Quasigroups and their use in cryptography

Andrea Frisová

March 24, 2010

Latin square

A *Latin square of order n* is an $n \times n$ table filled with n copies of each of n different symbols in which no symbol is repeated in any row or column.

Latin square

A *Latin square of order n* is an $n \times n$ table filled with n copies of each of n different symbols in which no symbol is repeated in any row or column.

1	2	3	4	5
2	3	5	1	4
3	5	4	2	1
4	1	2	5	3
5	4	1	3	2

3	1	2
2	3	1
1	2	3

Quasigroup

A quasigroup of order n is a set of n symbols with a binary operation such that its Cayley table corresponds to a Latin square of order n.

Quasigroup

A quasigroup of order n is a set of n symbols with a binary operation such that its Cayley table corresponds to a Latin square of order n.

1	0	3	2
0	3	2	1
2	1	0	3
3	2	1	0

$\cdot$	0	1	2	3
0	1	0	3	2
1	0	3	2	1
2	2	1	0	3
3	3	2	1	0

Quasigroup

A quasigroup of order n is a set of n symbols with a binary operation such that its Cayley table corresponds to a Latin square of order n.

1	0	3	2
0	3	2	1
2	1	0	3
3	2	1	0

$\cdot$	0	1	2	3
0	1	0	3	2
1	0	3	2	1
2	2	1	0	3
3	3	2	1	0

The number of Latin square of order n = The number of quasigroups of order n.

Formal definition of a quasigroup

Formal definition of a quasigroup

A *quasigroup* is a set Q with a binary operation $*\colon Q \times Q \to Q$ such that for each $u, v \in Q$ there exist unique $x, y \in Q$ which satisfy $u * x = v$ and $y * u = v$.

Formal definition of a quasigroup

A *quasigroup* is a set Q with a binary operation $*\colon Q \times Q \to Q$ such that for each $u, v \in Q$ there exist unique $x, y \in Q$ which satisfy $u * x = v$ and $y * u = v$.

Equivalently:

A *quasigroup* is a set Q with binary operations $*, \backslash, /$ such that for all $u, v \in Q$ the following conditions are satisfied:

$$u\backslash(u \cdot v) = v \qquad u \cdot (u\backslash v) = v$$

$$(v \cdot u)/u = v \qquad (v/u) \cdot u = v$$

The number of Latin squares/quasigroups of order n

There is no known easily-computable formula for the number of quasigroups of order n.

The number of Latin squares/quasigroups of order n

There is no known easily-computable formula for the number of quasigroups of order n.
There exist some lower and upper bounds for the number of the Latin squares/quasigroups, $L(n)$, where n is large. For example

$$\prod_{k=1}^{n} (k!)^{n/k} \geq L(n) \geq \frac{(n!)^{2n}}{n^{n^2}}$$

(given by van Lint and Wilson).

The number of Latin squares of order n

n	Number of Latin squares of order n	Reference
1	1	
2	2	
3	12	
4	576	
5	161280	Euler (1782), Cayley (1890), MacMahon (1915; incorrect value)
6	812851200	Frolov (1890) and Tarry (1900)
7	61479419904000	Frolov (1890, incorrect), Norton (1939, incomplete), Sade (1948), Saxena (1951)
8	108776032459082956800	Wells (1967)
9	5524751496156892842531225600	Bammel and Rothstein (1975)
10	9982437658213039871725064756920320000	McKay and Rogoyski (1995)
11	776966836171770144107444346734230682311065600000	McKay and Wanless (2005)
12	$12! \cdot 11! \cdot 1.62 \cdot 10^{44}$	McKay and Rogoyski (1995)
13	$13! \cdot 12! \cdot 2.51 \cdot 10^{56}$	McKay and Rogoyski (1995)
14	$14! \cdot 13! \cdot 2.33 \cdot 10^{70}$	McKay and Rogoyski (1995)
15	$15! \cdot 14! \cdot 1.5 \cdot 10^{86}$	McKay and Rogoyski (1995)

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

In terms of Latin squares, the map α corresponds to a permutation of rows, β to a permutation of columns, and γ to permutation of the set of symbols.

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

In terms of Latin squares, the map α corresponds to a permutation of rows, β to a permutation of columns, and γ to permutation of the set of symbols.

1	0	3	2
0	3	2	1
2	1	0	3
3	2	1	0

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

In terms of Latin squares, the map α corresponds to a permutation of rows, β to a permutation of columns, and γ to permutation of the set of symbols.

1	0	3	2		3	0	1	2
0	3	2	1		2	3	0	1
2	1	0	3		0	1	2	3
3	2	1	0		1	2	3	0

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

In terms of Latin squares, the map α corresponds to a permutation of rows, β to a permutation of columns, and γ to permutation of the set of symbols.

