

# On some Constructions of Shapeless Quasigroups

Aleksandra Mileva<sup>1</sup> and Smile Markovski<sup>2</sup>

<sup>1</sup> Faculty of Computer Science,  
University "Goce Delčev", Štip

<sup>2</sup> Faculty of Computer Science and Computer Engineering,  
University "Ss. Cyril and Methodius" - Skopje  
Republic of Macedonia

Loops'11

July 25-27, Třešt, Czech Republic

## Motivation

Today, we can already speak about quasigroup based cryptography, because the number of new defined cryptographic primitives that use quasigroups is growing up:

- stream cipher EDON-80 (**Gligoroski et al. (eSTREAM 2008)**),
- hash functions EDON-R (**Gligoroski et al. (SHA-3 2008)**) and NaSHA (**Markovski and Mileva (SHA-3 2008)**),
- digital signature algorithm MQQ-DSA (**Gligoroski et al. (ACAM 2008)**),
- public key cryptosystem LQLP- $s$  (for  $s \in \{104, 128, 160\}$ ) (**Markovski et al. (SCC 2010)**), etc.

## Motivation

Different authors seek quasigroups with different properties.

### Definition (Gligoroski et al (2006))

A 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

$$\underbrace{x * (x \cdots * (x * y))}_k = y, \quad y = ((y * x) * \cdots * x) * x \quad (1)$$

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$
- 3 Different generalizations of the Feistel Network as orthomorphisms
- 4 Some constructions of shapeless quasigroups
- 5 Conclusions

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$
- 3 Different generalizations of the Feistel Network as orthomorphisms
- 4 Some constructions of shapeless quasigroups
- 5 Conclusions

## Complete mappings and orthomorphisms

Definition (Mann (1949), Johnson et al (1961), Evans (1989))

A **complete mapping** of a quasigroup (group)  $(G, +)$  is a permutation  $\phi : G \rightarrow G$  such that the mapping  $\theta : G \rightarrow G$  defined by  $\theta(x) = x + \phi(x)$  ( $\theta = I + \phi$ , where  $I$  is the identity mapping) is again a permutation of  $G$ . The mapping  $\theta$  is the **orthomorphism** associated to the complete mapping  $\phi$ . A quasigroup (group)  $G$  is **admissible** if there is a complete mapping  $\phi : G \rightarrow G$ .

## Complete mappings and orthomorphisms

- If  $\theta$  is the orthomorphism associated to the complete mapping  $\phi$ , then  $-\phi$  is the orthomorphism associated to the complete mapping  $-\theta$ ,
- The inverse of the complete mapping (orthomorphism) is also a complete mapping (orthomorphism) (**Johnson et al (1961)**),
- Two orthomorphisms  $\theta_1$  and  $\theta_2$  of  $G$  are said to be orthogonal if and only if  $\theta_1\theta_2^{-1}$  is an orthomorphism of  $G$  too.
- Even more, every orthomorphism is orthogonal to  $I$  and  $\theta^{-1}$  is orthogonal to  $\theta$  if and only if  $\theta^2$  is an orthomorphism (**Johnson et al (1961)**)

## Sade's Diagonal method

**(Sade (1957))** Consider the group  $(\mathbb{Z}_n, +)$  and let  $\theta$  be a permutation of the set  $\mathbb{Z}_n$ , such that  $\phi(x) = x - \theta(x)$  is also a permutation. Define an operation  $\circ$  on  $\mathbb{Z}_n$  by:

$$x \circ y = \theta(x - y) + y \quad (2)$$

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  $\theta$ ).



## Generalization

### Theorem

Let  $\phi$  be a complete mapping of the admissible group  $(G, +)$  and let  $\theta$  be an orthomorphism associated to  $\phi$ . Define operations  $\circ$  and  $\bullet$  on  $G$  by

$$x \circ y = \phi(y - x) + y = \theta(y - x) + x, \quad (3)$$

$$x \bullet y = \theta(x - y) + y = \phi(x - y) + x, \quad (4)$$

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  $x, y \in G$ .

