

A Note on Algebraic Properties of Quasigroups in Edon80

Milan Vojvoda, Marek Sýs and Matúš Jókay

milan.vojvoda@stuba.sk, marek.sys@stuba.sk,
y@fornax.elf.stuba.sk

Department of Applied Informatics and Information Technology
Faculty of Electrical Engineering and Information Technology
Slovak University of Technology
Ilkovičova 3, 812 19 Bratislava, Slovak Republic

Abstract. Stream cipher Edon80 [6] is one of the submissions to the ECRYPT Stream Cipher Project – eSTREAM that passed to the Phase II of this project. The core of this cipher is based on pipelined quasigroup transformations using the so called e-transformers [6]. We study algebraic properties of the suggested quasigroups for use in the stream cipher Edon80 and prove that all the suggested quasigroups for use in Edon80 are isotopic with the quasigroup of modular subtraction of order 4, and also with the group $(\mathbb{Z}_4, +)$.

Keywords: stream cipher, hash function, quasigroup, isotopy.

2000 Mathematics Subject Classification: 94A60, 94A55, 68P25.

1 Introduction

The need for random and pseudorandom sequences arises in many applications, e.g. in modelling, simulations, and of course in cryptography. Pseudorandom sequences are the core of stream ciphers. They are popular due to their high encryption/decryption speed. Their simple and cheap hardware design is often preferred in real-world applications. The design goal in stream ciphers is to efficiently produce pseudorandom sequences - keystreams (i.e. sequences that possess properties common to truly random sequences and in some sense are "indistinguishable" from these sequences).

The usage of quasigroups (resp. Latin squares) in cryptography is not very common. In spite of that various cryptosystems based on quasigroups appeared in past few years. The isotopy of quasigroups was firstly considered in the design of the block cipher IDEA, where three non-isotopic groups were used. The theory of S-boxes based on quasigroups was studied in [14] and in [7] as well, where it was shown that in a quasigroup setting, it is possible to construct an S-box with the completely flat difference table. Stream ciphers based on quasigroups were proposed in [11] and in [13] (attacks against this cipher can be found in [15]

and [16]). The suitability of quasigroup transformation for cryptography was later studied in [12]. The possibility of using quasigroups for the design of hash functions and MACs was studied e.g. in [1], [5], [3], and [4]. Attacks against one version of hash function from [3], [4] can be found in [17].

Stream cipher Edon80 [6] is one of the submissions to the ECRYPT Stream Cipher Project – eSTREAM that passed to the Phase II of this project. Although it is not a focused Phase II submission, it is interesting from the design point of view. The core of this cipher is based on pipelined quasigroup transformations using the so called e-transformers [6]. The analysis of this cipher is at the very beginning. The only paper, except the submission [6] itself, dealing with analysis of Edon80 is [9]. Implementation of Edon80 is discussed in [10]. In this paper, we study some algebraic properties of the suggested quasigroups for use in the stream cipher Edon80 and prove that all the suggested quasigroups for use in Edon80 are isotopic with the quasigroup of modular subtraction of order 4, and also with the group $(Z_4, +)$.

The structure of this paper is as follows. Section 2 recalls some basic notions from the theory of quasigroups. The quasigroups used in Edon80 are described in Section 3. Main results of this paper are stated in Section 4. Finally, conclusions are given in Section 5, where also several open questions are stated.

2 Preliminaries

Definition 1. [2] *The structure $(Q, *)$, $Q = \{q_1, q_2, \dots, q_n\}$, $\|Q\| = n$ is called a finite quasigroup of order n if, when any two elements $a, b \in Q$ are given, the equations $a * x = b$ and $y * a = b$ each have exactly one solution. Thus the Cayley table of a finite quasigroup of order n is a Latin square, i.e. an $n \times n$ array with the property that each row and each column contains the permutation of symbols from Q .*

One of the ways how to deal with quasigroup operation is to store its Cayley table. However there are several special quasigroups, where the quasigroup operation can be specified using common arithmetic operations. One such an example is the quasigroup of modular subtraction (QMS), which was also used in [3], [4].

The operation $*_{MS}$ in QMS is then given as

$$a *_{MS} b = a + (n - b) \bmod n,$$

where $a, b \in Q$, and $n = \|Q\|$. Table 1 shows the specification of the QMS of order 4.