1	0	3	2	3	0	1	2	0	1	2	3
0	3	2	1	2	3	0	1	2	3	0	1
2	1	0	3	0	1	2	3	3	0	1	2
3	2	1	0	1	2	3	0	1	2	3	0

Isotopy

An *isotopy* between quasigroups $(Q, *)$ and $(P, \cdot)$ is a triple (α, β, γ) of bijections from Q onto P such that

$$\alpha(x) \cdot \beta(y) = \gamma(x * y) \quad \text{for all } x, y \text{ in } Q.$$

We then say that quasigroups $(Q, *)$ and $(P, \cdot)$ are *isotopic*.

In terms of Latin squares, the map α corresponds to a permutation of rows, β to a permutation of columns, and γ to permutation of the set of symbols.

1	0	3	2		3	0	1	2		0	1	2	3		1	0	2	3
0	3	2	1		2	3	0	1		2	3	0	1		2	3	1	0
2	1	0	3		0	1	2	3		3	0	1	2		3	1	0	2
3	2	1	0		1	2	3	0		1	2	3	0		0	2	3	1

Quasigroups

Quasigroups

Isotopic to a group

Loop

Loop

A *loop* is a quasigroup with a unit.

Loop

A *loop* is a quasigroup with a unit.

Proposition 1

Each quasigroup is isotopic to a loop.

Loop

A *loop* is a quasigroup with a unit.

Proposition 1

Each quasigroup is isotopic to a loop.

Proposition 2

Each loop isotopic to a group is a group.

