010)
53-59

ON THE PROP RATIO TABLES OF EXTENDED FEISTEL NETWORKS AND THEIR QUASIGROUPS

ALEKSANDRA MILEVA AND SMILE MARKOVSKI

Dedicated to Academician Ǵorǵi Čupona

Abstract. The extended Feistel networks are defined elsewhere. Here we analyse the prop ratio tables of the extended Feistel networks and of the quasigroups produced by them. Since the prop ratio tables are used in differential cryptanalysis, the obtained results can be useful in designing suitable cryptographic primitives, when extended Feistel networks and quasigroups produced by them are used. One new classification of quasigroups, according to their prop ratio table properties, is given as well.

1. Introduction

Extended Feistel networks (EFNs) are introduced in [5] as one generalization of the Feistel networks, introduced by H. Feistel [4]. The name was unhappily chosen, because it has been already used by several authors for denoting the *type-1*, *type-2* and *type-3* Feistel networks (introduced by Zheng et al [9]). Here we use the meaning of the EFNs as it is defined in [5].

In this paper we give further analysis of the EFNs and of the quasigroups produced by them, and especially we consider the so called prop ratio tables. The prop ratio tables, introduced by Daemen [3], can be used in analyzing the resistance of some cryptographic primitives again differential cryptanalysis.

Differential cryptanalysis, introduced by E. Biham and A. Shamir [1], is a chosen plaintext attack/chosen ciphertext attack, because the attacker is able to choose pairs of plaintexts such that there is a specified difference ΔX between members of the pair. For any particular cipher, the plaintext pair difference must be carefully chosen, if the attack has to be successful. The attacker then trace a path of highly probable difference through all rounds of the cipher until the difference of the corresponding ciphertext pairs ΔY, termed a differential characteristic, has suitable value. The resulting pair of differences $(\Delta X, \Delta Y)$ is called a differential. In an ideally randomized cipher, the probability that a particular output difference ΔY occurs, given a particular input difference ΔX, is 2^{-n}, where n is the number of input bits. Statistics of the differentials can discover where the cipher

2000 *Mathematics Subject Classification.* Primary 20N05; Secondary 94A60.
Key words and phrases. extended Feistel networks, quasigroups, prop ratio tables.

exhibits non-random behaviour resulting with recovering of the secret key. Statistical properties of differentials depend upon the nature of non-linear components of the cryptographic primitive, usually S-boxes, so they must be examined.

Let a and a^* be n-dimensional binary vectors with bitwise difference $a \oplus a^* = a'$. Let $b = h(a), b^* = h(a^*)$ and $b' = b \oplus b^*$. Hence, the difference a' propagates to the difference b' through the mapping h and this difference propagation is denoted by $(a' \dashv h \vdash b')$. The *prop ratio* R_p of a difference propagation $(a' \dashv h \vdash b')$ is defined by

$$R_p(a' \dashv h \vdash b') = 2^{-n} \sum_a \delta(b' \oplus h(a \oplus a') \oplus h(a)).$$

where $\delta(w)$ is the real-valued function equal to 1 if w is the zero vector and 0 otherwise. The prop ratio ranges between 0 and 1.

Differential cryptanalysis attacks are possible if there are predictable difference propagations over all but a few rounds that have prop ratio significantly larger than 2^{1-n}, where n is the block length in the block ciphers [3]. To be resistant against this attack, necessary condition is that there are no differential trails with predicted prop ratio higher than 2^{1-n}.

2. Extended Feistel Networks

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

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

It is shown in [5, 6] that if f is a bijection, then $F_{A,B,C}$ is an orthomorphism of the group $(G^2, +)$. Inversion of an orthomorphism is again an orthomorphism. Even more, for the group $(\mathbb{Z}_2^n, \oplus_n)$, any composition of two extended Feistel networks is an orthomorphism, too. We generalize the last statement for any Abelian group by the following Proposition.

