Cryptanalysis of some stream ciphers based on n-ary groupoids

Nadezhda N. Malyutina

Abstract. We research generalized Markovski algorithm based on i-invertible n-groupoids. We give lower bounds for cryptoattacks named as chosen ciphertext and plaintext attacks. Also we give modifications of these attacks.

1. Introduction

The use of quasigroups opens new ways in construction of stream and block ciphers [3, 4]. We continue researches of applications of n-ary groupoids that are invertible on i-th place in cryptology [2, 5].

Definition 1.1. n-Ary groupoid (Q, f) is called *invertible on the i-th place*, $i \in \overline{1,n}$, if the equation $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ has a unique solution for any elements $a_1, \dots, a_{i-1}$, $a_{i+1}, \dots$, $a_n, a_{n+1} \in Q$.

In this case the operation ${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = x_i$ is defined in a unique way and we have:

$$f(a_1, \dots, a_{i-1}, {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = a_{n+1},$$
$${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = x_i.$$

Algorithm 1.2. Let Q be a non-empty finite alphabet and k be a natural number, $u_j, v_j \in Q$, $j \in \{1, ..., k\}$. Define an n-ary groupoid (Q, f) which is invertible on the i-th place,$i \in \overline{1,n}$. Then the groupoid $(Q, {}^{(i,\,n+1)}f)$ is defined in a unique way.

Take the fixed elements $l_1^{(n-1)(n-1)}$ $(l_i \in Q)$, which are called *leaders.*

Let $u_1u_2...u_k$ be a k-tuple of letters from Q.

2010 Mathematics Subject Classification: 20N15, 20N05, 05B15, 94A60
Keywords: cipher, ciphertext, plaintext, Markovski algorithm, n-ary groupoid.

The following ciphering (encryption) procedure is proposed:

$$\begin{aligned}
&v_1 = f(l_1, \ldots, l_{i-1}, u_1, l_i, \ldots, l_{n-1}),\\
&v_2 = f(l_n, \ldots, l_{n+i-2}, u_2, l_{n+i-1}, \ldots, l_{2n-2}),\\
&\ldots\ldots\ldots\ldots\ldots,\\
&v_{n-1} = f(l_{n^2-3n+3}, \ldots, l_{n^2-3n+1+i}, u_{n-1}, l_{n^2-3n+2+i}, \ldots, l_{(n-1)^2}),\\
&v_n = f(v_1, \ldots, v_{i-1}, u_n, v_i, \ldots, v_{n-1}),\\
&v_{n+1} = f(v_2, \ldots, v_i, u_{n+1}, v_{i+1}, \ldots, v_n),\\
&\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{1}$$

Therefore we obtain the following ciphertext: $v_1 v_2 \ldots, v_{n-1}, v_n, v_{n+1}, \ldots$ The deciphering algorithm is constructed similarly to the binary case:

$$\begin{aligned}
&u_1 = {}^{(i,\,n+1)}f(l_1, \ldots, l_{i-1}, v_1, l_i, \ldots, l_{n-1}),\\
&u_2 = {}^{(i,\,n+1)}f(l_n, \ldots, l_{n+i-2}, v_2, l_{n+i-1}, \ldots, l_{2n-2}),\\
&\ldots\ldots\ldots\ldots\ldots,\\
&u_{n-1} = {}^{(i,\,n+1)}f(l_{n^2-3n+3}, \ldots, l_{n^2-3n+1+i}, v_{n-1}, l_{n^2-3n+2+i}, \ldots,\\
&l_{(n-1)^2})\\
&u_n = {}^{(i,\,n+1)}f(v_1, \ldots, v_{i-1}, v_n, v_i, \ldots, v_{n-1}),\\
&u_{n+1} = {}^{(i,\,n+1)}f(v_2, \ldots, v_i, v_{n+1}, v_{i+1}, \ldots, v_n),\\
&\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{2}$$

2.Results

2.1 Ciphertext attacks

S. Markovski, E. Ochodkova and V. Snashel proposed a new stream cipher to encrypt the file system [3, 4]. M. Vojvoda has given the cryptanalysis of the file encoding system based on binary quasigroups [6, 7] and showed how to break this cipher. These attacks are described by M. Vojvoda [7]. See [1] for the case of n-ary quasigrops.

We studied cryptographic attacks on the cipher using the generalized Markovski algorithm. In this article we will conduct a comparative analysis, identify positive and negative points in these attacks. Given examples provide lower bounds of such attacks.

Consider an attack with text constructed using an n-ary groupoid, which is invertible on the i-th place obtained using the generalized Markovski algorithm.

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext, where n is arity and m the order of an i-invertible groupoid:

$q_1q_1\cdots q_1q_1q_1q_1\cdots q_1q_2q_1q_1\cdots q_1q_m$
$q_1q_1\cdots q_2q_1q_1q_1\cdots q_2q_2q_1q_1\cdots q_2q_m$
$q_1q_1\cdots q_3q_1q_1q_1\cdots q_3q_2q_1q_1\cdots q_3q_m$
$\ldots\ldots\ldots\ldots\ldots$
$q_1q_1\cdots q_mq_1q_1q_1\cdots q_mq_2q_1q_1\cdots q_mq_m\cdots$

and enter it into the decryption device.

For a complete reconstruction of the table of values of the operation ${}^{(i,n+1)}f$, and hence the table of values of the operation f, it is sufficient to submit at the input: $A = (n \cdot m^{n-1} + 1)(m-1)$ characters to get all the values or $A - 1 = n \cdot m^{n-1}(m-1) + (m-2)$ characters, when the last value is found by the exception method.

We give numerical examples instead of "general case" in order to make the reading of this paper more convenient . We hope that any qualified student can be easy to write "general case" using these examples.

Example 2.1. Take the ternary groupoid (R_3, f), $R_3 = \{0, 1, 2\}$, which is defined over the ring $(R_3, +, \cdot)$ residue classes modulo 3 and which is invertible on first place.

Ternary operation f on the set R_3 is defined as:
$f(x_1, x_2, x_3) = \alpha x_1 + \beta x_2 + \gamma x_3 = x_4$, where

$$\alpha 0 = 2, \alpha 1 = 0, \alpha 2 = 1,$$
$$\beta 0 = 0, \beta 1 = 1, \beta 2 = 1,$$
$$\gamma 0 = 2, \gamma 1 = 0, \gamma 2 = 0.$$

Inverse operation for f or (14)-parastrophe is the following operation:
${}^{(1,4)}f(x_4, x_2, x_3) = x_1 = \alpha^{-1}(x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)$, where $\alpha^{-1}(0) = 1$, $\alpha^{-1}(1) = 2$, $\alpha^{-1}(2) = 0$.

Check.

$$f({}^{(1,4)}f(x_4, x_2, x_3), x_2, x_3) = \alpha(\alpha^{-1}(x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)) + \beta x_2 + \gamma x_3$$
$$= x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + \beta x_2 + \gamma x_3 = x_4.$$
$${}^{(1,4)}f(f(x_1, x_2, x_3), x_2, x_3) = \alpha^{-1}(\alpha x_1 + \beta x_2 + \gamma x_3 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)$$
$$= \alpha^{-1}(\alpha x_1) = x_1.$$

Elements: $l_1 = 0, l_2 = 2, l_3 = 1, l_4 = 2$ are used as leaders.
We will use Algorithm 1.2. and we can construct the following ciphertext:

$q_1q_1q_1q_1q_1q_2q_1q_1q_3q_1q_2q_1q_1q_2q_2q_1q_2q_3q_1q_3q_1q_1q_3q_2q_1q_3q_3$
$q_2q_1q_1q_2q_1q_2q_2q_1q_3q_2q_2q_1q_2q_2q_2q_2q_2q_3q_2q_3q_1q_2q_3q_2q_2q_3q_3$
q_3q_1
or
000001002010011012020021022
100101102110111112120121122
20

and enter it into the decryption device.