Quasigroups

Isotopic to a group

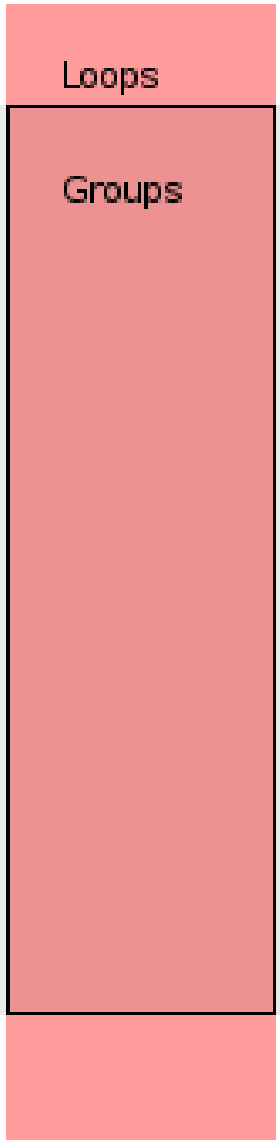
Quasigroups

Loops

Isotopic to a group

Quasigroups

Isotopic to a group

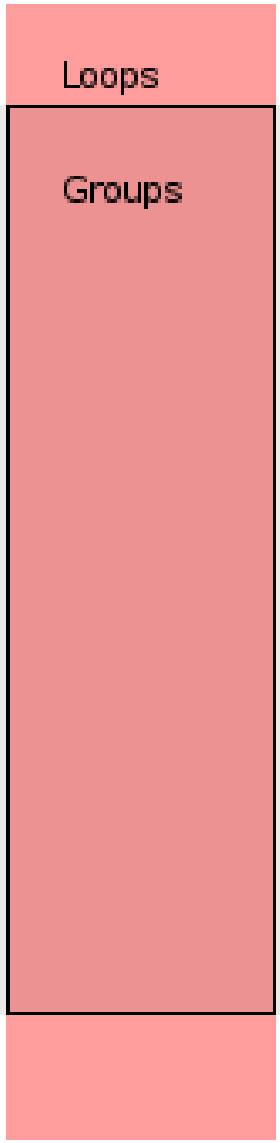


Proposition 3

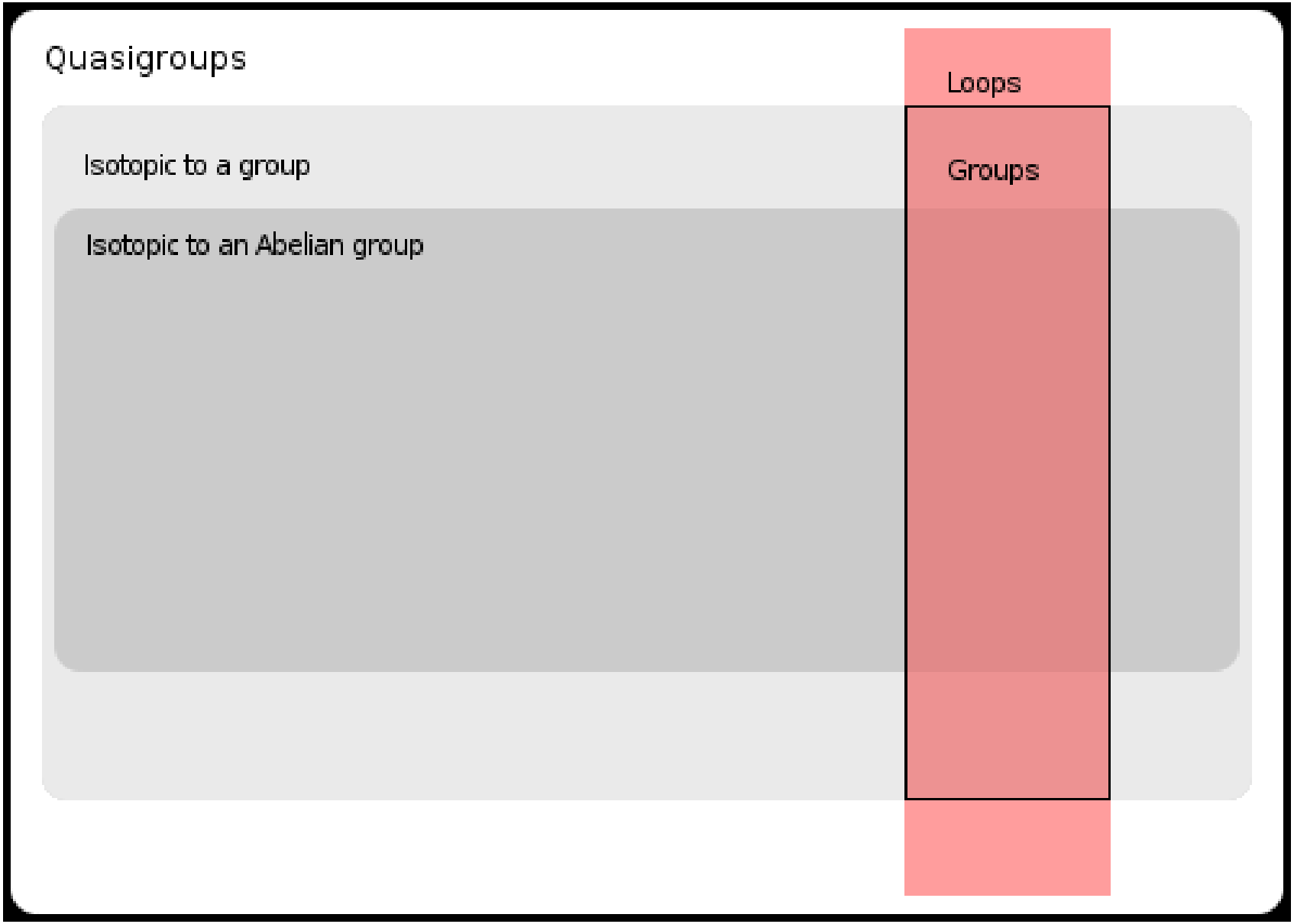
Isotopic groups are isomorphic.