Usage of such an "easy to evaluate" expression for the definition of the operation $*$ on a quasigroup allows us to use quasigroups with a very large number of elements. Moreover, the isotopism of quasigroups gives us the power to use a large number of isotopic quasigroups where the evaluation of quasigroup operations will be done almost only using the mentioned "easy to evaluate" expression.

Table 1. Quasigroup operation table in QMS, $n = 4$

$*_{MS}$	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Definition 2. [2] Let (G, \cdot) and $(H, *)$ be two quasigroups. An ordered triple (θ, φ, ψ) of one-to-one mappings θ, φ, ψ of the set G onto the set H is called an isotopism of (G, \cdot) upon $(H, *)$ if $\theta(x) * \varphi(y) = \psi(x \cdot y)$ for all x, y in G . The quasigroups (G, \cdot) and $(H, *)$ are then said to be isotopic.

It simply means that the Caley table of the quasigroup (G, \cdot) can be obtained from the Caley table of the quasigroup $(H, *)$, resp. vice versa, simply by rearranging rows, columns, and renaming elements.

Example 1. Let $(Q, *_{MS})$, $\|Q\| = 4$ be the QMS with the Caley table given in Table 1. Let $\theta = (\theta(0), \theta(1), \theta(2), \theta(3)) = (1, 2, 3, 0)$, $\varphi = (\varphi(0), \varphi(1), \varphi(2), \varphi(3)) = (3, 2, 1, 0)$, and $\psi = (\psi(0), \psi(1), \psi(2), \psi(3)) = (2, 0, 3, 1)$. Let (θ, φ, ψ) be the isotopism of (Q, \cdot) upon $(Q, *_{MS})$. Then the Caley table of the quasigroup (Q, \cdot) looks like the one shown in Table 2.

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

Table 2. Quasigroup operation in (Q, \cdot)

A nice trick is that the quasigroup operation in (Q, \cdot) may also be written as

$$a \cdot b = \psi^{-1}(\theta(a) + (n - \varphi(b)) \bmod n), \quad n = \|Q\|.$$

3 Quasigroups in Edon80

Edon80 employs in its core a pipelined architecture of 80 so-called e-transformers [6]. Each e-transformer has associated one of the four quasigroups of order 4. The quasigroups chosen for Edon80 are shown in Table 3. The association of quasigroups to e-transformers is determined by the key of the cipher. We omit the details of the cipher since we are dealing only with algebraic properties of the Edon80 quasigroups.

It is known that there are 576 quasigroups of order 4. According to [6, Part1], 384 of them are suitable, and 64 are very suitable for use in Edon80. These 64 quasigroups are listed in [6, Part5].

\bullet_0	0 1 2 3	\bullet_1	0 1 2 3
0	0 2 1 3	0	1 3 0 2
1	2 1 3 0	1	0 1 2 3
2	1 3 0 2	2	2 0 3 1
3	3 0 2 1	3	3 2 1 0

\bullet_2	0 1 2 3	\bullet_3	0 1 2 3
0	2 1 0 3	0	3 2 1 0
1	1 2 3 0	1	1 0 3 2
2	3 0 2 1	2	0 3 2 1
3	0 3 1 2	3	2 1 0 3

Table 3. Quasigroups suggested for use in Edon80

4 Results

In this Section we investigate some algebraic properties of the 64 quasigroups suitable for use in Edon80. According to [6, Part 3], the 4 quasigroups chosen for Edon80 (shown in Table 3) have a very small number of algebraic properties: they are not groups, not semigroups and they are not commutative.

Firstly, we studied the isotopism of the quasigroups suggested for use in Edon80 with the QMS. The motivation for this was that the isotopism of QMS was used in [3] and [4].

Theorem 1. *All the 64 quasigroups [6, Part5], suggested for use in Edon80, are isotopic to the quasigroup of modular subtraction.*

Proof. The proof of this Theorem was done by exhaustive search on a PC. The concrete mappings for the four quasigroups from [6, Part 1] (see also Table 3) are shown in Tables 4 and 5.

Moreover, we are able to prove that the number of different isotopic mappings of QMS upon some quasigroup isotopic to QMS is exactly $\Phi(n)n^2$, where Φ is the Euler totient function and n is the order of QMS.

Theorem 1 allows us to implement the quasigroup operations in Edon80 using QMS, that uses common arithmetic operations for its quasigroup operation, and some mappings that define the isotopism of QMS upon the concrete Edon80 quasigroups.

Moreover we believe that the alternate description of quasigroup operations in Edon80 might open a new way to attack the cipher.