The process of decrypting the text and the results are as follows:

Table 1: Decrypted text

$u_1 =^{(1,4)} f(v_1, l_1, l_2) =^{(1,4)} f(q_1, l_1, l_2)$ $=^{(1,4)} f(0,0,2) = 1$	$u_{29} =^{(1,4)} f(0,2,1) = 0$
$u_2 =^{(1,4)} f(v_2, l_3, l_4) =^{(1,4)} f(q_1, l_3, l_4)$ $=^{(1,4)} f(0,1,2) = 0$	$u_{30} =^{(1,4)} f(0,1,0) = 1$
$u_3 =^{(1,4)} f(v_3, v_1, v_2) =^{(1,4)} f(q_1, q_1, q_1)$ $=^{(1,4)} f(0,0,0) = 2 - (1)$	$u_{31} =^{(1,4)} f(1,0,0) = 0$
$u_4 =^{(1,4)} f(0,0,0) = 2$	$u_{32} =^{(1,4)} f(0,0,1) = 1$
$u_5 =^{(1,4)} f(0,0,0) = 2$	$u_{33} =^{(1,4)} f(1,1,0) = 2$
$u_6 =^{(1,4)} f(1,0,0) = 0 - (10)$	$u_{34} =^{(1,4)} f(1,0,1) = 2$
$u_7 =^{(1,4)} f(0,0,1) = 1 - (2)$	$u_{35} =^{(1,4)} f(0,1,1) = 0$
$u_8 =^{(1,4)} f(0,1,0) = 1 - (4)$	$u_{36} =^{(1,4)} f(2,1,0) = 0$
$u_9 =^{(1,4)} f(2,0,0) = 1 - (19)$	$u_{37} =^{(1,4)} f(1,0,2) = 2$
$u_{10} =^{(1,4)} f(0,0,2) = 1 - (3)$	$u_{38} =^{(1,4)} f(1,2,1) = 1 - (17)$
$u_{11} =^{(1,4)} f(1,2,0) = 2 - (16)$	$u_{39} =^{(1,4)} f(0,1,1) = 0$
$u_{12} =^{(1,4)} f(0,0,1) = 1$	$u_{40} =^{(1,4)} f(1,1,0) = 2$
$u_{13} =^{(1,4)} f(0,1,0) = 1$	$u_{41} =^{(1,4)} f(1,0,1) = 2$
$u_{14} =^{(1,4)} f(1,0,0) = 0$	$u_{42} =^{(1,4)} f(1,1,1) = 1 - (14)$
$u_{15} =^{(1,4)} f(1,0,1) = 2 - (11)$	$u_{43} =^{(1,4)} f(1,1,1) = 1$
$u_{16} =^{(1,4)} f(0,1,1) = 0 - (5)$	$u_{44} =^{(1,4)} f(1,1,1) = 1$
$u_{17} =^{(1,4)} f(1,1,0) = 2 - (13)$	$u_{45} =^{(1,4)} f(2,1,1) = 2 - (23)$
$u_{18} =^{(1,4)} f(2,0,1) = 0 - (20)$	$u_{46} =^{(1,4)} f(1,1,2) = 1 - (15)$
$u_{19} =^{(1,4)} f(0,1,2) = 0 - (6)$	$u_{47} =^{(1,4)} f(2,2,1) = 2 - (26)$
$u_{20} =^{(1,4)} f(2,2,0) = 0 - (25)$	$u_{48} =^{(1,4)} f(0,1,2) = 0$
$u_{21} =^{(1,4)} f(0,0,2) = 1$	$u_{49} =^{(1,4)} f(1,2,0) = 2$
$u_{22} =^{(1,4)} f(0,2,0) = 1 - (7)$	$u_{50} =^{(1,4)} f(2,0,1) = 0$
$u_{23} =^{(1,4)} f(2,0,0) = 1$	$u_{51} =^{(1,4)} f(1,1,2) = 1$
$u_{24} =^{(1,4)} f(1,0,2) = 2 - (12)$	$u_{52} =^{(1,4)} f(1,2,1) = 1$
$u_{25} =^{(1,4)} f(0,2,1) = 0 - (8)$	$u_{53} =^{(1,4)} f(2,1,1) = 2$
$u_{26} =^{(1,4)} f(2,1,0) = 0 - (22)$	$u_{54} =^{(1,4)} f(2,1,2) = 2 - (24)$
$u_{27} =^{(1,4)} f(2,0,2) = 0 - (21)$	$u_{55} =^{(1,4)} f(2,2,2) = 2 - (27)$
$u_{28} =^{(1,4)} f(1,2,2) = 1 - (18)$	$u_{56} =^{(1,4)} f(0,2,2) = 0 - (9)$

At the output we get:
10222011112110202000111200010101220021022111212020112220.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(1,4)}f$, and hence the table of values of the operation f, it is enough to supply 55 characters (without the last one) for the ternary groupoid at the input, or 56 characters to restore all values. The table of the decrypting function is hacked:

Table 2: Decryption function

N	Value	N	Value
(1)	${}^{(1,4)}f(0,0,0) = \alpha^{-1}(1) = 2$	(15)	${}^{(1,4)}f(1,1,2) = \alpha^{-1}(0) = 1$
(2)	${}^{(1,4)}f(0,0,1) = \alpha^{-1}(0) = 1$	(16)	${}^{(1,4)}f(1,2,0) = \alpha^{-1}(1) = 2$
(3)	${}^{(1,4)}f(0,0,2) = \alpha^{-1}(0) = 1$	(17)	${}^{(1,4)}f(1,2,1) = \alpha^{-1}(0) = 1$
(4)	${}^{(1,4)}f(0,1,0) = \alpha^{-1}(0) = 1$	(18)	${}^{(1,4)}f(1,2,2) = \alpha^{-1}(0) = 1$
(5)	${}^{(1,4)}f(0,1,1) = \alpha^{-1}(2) = 0$	(19)	${}^{(1,4)}f(2,0,0) = \alpha^{-1}(0) = 1$
(6)	${}^{(1,4)}f(0,1,2) = \alpha^{-1}(2) = 0$	(20)	${}^{(1,4)}f(2,0,1) = \alpha^{-1}(2) = 0$
(7)	${}^{(1,4)}f(0,2,0) = \alpha^{-1}(0) = 1$	(21)	${}^{(1,4)}f(2,0,2) = \alpha^{-1}(2) = 0$
(8)	${}^{(1,4)}f(0,2,1) = \alpha^{-1}(2) = 0$	(22)	${}^{(1,4)}f(2,1,0) = \alpha^{-1}(2) = 0$
(9)	${}^{(1,4)}f(0,2,2) = \alpha^{-1}(2) = 0$	(23)	${}^{(1,4)}f(2,1,1) = \alpha^{-1}(1) = 2$
(10)	${}^{(1,4)}f(1,0,0) = \alpha^{-1}(2) = 0$	(24)	${}^{(1,4)}f(2,1,2) = \alpha^{-1}(1) = 2$
(11)	${}^{(1,4)}f(1,0,1) = \alpha^{-1}(1) = 2$	(25)	${}^{(1,4)}f(2,2,0) = \alpha^{-1}(2) = 0$
(12)	${}^{(1,4)}f(1,0,2) = \alpha^{-1}(1) = 2$	(26)	${}^{(1,4)}f(2,2,1) = \alpha^{-1}(1) = 2$
(13)	${}^{(1,4)}f(1,1,0) = \alpha^{-1}(1) = 2$	(27)	${}^{(1,4)}f(2,2,2) = \alpha^{-1}(1) = 2$
(14)	${}^{(1,4)}f(1,1,1) = \alpha^{-1}(0) = 1$		

Knowing the value table for ${}^{(1,4)}f$ operation, value table is easily restored for f:

Table 3: Encryption function

N	Value	N	Value
(1)	$f(0,0,0) = 1$	(15)	$f(1,1,2) = 1$
(2)	$f(0,0,1) = 2$	(16)	$f(1,2,0) = 0$
(3)	$f(0,0,2) = 2$	(17)	$f(1,2,1) = 1$
(4)	$f(0,1,0) = 2$	(18)	$f(1,2,2) = 1$
(5)	$f(0,1,1) = 0$	(19)	$f(2,0,0) = 0$
(6)	$f(0,1,2) = 0$	(20)	$f(2,0,1) = 1$
(7)	$f(0,2,0) = 2$	(21)	$f(2,0,2) = 1$
(8)	$f(0,2,1) = 0$	(22)	$f(2,1,0) = 1$
(9)	$f(0,2,2) = 0$	(23)	$f(2,1,1) = 2$
(10)	$f(1,0,0) = 2$	(24)	$f(2,1,2) = 2$
(11)	$f(1,0,1) = 0$	(25)	$f(2,2,0) = 1$
(12)	$f(1,0,2) = 0$	(26)	$f(2,2,1) = 2$
(13)	$f(1,1,0) = 0$	(27)	$f(2,2,2) = 2$
(14)	$f(1,1,1) = 1$		