Quasigroups

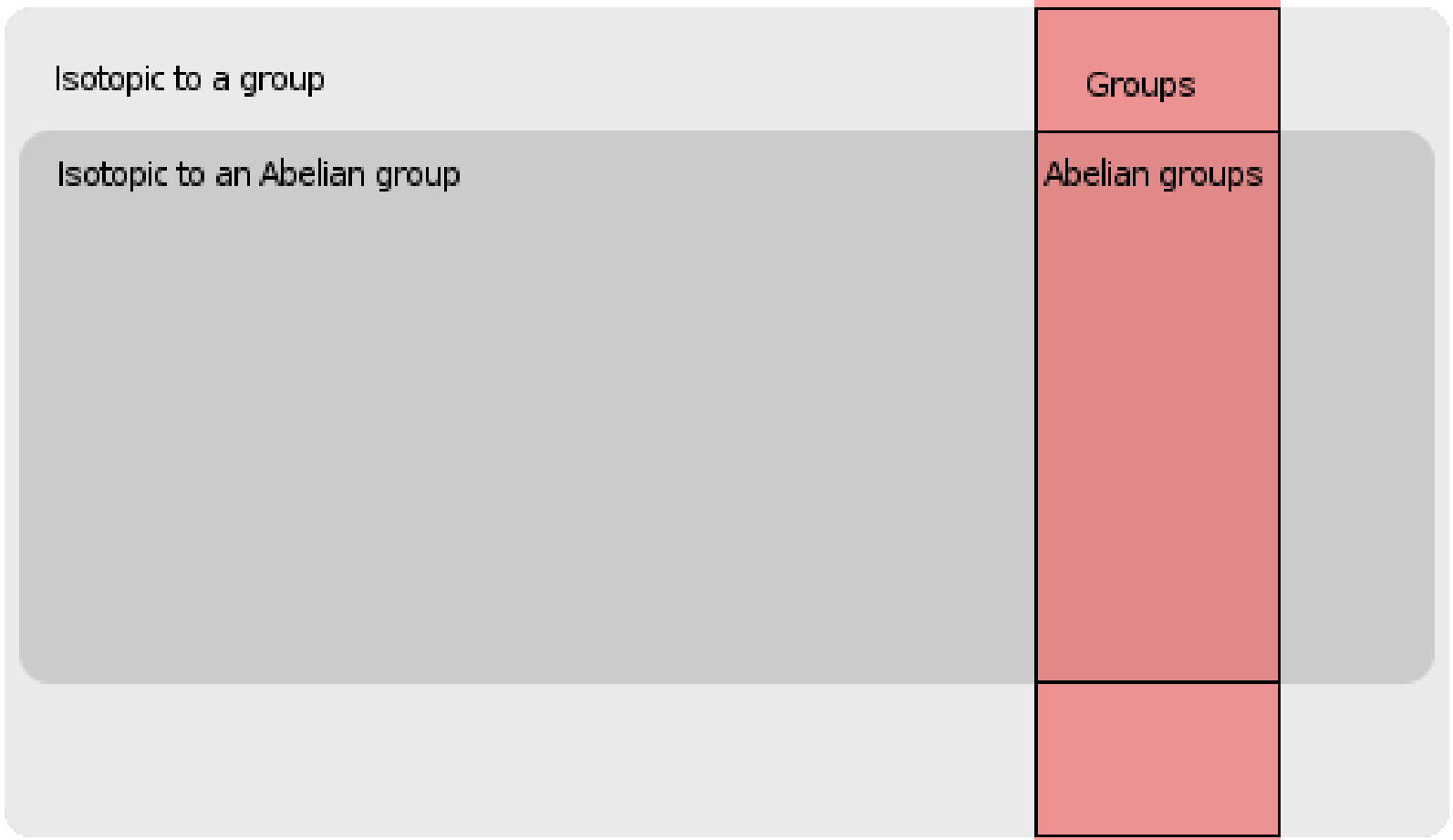
Isotopic to a group



Quasigroups



Quasigroups



Central and medial quasigroups

Central and medial quasigroups

A *central quasigroup* is a quasigroup $(Q, *)$ such that there exists an Abelian group $(Q, +)$, $\alpha, \beta \in \mathrm{Aut}((Q, +))$, and $c \in Q$ such that

$$x * y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.$$

Central and medial quasigroups

A *central quasigroup* is a quasigroup $(Q, *)$ such that there exists an Abelian group $(Q, +)$, $\alpha, \beta \in \mathrm{Aut}((Q, +))$, and $c \in Q$ such that

$$x * y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.$$

A *medial quasigroup* is a central quasigroup such that the automorphisms α and β commute.

Central and medial quasigroups

A *central quasigroup* is a quasigroup $(Q, *)$ such that there exists an Abelian group $(Q, +)$, $\alpha, \beta \in \mathrm{Aut}((Q, +))$, and $c \in Q$ such that

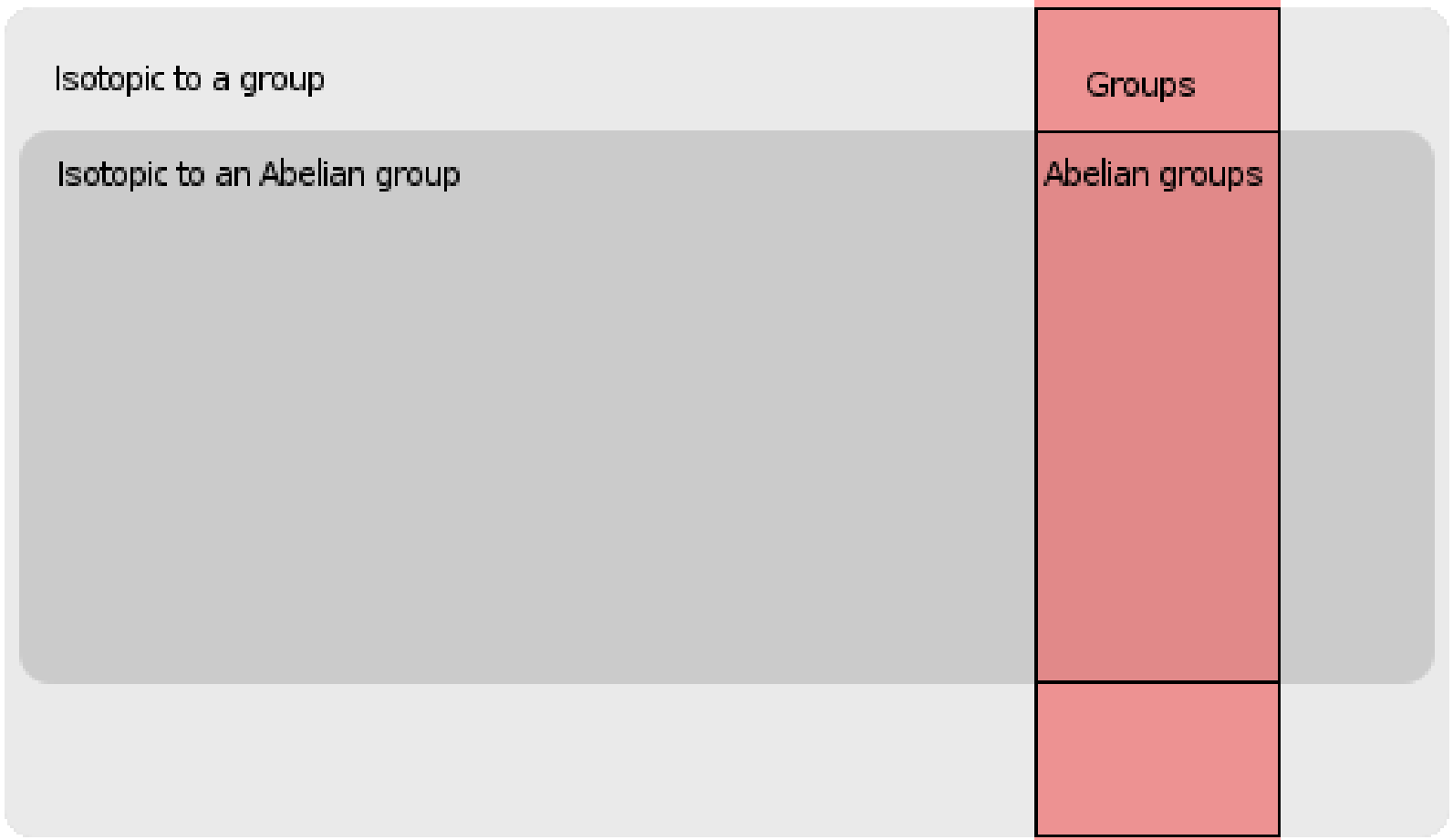
$$x * y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.$$

