Quasigroups and stream cipher Edon80

Andrea Frisová

Department of Algebra, Charles University in Prague

June 3, 2010
Edon80 is a binary additive stream cipher.

$K$ is a key

$k_i$ is an $i$th bit of the keystream

$m_i$ is an $i$th bit of the message

$c_i$ is an $i$th bit of the ciphertext
Properties of keystream

The keystream should
Properties of keystream

The keystream should

- be a pseudorandom sequence
Properties of keystream

The keystream should

- be a pseudorandom sequence
- have no period (or period longer than any admissible message).
Properties of keystream

The keystream should

- be a pseudorandom sequence
- have no period (or period longer than any admissible message).
Properties of keystream

The keystream should

- be a pseudorandom sequence
- have no period (or period longer than any admissible message).

If this condition is not satisfied, two parts of the message will be encrypted by the same binary sequence, which opens ways to attack the cipher:
Why is the period of keystream a security problem?

Let $+$ be an operation of addition in $\mathbb{Z}_2^t$. Then

$$c = m + k$$

$$c' = m' + k$$
Why is the period of keystream a security problem?

Let $+$ be an operation of addition in $\mathbb{Z}_2^t$. Then

$$c = m + k$$

$$c' = m' + k$$

and

$$c + c' = (m + k) + (m' + k) = m + (k + k) + m = m + m'.$$
Why is the period of keystream a security problem?

Let $+$ be an operation of addition in $\mathbb{Z}_2^t$. Then

$$c = m + k$$
$$c' = m' + k$$

and

$$c + c' = (m + k) + (m' + k) = m + (k + k) + m = m + m'.$$

Hence

$$m' = c + c' + m.$$
Why is the period of keystream a security problem?

Let \( + \) be an operation of addition in \( \mathbb{Z}_2^t \). Then

\[
\begin{align*}
c &= m + k \\
c' &= m' + k
\end{align*}
\]

and

\[
\begin{align*}
c + c' &= (m + k) + (m' + k) = m + (k + k) + m = m + m'.
\end{align*}
\]

Hence

\[
m' = c + c' + m.
\]

Because most messages contain enough redundancy, it is possible to recover both \( m \) and \( m' \) from \( m + m' \).
Description of the keystream generator

INPUT:
\[ K = K_0, \ldots, K_{79} \]

4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT:
\[ \text{keystream} = (k_i)_{i=0}^\infty \]

Step 1:
\[ K \rightarrow K^0, \ldots, K^{79} \]

Step 2:
\[ K, K^0, \ldots, K^{79} \rightarrow y = y_0, \ldots, y_{79}, y_i \in \{0, 1, 2, 3\} \]
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)
4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)
Description of the keystream generator

INPUT: \[ K = K_0 \ldots K_{79} \]
\[ \text{4 fixed quasigroup operations on the set } \{0, 1, 2, 3\} \]

OUTPUT: \[ \text{keystream } = (k_i)_{i \geq 0} \]
Description of the keystream generator

**INPUT:** \( K = K_0 \ldots K_{79} \)

4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

**OUTPUT:** \( keystream = (k_i)_{i=0}^{\infty} \)

**Step 1:** \( K \rightarrow *_0, \ldots, *_{79} \)
Description of the keystream generator

INPUT: $K = K_0 \ldots K_{79}$
4 fixed quasigroup operations on the set $\{0, 1, 2, 3\}$

OUTPUT: keystream $= (k_i)_{i=0}^{\infty}$

Step 1: $K \rightarrow *_0, \ldots, *_{79}$
Step 2: $K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\}$
Description of the keystream generator

**INPUT:** \( K = K_0 \ldots K_{79} \)

- 4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

**OUTPUT:** \( keystream = (k_i)_{i=0}^{\infty} \)

**Step 1:** \( K \rightarrow ^*_0, \ldots, ^*_79 \)

**Step 2:** \( K, ^*_0, \ldots, ^*_79 \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\} \)
Description of the keystream generator

INPUT: $K = K_0 \ldots K_{79}$
4 fixed quasigroup operations on the set \{0, 1, 2, 3\}

OUTPUT: keystream = $(k_i)_{i=0}^{\infty}$

Step 1: $K \rightarrow *_0, \ldots, *_{79}$
Step 2: $K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}$, $y_i \in \{0, 1, 2, 3\}$