The following Lemma points out one structural property of QMS.

Lemma 1. *Quasigroup of modular subtraction contains a right unit, namely it is 0.*

Proof. The operation $*_{MS}$ in QMS is given as

$$a *_{MS} b = a + (n - b) \bmod n,$$

θ_0	φ_0	ψ_0	θ_1	φ_1	ψ_1
(0,1,2,3)	(0,3,2,1)	(0,2,1,3)	(0,1,2,3)	(0,1,3,2)	(1,0,2,3)
(0,1,2,3)	(1,0,3,2)	(3,1,0,2)	(0,1,2,3)	(1,2,0,3)	(0,3,1,2)
(0,1,2,3)	(2,1,0,3)	(2,0,3,1)	(0,1,2,3)	(2,3,1,0)	(3,2,0,1)
(0,1,2,3)	(3,2,1,0)	(1,3,2,0)	(0,1,2,3)	(3,0,2,1)	(2,1,3,0)
(0,3,2,1)	(0,1,2,3)	(0,2,3,1)	(0,3,2,1)	(0,3,1,2)	(3,0,2,1)
(0,3,2,1)	(1,2,3,0)	(3,1,2,0)	(0,3,2,1)	(1,0,2,3)	(2,3,1,0)
(0,3,2,1)	(2,3,0,1)	(2,0,1,3)	(0,3,2,1)	(2,1,3,0)	(1,2,0,3)
(0,3,2,1)	(3,0,1,2)	(1,3,0,2)	(0,3,2,1)	(3,2,0,1)	(0,1,3,2)
(1,0,3,2)	(0,1,2,3)	(1,3,0,2)	(1,0,3,2)	(0,3,1,2)	(0,1,3,2)
(1,0,3,2)	(1,2,3,0)	(0,2,3,1)	(1,0,3,2)	(1,0,2,3)	(3,0,2,1)
(1,0,3,2)	(2,3,0,1)	(3,1,2,0)	(1,0,3,2)	(2,1,3,0)	(2,3,1,0)
(1,0,3,2)	(3,0,1,2)	(2,0,1,3)	(1,0,3,2)	(3,2,0,1)	(1,2,0,3)
(1,2,3,0)	(0,3,2,1)	(1,3,2,0)	(1,2,3,0)	(0,1,3,2)	(2,1,3,0)
(1,2,3,0)	(1,0,3,2)	(0,2,1,3)	(1,2,3,0)	(1,2,0,3)	(1,0,2,3)
(1,2,3,0)	(2,1,0,3)	(3,1,0,2)	(1,2,3,0)	(2,3,1,0)	(0,3,1,2)
(1,2,3,0)	(3,2,1,0)	(2,0,3,1)	(1,2,3,0)	(3,0,2,1)	(3,2,0,1)
(2,1,0,3)	(0,1,2,3)	(2,0,1,3)	(2,1,0,3)	(0,3,1,2)	(1,2,0,3)
(2,1,0,3)	(1,2,3,0)	(1,3,0,2)	(2,1,0,3)	(1,0,2,3)	(0,1,3,2)
(2,1,0,3)	(2,3,0,1)	(0,2,3,1)	(2,1,0,3)	(2,1,3,0)	(3,0,2,1)
(2,1,0,3)	(3,0,1,2)	(3,1,2,0)	(2,1,0,3)	(3,2,0,1)	(2,3,1,0)
(2,3,0,1)	(0,3,2,1)	(2,0,3,1)	(2,3,0,1)	(0,1,3,2)	(3,2,0,1)
(2,3,0,1)	(1,0,3,2)	(1,3,2,0)	(2,3,0,1)	(1,2,0,3)	(2,1,3,0)
(2,3,0,1)	(2,1,0,3)	(0,2,1,3)	(2,3,0,1)	(2,3,1,0)	(1,0,2,3)
(2,3,0,1)	(3,2,1,0)	(3,1,0,2)	(2,3,0,1)	(3,0,2,1)	(0,3,1,2)
(3,0,1,2)	(0,3,2,1)	(3,1,0,2)	(3,0,1,2)	(0,1,3,2)	(0,3,1,2)
(3,0,1,2)	(1,0,3,2)	(2,0,3,1)	(3,0,1,2)	(1,2,0,3)	(3,2,0,1)
(3,0,1,2)	(2,1,0,3)	(1,3,2,0)	(3,0,1,2)	(2,3,1,0)	(2,1,3,0)
(3,0,1,2)	(3,2,1,0)	(0,2,1,3)	(3,0,1,2)	(3,0,2,1)	(1,0,2,3)
(3,2,1,0)	(0,1,2,3)	(3,1,2,0)	(3,2,1,0)	(0,3,1,2)	(2,3,1,0)
(3,2,1,0)	(1,2,3,0)	(2,0,1,3)	(3,2,1,0)	(1,0,2,3)	(1,2,0,3)
(3,2,1,0)	(2,3,0,1)	(1,3,0,2)	(3,2,1,0)	(2,1,3,0)	(0,1,3,2)
(3,2,1,0)	(3,0,1,2)	(0,2,3,1)	(3,2,1,0)	(3,2,0,1)	(3,0,2,1)