Proposition 2.1. *Let $(G, +)$ be an Abelian group, let $f, g : G \to G$ be bijections, $A, B, C, A', B', C' \in G$ and let $F_{A,B,C}, H_{A',B',C'} : G^2 \to G^2$ be extended Feistel networks of the group $(G^2, +)$, created by f and g respectfully. Then the composite function $H_{A',B',C'} \circ F_{A,B,C}$ is an orthomorphism on $(G^2, +)$ too.*

Proof. Let $\Phi = H_{A',B',C'} \circ F_{A,B,C} - I$, where I is the identity mapping. Then, for every $l, r \in G$, we have

$$\Phi(l, r) = (B + A' + f(r + C), A + B' + g(l + B + C' + f(r + C))).$$

Define the function $\Omega : G^2 \to G^2$ by

$$\Omega(l, r) = (g^{-1}(r - A - B') - l + A' - C', f^{-1}(l - A' - B) - C).$$

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

2.1. **Prop ratio tables of the extended Feistel networks over** $(\mathbb{Z}_2^n, \oplus_n)$**.** In this subsection we consider extended Feistel networks of the Abelian groups $(\mathbb{Z}_2^n, \oplus_n)$ and their prop ratios. Our first result is the following.

Proposition 2.2. *Let $F_{A,B,C} : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^{2n}$ be an extended Feistel network of the Abelian group $(\mathbb{Z}_2^{2n}, \oplus_{2n})$ created by a bijection $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. If the maximal prop ratio of f is smaller than 1, then the extended Feistel network $F_{A,B,C}$ is uniquely determined by the parameters A, B and C.*

Proof. Let $(A, B, C) \neq (A', B', C')$ and $F_{A,B,C} = F_{A',B',C'}$. Then $F_{A,B,C}(l, r) = (r \oplus_n A, l \oplus_n B \oplus_n f(r \oplus_n C)) = (r \oplus_n A', l \oplus_n B' \oplus_n f(r \oplus_n C')) = F_{A',B',C'}(l, r)$, for every $l, r \in \mathbb{Z}_2^n$. Consequently, we have $A = A'$ and $B \oplus_n B' = f(r \oplus_n C) \oplus_n f(r \oplus_n C') = K$, where K is a constant. $K \neq 0$, since $B = B'$ implies $C = C'$. Then $C \oplus_n C' = R$ is also a nonzero constant. So, for every t, where $t = r \oplus_n C$, we have $f(t) \oplus_n f(t \oplus_n R) = K$.

The last equation means that we must have a nontrivial difference propagation for our starting bijection f, that propagates with probability 1. In other words, we must have a nonzero input difference R that propagates to the output difference K with probability 1, i.e., the maximal prop ratio of the starting bijection is 1. □

Theorem 2.1. *Let $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be bijection such that $R_p(a \dashv f \vdash b) = 1$ only for $a = b = 0$, and let $F_{A,B,C} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by f. Then $R_p(a' \dashv F_{A,B,C} \vdash b') = 1$ if and only if $a' = (x, 0)$ and $b' = (0, x)$ for some $x \in \mathbb{Z}_2^k$.*

Proof. Let $b' = (b'_1, b'_2)$, $a' = (a'_1, a'_2)$, where $b'_1, b'_2, a'_1, a'_2 \in \mathbb{Z}_2^k$. Then we have:

$R_p(a' \dashv F_{A,B,C} \vdash b') = 1$

$\Leftrightarrow 2^{-2k} \sum_a \delta(b' \oplus_{2k} F_{A,B,C}(a \oplus_{2k} a') \oplus_{2k} F_{A,B,C}(a)) = 1$

$\Leftrightarrow \sum_a \delta(b' \oplus_{2k} F_{A,B,C}(a \oplus_{2k} a') \oplus_{2k} F_{A,B,C}(a)) = 2^{2k}$

