Appl. Math. and Comp. Sci., 1996, vol.6, No.1, 109–121

A METHOD OF CONSTRUCTING QUASIGROUP-BASED STREAM-CIPHERS

CZESŁAW KOŚCIELNY*

A method for constructing endomorphic stream-ciphers over the alphabet of an arbitrary finite order q, based on quasigroups, is described. The presented ciphers, due to their simplicity, can be easily implemented, giving in consequence a very fast speed of enciphering and deciphering. The ciphers are also much more secure than the stream-cipher over $GF(2)$, because, if $q > 2$, the method allows one to form many invertible transformations which may be used to encipher and decipher; the number of these transformations increases very rapidly with respect to q.

1. Introduction

The aim of this paper is to focus the reader's attention on the existence of algebraic systems called quasigroups and to show that they can be beneficially applied in cryptography for constructing stream-ciphers. In the work it is demonstrated that it is possible to form quite easily a huge number of quasigroups using the concept of isotopy. An enormous number of quasigroups having more than a hundred elements would then allow us to construct more secure, much more easily implemented, and much faster cryptosystems than those involving huge integers or based on computing in finite fields of order of about 10^{100}, for which the enciphering and deciphering procedures are too slow and inefficient. Thus, the quasigroups are an advantageous alternative to the cryptographic tools exploited up to now (Beth *et al.*, 1992; Brassard, 1988), all the more so as these algebraic systems would probably be also useful in other cryptographic applications, e.g. block-ciphers, digital signatures, etc. It is also important for cryptology that some types of quasigroups can be easily generated.

2. Quasigroups and Isotopy

The concept of isotopy (Dénes and Keedwell, 1974) as well as the properties of quasigroups are not commonly known, therefore the most essential questions concerning these problems will be discussed in this section.

* Technical University of Zielona Góra, Department of Robotics and Software Engineering, ul. Podgórna 50, 65–246 Zielona Góra, Poland

An algebraic system Q consisting of a finite set of elements A in which a binary operation $(\circ)$ is defined

$$Q = \langle A, \circ \rangle \tag{1}$$

is called a *quasigroup* if, when any two elements $a, b \in A$ are given, each of the equations

$$a \circ x = b, \qquad y \circ a = b \tag{2}$$

has exactly one solution. Thus, a quasigroup is a rather simple algebraic system with one operation which need neither be commutative nor associative, but, according to (2), the operation table in a quasigroup must be a latin square. A quasigroup

$$L = \langle A, \circ \rangle \tag{3}$$

in which there exists an identity element $e \in A$ with the property that

$$\forall x \in A, \quad x \circ e = e \circ x = x \tag{4}$$

is called a *loop*. Let

$$Q_p = \langle G, \circ \rangle \tag{5}$$

and

$$Q_i = \langle H, \star \rangle \tag{6}$$

be two quasigroups. An ordered triple

$$(\pi_x, \ \pi_y, \ \pi_t) \tag{7}$$

of one-to-one mappings π_x, π_y, π_t of the set G onto the set H is called an *isotopism* of Q_p upon Q_i if

$$\pi_x(x) \star \pi_y(y) = \pi_t(x \circ y) \tag{8}$$

for all $x, y \in G$. It should be observed that the mapping π_t permutes the elements in the table of operations in a quasigroup Q_p, while π_x and π_y operate on the elements of the row and column border of this table, respectively. The quasigroups Q_p and Q_i are then said to be *isotopic*. It is also said that Q_i is an *isotope* of a primary quasigroup Q_p.

It follows from (8) that

$$X \star Y = \pi_t\left(\pi_x^{-1}(X) \circ \pi_y^{-1}(Y)\right) \tag{9}$$

for all $X, Y \in H$. Equation (9) allows one to operate on elements of Q_i if the table of operation in Q_p is known. It is evident that if $\pi_x = \pi_y = \pi_t$, then the algebraic systems (5) and (6) are isomorphic.