## Quasigroup conjugates

### Theorem

Let  $\phi : G \rightarrow G$  be a complete mapping of the abelian group  $(G, +)$  with associated orthomorphism  $\theta : G \rightarrow G$ . Then all the conjugates of the quasigroup  $(G, \bullet)$  can be obtained by the equation (4) and the following statements are true.

- The quasigroup  $(G, /)$  is derived by the orthomorphism  $\theta^{-1}$  associated to the complete mapping  $-\phi\theta^{-1}$ .
- The quasigroup  $(G, \backslash)$  is derived by the orthomorphism  $-\theta(-\phi)^{-1}$  associated to the complete mapping  $-\phi^{-1}$ .
- The quasigroup  $(G, //)$  is derived by the orthomorphism  $-\phi(-\theta)^{-1}$  associated to the complete mapping  $(-\theta)^{-1}$ .
- The quasigroup  $(G, \backslash\backslash)$  is derived by the orthomorphism  $-\phi^{-1}$  associated to the complete mapping  $-\theta\phi^{-1}$ .
- $(G, \cdot) = (G, \circ)$ .

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$**
- 3 Different generalizations of the Feistel Network as orthomorphisms
- 4 Some constructions of shapeless quasigroups
- 5 Conclusions

## Algebraic properties of the quasigroup $(G, \bullet)$

- If  $\theta(0) \neq 0$  then the quasigroup  $(G, \bullet)$  has no idempotent elements.
- $(G, \bullet)$  does not have a left unit and if  $\theta$  is different to the identity mapping it does not have a right unit either.
- $(G, \bullet)$  is non-associative quasigroup.
- If  $\theta(z) - \theta(-z) \neq z$  for some  $z \in G$  then  $(G, \bullet)$  is non-commutative quasigroup.

# Algebraic properties of the quasigroup $(G, \bullet)$

- The identity

$$y = ((y \bullet x) \bullet \dots) \bullet x$$

$\underbrace{\hspace{10em}}_I$

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

- The identity

$$x \bullet (\dots \bullet (x \bullet y)) = y$$

$\underbrace{\hspace{10em}}_I$

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

## Algebraic properties of the quasigroup $(G, \bullet)$

- If  $\theta$  has a cycle containing 0 of length greater than  $|G|/2$ , then the quasigroup  $(G, \bullet)$  cannot have a proper subquasigroup.
- The quasigroup  $(G, \bullet)$  is without a proper subquasigroup if  $|S| \geq |G|/2$ , where

$$S = \bigcup_{i=1}^{i=p+1} \{\theta^i(0)\} \cup \bigcup_{i=1}^{i=p+1} \{\theta(0) + \theta^i(0)\} \cup \bigcup_{i=1}^{i=p+1} \{\theta(-\theta^i(0)) + \theta^i(0)\} \cup$$

$$\bigcup_{i=1}^{i=p+1} \{\lambda^i(0)\} \cup \bigcup_{i=1}^{i=p+1} \{\lambda(0) + \lambda^i(0)\} \cup \bigcup_{i=1}^{i=p+1} \{\lambda(-\lambda^i(0)) + \lambda^i(0)\},$$

$$p = \lfloor |G|/2 \rfloor \text{ and } \lambda = -\theta(-\phi)^{-1}.$$

# Algebraic properties of the quasigroup $(G, \bullet)$

$$((x \bullet x) \bullet \dots) \bullet x = \theta^l(0) + x, \quad x \bullet (\dots \bullet (x \bullet x)) = -(-\phi)^l(0) + x. \quad (5)$$

$$((x/x)/\dots)/x = (\theta^{-1})^l(0) + x, \quad x/(\dots(x/x)) = -(\phi\theta^{-1})^l(0) + x, \quad (6)$$

$$((x \setminus x) \setminus \dots) \setminus x = (-\theta(-\phi)^{-1})^l(0) + x, \quad x \setminus (\dots \setminus (x \setminus x)) = -((-\phi)^{-1})^l(0) + x, \quad (7)$$

$$((x // x) // \dots) // x = (-\phi(-\theta)^{-1})^l(0) + x, \quad x // (\dots // (x // x)) = -(-(-\theta)^{-1})^l(0) + x, \quad (8)$$

$$((x \backslash\backslash x) \backslash\backslash \dots) \backslash\backslash x = (-\phi^{-1})^l(0) + x, \quad x \backslash\backslash (\dots \backslash\backslash (x \backslash\backslash x)) = -(\theta\phi^{-1})^l(0) + x. \quad (9)$$