$\Leftrightarrow \delta(b' \oplus_{2k} F_{A,B,C}(a \oplus_{2k} a') \oplus_{2k} F_{A,B,C}(a)) = 1 \ (\forall a \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow b' \oplus_{2k} F_{A,B,C}(a \oplus_{2k} a') \oplus_{2k} F_{A,B,C}(a) = 0 \ (\forall a \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} F_{A,B,C}((a_1, a_2) \oplus_{2k} (a'_1, a'_2)) \oplus_{2k} F_{A,B,C}(a_1, a_2) = 0 \ (\forall (a_1, a_2) \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} F_{A,B,C}(a_1 \oplus_k a'_1, a_2 \oplus_k a'_2) \oplus_{2k} F_{A,B,C}(a_1, a_2) = 0 \ (\forall (a_1, a_2) \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow b'_1 \oplus_k a_2 \oplus_k a'_2 \oplus_k A \oplus_k a_2 \oplus_k A = 0 \ \ \&$
$b'_2 \oplus_k a_1 \oplus_k a'_1 \oplus_k B \oplus_k f(a'_2 \oplus_k a_2 \oplus_k C) \oplus_k a_1 \oplus_k B \oplus_k f(a_2 \oplus_k C) = 0 \ (\forall a_1, a_2 \in \mathbb{Z}_2^k)$

$\Leftrightarrow b'_1 = a'_2 \ \ \& \ \ b'_2 \oplus_k a'_1 = f(a'_2 \oplus_k a_2 \oplus_k C) \oplus_k f(a_2 \oplus_k C) \ (\forall a_2 \in \mathbb{Z}_2^k)$.

Let put $a_2 = t \oplus_k C$. Then for every $t \in \mathbb{Z}_2^k$ we will have $b'_2 \oplus_k a'_1 = f(a'_2 \oplus_k t) \oplus_k f(t)$, i.e., $R_p(a'_2 \dashv f \vdash (b'_2 \oplus_k a'_1)) = 1$. It follows that $b'_1 = a'_2 = 0$ and $b'_2 = a'_1$. □

Corollary 2.1. *The prop ratio table of an extended Feistel network $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by a bijection $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ such that $R_p(a \dashv f \vdash b) = 1$ only for $a = b = 0$, has exactly 2^k ones.*

Theorem 2.2. *Let $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be a bijection such that $R_p(a \dashv f \vdash b) = 1$ only for $a = b = 0$, and let $F_{A,B,C} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by f. Then $R_p(a' \dashv F^2_{A,B,C} \vdash b') = 1$ if and only if $a' = b' = (0, 0)$.*

Proof. Let $b' = (b'_1, b'_2)$, $a' = (a'_1, a'_2)$, where $b'_1, b'_2, a'_1, a'_2 \in \mathbb{Z}_2^k$. Then we have (by avoiding some steps presented in the proof of Theorem 2.1):

$R_p(a' \dashv F^2_{A,B,C} \vdash b') = 1$

$\Leftrightarrow b' \oplus_{2k} F^2_{A,B,C}(a \oplus_{2k} a') \oplus_{2k} F^2_{A,B,C}(a) = 0 \ (\forall a \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} F^2_{A,B,C}((a_1, a_2) \oplus_{2k} (a'_1, a'_2)) \oplus_{2k} F^2_{A,B,C}(a_1, a_2) = 0 \ (\forall (a_1, a_2) \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} F^2_{A,B,C}(a_1 \oplus_k a'_1, a_2 \oplus_k a'_2) \oplus_{2k} F^2_{A,B,C}(a_1, a_2) = 0 \ (\forall (a_1, a_2) \in \mathbb{Z}_2^{2k})$

