Quasigroup String Transformations and Block Cipher Design

Aleksandra Mileva[1]
joint work with Smile Markovski[2] and Vesna Dimitrova[2]

[1] Faculty of Computer Science and Information Technology,
University "Goce Delčev", Štip
[2] Faculty of Natural Science, University "Ss. Cyril and Methodius" - Skopje
Republic of Macedonia

10th Central European Conference on Cryptology
Juny 10-12, Będlewo, Poland

Motivation

In the recent years, several cryptographic designs based on quasigroups, are introduced:

- stream cipher EDON-80 (**Gligoroski et al. (eSTREAM 08)**),
- hash functions EDON-R (**Gligoroski et al. (SHA-3 08)**) and NaSHA (**Markovski and Mileva (SHA-3 08)**),
- digital signature algorithm MQQ-DSA (**Gligoroski et al. (ACAM 08)**),
- public key cryptosystem LQLP-s (for $s \in \{104, 128, 160\}$) (**Markovski et al. (SCC 10)**), etc.

Motivation

- Little work is done for deployment of the quasigroups and quasigroup string transformations in the field of the block ciphers.
- **Carter et al. (SAC 95)**
  DESV - a version of DES in which XOR is replaced by an arbitrary quasigroup operation defined by a Latin square.

Quasigroup string transformations

Definition

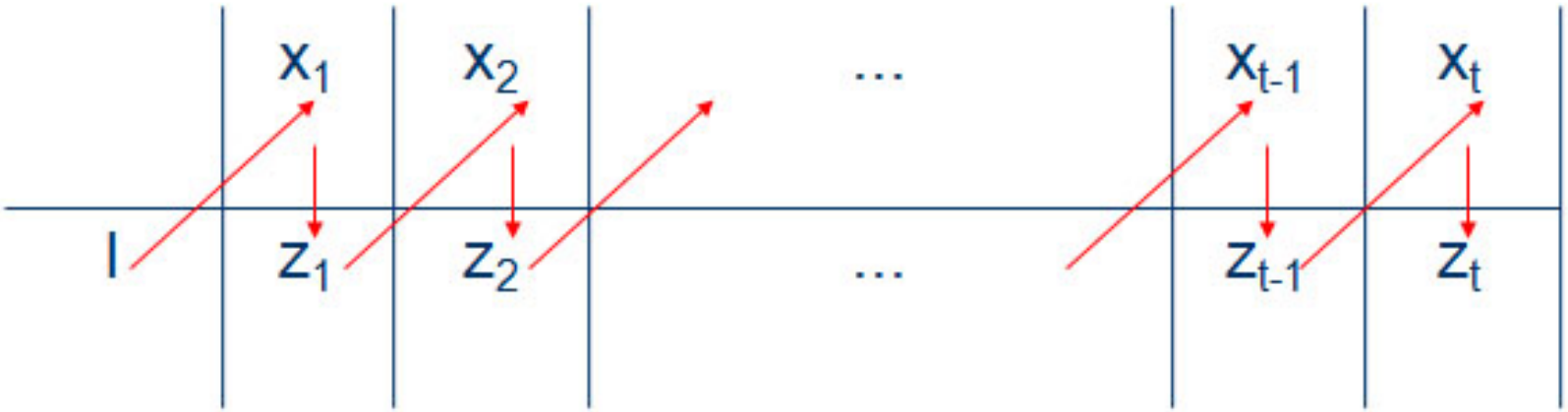
A quasigroup $(Q, *)$ is a groupoid, i.e., a pair of nonempty set Q and a binary operation $*$, such that for all $a, b \in Q$ there exist unique $x, y \in Q$ satisfying the equalities $a * x = b$ and $y * a = b$.