Tab. 1. The values of $(2^m!)^3$ versus m.

m	$(2^m!)^3$
2	13,824
3	6.55483×10^{13}
4	9.15923×10^{39}
5	1.82186×10^{106}
6	2.04292×10^{267}
7	5.73430×10^{646}
8	6.31226×10^{1520}
9	4.20458×10^{3499}

One can prove that the set of all isotopisms of a quasigroup of order q forms a group of order $(q!)^3$. However, the problem of classification and exact enumeration of quasigroups of order greater than 10 probably still remains unsolved. It is mentioned in (Dénes and Keedwell, 1974) that all reduced $n \times n$ latin squares (the ones which have their first row and column in natural order), are enumerated for $n \leq 9$. Since, in practice, the alphabets of order 2^m are used, the values of $(2^m!)^3$ are given in Tab. 1 to make the reader realize how many isotopes of one quasigroup of order 2^m can be formed.

3. Constructing a Quasigroup-Based Stream-Ciphers

The stream-ciphers discussed in this section are generalized in the sense that they can be constructed over any alphabet of q symbols, q denoting an arbitrary integer. Let

$$Q = \langle A, \check{+} \rangle \tag{10}$$

be an isotope of the primary algebraic system and let

$$M = m_1 \ m_2 \ \cdots \ m_i \ \cdots \tag{11}$$

$$K = k_1 \ k_2 \ \cdots \ k_i \ \cdots \tag{12}$$

$$C = c_1 \ c_2 \ \cdots \ c_i \ \cdots \tag{13}$$

denote the stream of characters of the plain-text, the stream of characters of the secret key and the stream of characters of the cryptogram, respectively. The characters of these three streams belong, of course, to the set A. The stream of characters of the cryptogram is generated by a generalized stream-cipher by means of an enciphering function f_e

$$c_i = f_e(m_i, k_i) \tag{14}$$

which, for each character of the plain-text and for the character of the key associated with it, determines a character of the cryptogram. During deciphering a function f_d

is used which reconstructs the character of the message, taking into account the character of the cryptogram and the corresponding character of the key

$$m_i = f_d(c_i, k_i) \tag{15}$$

It is obvious that

$$f_d\Big(f_e(m_i, k_i), k_i\Big) = m_i \tag{16}$$

must be satisfied for all $i = 1, 2, \ldots, n$, where n denotes the number of characters in the plain-text. Now it will be shown how the operations in a quasigroup can be applied as invertible transformations to form the stream-ciphers.

A table of addition in a quasigroup Q can be treated as the table of values of discrete two-variable function $\mathcal{S}$, for which

$$\mathcal{S}(x, y) = x \check{+} y, \qquad \mathcal{S}(y, x) = y \check{+} x \tag{17}$$

where $\check{+}$ denotes the operation in the quasigroup Q. Taking into account (17) one can define two operators ($\check{\ominus}$ and $\check{-}$) for performing "subtraction" in Q

$$\mathcal{S}(x, y) \check{\ominus} y = x, \qquad \mathcal{S}(y, x) \check{-} y = x \tag{18}$$

Further let us introduce two more functions

$$\mathcal{D}(x, y) = x \check{\ominus} y \tag{19}$$

$$\widehat{\mathcal{D}}(x, y) = x \check{-} y \tag{20}$$

It follows immediately from (18)–(20) that

$$D\Big(\mathcal{S}(x, y), y\Big) = x \tag{21}$$

$$\widehat{\mathcal{D}}\Big(\mathcal{S}(y, x), y\Big) = x \tag{22}$$

This means that (21) and (22) permit the determination of two other functions, which, together with the function $\mathcal{S}(x, y)$, are useful for constructing quasigroup-based stream-ciphers. One can prove, by applying similar reasoning, that

$$S\Big(\mathcal{D}(x, y), y\Big) = x \tag{23}$$

$$\widehat{\mathcal{D}}\Big(y, \mathcal{D}(y, x)\Big) = x \tag{24}$$

$$D\Big(y, \widehat{\mathcal{D}}(y, x)\Big) = x \tag{25}$$

$$\mathcal{S}\Big(y, \widehat{\mathcal{D}}(x, y)\Big) = x \tag{26}$$

Taking into consideration (18)–(26) and the property (16), one can observe that six pairs of functions