To understand the situation with hacking of the decrypted text and the leaders, consider the plaintext of the form: 101202$=u_1u_2u_3u_4u_5u_6$.
$v_1 = f(u_1, l_1, l_2) = f(1, l_1, l_2) =?$

$v_2 = f(u_2, l_3, l_4) = f(0, l_3, l_4) =?$
$v_3 = f(u_3, v_1, v_2) = f(1, v_1, v_2) =?$
$v_4 = f(u_4, v_2, v_3) = f(2, v_2, v_3) =?$
$v_5 = f(u_5, v_3, v_4) = f(0, v_3, v_4) =?$
$v_6 = f(u_6, v_4, v_5) = f(2, v_4, v_5) =?$

Analyzing the results obtained using the table of values of the function f, we obtain the following options for the text to be decoded ($f(1, *, *)$ and $f(0, *, *)$ take any values):

Table 4: Ciphertext values

v_1	v_2	v_3	v_4	v_5	v_6
0	0	$f(1,0,0) = 2$	$f(2,0,2) = 1$	$f(0,2,1) = 0$	$f(2,1,0) = 1$
0	1	$f(1,0,1) = 0$	$f(2,1,0) = 1$	$f(0,0,1) = 2$	$f(2,1,2) = 2$
1	0	$f(1,1,0) = 0$	$f(2,0,0) = 0$	$f(0,0,0) = 1$	$f(2,0,1) = 1$
1	1	$f(1,1,1) = 1$	$f(2,1,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
2	0	$f(1,2,0) = 0$	$f(2,0,0) = 0$	$f(0,0,0) = 1$	$f(2,0,1) = 1$
0	2	$f(1,0,2) = 0$	$f(2,2,0) = 1$	$f(0,0,1) = 2$	$f(2,1,2) = 2$
2	1	$f(1,2,1) = 1$	$f(2,1,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
1	2	$f(1,1,2) = 1$	$f(2,2,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
2	2	$f(1,2,2) = 1$	$f(2,2,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$

We get 9 options for possible decrypted text. Among which the first option is true. The possible values of the ciphertext will be only 9 options, i.e. to determine the true value is not particularly difficult.

The question of identifying leaders in this case loses its relevance. Thus different sets of leaders for a ternary groupoid will be $9^2 = 81$. Essentially, we do not need to determine the exact values of the leaders.

The ciphertext proposed in Example 2.1 is a generalized version of the chiphertext used by M. Vojvoda for binary quasigroups.

In the following example we tried to improve this result.

Example 2.2. Enter the other text into the decryption device:
$q_1q_1q_1q_2q_2q_2q_3q_3q_3$
$q_2q_1q_1q_3q_2q_2q_1q_3q_3$
$q_1q_2q_1q_2q_3q_2q_3q_1q_3$
q_1q_1
or
000111222
100211022
010121202
00

We get the following decryption process:

Table 5: Decrypted text

$u_1 =^{(1,4)} f(0,0,2) = 1$	$u_{16} =^{(1,4)} f(0,1,1) = 0 - (5)$
$u_2 =^{(1,4)} f(0,1,2) = 0$	$u_{17} =^{(1,4)} f(2,1,0) = 0 - (22)$
$u_3 =^{(1,4)} f(0,0,0) = 2 - (1)$	$u_{18} =^{(1,4)} f(2,0,2) = 0 - (21)$
$u_4 =^{(1,4)} f(1,0,0) = 0 - (10)$	$u_{19} =^{(1,4)} f(0,2,2) = 0 - (9)$
$u_5 =^{(1,4)} f(1,0,1) =$ 2-(11)	$u_{20} =^{(1,4)} f(1,2,0) = 2 - (16)$
$u_6 =^{(1,4)} f(1,1,1) = 1 - (14)$	$u_{21} =^{(1,4)} f(0,0,1) = 1 - (2)$
$u_7 =^{(1,4)} f(2,1,1) = 2 - (23)$	$u_{22} =^{(1,4)} f(1,1,0) = 2 - (13)$
$u_8 =^{(1,4)} f(2,1,2) = 2 - (24)$	$u_{23} =^{(1,4)} f(2,0,1) = 0 - (20)$
$u_9 =^{(1,4)} f(2,2,2) = 2 - (27)$	$u_{24} =^{(1,4)} f(1,1,2) = 1 - (15)$
$u_{10} =^{(1,4)} f(1,2,2) = 1 - (18)$	$u_{25} =^{(1,4)} f(2,2,1) = 2 - (26)$
$u_{11} =^{(1,4)} f(0,2,1) = 0 - (8)$	$u_{26} =^{(1,4)} f(0,1,2) = 0 - (6)$
$u_{12} =^{(1,4)} f(0,1,0) = 1 - (4)$	$u_{27} =^{(1,4)} f(2,2,0) = 0 - (25)$
$u_{13} =^{(1,4)} f(2,0,0) = 1 - (19)$	$u_{28} =^{(1,4)} f(0,0,2) = 1 - (3)$
$u_{14} =^{(1,4)} f(1,0,2) = 2 - (12)$	$u_{29} =^{(1,4)} f(0,2,0) = 1 - (7)$
$u_{15} =^{(1,4)} f(1,2,1) = 1 - (17)$	

At the output we get the following 29 characters:
10202122210112100002120120011.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(1,4)}f$ it is enough to supply 28 characters (without the last one) for the ternary groupoid at the input, or 29 to restore all values. This text has the smallest possible length, i.e. is the best option for ternary case.

Let's see what happens in the 4-ary case.

Example 2.3. Take the 4-ary groupoid (R_3, f), $R_3 = \{0,1,2\}$, which is defined over residue ring modulo three $(R_3, +, \cdot)$ and which is invertible on the fourth place.

We define 4-ary operation f on the set R_3 in the following way:
$f(x_1, x_2, x_3, x_4) = \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4 = x_5$, where

$$\begin{gathered}\alpha 0 = 1, \alpha 1 = 0, \alpha 2 = 2,\\ \beta 0 = 0, \beta 1 = 0, \beta 2 = 1,\\ \gamma 0 = 2, \gamma 1 = 1, \gamma 2 = 1,\\ \delta 0 = 2, \delta 1 = 0, \delta 2 = 1.\end{gathered}$$

The (45)-parastrophe for f is:

$${}^{(4,5)}f(x_1, x_2, x_3, x_5) = x_4 = \delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5),$$

where $\delta^{-1}(0) = 1, \delta^{-1}(1) = 2, \delta^{-1}(2) = 0$.
Check.

$f(x_1, x_2, x_3, {}^{(4,5)}f(x_1, x_2, x_3, x_5)) =$
$= \alpha x_1 + \beta x_2 + \gamma x_3 + \delta(\delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5)) =$
$= \alpha x_1 + \beta x_2 + \gamma x_3 + 2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5 = x_5$

$$^{(4,5)}f(x_1, x_2, x_3, f(x_1, x_2, x_3, x_4)) =$$
$$= \delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4) = \delta^{-1}(\delta x_4) = x_4.$$

We propose the following elements:
$l_1 = 1, l_2 = 0, l_3 = 0, l_4 = 2, l_5 = 1, l_6 = 1, l_7 = 0, l_8 = 0, l_9 = 0$
as leader elements.