Quasigroup string transformations

Given a finite quasigroup $(Q, *)$, consider the set Q as an alphabet with word set $Q^+ = \{x_1 x_2 \dots x_t \mid x_i \in Q, t \geq 1\}$. For fixed letter $l \in Q$ (called a leader) the following transformations are defined:

Markovski et al. (LIRA 97)

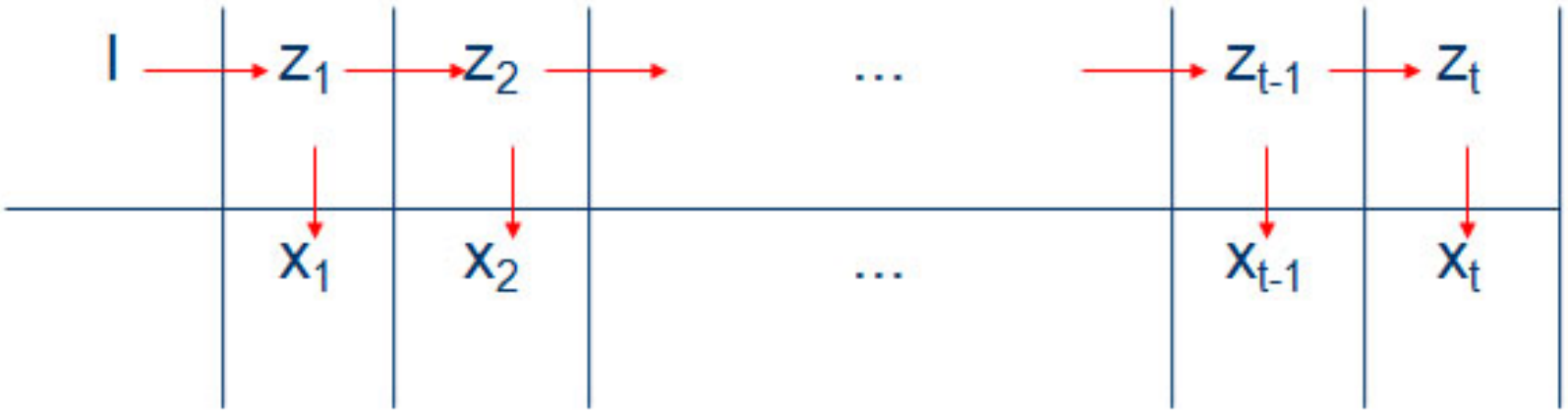
$$e_l(x_1 \dots x_t) = (z_1 \dots z_t) \Leftrightarrow z_j = \begin{cases} l * x_1, & j = 1 \\ z_{j-1} * x_j, & 2 \leq j \leq t \end{cases} \quad (1)$$



Quasigroup string transformations

Markovski et al. (LIRA 97)

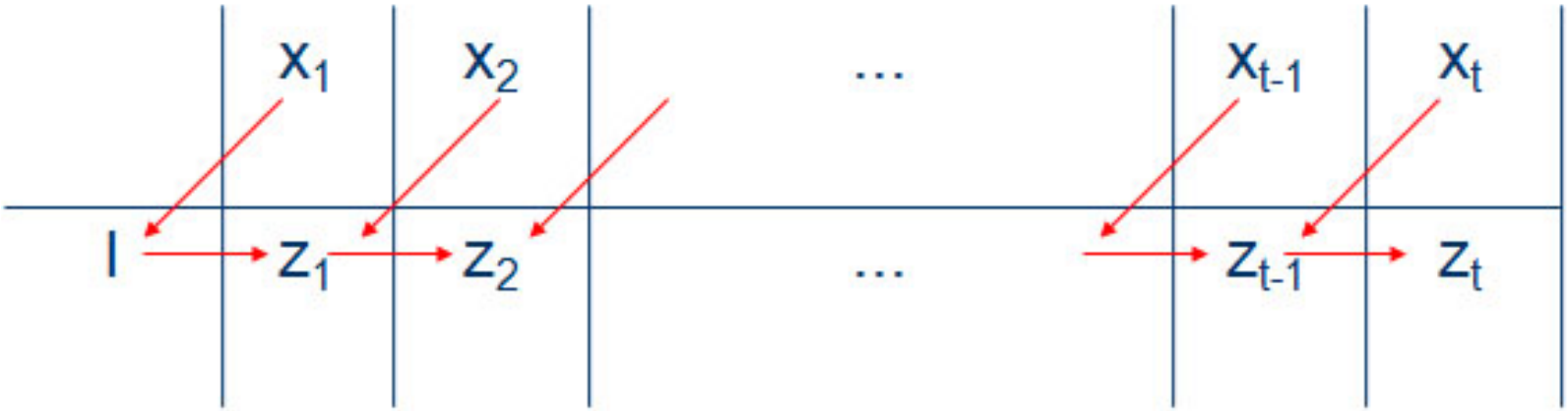
$$d_l(z_1 \dots z_t) = (x_1 \dots x_t) \Leftrightarrow x_j = \begin{cases} l * z_1, & j = 1 \\ z_{j-1} * z_j, & 2 \leq j \leq t \end{cases} \quad (2)$$