$\Leftrightarrow b'_1 \oplus_k a_1 \oplus_k a'_1 \oplus_k A \oplus_k B \oplus_k f(a'_2 \oplus_k a_2 \oplus_k C) \oplus_k a_1 \oplus_k A \oplus_k B \oplus_k f(a_2 \oplus_k C) = 0$
$\&\ b'_2 \oplus_k a_2 \oplus_k a'_2 \oplus_k A \oplus_k B \oplus_k f(a_1 \oplus_k a'_1 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a'_2 \oplus_k C)) \oplus_k a_2 \oplus_k A \oplus_k B \oplus_k f(a_1 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k C)) = 0 \ (\forall a_1, a_2 \in \mathbb{Z}_2^k)$

$\Leftrightarrow b'_1 \oplus_k a'_1 = f(a'_2 \oplus_k a_2 \oplus_k C) \oplus_k f(a_2 \oplus_k C) \ \ \&$
$b'_2 \oplus_k a'_2 = f(a_1 \oplus_k a'_1 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a'_2 \oplus_k C)) \oplus_k f(a_1 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k C)) \ (\forall a_1, a_2 \in \mathbb{Z}_2^k)$.

Let put $a_2 = t \oplus_k C$. Then for every $t \in \mathbb{Z}_2^k$ we have $b'_1 \oplus_k a'_1 = f(a'_2 \oplus_k t) \oplus_k f(t)$, which means $R_p(a'_2 \dashv f \vdash (b'_1 \oplus_k a'_1)) = 1$. So, $a'_2 = 0$ and $b'_1 = a'_1$. Now, from the second equality we have $b'_2 = f(a_1 \oplus_k a'_1 \oplus_k B \oplus_k C \oplus_k f(t)) \oplus_k f(a_1 \oplus_k B \oplus_k C \oplus_k f(t))$, for every $a_1, t \in \mathbb{Z}_2^k$. Let put $a_1 = r \oplus_k B \oplus_k C \oplus_k f(t)$. Then for every $r \in \mathbb{Z}_2^k$ we have $b'_2 = f(a'_1 \oplus_k r) \oplus_k f(r)$, i.e., $R_p(a'_1 \dashv f \vdash b'_2) = 1$. It follows that $a'_2 = 0$ and $b'_1 = a'_1 = b'_2 = 0$. □

The previous theorems show that the maximal prop ratio of $F^2_{A,B,C}$ is smaller than the maximal prop ratio of $F_{A,B,C}$ (which is equal to 1). Consequently, for getting higher resistance again differential cryptanalysis it should be used $F^2_{A,B,C}$, and then the price is paid by smaller efficiency.

3. Quasigroups by extended Feistel networks over $(\mathbb{Z}_2^n, \oplus_n)$

Let $(G,+)$ be an abelian group, let $f : G \to G$ be a bijection and let $F_{A,B,C}$ be an extended Feistel network created by f ($F_{A,B,C}$ is an orthomorphism of the group $(G^2,+)$). One can construct quasigroup $(G^2,\bullet)$ by using Sade's diagonal method [8] as a base [5, 6]. For all $X,Y \in G^2$, the quasigroup operation $\bullet$ is defined by

$$X \bullet Y = F_{A,B,C}(X - Y) + Y.$$

In the sequel we examine only Abelian group $(\mathbb{Z}_2^n, \oplus_n)$. We give the shape of prop ratio tables of the quasigroups produced by extended Feistel networks $F_{A,B,C}$ and $F^2_{A,B,C}$.

Theorem 3.1. *Let $Q_{F_{A,B,C}} : \mathbb{Z}_2^{4k} \to \mathbb{Z}_2^{2k}$ be a quasigroup generated by the extended Feistel network $F_{A,B,C} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by the bijection $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ such that $R_p(a \dashv f \vdash b) = 1$ only for $a = b = 0$. We have $R_p(a' \dashv Q_{F_{A,B,C}} \vdash b') = 1$ if and only if $a' = (x,y,z,y)$ and $b' = (z, x \oplus_k y \oplus_k z)$, for some $x,y,z \in \mathbb{Z}_2^k$.*