We will use Algorithm 1.2 and enter the following text into the decryption device:
000000010002001000110012002000210022
010001010102011001110112012001210122
020002010202021002110212022002210222
100010011002101010111012102010211022
110011011102111011111112112011211122
120012011202121012111212122012211222
20

In the table we give the values of the characters that allow us to determine the values of the $^{(4,5)}f$:

Table 6: Decrypted text (fragment)

$u_1 =^{(4,5)} f(l_1, l_2, l_3, v_1)$ $=^{(4,5)} f(1, 0, 0, 0) = 2$	$u_{63} =^{(4,5)} f(2, 0, 1, 2) = 0 - (60)$
$u_2 =^{(4,5)} f(l_4, l_5, l_6, v_2)$ $=^{(4,5)} f(2, 1, 1, 0) = 1$	$u_{68} =^{(4,5)} f(0, 1, 2, 1) = 0 - (17)$
$u_3 =^{(4,5)} f(l_7, l_8, l_9, v_3)$ $=^{(4,5)} f(0, 0, 0, 0) = 1$	$u_{69} =^{(4,5)} f(1, 2, 1, 0) = 2 - (49)$
$u_4 =^{(4,5)} f(v_1, v_2, v_3, v_4)$ $=^{(4,5)} f(0, 0, 0, 0) = 1 - (1)$	$u_{70} =^{(4,5)} f(2, 1, 0, 1) = 1 - (65)$
$u_8 =^{(4,5)} f(0, 0, 0, 1) = 2 - (2)$	$u_{71} =^{(4,5)} f(1, 0, 1, 2) = 2 - (33)$
$u_9 =^{(4,5)} f(0, 0, 1, 0) = 2 - (4)$	$u_{72} =^{(4,5)} f(0, 1, 2, 2) = 1 - (18)$
$u_{10} =^{(4,5)} f(0, 1, 0, 0) = 1 - (10)$	$u_{73} =^{(4,5)} f(1, 2, 2, 0) = 2 - (52)$
$u_{11} =^{(4,5)} f(1, 0, 0, 0) = 2 - (28)$	$u_{74} =^{(4,5)} f(2, 2, 0, 2) = 1 - (75)$
$u_{12} =^{(4,5)} f(0, 0, 0, 2) = 0 - (3)$	$u_{75} =^{(4,5)} f(2, 0, 2, 0) = 1 - (61)$
$u_{13} =^{(4,5)} f(0, 0, 2, 0) = 2 - (7)$	$u_{84} =^{(4,5)} f(0, 2, 0, 2) = 2 - (21)$
$u_{14} =^{(4,5)} f(0, 2, 0, 0) = 0 - (19)$	$u_{87} =^{(4,5)} f(2, 0, 2, 1) = 2 - (62)$
$u_{15} =^{(4,5)} f(2, 0, 0, 1) = 1 - (56)$	$u_{92} =^{(4,5)} f(0, 2, 1, 1) = 2 - (23)$
$u_{20} =^{(4,5)} f(0, 0, 1, 1) = 0 - (5)$	$u_{93} =^{(4,5)} f(2, 1, 1, 0) = 1 - (67)$
$u_{21} =^{(4,5)} f(0, 1, 1, 0) = 2 - (13)$	$u_{94} =^{(4,5)} f(1, 1, 0, 2) = 1 - (39)$
$u_{22} =^{(4,5)} f(1, 1, 0, 0) = 2 - (37)$	$u_{95} =^{(4,5)} f(1, 0, 2, 1) = 1 - (35)$
$u_{23} =^{(4,5)} f(1, 0, 0, 1) = 0 - (29)$	$u_{96} =^{(4,5)} f(0, 2, 1, 2) = 0 - (24)$
$u_{24} =^{(4,5)} f(0, 0, 1, 2) = 1 - (6)$	$u_{97} =^{(4,5)} f(2, 1, 2, 0) = 1 - (70)$
$u_{25} =^{(4,5)} f(0, 1, 2, 0) = 2 - (16)$	$u_{98} =^{(4,5)} f(1, 2, 0, 2) = 2 - (48)$
$u_{26} =^{(4,5)} f(1, 2, 0, 0) = 1 - (46)$	$u_{99} =^{(4,5)} f(2, 0, 2, 2) = 0 - (63)$

$u_{27} =^{(4,5)} f(2,0,0,2) = 2 - (57)$	$u_{104} =^{(4,5)} f(0,2,2,1) = 2 - (26)$
$u_{30} =^{(4,5)} f(2,0,0,0) = 0 - (55)$	$u_{105} =^{(4,5)} f(2,2,1,0) = 0 - (76)$
$u_{32} =^{(4,5)} f(0,0,2,1) = 0 - (8)$	$u_{106} =^{(4,5)} f(2,1,0,2) = 2 - (66)$
$u_{33} =^{(4,5)} f(0,2,1,0) = 1 - (22)$	$u_{107} =^{(4,5)} f(1,0,2,2) = 2 - (36)$
$u_{34} =^{(4,5)} f(2,1,0,0) = 0 - (64)$	$u_{108} =^{(4,5)} f(0,2,2,2) = 0 - (27)$
$u_{35} =^{(4,5)} f(1,0,0,2) = 1 - (30)$	$u_{109} =^{(4,5)} f(2,2,2,1) = 1 - (80)$
$u_{36} =^{(4,5)} f(0,0,2,2) = 1 - (9)$	$u_{146} =^{(4,5)} f(2,2,1,1) = 1 - (77)$
$u_{37} =^{(4,5)} f(0,2,2,0) = 1 - (25)$	$u_{159} =^{(4,5)} f(2,1,1,1) = 2 - (68)$
$u_{38} =^{(4,5)} f(2,2,0,1) = 0 - (74)$	$u_{164} =^{(4,5)} f(1,1,1,1) = 1 - (41)$
$u_{39} =^{(4,5)} f(2,0,1,0) = 1 - (58)$	$u_{168} =^{(4,5)} f(1,1,1,2) = 2 - (42)$
$u_{44} =^{(4,5)} f(0,1,0,1) = 2 - (11)$	$u_{169} =^{(4,5)} f(1,1,2,1) = 1 - (44)$
$u_{45} =^{(4,5)} f(1,0,1,0) = 0 - (31)$	$u_{170} =^{(4,5)} f(1,2,1,1) = 0 - (50)$
$u_{48} =^{(4,5)} f(0,1,0,2) = 0 - (12)$	$u_{171} =^{(4,5)} f(2,1,1,2) = 0 - (69)$
$u_{49} =^{(4,5)} f(1,0,2,0) = 0 - (34)$	$u_{180} =^{(4,5)} f(1,1,2,2) = 2 - (45)$
$u_{50} =^{(4,5)} f(0,2,0,1) = 1 - (20)$	$u_{181} =^{(4,5)} f(1,2,2,1) = 0 - (53)$
$u_{51} =^{(4,5)} f(2,0,1,10) = 2 - (59)$	$u_{182} =^{(4,5)} f(2,2,1,2) = 2 - (78)$
$u_{56} =^{(4,5)} f(0,1,1,1) = 0 - (14)$	$u_{195} =^{(4,5)} f(2,1,2,1) = 0 - (71)$
$u_{57} =^{(4,5)} f(1,1,1,0) = 0 - (40)$	$u_{204} =^{(4,5)} f(1,2,1,2) = 1 - (51)$
$u_{58} =^{(4,5)} f(1,1,0,1) = 0 - (38)$	$u_{207} =^{(4,5)} f(2,1,2,2) = 2 - (72)$
$u_{59} =^{(4,5)} f(1,0,1,1) = 1 - (32)$	$u_{216} =^{(4,5)} f(1,2,2,2) = 1 - (54)$
$u_{60} =^{(4,5)} f(0,1,1,2) = 1 - (15)$	$u_{217} =^{(4,5)} f(2,2,2,2) = 2 - (81)$
$u_{61} =^{(4,5)} f(1,1,2,0) = 0 - (43)$	$u_{218} =^{(4,5)} f(2,2,2,0) = 0 - (79)$
$u_{62} =^{(4,5)} f(1,2,0,1) = 2 - (47)$	

At the output we get 218 characters.Thus the table of the decrypting function is hacked.