Table 4. Isotopisms of the Edon80 quasigroups $(\{0, 1, 2, 3\}, \bullet_0)$, resp. $(\{0, 1, 2, 3\}, \bullet_1)$ upon QMS (of order 4)

where $a, b \in Q$, and $n = \|Q\|$. It is easy to see that $\forall a \in Q$ it holds that $a *_{MS} 0 = a$.

Theorem 2. *Quasigroup of modular subtraction of order n is isotopic with the group $(\mathbb{Z}_n, +)$.*

Proof. The following mappings define the isotopism of QMS upon $(\mathbb{Z}_n, +)$: θ and ψ are identities, and $\varphi(x) = (n - x) \bmod n$.

Using Theorem 1, Theorem 2 and a simple composition of mappings that define the isotopism we obtain the following Corrolary.

θ_2	φ_2	ψ_2	θ_3	φ_3	ψ_3
(0,2,1,3)	(0,2,1,3)	(3,2,0,1)	(0,2,1,3)	(0,1,2,3)	(1,2,3,0)
(0,2,1,3)	(1,3,2,0)	(2,1,3,0)	(0,2,1,3)	(1,2,3,0)	(0,1,2,3)
(0,2,1,3)	(2,0,3,1)	(1,0,2,3)	(0,2,1,3)	(2,3,0,1)	(3,0,1,2)
(0,2,1,3)	(3,1,0,2)	(0,3,1,2)	(0,2,1,3)	(3,0,1,2)	(2,3,0,1)
(0,2,3,1)	(0,2,3,1)	(1,2,0,3)	(0,2,3,1)	(0,3,2,1)	(3,2,1,0)
(0,2,3,1)	(1,3,0,2)	(0,1,3,2)	(0,2,3,1)	(1,0,3,2)	(2,1,0,3)
(0,2,3,1)	(2,0,1,3)	(3,0,2,1)	(0,2,3,1)	(2,1,0,3)	(1,0,3,2)
(0,2,3,1)	(3,1,2,0)	(2,3,1,0)	(0,2,3,1)	(3,2,1,0)	(0,3,2,1)
(1,3,0,2)	(0,2,3,1)	(2,3,1,0)	(1,3,0,2)	(0,3,2,1)	(0,3,2,1)
(1,3,0,2)	(1,3,0,2)	(1,2,0,3)	(1,3,0,2)	(1,0,3,2)	(3,2,1,0)
(1,3,0,2)	(2,0,1,3)	(0,1,3,2)	(1,3,0,2)	(2,1,0,3)	(2,1,0,3)
(1,3,0,2)	(3,1,2,0)	(3,0,2,1)	(1,3,0,2)	(3,2,1,0)	(1,0,3,2)
(1,3,2,0)	(0,2,1,3)	(0,3,1,2)	(1,3,2,0)	(0,1,2,3)	(2,3,0,1)
(1,3,2,0)	(1,3,2,0)	(3,2,0,1)	(1,3,2,0)	(1,2,3,0)	(1,2,3,0)
(1,3,2,0)	(2,0,3,1)	(2,1,3,0)	(1,3,2,0)	(2,3,0,1)	(0,1,2,3)
(1,3,2,0)	(3,1,0,2)	(1,0,2,3)	(1,3,2,0)	(3,0,1,2)	(3,0,1,2)
(2,0,1,3)	(0,2,3,1)	(3,0,2,1)	(2,0,1,3)	(0,3,2,1)	(1,0,3,2)
(2,0,1,3)	(1,3,0,2)	(2,3,1,0)	(2,0,1,3)	(1,0,3,2)	(0,3,2,1)
(2,0,1,3)	(2,0,1,3)	(1,2,0,3)	(2,0,1,3)	(2,1,0,3)	(3,2,1,0)
(2,0,1,3)	(3,1,2,0)	(0,1,3,2)	(2,0,1,3)	(3,2,1,0)	(2,1,0,3)
(2,0,3,1)	(0,2,1,3)	(1,0,2,3)	(2,0,3,1)	(0,1,2,3)	(3,0,1,2)
(2,0,3,1)	(1,3,2,0)	(0,3,1,2)	(2,0,3,1)	(1,2,3,0)	(2,3,0,1)
(2,0,3,1)	(2,0,3,1)	(3,2,0,1)	(2,0,3,1)	(2,3,0,1)	(1,2,3,0)
(2,0,3,1)	(3,1,0,2)	(2,1,3,0)	(2,0,3,1)	(3,0,1,2)	(0,1,2,3)
(3,1,0,2)	(0,2,1,3)	(2,1,3,0)	(3,1,0,2)	(0,1,2,3)	(0,1,2,3)
(3,1,0,2)	(1,3,2,0)	(1,0,2,3)	(3,1,0,2)	(1,2,3,0)	(3,0,1,2)
(3,1,0,2)	(2,0,3,1)	(0,3,1,2)	(3,1,0,2)	(2,3,0,1)	(2,3,0,1)
(3,1,0,2)	(3,1,0,2)	(3,2,0,1)	(3,1,0,2)	(3,0,1,2)	(1,2,3,0)
(3,1,2,0)	(0,2,3,1)	(0,1,3,2)	(3,1,2,0)	(0,3,2,1)	(2,1,0,3)
(3,1,2,0)	(1,3,0,2)	(3,0,2,1)	(3,1,2,0)	(1,0,3,2)	(1,0,3,2)
(3,1,2,0)	(2,0,1,3)	(2,3,1,0)	(3,1,2,0)	(2,1,0,3)	(0,3,2,1)
(3,1,2,0)	(3,1,2,0)	(1,2,0,3)	(3,1,2,0)	(3,2,1,0)	(3,2,1,0)