Proof. Let $b' = (b'_1, b'_2)$, $a' = (a'_1, a'_2, a'_3, a'_4)$, where $b'_1, b'_2, a'_1, a'_2, a'_3, a'_4 \in \mathbb{Z}_2^k$. Then we have (by avoiding some steps presented in the proof of Theorem 2.1):

$R_p(a' \dashv Q_{F_{A,B,C}} \vdash b') = 1$

$\Leftrightarrow b' \oplus_{2k} Q_{F_{A,B,C}}(a \oplus_{4k} a') \oplus_{2k} Q_{F_{A,B,C}}(a) = 0 \ (\forall a \in \mathbb{Z}_2^{4k})$

$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} Q_{F_{A,B,C}}(a_1 \oplus_k a'_1, a_2 \oplus_k a'_2, a_3 \oplus_k a'_3, a_4 \oplus_k a'_4) \oplus_{2k}$
$Q_{F_{A,B,C}}(a_1, a_2, a_3, a_4) = 0 \ (\forall a_1, a_2, a_3, a_4 \in \mathbb{Z}_2^k)$

$\Leftrightarrow b'_1 \oplus_k a_2 \oplus_k a'_2 \oplus_k a_3 \oplus_k a'_3 \oplus_k a_4 \oplus_k a'_4 \oplus_k A \oplus_k a_2 \oplus_k a_3 \oplus_k a_4 \oplus_k A = 0$ &
$b'_2 \oplus_k a_1 \oplus_k a'_1 \oplus_k a_3 \oplus_k a'_3 \oplus_k a_4 \oplus_k a'_4 \oplus_k B \oplus_k f(a'_2 \oplus_k a_2 \oplus_k a'_4 \oplus_k a_4 \oplus_k C) \oplus_k$
$a_1 \oplus_k a_3 \oplus_k a_4 \oplus_k B \oplus_k f(a_2 \oplus_k a_4 \oplus_k C) = 0 \ (\forall a_1, a_2, a_3, a_4 \in \mathbb{Z}_2^k)$

$\Leftrightarrow b'_1 = a'_2 \oplus_k a'_3 \oplus_k a'_4$ &

$b'_2 \oplus_k a'_1 \oplus_k a'_3 \oplus_k a'_4 = f(a'_2 \oplus_k a_2 \oplus_k a'_4 \oplus_k a_4 \oplus_k C) \oplus_k f(a_2 \oplus_k a_4 \oplus_k C) \ (\forall a_2, a_4 \in \mathbb{Z}_2^k)$.

It follows that $b'_1 = a'_2 \oplus_k a'_3 \oplus_k a'_4$ and, by putting $a_2 \oplus_k a_4 = t \oplus_k C$, we obtain $b'_2 \oplus_k a'_1 \oplus_k a'_3 \oplus_k a'_4 = f(a'_2 \oplus_k a'_4 \oplus_k t) \oplus_k f(t)$, for every $t \in \mathbb{Z}_2^k$. This means $R_p((a'_2 \oplus_k a'_4) \dashv f \vdash (b'_2 \oplus_k a'_1 \oplus_k a'_3 \oplus_k a'_4)) = 1$, implying $a'_2 = a'_4$ and $b'_2 = a'_1 \oplus_k a'_3 \oplus_k a'_4$. Hence, $a' = (x,y,z,y)$ and $b' = (z, x \oplus_k y \oplus_k z)$ for some $x,y,z \in \mathbb{Z}_2^k$. □

According to obtained prop ratio tables, quasigroups can be classified as:

1. *non-restricted quasigroups* - when all nontrivial difference propagations are of prop ratio 1
2. *weak restricted quasigroups* - when at least one nontrivial difference propagation is of prop ratio 1 and at least one nontrivial difference propagation is of prop ratio smaller than 1
3. *restricted quasigroups* - when there is no nontrivial difference propagations of prop ratio 1.