<table>
<thead>
<tr>
<th></th>
<th>*0</th>
<th>*1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>*0</td>
<td>*1</td>
</tr>
<tr>
<td></td>
<td>*79</td>
<td></td>
</tr>
</tbody>
</table>
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)
4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: \( keystream = (k_i)_{i=0}^\infty \)

Step 1: \( K \rightarrow *_0, \ldots, *_{79} \)
Step 2: \( K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, y_i \in \{0, 1, 2, 3\} \)

| \( *_0 \) | \( K_0 \) | \( K_1 \) | \( \ldots \) | \( K_{79} \) |
| \( *_1 \) | \( \ldots \) | \( \ldots \) | \( \ldots \) | \( \ldots \) |
Description of the keystream generator

INPUT: \[ K = K_0 \ldots K_{79} \]
\[ 4 \text{ fixed quasigroup operations on the set } \{0, 1, 2, 3\} \]

OUTPUT: \[ \text{keystream} = (k_i)_{i=0}^{\infty} \]

Step 1:
\[ K \rightarrow */0, \ldots, */79 \]

Step 2:
\[ K, */0, \ldots, */79 \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\} \]

<table>
<thead>
<tr>
<th>*0</th>
<th></th>
<th>*79</th>
</tr>
</thead>
<tbody>
<tr>
<td>*1</td>
<td>*78</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>*79</td>
<td>*0</td>
<td></td>
</tr>
</tbody>
</table>
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)
4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: \( keystream = (k_i)_{i=0}^\infty \)

Step 1: \( K \rightarrow *_{0}, \ldots, *_{79} \)
Step 2: \( K, *_{0}, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\} \)

\[
\begin{array}{c|} \hline
*_{0} & K_{79} & K_{79} *_{0} K_{0} \\
*_{1} & K_{78} & \vdots \\
*_{79} & K_{0} & \vdots \\
\hline
\end{array}
\]
Description of the keystream generator

INPUT: \[ K = K_0 \ldots K_{79} \]
4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: \( keystream = (k_i)_{i=0}^{\infty} \)

Step 1: \[ K \rightarrow *_0, \ldots, *_{79} \]
Step 2: \[ K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\} \]

<table>
<thead>
<tr>
<th>(*<em>0) (K</em>{79})</th>
<th>(K_0) (K_{79} *_0 K_0)</th>
<th>(K_1) ((K_{79} *_0 K_0) *_0 K_1)</th>
<th>(\ldots)</th>
<th>(K_{79})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*<em>0) (K</em>{79})</td>
<td>(K_0)</td>
<td>(K_1)</td>
<td>(\ldots)</td>
<td>(K_{79})</td>
</tr>
<tr>
<td>(*<em>1) (K</em>{78})</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
</tr>
<tr>
<td>(*_{79}) (K_0)</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
<td>(\ldots)</td>
</tr>
</tbody>
</table>
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)

4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: keystream = \( (k_i)_{i=0}^{\infty} \)

Step 1: \( K \rightarrow *_{0}, \ldots, *_{79} \)

Step 2: \( K, *_{0}, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, y_i \in \{0, 1, 2, 3\} \)

\[
\begin{array}{c|c|c|c|c}
*_{0} & *_{79} & K_0 & K_1 & \ldots & K_{79} \\
K_{79} & K_{79} *_{0} K_0 & (K_{79} *_{0} K_0) *_{0} K_1 & \ldots \\
*_{1} & K_{78} & & & & \\
\vdots & \vdots & & & & \\
*_{79} & K_0 & & & & \\
\end{array}
\]
Description of the keystream generator

INPUT: \[ K = K_0 \ldots K_{79} \]
4 fixed quasigroup operations on the set \{0, 1, 2, 3\}

OUTPUT: \[ keystream = (k_i)_{i=0}^{\infty} \]

Step 1: \[ K \rightarrow *_0, \ldots, *_{79} \]
Step 2: \[ K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, y_i \in \{0, 1, 2, 3\} \]
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)
4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: \( keystream = (k_i)_{i=0}^{\infty} \)