A *medial quasigroup* is a central quasigroup such that the automorphisms α and β commute.

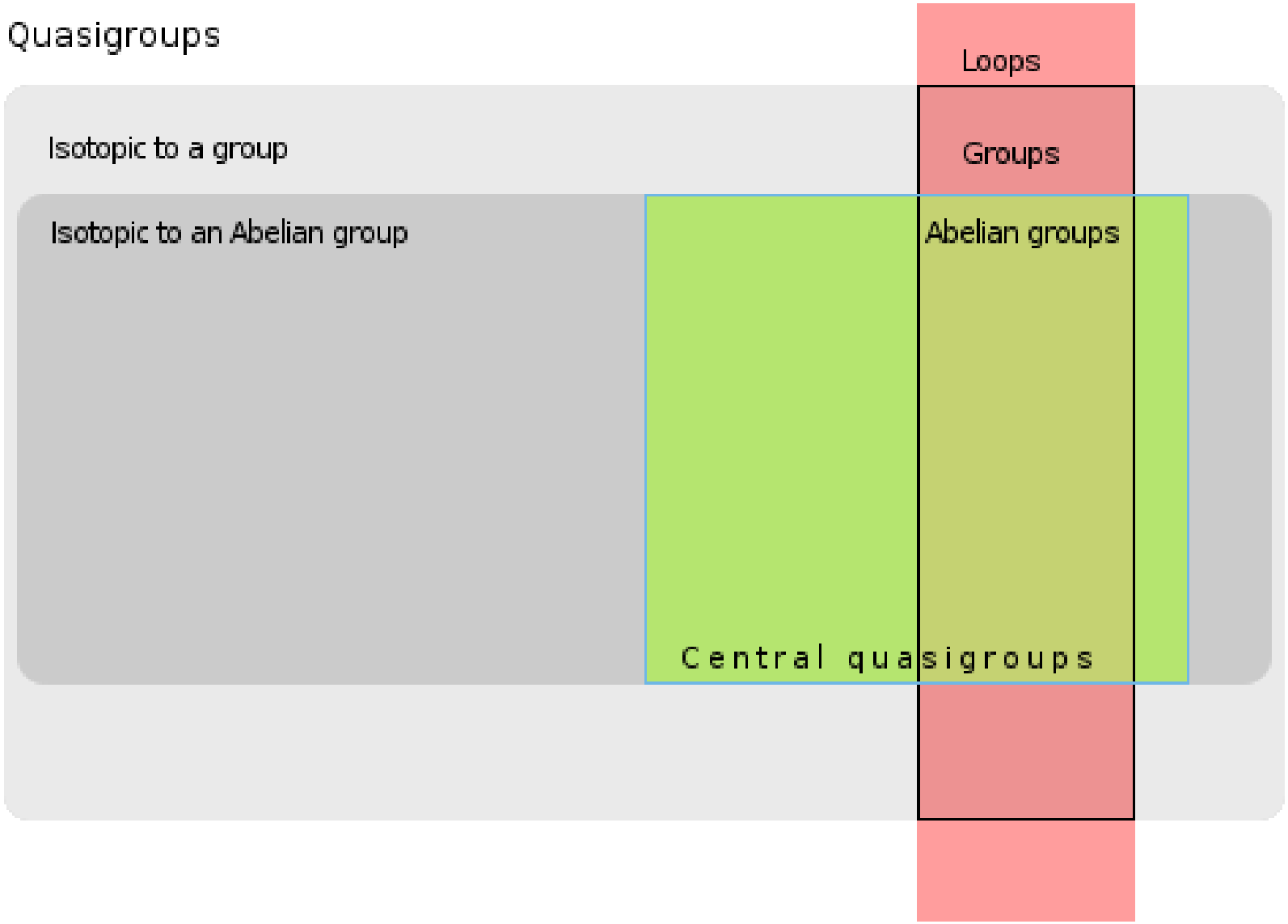
Proposition 4

Each central quasigroup is isotopic to an Abelian group.