Corollary 3.1. *Extended Feistel network* $F_{A,B,C} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ *of the group* $(\mathbb{Z}_2^{2k}, \oplus_{2k})$*, created by the bijection* $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ *such that* $R_p(a \dashv f \vdash b) = 1$ *only for* $a = b = 0$*, produces weak restricted quasigroups and, even more, its prop ratio table has* 2^{3k} *ones.*

The interpretation of the last corollary tell us that for exactly 2^{3k} input differences we can predict the proper output difference with probability 1. This is very useful for differential cryptanalysis, so we should not use this kind of quasigroups standalone. As alternative, we have to use better quasigroups, or to use these quasigroups in some quasigroup transformations.

Theorem 3.2. *Let* $Q_{F^2_{A,B,C}} : \mathbb{Z}_2^{4k} \to \mathbb{Z}_2^{2k}$ *be a quasigroup generated by the extended Feistel network* $F_{A,B,C} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ *of the group* $(\mathbb{Z}_2^{2k}, \oplus_{2k})$*, created by the bijection* $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ *such that* $R_p(a \dashv f \vdash b) = 1$ *only for* $a = b = 0$*. We have* $R_p(a' \dashv Q_{F^2_{A,B,C}} \vdash b') = 1$ *if and only if* $a' = (x, y, x, y)$ *and* $b' = (x, y)$*, for some* $x, y \in \mathbb{Z}_2^k$*.*

Proof. Let $b' = (b'_1, b'_2)$, $a' = (a'_1, a'_2, a'_3, a'_4)$, where $b'_1, b'_2, a'_1, a'_2, a'_3, a'_4 \in \mathbb{Z}_2^k$. Then we have (by avoiding some steps presented in the proof of Theorem 2.1):

$$R_p(a' \dashv Q_{F^2_{A,B,C}} \vdash b') = 1$$

$$\Leftrightarrow (b'_1, b'_2) \oplus_{2k} Q_{F^2_{A,B,C}}(a_1 \oplus_k a'_1, a_2 \oplus_k a'_2, a_3 \oplus_k a'_3, a_4 \oplus_k a'_4) \oplus_{2k} Q_{F^2_{A,B,C}}(a_1, a_2, a_3, a_4) = 0 \ (\forall a_1, a_2, a_3, a_4 \in \mathbb{Z}_2^k)$$

$$\Leftrightarrow b'_1 \oplus_k a_1 \oplus_k a'_1 \oplus_k A \oplus_k B \oplus_k f(a_2 \oplus_k a'_2 \oplus_k a_4 \oplus_k a'_4 \oplus_k C) \oplus_k a_1 \oplus_k A \oplus_k B \oplus_k f(a_2 \oplus_k a_4 \oplus_k C) = 0 \quad \& \quad b'_2 \oplus_k a_2 \oplus_k a'_2 \oplus_k A \oplus_k B \oplus_k f(a_1 \oplus_k a'_1 \oplus_k a_3 \oplus_k a'_3 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a'_2 \oplus_k a_4 \oplus_k a'_4 \oplus_k C)) \oplus_k a_2 \oplus_k A \oplus_k B \oplus_k f(a_1 \oplus_k a_3 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a_4 \oplus_k C)) = 0 \ (\forall a_1, a_2, a_3, a_4 \in \mathbb{Z}_2^k)$$

$$\Leftrightarrow b'_1 \oplus_k a'_1 = f(a_2 \oplus_k a'_2 \oplus_k a_4 \oplus_k a'_4 \oplus_k C) \oplus_k f(a_2 \oplus_k a_4 \oplus_k C) \quad \& \quad b'_2 \oplus_k a'_2 = f(a_1 \oplus_k a'_1 \oplus_k a_3 \oplus_k a'_3 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a'_2 \oplus_k a_4 \oplus_k a'_4 \oplus_k C)) \oplus_k f(a_1 \oplus_k a_3 \oplus_k B \oplus_k C \oplus_k f(a_2 \oplus_k a_4 \oplus_k C)) \ (\forall a_1, a_2, a_3, a_4 \in \mathbb{Z}_2^k)$$