Table 7: Decryption function

N	Value	N	Value	N	Value
(1)	$^{(4,5)}f(0,0,0,0) = 1$	(28)	$^{(4,5)}f(1,0,0,0) = 2$	(55)	$^{(4,5)}f(2,0,0,0) = 0$
(2)	$^{(4,5)}f(0,0,0,1) = 2$	(29)	$^{(4,5)}f(1,0,0,1) = 0$	(56)	$^{(4,5)}f(2,0,0,1) = 1$
(3)	$^{(4,5)}f(0,0,0,2) = 0$	(30)	$^{(4,5)}f(1,0,0,2) = 1$	(57)	$^{(4,5)}f(2,0,0,2) = 2$
(4)	$^{(4,5)}f(0,0,1,0) = 2$	(31)	$^{(4,5)}f(1,0,1,0) = 0$	(58)	$^{(4,5)}f(2,0,1,0) = 1$
(5)	$^{(4,5)}f(0,0,1,1) = 0$	(32)	$^{(4,5)}f(1,0,1,1) = 1$	(59)	$^{(4,5)}f(2,0,1,1) = 2$
(6)	$^{(4,5)}f(0,0,1,2) = 1$	(33)	$^{(4,5)}f(1,0,1,2) = 2$	(60)	$^{(4,5)}f(2,0,1,2) = 0$
(7)	$^{(4,5)}f(0,0,2,0) = 2$	(34)	$^{(4,5)}f(1,0,2,0) = 0$	(61)	$^{(4,5)}f(2,0,2,0) = 1$
(8)	$^{(4,5)}f(0,0,2,1) = 0$	(35)	$^{(4,5)}f(1,0,2,1) = 1$	(62)	$^{(4,5)}f(2,0,2,1) = 2$
(9)	$^{(4,5)}f(0,0,2,2) = 1$	(36)	$^{(4,5)}f(1,0,2,2) = 2$	(63)	$^{(4,5)}f(2,0,2,2) = 0$
(10)	$^{(4,5)}f(0,1,0,0) = 1$	(37)	$^{(4,5)}f(1,1,0,0) = 2$	(64)	$^{(4,5)}f(2,1,0,0) = 0$
(11)	$^{(4,5)}f(0,1,0,1) = 2$	(38)	$^{(4,5)}f(1,1,0,1) = 0$	(65)	$^{(4,5)}f(2,1,0,1) = 1$
(12)	$^{(4,5)}f(0,1,0,2) = 0$	(39)	$^{(4,5)}f(1,1,0,2) = 1$	(66)	$^{(4,5)}f(2,1,0,2) = 2$

(13)	${}^{(4,5)}f(0,1,1,0) = 2$	(40)	${}^{(4,5)}f(1,1,1,0) = 0$	(67)	${}^{(4,5)}f(2,1,1,0) = 1$
(14)	${}^{(4,5)}f(0,1,1,1) = 0$	(41)	${}^{(4,5)}f(1,1,1,1) = 1$	(68)	${}^{(4,5)}f(2,1,1,1) = 2$
(15)	${}^{(4,5)}f(0,1,1,2) = 1$	(42)	${}^{(4,5)}f(1,1,1,2) = 2$	(69)	${}^{(4,5)}f(2,1,1,2) = 0$
(16)	${}^{(4,5)}f(0,1,2,0) = 2$	(43)	${}^{(4,5)}f(1,1,2,0) = 0$	(70)	${}^{(4,5)}f(2,1,2,0) = 1$
(17)	${}^{(4,5)}f(0,1,2,1) = 0$	(44)	${}^{(4,5)}f(1,1,2,1) = 1$	(71)	${}^{(4,5)}f(2,1,2,1) = 0$
(18)	${}^{(4,5)}f(0,1,2,2) = 1$	(45)	${}^{(4,5)}f(1,1,2,2) = 2$	(72)	${}^{(4,5)}f(2,1,2,2) = 2$
(19)	${}^{(4,5)}f(0,2,0,0) = 0$	(46)	${}^{(4,5)}f(1,2,0,0) = 1$	(73)	${}^{(4,5)}f(2,2,0,0) = 2$
(20)	${}^{(4,5)}f(0,2,0,1) = 1$	(47)	${}^{(4,5)}f(1,2,0,1) = 2$	(74)	${}^{(4,5)}f(2,2,0,1) = 0$
(21)	${}^{(4,5)}f(0,2,0,2) = 2$	(48)	${}^{(4,5)}f(1,2,0,2) = 0$	(75)	${}^{(4,5)}f(2,2,0,2) = 1$
(22)	${}^{(4,5)}f(0,2,1,0) = 1$	(49)	${}^{(4,5)}f(1,2,1,0) = 2$	(76)	${}^{(4,5)}f(2,2,1,0) = 0$
(23)	${}^{(4,5)}f(0,2,1,1) = 2$	(50)	${}^{(4,5)}f(1,2,1,1) = 0$	(77)	${}^{(4,5)}f(2,2,1,1) = 1$
(24)	${}^{(4,5)}f(0,2,1,2) = 0$	(51)	${}^{(4,5)}f(1,2,1,2) = 1$	(78)	${}^{(4,5)}f(2,2,1,2) = 2$
(25)	${}^{(4,5)}f(0,2,2,0) = 1$	(52)	${}^{(4,5)}f(1,2,2,0) = 2$	(79)	${}^{(4,5)}f(2,2,2,0) = 0$
(26)	${}^{(4,5)}f(0,2,2,1) = 2$	(53)	${}^{(4,5)}f(1,2,2,1) = 0$	(80)	${}^{(4,5)}f(2,2,2,1) = 1$
(27)	${}^{(4,5)}f(0,2,2,2) = 0$	(54)	${}^{(4,5)}f(1,2,2,2) = 1$	(81)	${}^{(4,5)}f(2,2,2,2) = 2$

Thus, for a complete reconstruction of the table of values of the operation ${}^{(4,5)}f$, and hence the table of values of the operation f it is sufficient to supply 218 (or 217) characters for the 4-ary groupoid at the input.

Knowing Cayley table for operation ${}^{(4,5)}f$, we easily restored the operation f:

Table 8: Encryption function

N	Value	N	Value	N	Value
(1)	$f(0,0,0,0) = 2$	(28)	$f(1,0,0,0) = 1$	(55)	$f(2,0,0,0) = 0$
(2)	$f(0,0,0,1) = 0$	(29)	$f(1,0,0,1) = 2$	(56)	$f(2,0,0,1) = 1$
(3)	$f(0,0,0,2) = 1$	(30)	$f(1,0,0,2) = 0$	(57)	$f(2,0,0,2) = 2$
(4)	$f(0,0,1,0) = 1$	(31)	$f(1,0,1,0) = 0$	(58)	$f(2,0,1,0) = 2$
(5)	$f(0,0,1,1) = 2$	(32)	$f(1,0,1,1) = 1$	(59)	$f(2,0,1,1) = 0$
(6)	$f(0,0,1,2) = 0$	(33)	$f(1,0,1,2) = 2$	(60)	$f(2,0,1,2) = 1$
(7)	$f(0,0,2,0) = 1$	(34)	$f(1,0,2,0) = 0$	(61)	$f(2,0,2,0) = 2$
(8)	$f(0,0,2,1) = 2$	(35)	$f(1,0,2,1) = 1$	(62)	$f(2,0,2,1) = 0$
(9)	$f(0,0,2,2) = 0$	(36)	$f(1,0,2,2) = 2$	(63)	$f(2,0,2,2) = 1$
(10)	$f(0,1,0,0) = 2$	(37)	$f(1,1,0,0) = 1$	(64)	$f(2,1,0,0) = 0$
(11)	$f(0,1,0,1) = 0$	(38)	$f(1,1,0,1) = 2$	(65)	$f(2,1,0,1) = 1$
(12)	$f(0,1,0,2) = 1$	(39)	$f(1,1,0,2) = 0$	(66)	$f(2,1,0,2) = 2$
(13)	$f(0,1,1,0) = 1$	(40)	$f(1,1,1,0) = 0$	(67)	$f(2,1,1,0) = 2$
(14)	$f(0,1,1,1) = 2$	(41)	$f(1,1,1,1) = 1$	(68)	$f(2,1,1,1) = 0$
(15)	$f(0,1,1,2) = 0$	(42)	$f(1,1,1,2) = 2$	(69)	$f(2,1,1,2) = 1$
(16)	$f(0,1,2,0) = 1$	(43)	$f(1,1,2,0) = 0$	(70)	$f(2,1,2,0) = 2$
(17)	$f(0,1,2,1) = 2$	(44)	$f(1,1,2,1) = 1$	(71)	$f(2,1,2,1) = 0$
(18)	$f(0,1,2,2) = 0$	(45)	$f(1,1,2,2) = 2$	(72)	$f(2,1,2,2) = 1$

(19)	$f(0,2,0,0)=0$	(46)	$f(1,2,0,0)=2$	(73)	$f(2,2,0,0)=1$
(20)	$f(0,2,0,1)=1$	(47)	$f(1,2,0,1)=0$	(74)	$f(2,2,0,1)=2$
(21)	$f(0,2,0,2)=2$	(48)	$f(1,2,0,2)=1$	(75)	$f(2,2,0,2)=0$
(22)	$f(0,2,1,0)=2$	(49)	$f(1,2,1,0)=1$	(76)	$f(2,2,1,0)=0$
(23)	$f(0,2,1,1)=0$	(50)	$f(1,2,1,1)=2$	(77)	$f(2,2,1,1)=1$
(24)	$f(0,2,1,2)=1$	(51)	$f(1,2,1,2)=0$	(78)	$f(2,2,1,2)=2$
(25)	$f(0,2,2,0)=2$	(52)	$f(1,2,2,0)=1$	(79)	$f(2,2,2,0)=0$
(26)	$f(0,2,2,1)=0$	(53)	$f(1,2,2,1)=2$	(80)	$f(2,2,2,1)=1$
(27)	$f(0,2,2,2)=1$	(54)	$f(1,2,2,2)=0$	(81)	$f(2,2,2,2)=2$

Currently, we are looking for the type of text of minimum length for a 4-ary groupoid.