Table 5. Isotopisms of the Edon80 quasigroups $(\{0, 1, 2, 3\}, \bullet_2)$, resp. $(\{0, 1, 2, 3\}, \bullet_3)$ upon QMS (of order 4)

Corollary 1. *All the 64 quasigroups [6, Part5], suggested for use in Edon80, are isotopic with the group $(\mathbb{Z}_n, +)$. (The concrete mappings for the four quasigroups from [6, Part 1] (see also Table 3) are shown in Tables 6 and 7.)*

5 Conclusion

Stream cipher Edon80 [6] is one of the submissions to the ECRYPT Stream Cipher Project – eSTREAM that passed to the Phase II of this project. Although

θ_0	φ_0	ψ_0	θ_1	φ_1	ψ_1
(0,1,2,3)	(0,1,2,3)	(0,2,1,3)	(0,1,2,3)	(0,3,1,2)	(1,0,2,3)
(0,1,2,3)	(1,2,3,0)	(1,3,2,0)	(0,1,2,3)	(1,0,2,3)	(2,1,3,0)
(0,1,2,3)	(2,3,0,1)	(2,0,3,1)	(0,1,2,3)	(2,1,3,0)	(3,2,0,1)
(0,1,2,3)	(3,0,1,2)	(3,1,0,2)	(0,1,2,3)	(3,2,0,1)	(0,3,1,2)
(0,3,2,1)	(0,3,2,1)	(0,2,3,1)	(0,3,2,1)	(0,1,3,2)	(3,0,2,1)
(0,3,2,1)	(1,0,3,2)	(1,3,0,2)	(0,3,2,1)	(1,2,0,3)	(0,1,3,2)
(0,3,2,1)	(2,1,0,3)	(2,0,1,3)	(0,3,2,1)	(2,3,1,0)	(1,2,0,3)
(0,3,2,1)	(3,2,1,0)	(3,1,2,0)	(0,3,2,1)	(3,0,2,1)	(2,3,1,0)
(1,0,3,2)	(0,3,2,1)	(1,3,0,2)	(1,0,3,2)	(0,1,3,2)	(0,1,3,2)
(1,0,3,2)	(1,0,3,2)	(2,0,1,3)	(1,0,3,2)	(1,2,0,3)	(1,2,0,3)
(1,0,3,2)	(2,1,0,3)	(3,1,2,0)	(1,0,3,2)	(2,3,1,0)	(2,3,1,0)
(1,0,3,2)	(3,2,1,0)	(0,2,3,1)	(1,0,3,2)	(3,0,2,1)	(3,0,2,1)
(1,2,3,0)	(0,1,2,3)	(1,3,2,0)	(1,2,3,0)	(0,3,1,2)	(2,1,3,0)
(1,2,3,0)	(1,2,3,0)	(2,0,3,1)	(1,2,3,0)	(1,0,2,3)	(3,2,0,1)
(1,2,3,0)	(2,3,0,1)	(3,1,0,2)	(1,2,3,0)	(2,1,3,0)	(0,3,1,2)
(1,2,3,0)	(3,0,1,2)	(0,2,1,3)	(1,2,3,0)	(3,2,0,1)	(1,0,2,3)