Step 1: \( K \rightarrow ^*0, \ldots, ^*79 \)
Step 2: \( K, ^*0, \ldots, ^*79 \rightarrow y = y_0 \ldots y_{79}, \quad y_i \in \{0, 1, 2, 3\} \)

<table>
<thead>
<tr>
<th>( ^*0 )</th>
<th>( K_{79} )</th>
<th>( K_{79} \times 0 K_0 )</th>
<th>( (K_{79} \times 0 K_0) \times 0 K_1 )</th>
<th>( \ldots )</th>
<th>( K_{79} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( ^*79 )</td>
<td>( K_0 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( ^*1 )</td>
<td>( K_{78} )</td>
<td>( K_{78} \times 1 (K_{79} \times 0 K_0) )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ 0 \times 0 = 2, \quad 0 \times 1 = 7, \quad 0 \times 2 = 1, \quad 0 \times 3 = 3, \quad 1 \times 0 = 1, \quad 1 \times 1 = 0, \quad 1 \times 2 = 2, \quad 1 \times 3 = 3, \quad 2 \times 0 = 0, \quad 2 \times 1 = 1, \quad 2 \times 2 = 0, \quad 2 \times 3 = 1, \quad 3 \times 0 = 1, \quad 3 \times 1 = 2, \quad 3 \times 2 = 3, \quad 3 \times 3 = 0. \]
Description of the keystream generator

INPUT: \( K = K_0 \ldots K_{79} \)

4 fixed quasigroup operations on the set \( \{0, 1, 2, 3\} \)

OUTPUT: \( \text{keystream} = (k_i)_{i=0}^{\infty} \)

Step 1: \( K \longrightarrow *_0, \ldots, *_{79} \)
Step 2: \( K, *_0, \ldots, *_{79} \longrightarrow y = y_0 \ldots y_{79}, y_i \in \{0, 1, 2, 3\} \)

| \( *_0 \) | \( K_{79} \) | \( K_{79} *_0 K_0 \) | \( (K_{79} *_0 K_0) *_0 K_1 \) | \( \cdots \) | \( K_{79} \) |
| \( *_1 \) | \( K_{78} \) | \( K_{78} *_1 (K_{79} *_0 K_0) \) |
| \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) | \( \vdots \) |
| \( *_{79} \) | \( K_0 \) | \( y_0 \) | \( y_1 \) | \( \cdots \) | \( y_{79} \) |
Description of the keystream generator

Step 2: \( K, *_0, \ldots, *_{79} \rightarrow y = y_0 \ldots y_{79}, \ y_i \in \{0, 1, 2, 3\} \)
Step 2: $K, *_0, \ldots, *_{79} \longrightarrow y = y_0 \ldots y_{79}$, $y_i \in \{0, 1, 2, 3\}$

Formally

$$y = \tau_{K_0,*_{79}} \circ \tau_{K_1,*_{78}} \circ \cdots \circ \tau_{K_{79},*_0}(K_0, \ldots, K_{79}),$$

where $\tau_{y,*}: (a_i) \mapsto (b_i)$ such that

$$b_0 = y * a_0,$$

$$b_i = b_{i-1} * a_i \text{ for } i > 0.$$
Description of the keystream generator

Step 3: $y, *_0, \ldots, *_{79} \rightarrow keystream$
Description of the keystream generator

Step 3: $y, *_0, \ldots, *_{79} \rightarrow keystream$

Figure: System A
Description of the keystream generator

Step 3: $y, *_0, \ldots, *_{79} \rightarrow $ keystream

Figure: System A
Description of the keystream generator

Step 3: $y, *_0, \ldots, *_{79} \rightarrow keystream$

<table>
<thead>
<tr>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>79</td>
<td>79</td>
</tr>
</tbody>
</table>

Figure: System A
Description of the keystream generator

Step 3: $y, *_0, \ldots, *_{79} \rightarrow \text{keystream}$

<table>
<thead>
<tr>
<th>$*_0$</th>
<th>$y_0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$*_1$</td>
<td>$y_1$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$*_79$</td>
<td>$y_{79}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>...</th>
</tr>
</thead>
</table>