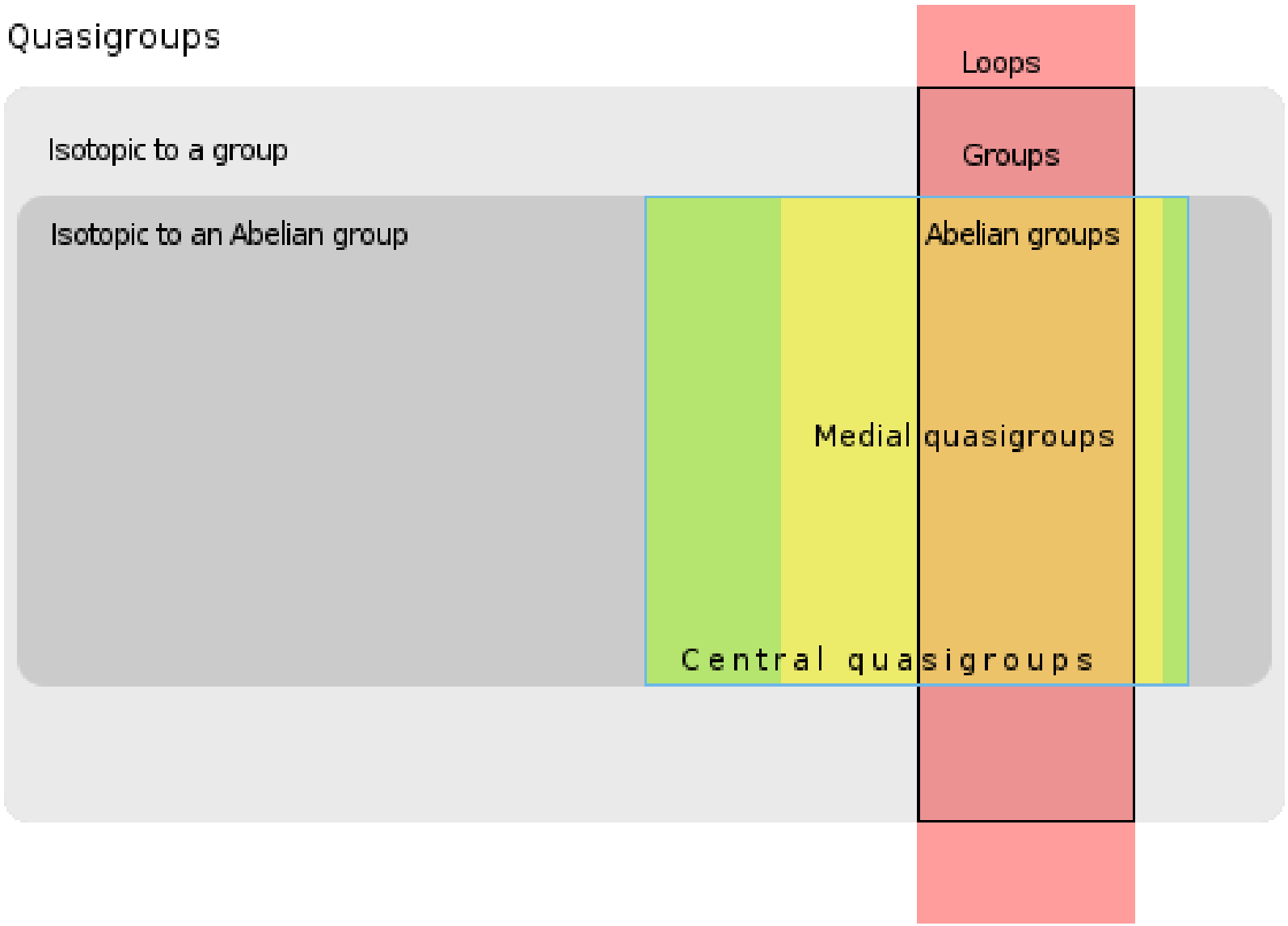
Quasigroups



Quasigroups



Quasigroups



Quasigroups in cryptography

Quasigroups can be used in

- symmetric-key cryptography – stream cipher Edon-80

All designed by D. Gligoroski and collaborators.

Quasigroups in cryptography

Quasigroups can be used in

- symmetric-key cryptography – stream cipher Edon-80
- public-key cryptography – MQQ (next talk by Adam Christov)

All designed by D. Gligoroski and collaborators.

Quasigroups in cryptography

Quasigroups can be used in

- symmetric-key cryptography – stream cipher Edon-80
- public-key cryptography – MQQ (next talk by Adam Christov)
- hash functions – Edon-R.

All designed by D. Gligoroski and collaborators.

Edon-R

Edon-R

Quasigroups which are used in the hash function Edon-R have large order.

Edon-R

Quasigroups which are used in the hash function Edon-R have large order.
They are isotopic to the Abelian group $(\mathbb{Z}_2^n, +)$ for $n = 256$ or $n = 512$.