$$(\mathcal{S},\ \mathcal{D}),\quad (\mathcal{S},\ \widehat{\mathcal{D}}),\quad (\mathcal{D},\ \widehat{\mathcal{D}}),\quad (\mathcal{D},\ \mathcal{S}),\quad (\widehat{\mathcal{D}},\ \mathcal{S}),\quad (\widehat{\mathcal{D}},\ \mathcal{D}) \tag{27}$$

can be used, each being a pair of invertible transformations (f_e, f_d). Therefore, if a quasigroup Q is not abelian, then for one pair of characters (m_i, k_i) there may exist up to six distinct characters c_i of the cryptogram. This is a substantial progress in comparison with the stream-ciphers built over $GF(2)$, where the unique operation XOR can only be applied.

4. Methods of Forming Primary Algebraic Systems

In order to construct quasigroups using the concept of isotopy, one ought to know how to form a primary algebraic system Q_p, which will be transformed onto an isotope. In this section, three ways of constructing such initial systems are considered.

4.1. A Method of Constructing a Group, Isomorphic to the Additive Group of $GF(q)$

Let $q = p^m$, p—prime, m—an arbitrary integer ≥ 1, and let

$$G = \langle F,\ \dot{+}\rangle \tag{28}$$

be a group of order q. To simplify the notation it is assumed for convenience that

$$F = \{0,\ 1,\ \ldots,\ q-1\} \tag{29}$$

Let $x,\ y\ \in\ F$. Since $q = p^m$, x and y can be represented in the base p by means of m p–ary digits

$$x = a_{x,m-1}\ a_{x,m-2}\ \cdots\ a_{x,0} = \sum_{i=1}^{m} a_{x,m-i}\cdot p^{m-i} \tag{30}$$

$$y = a_{y,m-1}\ a_{y,m-2}\ \cdots\ a_{y,0} = \sum_{i=1}^{m} a_{y,m-i}\cdot p^{m-i} \tag{31}$$

where

$$0\ \leq a_{x,m-i},\ a_{y,m-i}\ \leq\ p-1 \tag{32}$$

for $i = 1,\ 2,\ \ldots,\ m$. Assuming that the element 0 denotes an identity element under addition, the additive operations involving this element have the following properties:

$$\forall\ x \in F,\qquad x \dot{+} 0 = 0 \dot{+} x = x \tag{33}$$

$$\forall\ x \in F,\qquad x \dot{+} (\dot{-}\ x) = (\dot{-}\ x) \dot{+} x = 0 \tag{34}$$

where

$$\forall\, x \in F\ \exists\ \dot{-}\, x \in F \left(\dot{-}\, x = \sum_{i=1}^{m} \left((p-1) \odot a_{x,m-i} \right) \cdot p^{m-i} \right) \tag{35}$$

If addition in F is defined according to

$$\forall x, y \in F\ \exists\, (x \dot{+} y) \in F \left((x \dot{+} y) = \sum_{i=1}^{m} (a_{x,m-i} \oplus a_{y,m-i}) \cdot p^{m-i} \right) \tag{36}$$

then one can easily prove that the system $\langle F, \dot{+} \rangle$ is isomorphic to the additive group of $GF(q)$. If a scalar multiplication of (30) by an element of $GF(p)$ is defined in F as

$$\forall\, x \in F,\ \forall\, 0 \leq c \leq p-1\ \exists\, c \circ x \in F \left(c \circ x = \sum_{i=1}^{m} (c \odot a_{x,m-i}) \cdot p^{m-i} \right) \tag{37}$$

then system (28) will have the properties of a vector space of dimension m over $GF(p)$. It should be remarked that in the formulae written above the symbols $\oplus$, $\odot$, $\cdot$, $-$ denote addition and multiplication modulo p and usual multiplicaton and subtraction, respectively, while $\dot{+}$ and $\dot{-}$ denote the operations in the group G. This convention will also be used in the next subsections.