**Figure:** System A
Step 3: \( y_0, y_1, \ldots, y_{79} \rightarrow \text{keystream} \)

<table>
<thead>
<tr>
<th>( y_i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>( \ldots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y_0 )</td>
<td>( y_0 \times_0 0 )</td>
<td>( (y_0 \times_0 0) \times_0 1 )</td>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( y_1 )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( y_{79} )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\( \text{Figure: System A} \)
Step 3: $y, *_0, \ldots, *_{79} \rightarrow \text{keystream}$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>\ldots</th>
</tr>
</thead>
<tbody>
<tr>
<td>$*_0$</td>
<td>$y_0$</td>
<td>$y_0 *_0 0$</td>
<td>$(y_0 *_0 0) *_0 1$</td>
<td>\ldots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$*_1$</td>
<td>$y_1$</td>
<td>$y_1 *_1 (y_0 *_0 0)$</td>
<td>\ldots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$*_{79}$</td>
<td>$y_{79}$</td>
<td>\ldots</td>
<td>\ldots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure:** System A
Description of the keystream generator

Step 3: $y, *, 0, \ldots, *, 79 \rightarrow \text{keystream}$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0</td>
<td>$y_0$</td>
<td>$y_0 * 0$</td>
<td>$(y_0 * 0) * 0$</td>
<td>1</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*1</td>
<td>$y_1$</td>
<td>$y_1 * 1 (y_0 * 0)$</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*79</td>
<td>$y_{79}$</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

**Figure:** System A
Step 3: $y, *_0, \ldots, *_{79} \rightarrow \text{keystream}$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$*_0$</td>
<td>$y_0$</td>
<td>$y_0 *_0 0$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$*_1$</td>
<td>$y_1$</td>
<td>$y_1 *_1 (y_0 *_0 0)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$...$</td>
<td>$...$</td>
<td>$...$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$*_79$</td>
<td>$y_{79}$</td>
<td>$a_{79,0}$</td>
<td>$k_0$</td>
<td>$a_{79,2}$</td>
<td>$k_1$</td>
<td>$a_{79,4}$</td>
<td>$k_2$</td>
</tr>
</tbody>
</table>

**Figure:** System A
Periods of the Edon80 keystream

J. Hong, Remarks on the Period of Edon80 – He showed that there is quite a large number of the pairs \(\{\ast_0, \ldots, \ast_{80}\}, y\) that produce the same sequence of period 2 and also that a random key produces a short period of the keystream \((2^{55}, 2^{63})\) with some probability \((2^{-71}, 2^{-60})\).

D. Gligoroski, S. Markovski, L. Kocarev and M. Gusev, Understanding Periods in Edon80 - Response on Remarks on the Period of Edon80, by Jin Hong – Based on the previous paper they made a statistical model of Edon80 which indicates the existence of weak keys. But they claim that Edon80 is a good cipher anyway because the best attack on Edon80 is still the exhaustive search in the space of all keys. It is also possible to increase the security by using 160 operations instead of 80.

Andrea Frisová Quasigroups and stream cipher Edon80
J. Hong, *Remarks on the Period of Edon80* – He showed that there is quite a large number of the pairs \(\{\ast_0, \ldots, \ast_{80}\}, y\) that produce the same sequence of period 2 and also that a random key produces a short period of the keystream \((2^{55}, 2^{63})\) with some probability \((2^{-71}, 2^{-60})\).
Periods of the Edon80 keystream

- J. Hong, *Remarks on the Period of Edon80* – He showed that there is quite a large number of the pairs ($\{*_0, \ldots, *_{80}\}, y$) that produce the same sequence of period 2 and also that a random key produces a short period of the keystream ($2^{55}, 2^{63}$) with some probability ($2^{-71}, 2^{-60}$).

- D. Gligoroski, S. Markovski, L. Kocarev and M. Gušev, *Understanding Periods in Edon80- Response on Remarks on the Period of Edon80, by Jin Hong* – Based on the previous paper they made a statistical model of Edon80 which indicates the existence of weak keys. But they claim that Edon80 is a good cipher anyway because the best attack on Edon80 is still the exhaustive search in the space of all keys. It is also possible to increase the security by using 160 operations instead of 80.
Our setting

We suppose that

\[ x_i \in \mathbb{Q}^N \]

is a periodic sequence with a period \( P \) instead of sequence 012301230123...

and

\[ y_i \in \mathbb{Q}^N \]

is a sequence with no special property (we have arbitrary number of rows).
Our setting