## $(G, \bullet)$ as an shapeless quasigroup

### Theorem

Let  $\theta$  be an orthomorphism of the abelian group  $(G, +)$ , and let  $(G, \bullet)$  be a quasigroup derived by  $\theta$  by the equation (4). If  $\theta$  is with the following properties:

- a)  $\theta(0) \neq 0$
  - b)  $\theta^k \neq I$  for all  $k < 2|G|$
  - c)  $(I - \theta)^k \neq I$  for all  $k < 2|G|$
  - d)  $\theta(Z) - \theta(-Z) \neq Z$  for some  $Z \in G$
  - e)  $|S| \geq |G|/2$ ,
- then  $(G, \bullet)$  is a shapeless quasigroup.



## Example of a shapeless quasigroup

The abelian group  $(\mathbb{Z}_2^4, \oplus)$  is given.

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

We define the quasigroup operation as

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

# Example of a shapeless quasigroup

$\bullet$	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

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$
- 3 Different generalizations of the Feistel Network as orthomorphisms**
- 4 Some constructions of shapeless quasigroups
- 5 Conclusions

## Different generalizations of the Feistel Network

Feistel Networks are introduced by H. Feistel (Scientific American, 1973).

- Parameterized Feistel Network (PFN) (**Markovski and Mileva (QRS 2009)**),
- Extended Feistel networks *type-1*, *type-2* and *type-3* (**Zheng et al (CRYPTO 1989)**),
- Generalized Feistel-Non Linear Feedback Shift Register (GF-NLFSR) (**Choy et al (ACISP 2009)**).

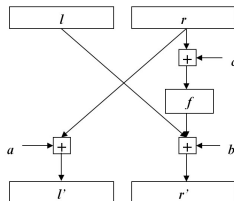
We will redefine the last two generalizations with parameters and over abelian groups.

# Parameterized Feistel Network (PFN)

## Definition

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

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



## Parameterized Feistel Network (PFN)

In **(Markovski and Mileva (QRS 2009))** is shown that if starting mapping  $f$  is bijection, the Parameterized Feistel Network  $F_{A,B,C}$  and its square  $F_{A,B,C}^2$  are orthomorphisms of the group  $(G^2, +)$ . More over, they are orthogonal orthomorphisms.

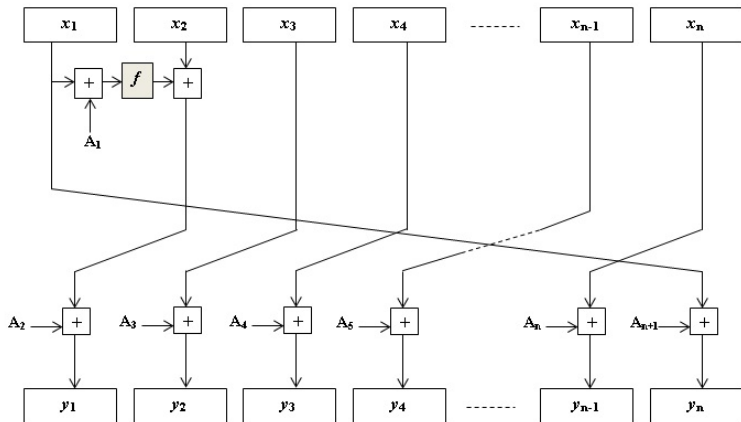
# Parameterized Extended Feistel Network (PEFN) *type-1*

## Definition

Let  $(G, +)$  be an abelian group, let  $f : G \rightarrow G$  be a mapping, let  $A_1, A_2, \dots, A_{n+1} \in G$  are constants and let  $n > 1$  be an integer. The **Parameterized Extended Feistel Network (PEFN) type-1**  $F_{A_1, A_2, \dots, A_{n+1}} : G^n \rightarrow G^n$  created by  $f$  is defined for every  $(x_1, x_2, \dots, x_n) \in G^n$  by