To understand the situation with burglary of the decrypted text and the leaders, consider the plaintext of the form: 101202$=u_1u_2u_3u_4u_5u_6$. For this text we have:

$v_1 = f(l_1, l_2, l_3, u_1) = f(l_1, l_2, l_3, 1) =?$
$v_2 = f(l_4, l_5, l_6, u_2) = f(l_4, l_5, l_6, 0) =?$
$v_3 = f(l_7, l_8, l_9, u_3) = f(l_7, l_8, l_9, 1) =?$
$v_4 = f(v_1, v_2, v_3, u_4) = f(v_1, v_2, v_3, 2) =?$
$v_5 = f(v_2, v_3, v_4, u_5) = f(v_2, v_3, v_4, 0) =?$
$v_6 = f(v_3, v_4, v_5, u_6) = f(v_3, v_4, v_5, 2) =?$

Analyzing the results obtained using the table of values of the function f, we obtain the following: $f(*,*,*,1)$ and $f(*,*,*,2)$ take any values.

Table 9: Ciphertext values

v_1	v_2	v_3	v_4	v_5	v_6
0	0	0	$f(0,0,0,2)=1$	$f(0,0,1,0)=1$	$f(0,1,0,2)=1$
0	0	1	$f(0,0,1,2)=0$	$f(0,0,0,0)=2$	$f(0,0,2,2)=0$
0	0	2	$f(0,0,2,2)=0$	$f(0,2,2,0)=2$	$f(2,0,2,2)=1$
0	1	0	$f(0,1,0,2)=1$	$f(1,0,1,0)=0$	$f(0,1,0,2)=1$
0	1	1	$f(0,1,1,2)=0$	$f(1,1,0,0)=1$	$f(1,0,1,2)=2$
0	1	2	$f(0,1,2,2)=0$	$f(1,2,0,0)=2$	$f(2,0,2,2)=1$
0	2	0	$f(0,2,0,2)=2$	$f(2,0,2,0)=2$	$f(0,2,2,2)=1$
0	2	1	$f(0,2,1,2)=1$	$f(2,1,1,0)=2$	$f(1,1,2,2)=2$
0	2	2	$f(0,2,2,2)=1$	$f(2,2,1,0)=0$	$f(2,1,0,2)=2$
1	0	0	$f(1,0,0,2)=0$	$f(0,0,0,0)=2$	$f(0,0,2,2)=0$
1	0	1	$f(1,0,1,2)=2$	$f(0,1,2,0)=1$	$f(1,2,1,2)=0$
1	0	2	$f(1,0,2,2)=2$	$f(0,2,2,0)=2$	$f(2,2,2,2)=2$
1	1	0	$f(1,1,0,2)=0$	$f(1,0,0,0)=1$	$f(0,0,1,2)=0$
1	1	1	$f(1,1,1,2)=2$	$f(1,1,2,0)=0$	$f(1,2,0,2)=1$

1	1	2	$f(1,1,2,2)=2$	$f(1,2,2,0)=1$	$f(2,2,1,2)=2$
1	2	0	$f(1,2,0,2)=1$	$f(2,0,1,0)=2$	$f(0,1,2,2)=0$
1	2	1	$f(1,2,1,2)=0$	$f(2,1,0,0)=0$	$f(1,0,0,2)=0$
1	2	2	$f(1,2,2,2)=0$	$f(2,2,0,0)=1$	$f(2,0,1,2)=1$
2	0	0	$f(2,0,0,2)=2$	$f(0,0,2,0)=1$	$f(0,2,1,2)=1$
2	0	1	$f(2,0,1,2)=1$	$f(0,1,1,0)=1$	$f(1,1,1,2)=2$
2	0	2	$f(2,0,2,2)=1$	$f(0,2,1,0)=2$	$f(2,1,2,2)=1$
2	1	0	$f(2,1,0,2)=2$	$f(1,0,2,0)=0$	$f(0,2,0,2)=2$
2	1	1	$f(2,1,1,2)=1$	$f(1,1,1,0)=0$	$f(1,1,0,2)=0$
2	1	2	$f(2,1,2,2)=1$	$f(1,2,1,0)=1$	$f(2,1,1,2)=1$
2	2	0	$f(2,2,0,2)=0$	$f(2,0,0,0)=0$	$f(0,0,0,2)=1$
2	2	1	$f(2,2,1,2)=2$	$f(2,1,2,0)=2$	$f(1,2,2,2)=0$
2	2	2	$f(2,2,2,2)=2$	$f(2,2,2,0)=0$	$f(2,2,0,2)=0$

We get 27 options for possible decrypted text, among which the 25-th option is true.

Thus, we confirmed the result that for an n-ary groupoid, the required number of characters is: $(n \cdot m^{n-1}+1)(m-1)$ characters to get all the values or $n \cdot m^{n-1}(m-1)+(m-2)$ characters, when the last value is found by the exception method.

So the minimum number of characters in a modified attack will be: $m^n+(n-1)$.

The main question is the choice of text of minimum length for groupoids of different arity and order.

2.2 Plaintext attacks

Consider an attack with the plaintext constructed using an n-ary groupoid, which is invertible on the i-th place obtained using the generalized Markovski algorithm.

Assume the cryptanalyst has access to the encryption device loaded with the key. He can then construct the following plaintext:

$$q_1q_1\cdots q_1q_1q_1q_1\cdots q_1q_2q_1q_1\cdots q_1q_m$$
$$q_1q_1\cdots q_2q_1q_1q_1\cdots q_2q_2q_1q_1\cdots q_2q_m$$
$$q_1q_1\cdots q_3q_1q_1q_1\cdots q_3q_2q_1q_1\cdots q_3q_m$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$q_1q_1\cdots q_mq_1q_1q_1\cdots q_mq_2q_1q_1\cdots q_mq_m\cdots$$

and enter it into the encryption device.

The number of characters required to restore the encryption table depends on the values of the selected leaders. Therefore, the question of determining the length of the plaintext used remains open.

Example 2.4. We consider the plaintext attack for the Example 2.1 and we chose the following plaintext:

$q_1q_1q_1q_1q_1q_2q_1q_1q_3q_1q_2q_1q_1q_2q_2q_1q_2q_3q_1q_3q_1q_1q_3q_2q_1q_3q_3$
$q_2q_1q_1q_2q_1q_2q_2q_1q_3q_2q_2q_1q_2q_2q_2q_2q_2q_3q_2q_3q_1q_2q_3q_2q_2q_3q_3$
$q_3q_1q_1q_3q_1q_2q_3q_1q_3q_3q_2q_1q_3q_2q_2q_3q_2q_3q_3q_3q_1q_3q_3q_2q_3q_3q_3$
or
000001002010011012020021022
100101102110111112120121122
200201202210211212220221222

The process of encrypting the text and the results are as follows:

Table 10: Encrypted text

$v_1 = f(u_1, l_1, l_2) = f(q_1, l_1, l_2)$ $= f(0,0,2) = 2$	$v_{42} = f(1,0,2) = 0$
$v_2 = f(u_2, l_3, l_4) = f(q_1, l_3, l_4)$ $= f(0,1,2) = 0$	$v_{43} = f(1,2,0) = 0$
$v_3 = f(u_3, v_1, v_2) = f(q_1, v_1, v_2)$ $= f(0,2,0) = 2 - (7)$	$v_{44} = f(1,0,0) = 2$
$v_4 = f(u_4, v_2, v_3) = f(0,0,2) = 2 - (3)$	$v_{45} = f(2,0,2) = 1$
$v_5 = f(0,2,2) = 0 - (9)$	$v_{46} = f(1,2,1) = 1$
$v_6 = f(1,2,0) = 0 - (16)$	$v_{47} = f(2,1,1) = 2 - (23)$
$v_7 = f(0,0,0) = 1 - (1)$	$v_{48} = f(0,1,2) = 0 - (6)$
$v_8 = f(0,0,1) = 2 - (24)$	$v_{49} = f(1,2,0) = 0$
$v_9 = f(2,1,2) = 2 - (24)$	$v_{50} = f(2,0,0) = 0$
$v_{10} = f(0,2,2) = 0$	$v_{51} = f(1,0,0) = 2$
$v_{11} = f(1,2,0) = 0$	$v_{52} = f(1,0,2) = 0$
$v_{12} = f(0,0,0) = 1$	$v_{53} = f(2,2,0) = 1 - (25)$
$v_{13} = f(0,0,1) = 2$	$v_{54} = f(2,0,1) = 1$
$v_{14} = f(1,1,2) = 1 - (15)$	$v_{55} = f(2,1,1) = 2$
$v_{15} = f(1,2,1) = 1 - (17)$	$v_{56} = f(0,1,2) = 0$
$v_{16} = f(0,1,1) = 0 - (5)$	$v_{57} = f(0,2,0) = 2$
$v_{17} = f(1,1,0) = 0 - (13)$	$v_{58} = f(2,0,2) = 1$
$v_{18} = f(2,0,0) = 0 - (19)$	$v_{59} = f(0,2,1) = 0 - (8)$
$v_{19} = (0,0,0) = 1$	$v_{60} = f(1,1,0) = 0$
$v_{20} = f(2,0,1) = 1 - (20)$	$v_{61} = f(2,0,0) = 0$
$v_{21} = f(0,0,1) = 0$	$v_{62} = f(0,0,0) = 1$
$v_{22} = f(0,1,0) = 2 - (4)$	$v_{63} = f(2,0,1) = 1$
$v_{23} = f(2,0,2) = 1 - (21)$	$v_{64} = f(2,1,1) = 2$
$v_{24} = f(1,2,1) = 1$	$v_{65} = f(1,1,2) = 1$
$v_{25} = f(0,1,1) = 0$	$v_{66} = f(0,2,1) = 0$
$v_{26} = f(2,1,0) = 1 - (22)$	$v_{67} = f(2,1,0) = 1$
$v_{27} = f(2,0,1) = 1$	$v_{68} = f(1,0,1) = 0 - (11)$
$v_{28} = f(1,1,1) = 1 - (14)$	$v_{69} = f(1,1,0) = 0$
$v_{29} = f(0,1,1) = 0$	$v_{70} = f(2,0,0) = 0$

$v_{30} = f(0,1,0) = 2$	$v_{71} = f(1,0,0) = 2$
$v_{31} = f(1,0,2) = 0 - (12)$	$v_{72} = f(2,0,2) = 1$
$v_{32} = f(0,2,0) = 2$	$v_{73} = f(2,2,1) = 2 - (26)$
$v_{33} = f(1,0,2) = 0$	$v_{74} = f(2,1,2) = 2$
$v_{34} = f(1,2,0) = 0$	$v_{75} = f(0,2,2) = 0$
$v_{35} = f(0,0,0) = 1$	$v_{76} = f(2,2,0) = 1$
$v_{36} = f(2,0,1) = 1$	$v_{77} = f(2,0,1) = 1$
$v_{37} = f(1,1,1) = 1$	$v_{78} = f(1,1,1) = 1$
$v_{38} = f(1,1,1) = 1$	$v_{79} = f(2,1,1) = 2$
$v_{39} = f(0,1,1) = 0$	$v_{80} = f(2,1,2) = 2$
$v_{40} = f(1,1,0) = 0$	$v_{81} = f(2,2,2) = 2 - (27)$
$v_{41} = f(1,0,0) = 2 - (10)$	

At the output of the encryption device, we get the following 81 characters:
20220012200121100011021101110202001111002002112000201120210001121010
0021220111222.

These characters will be enough to restore the table of values of the function f (Table 3). Knowing Cayley table for operation f, we easily restored the operation ${}^{(1,4)}f$ (Table 2).

Take some encrypted text and try to crack it. For example, we have the following ciphertext: 002101$=v_1v_2v_3v_4v_5v_6$. Then we have:

$u_1 =^{(1,4)} f(v_1, l_1, l_2) = (0, l_1, l_2) =? \Rightarrow u_1 =?$
$u_2 =^{(1,4)} f(v_2, l_3, l_4) =^{(1,4)} f(0, l_3, l_4) =? \Rightarrow u_2 =?$
$u_3 =^{(1,4)} f(v_3, v_1, v_2) =^{(1,4)} f(2,0,0) = 1 \Rightarrow u_3 = 1,$
$u_4 =^{(1,4)} f(v_4, v_2, v_3) =^{(1,4)} f(1,0,2) = 2 \Rightarrow u_4 = 2,$
$u_5 =^{(1,4)} f(v_5, v_3, v_4) =^{(1,4)} f(0,2,1) = 0 \Rightarrow u_5 = 0,$
$u_6 =^{(1,4)} f(v_6, v_4, v_5) =^{(1,4)} f(1,1,0) = 2 \Rightarrow u_6 = 2.$

Analyzing the results obtained using the table of values of the function f, we obtain the following: $f(0, *, *)$ takes any values. The possible values of the ciphertext will be only of 9 options:

Table 11: Plaintext values

u_1	u_2	u_3	u_4	u_5	u_6
0	0	1	2	0	2
0	1	1	2	0	2
1	0	1	2	0	2
1	1	1	2	0	2
2	0	1	2	0	2
0	2	1	2	0	2
2	1	1	2	0	2
1	2	1	2	0	2

2	2	1	2	0	2

Among them only the third option is correct.

For an n-ary groupoid in plaintext of length k, the first $(n-1)$ characters are not cracked. The rest are unequivocally.

Example 2.5. We consider the plaintext attack for the Example 2.3 and we chose the following plaintext:
000000010002001000110012002000210022
010001010102011001110112012001210122
020002010202021002110212022002210222
100010011002101010111012102010211022
110011011102111011111112112011211122
120012011202121012111212122012211222
200020012002201020112012202020212022
210021012102211021112112212021212122
220022012202221022112212222022212222
0000000100020010

The process of encrypting the text and the results are as follows:

Table 12: Encrypted (fragment)

$v_4 = f(1,2,2,0) = 1 - (52)$	$v_{86} = f(1,2,0,2) = 1 - (48)$
$v_5 = f(2,2,1,0) = 0 - (76)$	$v_{93} = f(2,0,1,0) = 2 - (58)$
$v_6 = f(2,1,0,0) = 0 - (64)$	$v_{94} = f(0,1,2,2) = 0 - (18)$
$v_7 = f(1,0,0,0) = 1 - (28)$	$v_{96} = f(2,0,0,2) = 2 - (57)$
$v_8 = f(0,0,1,1) = 2 - (5)$	$v_{97} = f(0,0,2,0) = 1 - (7)$
$v_9 = f(0,1,2,0) = 1 - (16)$	$v_{98} = f(0,2,1,2) = 1 - (24)$
$v_{10} = f(1,2,1,0) = 1 - (49)$	$v_{99} = f(2,1,1,2) = 1 - (69)$
$v_{11} = f(2,1,1,0) = 2 - (67)$	$v_{101} = f(1,1,0,0) = 1 - (37)$
$v_{12} = f(1,1,2,2) = 2 - (45)$	$v_{102} = f(1,0,1,2) = 2 - (33)$
$v_{15} = f(2,1,0,1) = 1 - (65)$	$v_{109} = f(1,0,1,1) = 1 - (32)$
$v_{16} = f(1,0,1,0) = 0 - (31)$	$v_{116} = f(1,1,0,1) = 2 - (38)$
$v_{17} = f(0,1,0,0) = 2 - (10)$	$v_{117} = f(1,0,2,1) = 1 - (35)$
$v_{18} = f(1,0,2,0) = 0 - (34)$	$v_{118} = f(0,2,1,0) = 2 - (22)$
$v_{19} = f(0,2,0,1) = 1 - (20)$	$v_{119} = f(2,1,2,0) = 2 - (70)$
$v_{20} = f(2,0,1,1) = 0 - (59)$	$v_{121} = f(2,2,0,1) = 2 - (74)$
$v_{24} = f(2,0,1,2) = 1 - (60)$	$v_{128} = f(0,2,1,1) = 0 - (23)$
$v_{25} = f(0,1,1,0) = 1 - (13)$	$v_{131} = f(0,1,0,1) = 0 - (11)$
$v_{26} = f(1,1,1,0) = 0 - (40)$	$v_{132} = f(1,0,0,2) = 0 - (30)$
$v_{27} = (1,1,0,2) = 0 - (39)$	$v_{133} = f(0,0,0,1) = 0 - (2)$
$v_{29} = f(0,0,1,0) = 1 - (4)$	$v_{134} = f(0,0,0,0) = 2 - (1)$