Quasigroup string transformations

Markovski et al. (CONT 99)

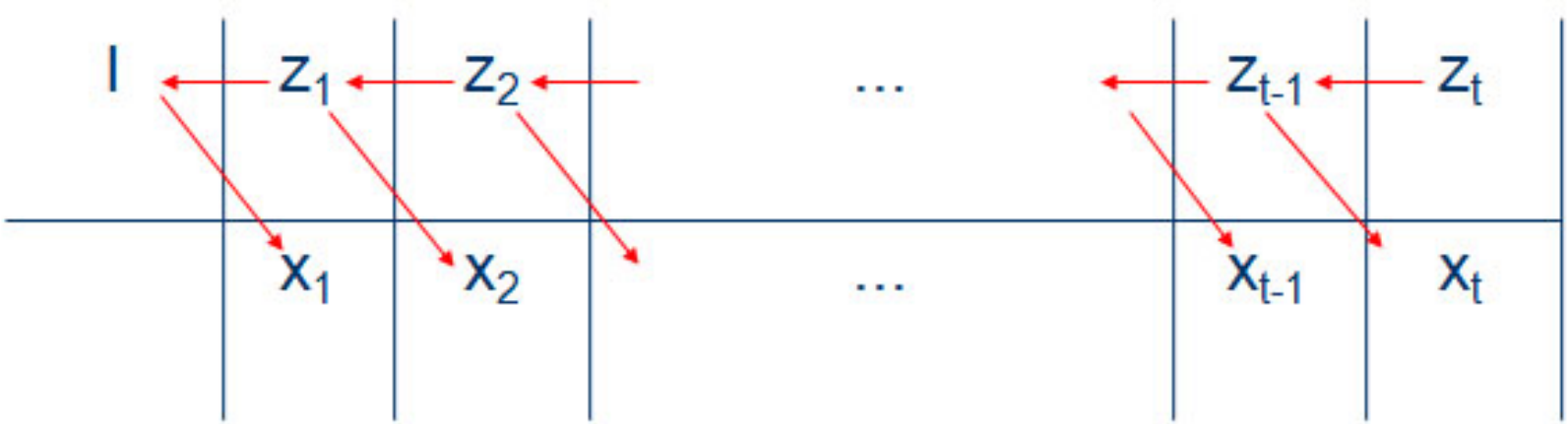
$$e'_l(x_1 \dots x_t) = (z_1 \dots z_t) \Leftrightarrow z_j = \begin{cases} x_1 * l, & j = 1 \\ x_j * z_{j-1}, & 2 \leq j \leq t \end{cases} \quad (3)$$



Quasigroup string transformations

Markovski et al. (CONT 99)

$$d'_l(z_1 \dots z_t) = (x_1 \dots x_t) \Leftrightarrow x_j = \begin{cases} z_1 * l, & j = 1 \\ z_j * z_{j-1}, & 2 \leq j \leq t \end{cases} \quad (4)$$