Edon-R

Quasigroups which are used in the hash function Edon-R have large order.
They are isotopic to the Abelian group $(\mathbb{Z}_2^n, +)$ for $n = 256$ or $n = 512$.
Bijections α and β are generated by using certain matrices.

Edon-80 – quasigroups

Edon-80 – quasigroups

Stream cipher Edon-80 uses four quasigroups of order 4.

Edon-80 – quasigroups

Stream cipher Edon-80 uses four quasigroups of order 4. They are:

- isotopic to an Abelian group $(\mathbb{Z}_4, +)$

Edon-80 – quasigroups

Stream cipher Edon-80 uses four quasigroups of order 4. They are:

- isotopic to an Abelian group $(\mathbb{Z}_4, +)$
- non-medial

Edon-80 – quasigroups

Stream cipher Edon-80 uses four quasigroups of order 4. They are:

- isotopic to an Abelian group $(\mathbb{Z}_4, +)$
- non-medial
- non-central

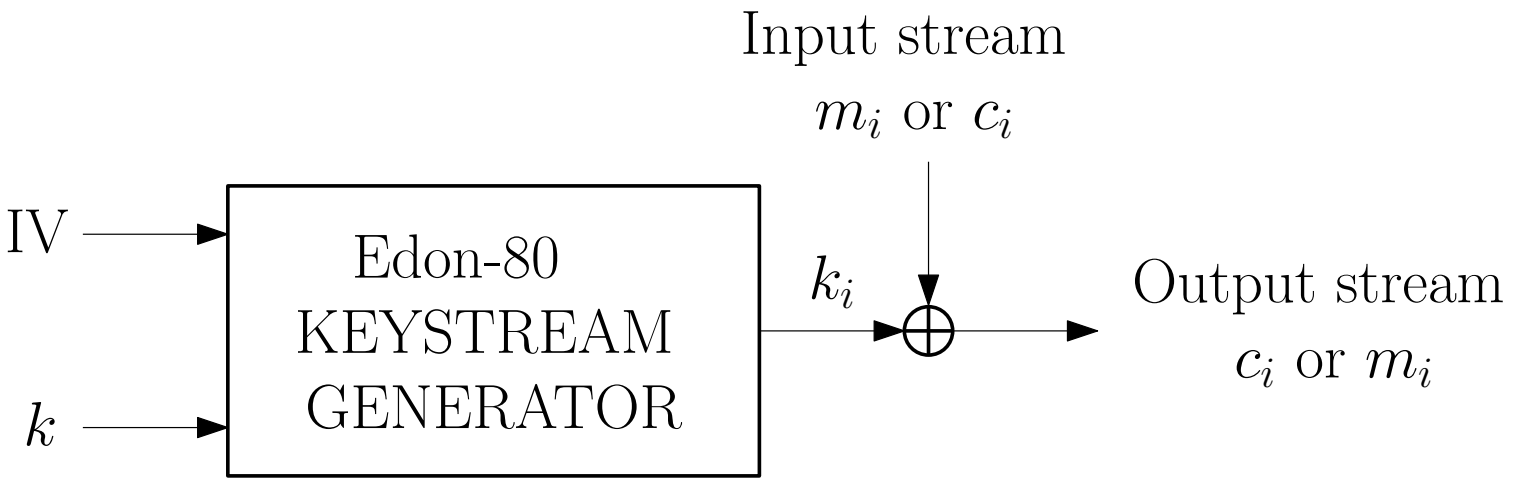
Edon-80 – Description

Edon-80 – Description

Edon-80 is a binary additive stream cipher:

Edon-80 – Description

Edon-80 is a binary additive stream cipher:



$k = K_0 \ldots K_{39}$ is a key
$IV = v_0 \ldots v_{39}$ is an initialisation value

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y					

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y	$y * a_0$				

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y	$y * a_0$	$(y * a_0) * a_1$			

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y	$y * a_0$	$(y * a_0) * a_1$	$((y * a_0) * a_1) * a_2$		

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y	$y * a_0$	$(y * a_0) * a_1$	$((y * a_0) * a_1) * a_2$	$\ldots$	

Edon-80 – Description

A keystream is generated using the following map:

$$\tau(*, y)\colon (a_i) \to (b_i).$$

		a_0	a_1	a_2	a_3	$\ldots$
$*$	y	$y * a_0$	$(y * a_0) * a_1$	$((y * a_0) * a_1) * a_2$	$\ldots$	

$$b_0 = y * a_0,$$
$$b_i = b_{i-1} * a_i \quad \text{for } i > 0.$$

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

$*_i$		0	1	2	3	0	1	2	$\cdots$
$*_0$	y_0								
$*_1$	y_1								
$\vdots$	$\vdots$								
$*_{79}$	y_{79}								

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

$*_i$		0	1	2	3	0	1	2	$\cdots$
$*_0$	y_0	$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$	$t_{0,4}$	$t_{0,5}$	$t_{0,6}$	$\cdots$
$*_1$	y_1								
$\vdots$	$\vdots$								
$*_{79}$	y_{79}								