(2,1,0,3)	(0,3,2,1)	(2,0,1,3)	(2,1,0,3)	(0,1,3,2)	(1,2,0,3)
(2,1,0,3)	(1,0,3,2)	(3,1,2,0)	(2,1,0,3)	(1,2,0,3)	(2,3,1,0)
(2,1,0,3)	(2,1,0,3)	(0,2,3,1)	(2,1,0,3)	(2,3,1,0)	(3,0,2,1)
(2,1,0,3)	(3,2,1,0)	(1,3,0,2)	(2,1,0,3)	(3,0,2,1)	(0,1,3,2)
(2,3,0,1)	(0,1,2,3)	(2,0,3,1)	(2,3,0,1)	(0,3,1,2)	(3,2,0,1)
(2,3,0,1)	(1,2,3,0)	(3,1,0,2)	(2,3,0,1)	(1,0,2,3)	(0,3,1,2)
(2,3,0,1)	(2,3,0,1)	(0,2,1,3)	(2,3,0,1)	(2,1,3,0)	(1,0,2,3)
(2,3,0,1)	(3,0,1,2)	(1,3,2,0)	(2,3,0,1)	(3,2,0,1)	(2,1,3,0)
(3,0,1,2)	(0,1,2,3)	(3,1,0,2)	(3,0,1,2)	(0,3,1,2)	(0,3,1,2)
(3,0,1,2)	(1,2,3,0)	(0,2,1,3)	(3,0,1,2)	(1,0,2,3)	(1,0,2,3)
(3,0,1,2)	(2,3,0,1)	(1,3,2,0)	(3,0,1,2)	(2,1,3,0)	(2,1,3,0)
(3,0,1,2)	(3,0,1,2)	(2,0,3,1)	(3,0,1,2)	(3,2,0,1)	(3,2,0,1)
(3,2,1,0)	(0,3,2,1)	(3,1,2,0)	(3,2,1,0)	(0,1,3,2)	(2,3,1,0)
(3,2,1,0)	(1,0,3,2)	(0,2,3,1)	(3,2,1,0)	(1,2,0,3)	(3,0,2,1)
(3,2,1,0)	(2,1,0,3)	(1,3,0,2)	(3,2,1,0)	(2,3,1,0)	(0,1,3,2)
(3,2,1,0)	(3,2,1,0)	(2,0,1,3)	(3,2,1,0)	(3,0,2,1)	(1,2,0,3)

Table 6. Isotopisms of the Edon80 quasigroups $(\{0, 1, 2, 3\}, \bullet_0)$, resp. $(\{0, 1, 2, 3\}, \bullet_1)$ upon $(Z_4, +)$

it is not a focused Phase II submission, it is interesting from the design point of view. The use of quasigroup is a non-standard technique in cryptography.

In this paper, we studied some algebraic properties of the suggested quasigroups for use in the stream cipher Edon80. We proved that all the suggested quasigroups for use in Edon80 are isotopic with the quasigroup of modular subtraction of order 4, and also with the group $(Z_4, +)$.

