Quasigroups and stream cipher Edon-80

Andrea Frisová
e-mail: andrea.frisova@gmail.com
Charles University in Prague, Departement of Algebra

Edon-80 is a binary stream cipher. The keystream in Edon-80 is generated as a row of a certain infinite matrix whose elements are defined iteratively using quasigroup operations.

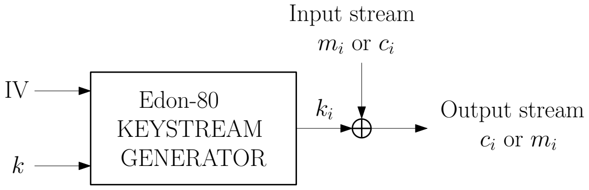

FIGURE 1. Graphical representation of Edon-80

The main problem of Edon-80 keystream generator is the question whether there exist weak keys, i.e. keys which induce a short period of the keystream. There are some indications that such keys exist, but their existence is based upon heuristic arguments [2] and statistical models [3] that do not seem to be completely substantiated. However, no weak key seems to have been explicitly described and its existence is thus still hypothetical.

The task to decide the existence of weak keys fully formally seems to be quite complicated. In our current work, we try to solve a related problem for which we have developed a formalism that might be useful in the future.

We do not compute the distribution of keystream period lengths, but we compute the lengths of periods of formal expressions that can be regarded as elements of a certain group ring. The keystream periods are then obtained by substituting into these expression variables that reflect the input data (in particular, the key) of the cipher.

Unfortunately, up to now we were able to perform calculations only for some classes of the quasigroups - the medial quasigroups and the central quasigroups. A *central quasigroup* is a quasigroup $(Q,*)$ such that there exists an Abelian group $(Q,+)$, $\alpha,\beta \in Aut((Q,+))$, 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.

This covers 19 of the 35 quasigroups of order four. Nevertheless, the four quasigroups of order four that are used in Edon-80 are not among those 19 quasigroups.

The stream cipher Edon-80 uses four fixed quasigroups of order 4.

The quasigroups $(Q,\cdot_0)$, $(Q,\cdot_1)$, $(Q,\cdot_2)$, $(Q,\cdot_3)$ are isotopic to the group $\mathbb{Z}_4$ and they are right holomorphic or only isotopic to the Abelian group $\mathbb{Z}_4$. (All quasigroups of order 4 are isotopic to an Abelian group.) A quasigroup is called *left (right) holomorphic* if it can be expressed as a principal isotope $G[\alpha,\beta]$ of

$\cdot_0$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

$\cdot_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

$\cdot_2$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$\cdot_3$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	3	2	1
3	2	1	0	3

FIGURE 2. The quasigroups used in Edon-80

group G, where α is a holomorphic permutation (respectively β is holomorphic). However, the other quasigroups can be obtained by a modification of the central quasigroups and that gives hope that we shall be able to extend the results in the future.

Our results can also justify why the central quasigroups are not actually used in Edon-80. These quasigroups were chosen based on computer experiments, because they gave the longest periods and no regular output.

Let $(Q, *)$ be a quasigroup and $Y = (y_i)_{i=1}^{\infty}$ be a sequence of elements from Q. From a periodic sequence $X \in Q^{\mathbb{N}}$ we generated sequences using the left iterated translations $\tau_{y_i,(Q.*)}$ and we tried to describe how the periods of the generated sequence change. We have found out that for central quasigroup $(Q, *)$ of order 4 the periods of these sequences increase at most linearly. This means that the periods increase slowly, however Edon-80 needs to generate sequences whose periods grow rapidly. It means that the central quasigroups of order 4 are not very suitable for implementation in Edon-80.

Our results indicates that the periods increase much faster when using the quasigroups for which the exponent of the underlying group factorises to a bigger number of distinct primes. Further, it is more convenient to use non-central quasigroups. For those the authors of Edon-80 conjecture that the periods increase exponentially, but left holomorphic quasigroup give the shorter periods.

REFERENCES

[1] eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/edon80p3.html`

[2] J. Hong, *Remarks on the Period of Edon80*, eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/papersdir/041.pdf`

[3] D. Gligoroski, S. Markovski, L. Kocarev and M. Gušev, *Understanding Periods in Edon80*, eSTREAM, ECRYPT stream cipher project,
`http://www.ecrypt.eu.org/stream/papersdir/054.pdf`

[4] Diploma Thesis of Andrea Frisová,
`http://artax.karlin.mff.cuni.cz/~chria3am/thesis/`

[5] Aleš Drápal, *Group isotopes and a holomorphic actions*, Results in Mathematics 54 (2009), 253-272.