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

$*_i$		0	1	2	3	0	1	2	$\cdots$
$*_0$	y_0	$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$	$t_{0,4}$	$t_{0,5}$	$t_{0,6}$	$\cdots$
$*_1$	y_1	$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$t_{1,6}$	$\cdots$
$\vdots$	$\vdots$								
$*_{79}$	y_{79}								

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

$*_i$		0	1	2	3	0	1	2	$\cdots$
$*_0$	y_0	$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$	$t_{0,4}$	$t_{0,5}$	$t_{0,6}$	$\cdots$
$*_1$	y_1	$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$t_{1,6}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$*_{79}$	y_{79}								

Edon-80 – Keystream generator

Keystream generator of Edon-80 has 3 phases:

- *KeySetup* – the output is 80 quasigroups $(Q, *_i)$ $i = 0, 1, \ldots, 79$
- *IVSetup* – values $y_0, \ldots, y_{79}$, $y_i \in \{0, 1, 2, 3\}$ are generated from IV and the key
- *Keystream*

$*_i$		0	1	2	3	0	1	2	$\cdots$
$*_0$	y_0	$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$	$t_{0,4}$	$t_{0,5}$	$t_{0,6}$	$\cdots$
$*_1$	y_1	$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$t_{1,6}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$*_{79}$	y_{79}	$t_{79,0}$	$\mathbf{t_{79,1}}$	$t_{79,2}$	$\mathbf{t_{79,3}}$	$t_{79,4}$	$\mathbf{t_{79,5}}$	$t_{79,6}$	$\cdots$

Our modification

We suppose that

Our modification

We suppose that

- $* = *_i$ for all $i = 1, 2, \ldots, 79$ (we use only one quasigroup),

$*$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	$\cdots$
y_0								
y_1								
y_2								
y_3								
$\vdots$								

Our modification

We suppose that

- $* = *_i$ for all $i = 1, 2, \ldots, 79$ (we use only one quasigroup),
- $X = (x_i)$ a periodic sequence with a period P_X instead of sequence $012301230123\ldots$, and

$*$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	$\cdots$
y_0								
y_1								
y_2								
y_3								
$\vdots$								

Our modification

We suppose that

- $* = *_i$ for all $i = 1, 2, \ldots, 79$ (we use only one quasigroup),
- $X = (x_i)$ a periodic sequence with a period P_X instead of sequence $012301230123\ldots$, and
- $Y = (y_i)$ a sequence with no special property (we have arbitrary number of rows).

$*$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	$\cdots$
y_0								
y_1								
y_2								
y_3								
$\vdots$								

Periods

We want to know something about the periods of the rows.
Why?

Periods

We want to know something about the periods of the rows. Why?

- There are some indications that Edon-80 may generate a keystream with short periods (for some input values). This is a main reason for its failure in eSTREAM, ECRYPT stream cipher project.

Periods

We want to know something about the periods of the rows. Why?

- There are some indications that Edon-80 may generate a keystream with short periods (for some input values). This is a main reason for its failure in eSTREAM, ECRYPT stream cipher project.
- Which quasigroups are the most suitable for Edon-80?

Periods for central quasigroups

For central quasigroups, this problem leads to the problem in the group ring $\mathbb{Z}_{e_G}[Aut(G)]$.

Periods for central quasigroups

For central quasigroups, this problem leads to the problem in the group ring $\mathbb{Z}_{e_G}[Aut(G)]$.
We already have 'good' upper bound of the periods for medial quasigroups and for central quasigroups of order 4.

Periods for central quasigroups

For central quasigroups, this problem leads to the problem in the group ring $\mathbb{Z}_{e_G}[Aut(G)]$.
We already have 'good' upper bound of the periods for medial quasigroups and for central quasigroups of order 4.

Quasigroup type	Underlying group	P_i	$e_G \operatorname{lcm}(P_X, P_i)$
Medial	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$2^{\lceil \log_2 i \rceil}$	$2 \operatorname{lcm}(P_X, 2^{\lceil \log_2 i \rceil})$
Central, non-medial	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\frac{3}{2} \cdot 2^{\lceil \log_2 i \rceil}$	$2 \operatorname{lcm}(P_X, \frac{3}{2} \cdot 2^{\lceil \log_2 i \rceil})$
Central, non-medial	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$2 \cdot 2^{\lceil \log_2 i \rceil}$	$2 \operatorname{lcm}(P_X, 2 \cdot 2^{\lceil \log_2 i \rceil})$
Medial	$\mathbb{Z}_4$	$2 \cdot 2^{\lceil \log_2 i \rceil}$	$4 \operatorname{lcm}(P_X, 2 \cdot 2^{\lceil \log_2 i \rceil})$
Medial	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$3 \cdot 2^{\lceil \log_2 i \rceil}$	$2 \operatorname{lcm}(P_X, 3 \cdot 2^{\lceil \log_2 i \rceil})$

Thank you for your attention!