Let put $a_2 \oplus_k a_4 = t \oplus_k C$. Then for every $t \in \mathbb{Z}_2^k$ we have $b'_1 \oplus_k a'_1 = f(a'_2 \oplus_k a'_4 \oplus_k t) \oplus_k f(t)$, which means $R_p((a'_2 \oplus_k a'_4) \dashv f \vdash (b'_1 \oplus_k a'_1)) = 1$. So, $a'_2 = a'_4$ and $b'_1 = a'_1$. Now, from the second equality we have $b'_2 \oplus_k a'_2 = f(a_1 \oplus_k a'_1 \oplus_k a_3 \oplus_k a'_3 \oplus_k B \oplus_k C \oplus_k f(t)) \oplus_k f(a_1 \oplus_k a_3 \oplus_k B \oplus_k C \oplus_k f(t))$ for

every $a_1, a_2, t \in \mathbb{Z}_2^k$. Putting $a_1 \oplus_k a_3 = r \oplus_k B \oplus_k C \oplus_k f(t)$, we get $b'_2 \oplus_k a'_2 = f(r \oplus_k a'_1 \oplus_k a'_3) \oplus_k f(r)$ for every $t \in \mathbb{Z}_2^k$, i.e., $R_p((a'_1 \oplus_k a'_3) \dashv f \vdash (b'_2 \oplus_k a'_2)) = 1$. Then, altogether, we obtain $a'_2 = a'_4$ and $b'_1 = a'_1$ and $a'_1 = a'_3$ and $b'_2 = a'_2$, which means that $a' = (x, y, x, y)$ and $b' = (x, y)$ for some $x, y \in \mathbb{Z}_2^k$. □

Corollary 3.2. *Extended Feistel network $F^2_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by the bijection $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ such that $R_p(a \dashv f \vdash b) = 1$ only for $a = b = 0$, produces weak restricted quasigroups and, even more, its prop ratio table contains 2^{2k} ones.*

Quasigroup produced by $F^2_{a,b,c}$ have better prop ratio tables than those produced by $F_{a,b,c}$, but still we have that 2^{2k} input differences propagate to the proper output difference with probability 1. They are also not suitable for building cryptographic primitives as they are, so some additional transformations should be applied, if we choose to use them.

References

[1] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Advances in Cryptology, EUROCRYPT 1990, pp. 2–21.

[2] J. Daemen, R. Govaerts and J. Vandewalle, *Correlation matrices*, FSE 1994, LNCS **1008**, (1995), 275 – 285.

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

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

[5] S. Markovski and A. Mileva, *Generating huge quasigroups from small non-linear bijections via extended Feistel function*, Quasigroups and Related Systems, **17(1)** (2009), 91 – 106.

[6] A. Mileva, *Cryptographic primitives with quasigroup string transformations*, PhD thesis, University "Ss Cyril and Methodious" - Skopje, 2010.

[7] A. Mileva, S. Markovski, *Quasigroup String Transformations and Hash Function Design. A Case Study: The NaSHA Hash Function*, In D. Davcev and J. M. Gómez, editor, ICT Innovations 2009, (2009), 367–376.

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

[9] Y. Zheng, T. Matsumoto, and H. Imai, *On the construction of block ciphers provably secure and not relying on any unproved hypotheses*, CRYPTO 1989, LNCS **435**, (1990), 461–480.

Faculty of Informatics, "Goce Delčev" University, Štip, Republic of Macedonia
E-mail address: aleksandra.mileva@ugd.edu.mk

Institut of Informatics, Faculty of Natural Science,
"Ss Cyril and Methodious" University, Skopje, Republic of Macedonia
E-mail address: smile@ii.edu.mk