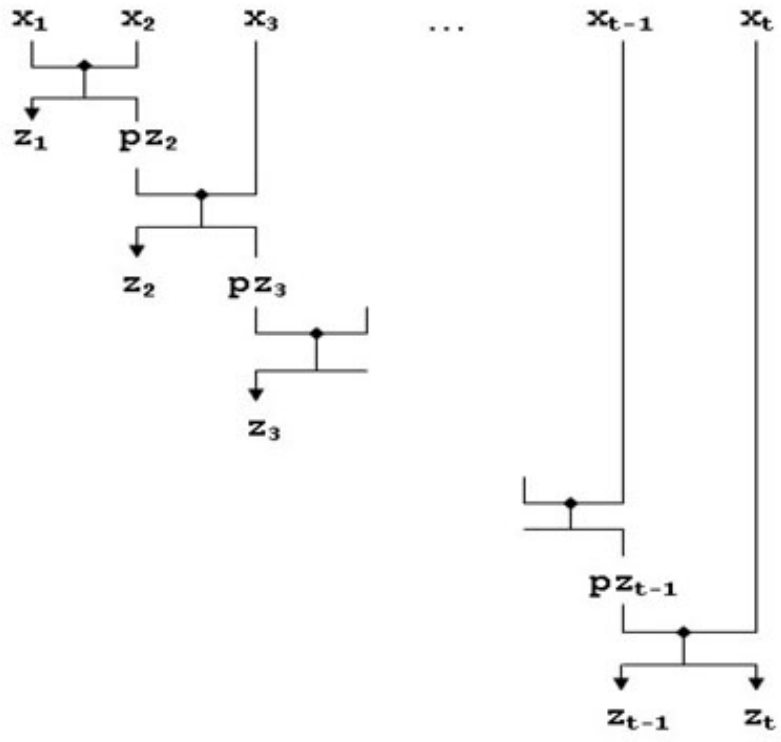


Quasigroup string transformations

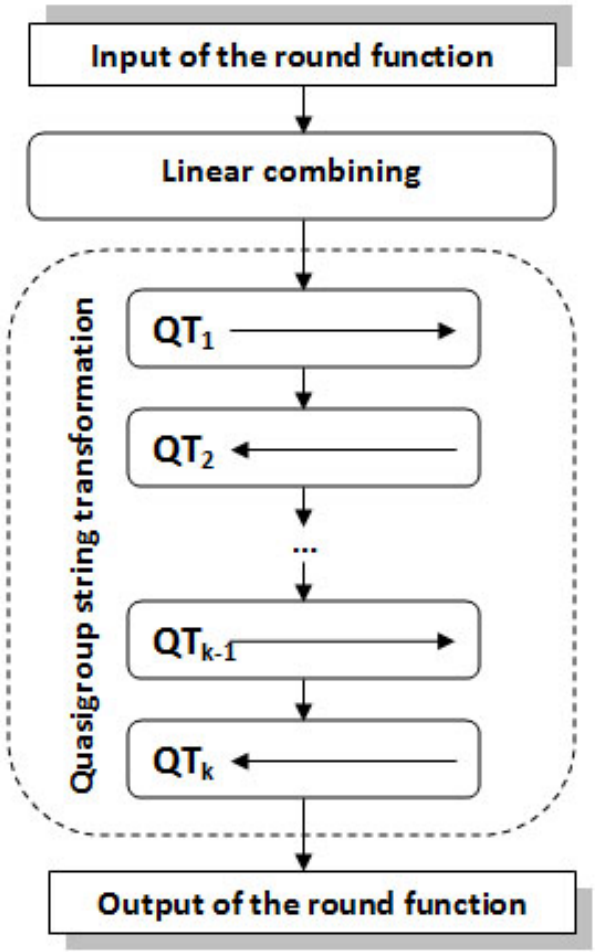
Mileva, Markovski (ICT 09)

Let Q be endowed with two orthogonal quasigroup operations $*_1$ and $*_2$. Then an orthogonal quasigroup string transformation $OT : Q^+ \rightarrow Q^+$ is defined by the following iterative procedure.

$OT(x_1) = x_1$,
$OT(x_1, x_2) = (x_1 *_1 x_2, x_1 *_2 x_2)$,
and if
$OT(x_1, x_2, \ldots, x_{t-2}, x_{t-1}) =$
$(z_1, z_2, \ldots, z_{t-1})$ is defined for
$t > 2$, then
$OT(x_1, x_2, \ldots, x_{t-1}, x_t) =$
$(z_1, z_2, \ldots, z_{t-1} *_1 x_t, z_{t-1} *_2 x_t)$,
where $x_i \in Q$.