Theorem 1 allows to implement the quasigroup operations in Edon80 using QMS, that uses only common arithmetic operations for its quasigroup operation,

θ_2	φ_2	ψ_2	θ_3	φ_3	ψ_3
(0,2,1,3)	(0,2,3,1)	(3,2,0,1)	(0,2,1,3)	(0,3,2,1)	(1,2,3,0)
(0,2,1,3)	(1,3,0,2)	(0,3,1,2)	(0,2,1,3)	(1,0,3,2)	(2,3,0,1)
(0,2,1,3)	(2,0,1,3)	(1,0,2,3)	(0,2,1,3)	(2,1,0,3)	(3,0,1,2)
(0,2,1,3)	(3,1,2,0)	(2,1,3,0)	(0,2,1,3)	(3,2,1,0)	(0,1,2,3)
(0,2,3,1)	(0,2,1,3)	(1,2,0,3)	(0,2,3,1)	(0,1,2,3)	(3,2,1,0)
(0,2,3,1)	(1,3,2,0)	(2,3,1,0)	(0,2,3,1)	(1,2,3,0)	(0,3,2,1)
(0,2,3,1)	(2,0,3,1)	(3,0,2,1)	(0,2,3,1)	(2,3,0,1)	(1,0,3,2)
(0,2,3,1)	(3,1,0,2)	(0,1,3,2)	(0,2,3,1)	(3,0,1,2)	(2,1,0,3)
(1,3,0,2)	(0,2,1,3)	(2,3,1,0)	(1,3,0,2)	(0,1,2,3)	(0,3,2,1)
(1,3,0,2)	(1,3,2,0)	(3,0,2,1)	(1,3,0,2)	(1,2,3,0)	(1,0,3,2)
(1,3,0,2)	(2,0,3,1)	(0,1,3,2)	(1,3,0,2)	(2,3,0,1)	(2,1,0,3)
(1,3,0,2)	(3,1,0,2)	(1,2,0,3)	(1,3,0,2)	(3,0,1,2)	(3,2,1,0)
(1,3,2,0)	(0,2,3,1)	(0,3,1,2)	(1,3,2,0)	(0,3,2,1)	(2,3,0,1)
(1,3,2,0)	(1,3,0,2)	(1,0,2,3)	(1,3,2,0)	(1,0,3,2)	(3,0,1,2)
(1,3,2,0)	(2,0,1,3)	(2,1,3,0)	(1,3,2,0)	(2,1,0,3)	(0,1,2,3)
(1,3,2,0)	(3,1,2,0)	(3,2,0,1)	(1,3,2,0)	(3,2,1,0)	(1,2,3,0)
(2,0,1,3)	(0,2,1,3)	(3,0,2,1)	(2,0,1,3)	(0,1,2,3)	(1,0,3,2)
(2,0,1,3)	(1,3,2,0)	(0,1,3,2)	(2,0,1,3)	(1,2,3,0)	(2,1,0,3)
(2,0,1,3)	(2,0,3,1)	(1,2,0,3)	(2,0,1,3)	(2,3,0,1)	(3,2,1,0)
(2,0,1,3)	(3,1,0,2)	(2,3,1,0)	(2,0,1,3)	(3,0,1,2)	(0,3,2,1)
(2,0,3,1)	(0,2,3,1)	(1,0,2,3)	(2,0,3,1)	(0,3,2,1)	(3,0,1,2)
(2,0,3,1)	(1,3,0,2)	(2,1,3,0)	(2,0,3,1)	(1,0,3,2)	(0,1,2,3)
(2,0,3,1)	(2,0,1,3)	(3,2,0,1)	(2,0,3,1)	(2,1,0,3)	(1,2,3,0)
(2,0,3,1)	(3,1,2,0)	(0,3,1,2)	(2,0,3,1)	(3,2,1,0)	(2,3,0,1)
(3,1,0,2)	(0,2,3,1)	(2,1,3,0)	(3,1,0,2)	(0,3,2,1)	(0,1,2,3)
(3,1,0,2)	(1,3,0,2)	(3,2,0,1)	(3,1,0,2)	(1,0,3,2)	(1,2,3,0)
(3,1,0,2)	(2,0,1,3)	(0,3,1,2)	(3,1,0,2)	(2,1,0,3)	(2,3,0,1)
(3,1,0,2)	(3,1,2,0)	(1,0,2,3)	(3,1,0,2)	(3,2,1,0)	(3,0,1,2)
(3,1,2,0)	(0,2,1,3)	(0,1,3,2)	(3,1,2,0)	(0,1,2,3)	(2,1,0,3)
(3,1,2,0)	(1,3,2,0)	(1,2,0,3)	(3,1,2,0)	(1,2,3,0)	(3,2,1,0)
(3,1,2,0)	(2,0,3,1)	(2,3,1,0)	(3,1,2,0)	(2,3,0,1)	(0,3,2,1)
(3,1,2,0)	(3,1,0,2)	(3,0,2,1)	(3,1,2,0)	(3,0,1,2)	(1,0,3,2)

Table 7. Isotopisms of the Edon80 quasigroups $(\{0, 1, 2, 3\}, \bullet_2)$, resp. $(\{0, 1, 2, 3\}, \bullet_3)$ upon $(Z_4, +)$

and some mappings that define the isotopism of QMS upon the concrete Edon80 quasigroups.