4.2. A Method of Constructing a Group Isomorphic to the Cyclic Group of Order q

Let q be equal to an arbitrary integer > 1 and let

$$C = \langle F, \dot{+} \rangle \tag{38}$$

be a group isomorphic to a cyclic group of order q, where F is as in (29). Then the operation $\dot{+}$ in F may be defined according to

$$\forall\, x, y \in F\ \exists\, (x \dot{+} y) \in F \left(x \dot{+} y \equiv x + y \pmod{q} \right) \tag{39}$$

In this case it is easy to note that 0 is also an identity element under the operation $\dot{+}$ and that

$$\forall x \in F\ \ \exists\ \dot{-}\, x \in F,\ \dot{-}\, x = \begin{cases} q - x & \text{if } x \neq 0 \\ x & \text{if } x = 0 \end{cases} \tag{40}$$

4.3. Method of Constructing an Abelian Loop of Even Order q

It was observed by the author (Kościelny, 1995) that for every even integer q there exists an abelian loop of this order

$$L = \langle F, \dot{+} \rangle \tag{41}$$

where F, as usual, denotes the set (29), with the following rule of operation $\dot{+}$:

$$x \dot{+} y = \begin{cases} 0 & \text{if } x = y \\ x + y & \text{if } x = 0 \vee y = 0 \\ 1 + \Big[\min\{x, y\} - 1 + Z(|x - y|) \pmod{q-1} \Big] & \text{otherwise} \end{cases} \tag{42}$$

where

$$Z(2k-1) = q/2 + k - 1, \quad Z(2k) = k, \quad k = 1, 2, \ldots, (q-2)/2 \tag{43}$$

An identity element of this loop is also denoted by 0.

5. Example

As an example, a cipher over an alphabet of 16 symbols will be presented. It is assumed that a primary system which will be transformed onto a quasigroup is the group, isomorphic to the additive group of $GF(16)$, the elements of which are represented as hexadecimal numbers

$$Q_p = \langle \{0,\ 1,\ \ldots,\ 9,\ A,\ B\ \ldots,\ F\}, \dot{+} \rangle \tag{44}$$

with the operation of addition defined as

$$\forall x,\ y\ \in \{0,\ 1,\ \ldots,\ 9,\ A,\ B\ \ldots,\ F\}\ (x \dot{+} y = x\ XOR\ y) \tag{45}$$

The addition table in system (44) is given in Tab. 2.

Tab. 2. Addition table of the group isomorphic to the additive group of $GF(16)$.

$\dot{+}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

To construct an isotope Q_i of (44) the following three permutations are chosen

$$\pi_x = \begin{pmatrix} \texttt{0123456789ABCDEF} \\ \texttt{0E4AF1B5C2863D79} \end{pmatrix}$$

$$\pi_y = \begin{pmatrix} \texttt{0123456789ABCDEF} \\ \texttt{0BA1D67C4FE59238} \end{pmatrix} \tag{46}$$

$$\pi_t = \begin{pmatrix} \texttt{0123456789ABCDEF} \\ \texttt{0437BF8C5162EAD9} \end{pmatrix}$$

After permuting the row and column borders in Tab. 2 by means of π_x and π_y, respectively, and after using π_t for permuting the body of this Table, the table of operation in the isotope Q_i of (44),

$$Q_i = \langle \{0,\ 1,\ \ldots,\ 9,\ A,\ B\ \ldots,\ F\}, \dot{+} \rangle \tag{47}$$

presented in Tab. 3, is obtained.

Tab. 3. Addition table of the quasigroup formed by means of mappings (46) from the group defined by Tab. 2.