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

# Parameterized Extended Feistel Network (PEFN) *type-1*





# Parameterized Extended Feistel Network (PEFN) *type-1*

## Theorem

*Let  $(G, +)$  be an abelian group, let  $n > 1$  be an integer and  $A_1, A_2, \dots, A_{n+1} \in G$ . If  $F_{A_1, A_2, \dots, A_{n+1}} : G^n \rightarrow G^n$  is a PEFN type-1 created by a bijection  $f : G \rightarrow G$ , then  $F_{A_1, A_2, \dots, A_{n+1}}$  is an orthomorphism of the group  $(G^n, +)$ .*

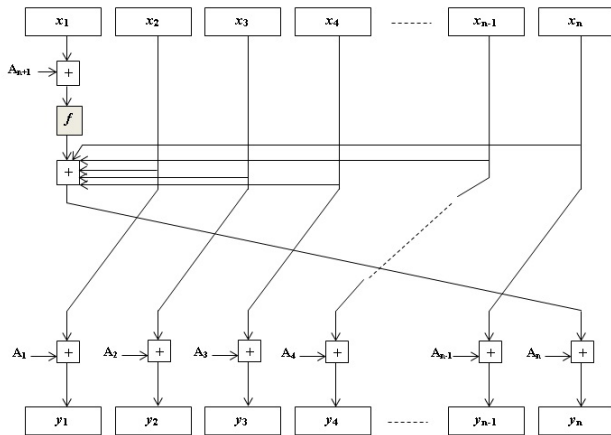
# Parameterized Generalized Feistel-Non Linear Feedback Shift Register (PGF-NLFSR)

## Definition

Let  $(G, +)$  be an abelian group, let  $f : G \rightarrow G$  be a mapping, let  $A_1, A_2, \dots, A_{n+1} \in G$  be constants and let  $n > 1$  be an integer. The **Parameterized Generalized Feistel-Non Linear Feedback Shift Register (PGF-NLFSR)**  $F_{A_1, A_2, \dots, A_{n+1}} : G^n \rightarrow G^n$  created by  $f$  is defined for every  $(x_1, x_2, \dots, x_n) \in G^n$  by

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

# Parameterized Generalized Feistel-Non Linear Feedback Shift Register (PGF-NLFSR)



# Parameterized Generalized Feistel-Non Linear Feedback Shift Register (PGF-NLFSR)

## Theorem

Let us use the abelian group  $(\mathbb{Z}_2^m, \oplus)$ , let  $n = 2k$  be an integer and  $A_1, A_2, \dots, A_{n+1} \in \mathbb{Z}_2^m$ . If  $F_{A_1, A_2, \dots, A_{n+1}} : (\mathbb{Z}_2^m)^n \rightarrow (\mathbb{Z}_2^m)^n$  is a PGF-NLFSR created by a bijection  $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ , then  $F_{A_1, A_2, \dots, A_{n+1}}$  is an orthomorphism of the group  $((\mathbb{Z}_2^m)^n, \oplus)$ .

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$
- 3 Different generalizations of the Feistel Network as orthomorphisms
- 4 Some constructions of shapeless quasigroups**
- 5 Conclusions

## Quasigroups derived by the PFN $F_{A,B,C}$

### Proposition

Let  $(G, +)$  be an abelian group and let  $f : G \rightarrow G$  be a bijection. Let  $F_{A,B,C}$  be a Parameterized Feistel Network created by  $f$ , and let  $(G^2, \bullet)$  be a quasigroup derived by  $F_{A,B,C}$  by the equation (4). If  $F_{A,B,C}$  is with the following properties:

- a)  $A \neq 0$  or  $B \neq -f(C)$
- b)  $F_{A,B,C}^k \neq I$  for all  $k < 2|G^2|$
- c)  $(I - F_{A,B,C})^k \neq I$  for all  $k < 2|G^2|$
- d)  $|S| \geq |G^2|/2$ ,

then  $(G^2, \bullet)$  is a shapeless quasigroup.