New design of the round function



New design of the round function

- The linear combining layer produce high diffusion of the input.
- Quasigroup string transformations should be done with different quasigroups that are obtained from the key, i.e. keyed quasigroups.
- If leader is needed, it should be produced from the key and different for each quasigroup transformation.

New design of the round function

Multiset attacks
(SQUARE attack - **Knudsen (FSE 97)**, Saturation attack, **Lucks (FSE 01)**, form of structural cryptanalysis - **Biryukov, Shamir (EC 01)**, Integral cryptanalysis - **Knudsen, Wagner (FSE 02)**)

- Constant multiset
- Permutation or saturated multiset
- Even multiset
- Balanced multiset

New design of the round function

Multiset attack have been deployed on the block ciphers with nonlinear layer, consisting of functions $f : 2^w \longrightarrow 2^w$ applied in *parallel*. Usually w is a small number, for example 8 (exception, Lucks applied the attack in Twofish for $w = 32$).

New design of the round function

Multiset attack have been deployed on the block ciphers with nonlinear layer, consisting of functions $f : 2^w \longrightarrow 2^w$ applied in *parallel*. Usually w is a small number, for example 8 (exception, Lucks applied the attack in Twofish for $w = 32$).

First observation

Our nonlinear layer consists of functions f applied *sequentially*.

New design of the round function

Multiset attack have been deployed on the block ciphers with nonlinear layer, consisting of functions $f : 2^w \longrightarrow 2^w$ applied in *parallel*. Usually w is a small number, for example 8 (exception, Lucks applied the attack in Twofish for $w = 32$).

First observation

Our nonlinear layer consists of functions f applied *sequentially*.

Naturally, one possibility in our case is w to be $log_2|Q|$.

New design of the round function

Multiset attack have been deployed on the block ciphers with nonlinear layer, consisting of functions $f : 2^w \longrightarrow 2^w$ applied in *parallel*. Usually w is a small number, for example 8 (exception, Lucks applied the attack in Twofish for $w = 32$).

First observation

Our nonlinear layer consists of functions f applied *sequentially*.

Naturally, one possibility in our case is w to be $log_2|Q|$.

Second observation

Size of the saturated multiset is equal to the order of used quasigroup.

New design of the round function

Constant multiset $\mathcal{C}$ retains its special property after applying:

- e-transformation with a fixed leader l, only if $l * c = l$, $c \in \mathcal{C}$. If the quasigroup has a right unit and the right unit is the constant value, constant string will remain constant.
- e'-transformation with a fixed leader l, only if $c * l = l$, $c \in \mathcal{C}$. If the quasigroup has a left unit and the left unit is the constant value, constant string will remain constant.
- d and d'-transformation with a fixed leader l, only if $c = l$, $c \in \mathcal{C}$
- OT-transformation, only if the two orthogonal quasigroups have the same idempotent element and it is used as constant value.

New design of the round function

For e, e', d or d' transformation with a variable leader, if quasigroup is without left nor right unit, we can not say anything about constant multiset.

For OT transformation, if used orthogonal quasigroups are without the same idempotent element, we can not say anything about constant multiset.

New design of the round function

Saturated multiset

- For a fixed leader, saturated multiset retains saturated, regardless the used quasigroup transformation.
- For a variable leader, we can not say anything.
- Saturated multiset retains saturated after OT transformation.

New design of the round function

- In general, for a fixed leader, for even multiset, we can not say anything, regardless the used quasigroup transformation. The same holds for OT transformation, too.
- In general, for a fixed leader, for balanced non-saturated multiset, we can not say anything, regardless the used quasigroup transformation. The same holds for OT transformation, too.