$\dot{+}$	0	B	A	1	D	6	7	C	4	F	E	5	9	2	3	8
0	0	4	3	7	B	F	8	C	5	1	6	2	E	A	D	9
E	4	0	7	3	F	B	C	8	1	5	2	6	A	E	9	D
4	3	7	0	4	8	C	B	F	6	2	5	1	D	9	E	A
A	7	3	4	0	C	8	F	B	2	6	1	5	9	D	A	E
F	B	F	8	C	0	4	3	7	E	A	D	9	5	1	6	2
1	F	B	C	8	4	0	7	3	A	E	9	D	1	5	2	6
B	8	C	B	F	3	7	0	4	D	9	E	A	6	2	5	1
5	C	8	F	B	7	3	4	0	9	D	A	E	2	6	1	5
C	5	1	6	2	E	A	D	9	0	4	3	7	B	F	8	C
2	1	5	2	6	A	E	9	D	4	0	7	3	F	B	C	8
8	6	2	5	1	D	9	E	A	3	7	0	4	8	C	B	F
6	2	6	1	5	9	D	A	E	7	3	4	0	C	8	F	B
3	E	A	D	9	5	1	6	2	B	F	8	C	0	4	3	7
D	A	E	9	D	1	5	2	6	F	B	C	8	4	0	7	3
7	D	9	E	A	6	2	5	1	8	C	B	F	3	7	0	4
9	9	D	A	E	2	6	1	5	C	8	F	B	7	3	4	0

An ordered form of Tab. 3 is given in Tab. 4 which was calculated using the inverse permutations

$$\pi_x^{-1} = \begin{pmatrix} \texttt{0123456789ABCDEF} \\ \texttt{059C27BEAF368D14} \end{pmatrix}$$
$$\pi_y^{-1} = \begin{pmatrix} \texttt{0123456789ABCDEF} \\ \texttt{03DE8B56FC2174A9} \end{pmatrix} \tag{48}$$

and formula (9). Table 4 contains the values of a discrete function of two variables $\mathcal{S}(x,y)$. Knowing this function, the two other functions $\mathcal{D}(x,y)$ and $\widehat{\mathcal{D}}(x,y)$ can be determined by means of (21) and (22); the former two functions in Tab. 5 and Tab. 6, respectively, are presented.

Now one can easily use a quasigroup (47) for constructing a stream-cipher assuming that the following encrypting formulae are used

$$\begin{aligned} c_{1,i} &= \mathcal{S}(m_i, k_i), \quad & c_{2,i} &= \mathcal{S}(k_i, m_i), \quad & c_{3,i} &= \mathcal{D}(m_i, k_i) \\ c_{4,i} &= \mathcal{D}(k_i, m_i), \quad & c_{5,i} &= \widehat{\mathcal{D}}(m_i, k_i), \quad & c_{6,i} &= \widehat{\mathcal{D}}(k_i, m_i) \end{aligned} \tag{49}$$

Tab. 4. Table of values of function $\mathcal{S}(x,y)$ (x-row, y-column) (An ordered Tab. 3).

$\check{+}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	7	A	D	5	2	F	8	9	E	3	4	C	B	6	1
1	F	8	5	2	A	D	0	7	6	1	C	B	3	4	9	E
2	1	6	B	C	4	3	E	9	8	F	2	5	D	A	7	0
3	E	9	4	3	B	C	1	6	7	0	D	A	2	5	8	F
4	3	4	9	E	6	1	C	B	A	D	0	7	F	8	5	2
5	C	B	6	1	9	E	3	4	5	2	F	8	0	7	A	D
6	2	5	8	F	7	0	D	A	B	C	1	6	E	9	4	3
7	D	A	7	0	8	F	2	5	4	3	E	9	1	6	B	C
8	6	1	C	B	3	4	9	E	F	8	5	2	A	D	0	7
9	9	E	3	4	C	B	6	1	0	7	A	D	5	2	F	8
A	7	0	D	A	2	5	8	F	E	9	4	3	B	C	1	6
B	8	F	2	5	D	A	7	0	1	6	B	C	4	3	E	9
C	5	2	F	8	0	7	A	D	C	B	6	1	9	E	3	4
D	A	D	0	7	F	8	5	2	3	4	9	E	6	1	C	B
E	4	3	E	9	1	6	B	C	D	A	7	0	8	F	2	5
F	B	C	1	6	E	9	4	3	2	5	8	F	7	0	D	A

Tab. 5. Table of values of function $\mathcal{D}(x,y)$ (x-row, y-column), formed by means of (21).