## Quasigroups derived by the PFN $F_{A,B,C}$

We made a m-file in MatLab that produce a starting bijection  $f : Z_2^n \rightarrow Z_2^n$  and parameters  $A, B$  and  $C$  for the orthomorphism PFN  $F_{A,B,C}$  which produce a shapeless quasigroup. The group operation is XOR. For  $n = 3, 4, 5, 6$  execution time is less than a minute and for  $n = 7$  is less than five minutes. These results correspond to shapeless quasigroups of order  $2^6, 2^8, 2^{10}, 2^{12}$  and  $2^{14}$ .

# Quasigroups derived by the PEFN *type-1* $F_{A_1, A_2, \dots, A_{n+1}}$

## Proposition

Let  $(G, +)$  be an abelian group, let  $n > 1$  be an integer, let  $A_1, A_2, \dots, A_{n+1} \in G$  and let  $f : G \rightarrow G$  be a bijection. Let  $F_{A_1, A_2, \dots, A_{n+1}}$  be a PEFN *type-1* created by  $f$ , and let  $(G^n, \bullet)$  be a quasigroup derived by  $F_{A_1, A_2, \dots, A_{n+1}}$  by the equation (4). If  $F_{A_1, A_2, \dots, A_{n+1}}$  is with the following properties:

- a)  $A_i \neq 0$  for some  $i \in \{3, 4, \dots, n+1\}$  or  $A_2 \neq -f(A_1)$
- b)  $F_{A_1, A_2, \dots, A_{n+1}}^k \neq I$  for all  $k < 2|G^n|$
- c)  $(I - F_{A_1, A_2, \dots, A_{n+1}})^k \neq I$  for all  $k < 2|G^n|$
- d)  $|S| \geq |G^n|/2$ ,

then  $(G^n, \bullet)$  is a shapeless quasigroup.



## Quasigroups derived by the PGF-NLFSR $F_{A_1, A_2, \dots, A_{n+1}}$

### Proposition

Let us use the abelian group  $(\mathbb{Z}_2^m, \oplus)$ , let  $n = 2k$  be an integer, let  $A_1, A_2, \dots, A_{n+1} \in \mathbb{Z}_2^m$  and let  $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$  be a bijection. Let  $F_{A_1, A_2, \dots, A_{n+1}}$  be a PGF-NLFSR created by  $f$ , and let  $((\mathbb{Z}_2^m)^n, \bullet)$  be a quasigroup derived by  $F_{A_1, A_2, \dots, A_{n+1}}$  by the equation (4). If  $F_{A_1, A_2, \dots, A_{n+1}}$  is with the following properties:

- $A_i \neq 0$  for some  $i \in \{1, 2, \dots, n-1\}$  or  $A_n \neq -f(A_{n+1})$
- $F_{A_1, A_2, \dots, A_{n+1}}^k \neq I$  for all  $k < 2|G^n|$
- $(I - F_{A_1, A_2, \dots, A_{n+1}})^k \neq I$  for all  $k < 2|G^n|$
- $|S| \geq |G^n|/2$ ,

then  $((\mathbb{Z}_2^m)^n, \bullet)$  is a shapeless quasigroup.

- 1 Diagonal method and orthomorphisms
- 2 Algebraic properties of the quasigroup  $(G, \bullet)$
- 3 Different generalizations of the Feistel Network as orthomorphisms
- 4 Some constructions of shapeless quasigroups
- 5 Conclusions

## Conclusions

We give some constructions of shapeless quasigroups of different orders by using quasigroups produced by diagonal method from orthomorphisms. We show that PEFN *type-1* produced by a bijection is an orthomorphism of the abelian group  $(G^n, +)$  and that PGF-NLFSR produced by a bijection is an orthomorphism of the  $((\mathbb{Z}_2^m)^n, \oplus)$ . Also, we parameterized these orthomorphisms for the need of cryptography, so we can work with different quasigroups in every iterations of the future cryptographic primitives.

THANKS  
FOR  
YOUR ATTENTION!!!