We suppose that

- $\ast = \ast_i$ for all $i = 1, 2, \ldots, 79$, but we work with a general finite quasigroup $(Q, \ast)$,
Our setting

We suppose that

- $\ast = \ast_i$ for all $i = 1, 2, \ldots, 79$, but we work with a general finite quasigroup $(Q, \ast)$,
- $X = (x_i) \in Q^N$ a periodic sequence with a period $P_X$ instead of sequence 012301230123\ldots, and
Our setting

We suppose that

- $* = *_i$ for all $i = 1, 2, \ldots, 79$, but we work with a general finite quasigroup $(Q, *)$,
- $X = (x_i) \in Q^\mathbb{N}$ a periodic sequence with a period $P_X$ instead of sequence 012301230123 $\ldots$, and
- $Y = (y_i) \in Q^\mathbb{N}$ a sequence with no special property (we have arbitrary number of rows).
### System B

<table>
<thead>
<tr>
<th></th>
<th>$x_0$</th>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>\cdots</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y_0$</td>
<td>$y_0 \ast x_0$</td>
<td>$(y_0 \ast x_0) \ast x_1$</td>
<td>\cdots</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$y_1$</td>
<td>$y_1 \ast (y_0 \ast x_0)$</td>
<td>$(y_1 \ast (y_0 \ast x_0)) \ast ((y_0 \ast x_0) \ast x_1)$</td>
<td>\cdots</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$y_2$</td>
<td>$y_2 \ast (y_1 \ast (y_0 \ast x_0))$</td>
<td>\cdots</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$y_3$</td>
<td>\vdots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure:** System B
Proposition

Each row of System B is periodic, for any sequence 
\[ Y = (y_i)_{i=1}^{\infty} \in \mathbb{Q}^N. \]
Proposition

Each row of System B is periodic, for any sequence $Y = (y_i)_{i=1}^\infty \in Q^\mathbb{N}$.
Moreover, denote by $P_0$ be the period of the sequence $X$ and by $P_i$ the period of the $i$th row of System B. Then there exists $k_i \in \{1, 2, \ldots, |Q|\}$ such that

$$P_i = k_i \cdot P_{i-1} \quad \text{for each } i \geq 1.$$
Proposition

Each row of System B is periodic, for any sequence $Y = (y_i)_{i=1}^\infty \in Q^N$. Moreover, denote by $P_0$ be the period of the sequence $X$ and by $P_i$ the period of the $i$th row of System B. Then there exists $k_i \in \{1, 2, \ldots, |Q|\}$ such that

$$P_i = k_i \cdot P_{i-1} \quad \text{for each } i \geq 1.$$ 

Corollary

- Each row of System A is periodic.
Proposition

Each row of System B is periodic, for any sequence
\[ Y = (y_i)_{i=1}^{\infty} \in Q^N. \]
Moreover, denote by \( P_0 \) be the period of the sequence \( X \) and
by \( P_i \) the period of the \( i \)th row of System B. Then there exists
\( k_i \in \{1, 2, \ldots, |Q|\} \) such that

\[ P_i = k_i \cdot P_{i-1} \quad \text{for each } i \geq 1. \]

Corollary

- Each row of System A is periodic.
- The keystream has period \( 2^n \) for some \( n = 0, \ldots, 161 \).
Periods for central quasigroups

A central quasigroup (T-quasigroup, linear over an Abelian group) is a quasigroup \((Q, \ast)\) such that there exists an Abelian group \(G = (Q, +)\), \(\alpha, \beta \in \text{Aut}(G)\), and \(c \in Q\) such that \(x \ast y = \alpha(x) + \beta(y) + c\) for all \(x, y \in Q\).

A medial quasigroup (entropic quasigroup) is a central quasigroup such that the automorphisms \(\alpha\) and \(\beta\) commute.