$\check{\ominus}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	A	D	7	C	6	1	B	9	3	4	E	5	F	8	2
1	2	8	F	5	E	4	3	9	B	1	6	C	7	D	A	0
2	6	C	B	1	A	0	7	D	F	5	2	8	3	9	E	4
3	4	E	9	3	8	2	5	F	D	7	0	A	1	B	C	6
4	E	4	3	9	2	8	F	5	7	D	A	0	B	1	6	C
5	C	6	1	B	0	A	D	7	5	F	8	2	9	3	4	E
6	8	2	5	F	4	E	9	3	1	B	C	6	D	7	0	A
7	A	0	7	D	6	C	B	1	3	9	E	4	F	5	2	8
8	B	1	6	C	7	D	A	0	2	8	F	5	E	4	3	9
9	9	3	4	E	5	F	8	2	0	A	D	7	C	6	1	B
A	D	7	0	A	1	B	C	6	4	E	9	3	8	2	5	F
B	F	5	2	8	3	9	E	4	6	C	B	1	A	0	7	D
C	5	F	8	2	9	3	4	E	C	6	1	B	0	A	D	7
D	7	D	A	0	B	1	6	C	E	4	3	9	2	8	F	5
E	3	9	E	4	F	5	2	8	A	0	7	D	6	C	B	1
F	1	B	C	6	D	7	0	A	8	2	5	F	4	E	9	3

Tab. 6. Table of values of function $\widehat{\mathcal{D}}(x,y)$ (x-row, y-column), formed by means of (22).

$\check{-}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	6	F	9	A	C	5	3	E	8	1	7	4	2	B	D
1	F	9	0	6	5	3	A	C	1	7	E	8	B	D	4	2
2	5	3	A	C	F	9	0	6	B	D	4	2	1	7	E	8
3	A	C	5	3	0	6	F	9	4	2	B	D	E	8	1	7
4	B	D	4	2	1	7	E	8	5	3	A	C	F	9	0	6
5	4	2	B	D	E	8	1	7	A	C	5	3	0	6	F	9
6	E	8	1	7	4	2	B	D	0	6	F	9	A	C	5	3
7	1	7	E	8	B	D	4	2	F	9	0	6	5	3	A	C
8	7	1	8	E	D	B	2	4	9	F	6	0	3	5	C	A
9	8	E	7	1	2	4	D	B	6	0	9	F	C	A	3	5
A	2	4	D	B	8	E	7	1	C	A	3	5	6	0	9	F
B	D	B	2	4	7	1	8	E	3	5	C	A	9	F	6	0
C	C	A	3	5	6	0	9	F	2	4	D	B	8	E	7	1
D	3	5	C	A	9	F	6	0	D	B	2	4	7	1	8	E
E	9	F	6	0	3	5	C	A	7	1	8	E	D	B	2	4
F	6	0	9	F	C	A	3	5	8	E	7	1	2	4	D	B

Tab. 7. Example of cryptograms generated by the stream-cipher based on the quasigroup defined by Tab. 4.

i	m_i	k_i	$c_{1,i}$	$c_{2,i}$	$c_{3,i}$	$c_{4,i}$	$c_{5,i}$	$c_{6,i}$
1	3	7	6	0	F	D	9	8
2	C	8	C	A	C	E	2	3
3	5	F	D	9	E	7	9	A

In Tab. 7 six cryptograms for a message containing three characters were calculated. The reader can verify, using Tabs. 4, 5 and 6, that by means of the formulae

$$\begin{aligned} m_i &= \mathcal{D}(c_{1,i}, k_i) = \widehat{\mathcal{D}}(c_{2,i}, k_i) = \mathcal{S}(c_{3,i} k_i) \\ &= \widehat{\mathcal{D}}(k_i, c_{4,i}) = \mathcal{S}(k_i, c_{5,i}) = \mathcal{D}(k_i, c_{6,i}) \end{aligned} \tag{50}$$

all the six cryptograms can be correctly decrypted. It should be observed that the permutations (46) are chosen such that they can be generated by means of the following matrices over $GF(2)$:

$$M_{\pi_x} = \begin{bmatrix} 0010 \\ 1010 \\ 1111 \\ 1011 \end{bmatrix}, \quad M_{\pi_y} = \begin{bmatrix} 1010 \\ 1100 \\ 0011 \\ 1110 \end{bmatrix}, \quad M_{\pi_t} = \begin{bmatrix} 0111 \\ 0110 \\ 1001 \\ 0010 \end{bmatrix} \tag{51}$$