Moreover we believe that the alternate description of quasigroup operations in Edon80 might open a new way to attack the cipher.

Acknowledgement

The author gratefully acknowledges many helpful suggestions of Professor Otokar Grošek during the preparation of this paper. This work was partially supported by VEGA-grant 1/3115/06 and by the ESF grant JPD 3 2005/1-062.

References

1. Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: A Message Authentication Code Based on Latin Squares, Australian Conference on Information Security and Privacy (ACISP '97), Springer-Verlag, 1997, LNCS 1270, pp. 194-203.
2. Dénes, J., Keedwell, A.D.: Latin Squares and Their Applications, Academic Press, NY, 1974.
3. Dvorský, J., Ochodková, E., Snášel, V.: Hash Function Based on Quasigroups ("Hashovací funkce založená na kvazigrupách"), *Proceedings of Mikulášská kryptobesídka*, Praha, 2001, pp. 27-36 (in Czech).
4. Dvorský, J., Ochodková, E., Snášel, V.: Hash Functions Based on Large Quasigroups, *Proceedings of Velikonoční kryptologie*, Brno, 2002, pp. 1-8.
5. Gligoroski, D., Markovski, S., Bakeva, V.: On Infinite Class of Strongly Collision Resistant Hash Functions "Edon-F" with Variable Length of Output, Proceedings of 1st International Conference On Mathematics and Informatics for Industry, April, 2003, Thessaloniki, Greece.
6. Gligoroski, D., Markovski, S., Kocarev, L., Gusev, M.: Edon80, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/007, 2005, <http://www.ecrypt.eu.org/stream>.
7. Grošek, O., Satko, L., Nemoga, K.: Ideal Difference Tables from an Algebraic Point of View, Cryptology and Information Security, Proceedings of VI RECSI, Tenerife, Spain, September 2000, ammendment to CRIPTOLOGÍA y SEGURIDAD de la INFORMACIÓN, editors - P.Caballero-Gil and C.Hernández-Goya, RA-MA, Madrid, 2000, pp. 453-454.
8. Grošek, O., Horák, P., van Tran, T.: On Non-polynomial Latin Squares, Designs, Codes and Cryptography 32(1-3, 2004), pp. 217-226.
9. Hong, J.: Remarks on the Period of Edon80, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/041, 2005, <http://www.ecrypt.eu.org/stream>.
10. Kasper, M., Kumar, S., Lemke-Rust, K., Paar, C.: A Compact Implementation of Edon80, eSTREAM, ECRYPT Stream Cipher Project, Report 2006/057, 2006, <http://www.ecrypt.eu.org/stream>.
11. Markovski, S., Gligoroski, D., Andova, S.: Using Quasigroups for One-one Secure Encoding, Proceedings of LIRA '97 - Novi Sad Yugoslavia.
12. Markovski, S., Gligoroski, D., Kocarev, L.: Unbiased Random Sequences from Quasigroup String Transformations, Proceedings of Fast Software Encryption 2005, LNCS 3557, Springer-Verlag, 2005, pp. 163-180.
13. Ochodková, E., Snášel, V.: Using Quasigroups for Secure Encoding of File System, Proceedings of the International Scientific NATO PfP/PWP Conference "Security and Information Protection 2001", May 9-11, 2001, Brno, Czech Republic, pp.175-181.
14. Satko, L., Grošek, O.: Extremal Generalized S-Boxes, Computing and Informatics, Vol. 22(2003), No.1, pp. 85-99.
15. Vojvoda, M.: Cryptanalysis of a File Encoding System Based on a Quasigroup, Journal of Electrical Engineering, Vol. 54(2003), No. 12/s, pp. 69-71.
16. Vojvoda, M.: Attacks on a File Encryption System Based on Quasigroup, Proceedings of Elitech 2003, FEI STU Bratislava, 2003, pp. 54-56.
17. Vojvoda, M.: Cryptanalysis of One Hash Function Based on Quasigroup, Tatra Mountains Mathematical Publications, Vol. 29(2004), pp. 173-181.