New design of the round function

- The sequenced processing of the string together with the deployment of the keyed leaders and keyed quasigroups with or without some properties, different for each quasigroup transformation, give us protection against the multiset attacks.
- OT transformation should be mixed with other quasigroup transformations, to avoid multiset attacks.

Constructions with small quasigroups

One approach is to use a set of several fixed small quasigroups of order $4, 8$ or 16 and to use the key for choosing which quasigroup will be applied on the current quasigroup string transformation (similar to the design of Edon-80).

- The set should be kept in the memory (order of the set/occupied memory tradeoff).
- Freedom in choosing quasigroups with desirable properties. Quasigroups should be at least shapeless (Gligoroski et al. (NIST 06)).
- Expected to be very poor in the performances.

Constructions with huge quasigroups

Another approach is to use a computational method for producing different quasigroups of huge order $2^{16}, 2^{32}$, 2^{64}, etc.

- Quasigroups are **not** kept in memory.
- Ideally, chosen method should produce shapeless quasigroups at least.
- Depending on the chosen method, some structural properties can be present in the quasigroups.
- Expected to have much better performances, but they will depend on the chosen method.

Constructions with huge quasigroups, first direction

Extended Feistel Networks (Markovski and Mileva (QRS 09))
Let $(G, +)$ be an Abelian group, let $f : G \to G$ be a mapping and let $a, b, c \in G$ are constants. $F_{A,B,C} : G^2 \to G^2$ is defined as

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

When f is a bijection, $F_{A,B,C}$ is an orthomorphism. Algorithm exists for producing $F_{A,B,C}$ of order 2^{k2^s} from f of small order 2^s (for example, $s = 8$).
Quasigroup operation can be defined by Sade's diagonal method (CJM 57) as

$$X *_{F_{A,B,C}} Y = F_{A,B,C}(X - Y) + Y$$

Constructions with huge quasigroups, first direction

- Parameters A, B and C can be obtained from the key, so, produced quasigroups will be keyed and different for every transformation.
- Only starting bijection is kept in the memory.
- Depending on the chosen starting bijection and the group operation, one can produce a shapeless quasigroup.

Constructions with huge quasigroups, first direction

- Every $F_{A,B,C}$ and its square $F^2_{A,B,C}$ are orthogonal orthomorphisms on the abelian group $(G,+)$. They can be used for producing two orthogonal quasigroups needed for the OT transformation, given by

$$X *_{F_{A,B,C}} Y = X + F_{A,B,C}(Y), \quad X *_{F^2_{A,B,C}} Y = X + F^2_{A,B,C}(Y).$$

Constructions with huge quasigroups, second direction

(Rivest (FFTA 01))
Huge quasigroups can be defined by using bivariate polynomials $P(x, y) = a_0 + a_1 x + \ldots a_k x^k$ over the ring $(\mathbb{Z}_{2^w}, +, \cdot)$, where quasigroup $(\mathbb{Z}_{2^w}, *)$ is defined by $x * y = P(x, y)$.

Constructions with huge quasigroups, second direction

- The coefficients a_i can be derived from the key, so, produced quasigroups will be keyed and different for every transformation.
- There are no polynomials $P_1(x, y)$ and $P_2(x, y)$ modulo 2^w, $w \geq 1$ that form a pair of orthogonal quasigroups (Rivest).
- All parastrophic operations of a polynomial binary quasigroup $(\mathbb{Z}_{2^w}, *)$, have polynomial representations over the ring $(\mathbb{Z}_{2^w}, +, \cdot)$. (Samardziska (MsC thesis 09)).
- Algorithm for finding parastrophic quasigroup operation (Samardziska (MsC thesis 09)).

Constructions with huge quasigroups, third direction

(Samardziska et al (SCC 10))

- Characterization of the T-functions that define quasigroups.
- Only in special cases, time for calculating the quasigroup operation and one its parastrophic quasigroup operation is the same.

Future work

- Additional analysis of existing methods for computing the huge quasigroup operations.
- Deployment of suggested design for building particular block cipher with software implementation, security and performance analysis, etc.
- Finding new faster computation of huge quasigroup operations.

THANKS

FOR

YOUR ATTENTION!!!