After computing the inverses

$$M_{\pi_x}^{-1} = \begin{bmatrix} 1100 \\ 0011 \\ 1000 \\ 0101 \end{bmatrix}, \quad = M_{\pi_y}^{-1} = \begin{bmatrix} 1101 \\ 1001 \\ 0101 \\ 0111 \end{bmatrix} \tag{52}$$

one can express the funtion $\mathcal{S}$ as follows:

$$\mathcal{S}(x,y) = x\check{+}y = M_{\pi_t}(M_{\pi_x}^{-1} \cdot x \oplus M_{\pi_y}^{-1} \cdot y) \tag{53}$$

where

$$x = [a_{x,0} \;\; a_{x,1} \;\; a_{x,2} \;\; a_{x,3}]^T, \qquad y = [a_{y,0} \;\; a_{y,1} \;\; a_{y,2} \;\; a_{y,3}]^T \tag{54}$$

and matrix multiplications and additions are performed over $GF(2)$. After completing the operations on the right-hand side of (53) one has

$$\mathcal{S}(x,y) = \begin{bmatrix} a_{x,0} \oplus a_{x,1} \oplus a_{x,2} \oplus a_{y,0} \oplus a_{y,2} \oplus a_{y,3} \\ a_{x,0} \oplus a_{x,2} \oplus a_{x,3} \oplus a_{y,0} \oplus a_{y,1} \\ a_{x,0} \oplus a_{x,3} \oplus a_{y,0} \oplus a_{y,2} \\ a_{x,0} \oplus a_{y,1} \oplus a_{y,3} \end{bmatrix} \tag{55}$$

where, evidently, $\oplus$ symbolizes the XOR operation. It is amazing that such simple equations give so messy table of values of the function $\mathcal{S}$. It follows from (55) that the cryptograms of quasigroup-based stream-ciphers can be generated and decrypted with a very high speed. Then, it may be hoped that the implementation of the ciphers considered here by means of microprogrammed devices, or using appropriate hardware, could satisfy the requirements of any application from the point of view of the encryption/decryption speed.

6. Conclusions

A new method of constructing generalized stream-ciphers based on the application of quasigroups has been given. The ciphers, formed by means of the proposed method have the following main advantages:

- cryptograms are not redundant and have the same volume as plain-texts;
- the number of errors, appearing in the deciphered plain-text is the same as in the corresponding cryptogram, i.e. the phenomenon of propagation of errors does not occur;
- the secret key may have five components: the sequence of characters interacting with the stream of characters of a plain-text, the primary algebraic system Q_p, and three permutations, needed to form a quasigroup Q_i by means of Q_p; this may be useful for some applications;

- the ciphers can be very secure, because there exists no better algorithm of cryptanalysis than the exhaustive search of all $(q!)^3$ quasigroups which can be formed by means of this primary system and verification of all possible streams of characters which are "added" to the stream of characters of the plain-text for any quasigroup;
- the proposed method, being extremly simple, offers very fast implementations of encrypting and decrypting procedures.

It is evident that many other encrypting algorithms can be formed on the basis of quasigroups (e.g. the one which changes the quasigroup for each character of the plain-text), offering new possibilities for cryptography. Therefore, quasigroups could be applied in such applications as block-ciphers, digital signatures, user identification, etc.

References

Beth T., Frisch M. and Simmons G.J. (1992): *Public–Key Cryptography: State of the Art and Future Directions.* — Lecture Notes in Computer Science, v.578, Berlin: Springer Verlag.

Brassard G. (1988): *Modern Cryptology.* — Lecture Notes in Computer Science, v.325, Berlin: Springer Verlag.

Dénes J. and Keedwell A.D. (1974): *Latin Squares and Their Applications.* — Budapest: Akadémiai Kiadó.

Kościelny C. (1995): *Spurious Galois fields.* — Appl. Math. and Comp. Sci., v.5, No.1, pp.169–188.

Received: September 22, 1995
Revised: December 21, 1995