For central quasigroups, the problem to compute periods of System B leads to the problem to compute periods in the group ring \(\mathbb{Z}[eG]\).
A central quasigroup (T-quasigroup, linear over an Abelian group) is a quasigroup \((Q, \ast)\) such that there exists an Abelian group \(G = (Q, +)\), \(\alpha, \beta \in \text{Aut}(G)\), and \(c \in Q\) such that

\[
x \ast y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.
\]
A *central quasigroup* (T-quasigroup, linear over an Abelian group) is a quasigroup \((Q, \ast)\) such that there exists an Abelian group \(G = (Q, +)\), \(\alpha, \beta \in \text{Aut}(G)\), and \(c \in Q\) such that

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

A *medial quasigroup* (entropic quasigroup) is a central quasigroup such that the automorphisms \(\alpha\) and \(\beta\) commute.
A central quasigroup (T-quasigroup, linear over an Abelian group) is a quasigroup \((Q, \ast)\) such that there exists an Abelian group \(G = (Q, +)\), \(\alpha, \beta \in \text{Aut}(G)\), and \(c \in Q\) such that
\[
x \ast y = \alpha(x) + \beta(y) + c \quad \text{for all } x, y \in Q.
\]

A medial quasigroup (entropic quasigroup) is a central quasigroup such that the automorphisms \(\alpha\) and \(\beta\) commute.

For central quasigroups, the problem to compute periods of System B leads to the problem to compute periods in the group ring \(\mathbb{Z}_e G[\text{Aut}(G)]\).
<table>
<thead>
<tr>
<th>$id_G$</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta$</td>
<td>$\alpha \beta + \beta \alpha$</td>
<td>$\alpha^2 \beta + \alpha \beta \alpha + \beta \alpha^2$</td>
</tr>
<tr>
<td>$\beta^2$</td>
<td>$\alpha \beta^2 + \beta \alpha \beta + \beta^2 \alpha$</td>
<td>$\alpha^2 \beta^2 + \alpha \beta \alpha \beta + \alpha \beta^2 \alpha + \beta \alpha^2 \beta + \beta \alpha \beta \alpha + \beta^2 \alpha^2$</td>
</tr>
<tr>
<td>$\beta^3$</td>
<td>$\alpha \beta^3 + \beta \alpha \beta^2 + \beta^2 \alpha \beta + \beta^3 \alpha$</td>
<td></td>
</tr>
<tr>
<td>$\beta^4$</td>
<td>$\alpha \beta^4 + \beta \alpha \beta^3 + \beta^2 \alpha \beta^2 + \beta^3 \alpha \beta + \beta^4 \alpha$</td>
<td></td>
</tr>
</tbody>
</table>

Figure: System C
### Proposition

Denote by $P_X$ be the period of the sequence $X$ and by $P_i$ the period of the $i$th row of System C. Then for each $i \in \mathbb{N}$, $e_G \cdot \text{lcm}(P_X, P_i)$ is a period (not necessary minimal) of the $i$th row of System B.
Proposition

Let \( e_G = p_1^{r_1} \cdots p_n^{r_n} \), where \( p_k \) are distinct primes. Let \( (Q, *) \) be a medial quasigroup. Denote by \( P_i \) the period of the \( i \)th row of System B. Then there is a constant \( C > 0 \) such that \( P_i < C \cdot i^n \) holds for all sufficiently large \( i \).
Proposition

Let \( e_G = p_1^{r_1} \cdots p_n^{r_n} \), where \( p_k \) are distinct primes. Let \((Q, \ast)\) be a medial quasigroup. Denote by \( P_i \) the period of the \( i \)th row of System B. Then there is a constant \( C > 0 \) such that \( P_i < C \cdot i^n \) holds for all sufficiently large \( i \).

Proposition

Let \((Q, \ast)\) be a central quasigroup of order 4. Denote by \( P_i \) the period of the \( i \)th row of System B. Then there is a constant \( C > 0 \) such that \( P_i < C \cdot i \) holds for all sufficiently large \( i \).
We have found that for central quasigroup \((Q, \ast)\) of order 4 the periods increase at most linearly, but Edon80 needs to generate sequences whose periods grow rapidly. This implies that the central quasigroups are not suitable for implementation of Edon80.
Further directions of research

- Analyse System B for non-central quasigroups.
Further directions of research

- Analyse System B for non-central quasigroups.
- Prove the conjecture that periods increase exponentially for non-central quasigroups.
Further directions of research

- Analyse System B for non-central quasigroups.
- Prove the conjecture that periods increase exponentially for non-central quasigroups.
- Find a concrete weak key for Edon80 or disprove its existence.