$v_{31} = f(1,1,1,2) = 2 - (42)$	$v_{135} = f(0,0,2,2) = 0 - (9)$
$v_{32} = f(1,1,2,1) = 1 - (44)$	$v_{139} = f(0,1,1,2) = 0 - (15)$
$v_{36} = f(1,2,2,2) = 0 - (54)$	$v_{143} = f(2,1,2,2) = 1 - (72)$
$v_{37} = f(2,2,0,0) = 1 - (73)$	$v_{144} = f(1,2,1,2) = 0 - (51)$
$v_{41} = f(0,2,0,0) = 0 - (19)$	$v_{161} = f(1,0,0,1) = 2 - (29)$
$v_{42} = f(2,0,0,1) = 1 - (56)$	$v_{162} = f(0,0,2,1) = 2 - (8)$
$v_{44} = f(0,1,1,1) = 2 - (14)$	$v_{173} = f(2,2,1,1) = 1 - (77)$
$v_{45} = f(1,1,2,0) = 0 - (43)$	$v_{174} = f(2,1,1,1) = 0 - (68)$
$v_{46} = f(1,2,0,1) = 0 - (47)$	$v_{179} = f(2,2,0,2) = 0 - (75)$
$v_{47} = f(2,0,0,0) = 0 - (55)$	$v_{182} = f(0,2,2,2) = 1 - (27)$
$v_{48} = f(0,0,0,2) = 1 - (3)$	$v_{192} = f(2,0,2,2) = 1 - (63)$
$v_{55} = f(1,2,1,1) = 2 - (50)$	$v_{194} = f(2,1,0,2) = 2 - (66)$
$v_{56} = f(2,1,2,1) = 0 - (71)$	$v_{212} = f(0,1,2,1) = 2 - (17)$
$v_{57} = f(1,2,0,0) = 2 - (46)$	$v_{213} = f(1,2,2,1) = 2 - (53)$
$v_{58} = f(2,0,2,1) = 0 - (62)$	$v_{214} = f(2,2,2,2) = 2 - (81)$
$v_{62} = f(1,1,1,1) = 1 - (41)$	$v_{218} = f(2,2,2,0) = 0 - (79)$
$v_{67} = f(0,2,0,2) = 2 - (21)$	$v_{227} = f(0,0,0,0) = 2 - (1)$
$v_{71} = f(0,0,1,2) = 0 - (6)$	$v_{288} = f(1,0,2,2) = 2 - (36)$
$v_{72} = f(0,1,0,2) = 1 - (12)$	$v_{290} = f(2,2,1,2) = 2 - (78)$
$v_{79} = f(2,0,2,0) = 2 - (61)$	$v_{338} = f(0,2,2,0) = 2 - (25)$
$v_{80} = f(0,2,2,1) = 0 - (26)$	$v_{339} = f(2,2,2,1) = 1 - (80)$

At the output of the encryption device we get 339 characters.They will be enough to restore the table of values of the function f (Table 8). Knowing Cayley table for the operation f, we easily restored the operation ${}^{(4,5)}f$ (Table 7).

Take some encrypted text and try to crack it. For example, we have the following ciphertext: 220001=$v_1v_2v_3v_4v_5v_6$. Then we have:

$u_1 =^{(4,5)} f(l_1, l_2, l_3, v_1,) =^{(4,5)} f(l_1, l_2, l_3, 2) =? \Rightarrow u_1 =?$
$u_2 =^{(4,5)} f(l_4, l_5, l_6, v_2,) =^{(4,5)} f(l_4, l_5, l_6, 2) =? \Rightarrow u_2 =?$
$u_3 =^{(4,5)} f(l_7, l_8, l_9, v_3) =^{(4,5)} f(l_7, l_8, l_9, 0) =? \Rightarrow u_3 =?$
$u_4 =^{(4,5)} f(v_1, v_2, v_3, v_4) =^{(4,5)} f(2,2,0,0) = 2 \Rightarrow u_4 = 2,$
$u_5 =^{(4,5)} f(v_2, v_3, v_4, v_5) =^{(4,5)} f(2,0,0,0) = 0 \Rightarrow u_5 = 0,$
$u_6 =^{(4,5)} f(v_3, v_4, v_5, v_6) =^{(4,5)} f(0,0,0,1) = 2 \Rightarrow u_6 = 2.$

Analyzing the results obtained using the table of values of the function ${}^{(4,5)}f$, we obtain the following: $f(*,*,*,2)$ and $f(*,*,*,0)$ take any values.The possible values of the ciphertext will be 27 options:

Table 13: Plaintext values

u_1	u_2	u_3	u_4	u_5	u_6
0	0	0	2	0	2
0	0	1	2	0	2

0	0	2	2	0	2
0	1	0	2	0	2
0	1	1	2	0	2
0	1	2	2	0	2
0	2	0	2	0	2
0	2	1	2	0	2
0	2	2	2	0	2
1	0	0	2	0	2
1	0	1	2	0	2
1	0	2	2	0	2
1	1	0	2	0	2
1	1	1	2	0	2
1	1	2	2	0	2
1	2	0	2	0	2
1	2	1	2	0	2
1	2	2	2	0	2
2	0	0	2	0	2
2	0	1	2	0	2
2	0	2	2	0	2
2	1	0	2	0	2
2	1	1	2	0	2
2	1	2	2	0	2
2	2	0	2	0	2
2	2	1	2	0	2
2	2	2	2	0	2

Among them the 11th option is correct.

3. Conclusion

A cryptanalysis is done on cipher and there are analyzed cryptoattacks, built by M. Vojvoda for quasigroups, chosen ciphertext and plaintext.

In this article, we looked at some types of attacks on the Markovski cipher with the help of open and encrypted texts.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(i,n+1)})f$ and hence, the table of values of the operation f using cryptotext attack, it is sufficient to submit at the input: $A = (n \cdot m^{n-1} + 1)(m-1)$ characters to get all the values.

The minimum number of characters in a modified cryptotext attack will be $m^n + (n-1)$ symbols, where n is arity and m the order of an i-invertible groupoid. As for the plaintext attack, it was possible to establish the lower limit value of the necessary characters to restore the table of the values of function f.

But the following question remains. What kind of text to give at the input of the encrypting device so as not to exceed the received limit of characters and will it always be possible?

We plan to continue attacks on the cipher built with the help of generalized Markovski algorithms on i-invertible groupoids.

Acknowledgement. The author thanks Referee for his helpful comments.

References

[1] **P. Csorgo, V.A. Shcherbacov**, *On some quasigroup cryptographical primitives*, arXiv:1110.6591, 11 pages.

[2] **N.N. Malyutina, A.V. Scerbacova, V.A. Shcherbacov**, *Markovsky algorithm on i-invertibile groupoids*, arXiv:1806.02267, 3 pages.

[3] **S. Markovski, D. Gligoroski, S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. VIII Conf. Logic and Computer Science "LIRA'97", Novi Sad, 1997, 157–167.

[4] **E. Ochodková, V. Snashel**, *Using quasigroups for secure encoding of file system*, Proc. Intern. Sci. NATO PfP/PWP Conf. "Security and Information Protection 2001", Brno, Czech Republic, 175–181.

[5] **V.A. Shcherbacov, N.N. Malyutina**, *Role of quasigroups in cryptosystems. Generalization of Markovski algorithm*, Bull. Transnistrian Univ., **60** (2018), no.3, 53–57.

[6] **M. Vojvoda**, *Cryptanalysis of a file encoding system based on quasigroup*, J. Electr. Engineering, **54** (2003), No. 12/S, 69–71.

[7] **M. Vojvoda**, *Stream ciphers and hash functions – analysis of some new design approaches*, PhD thesis, Slovak University of Technology, July, 2004.

Received March 15, 2019
Revised February 25, 2020

Department of Mathematics
State University Dimitrie Cantemir
Academiei str. 3/2
MD-2028 Chişinău
Moldova
E-mail: 231003.Bab.Nadezhda@mail.ru