Quasigroup-based Hybrid of a Code and a Cipher

Victor A. Shcherbacov

Institute of Mathematics and Computer Science
of the Academy of Sciences of Moldova, Academiei str. 5,
MD−2028 Chişinău, Moldova

Abstract. We construct quasigroup-based hybrid of a code and a cipher.
2000 Mathematics Subject Classification: 94A60, 20N05, 20N15.

Keywords: cipher, code, quasigroup, T-quasigroup, orthogonality, n-ary groupoid, system of orthogonal n-ary groupoids

1 Introduction

We construct quasigroup-based hybrid of a code and a cipher and give an algorithm that describes this construction. Some results presented in this paper are taken from [18].

Hybrid idea is sufficiently known, see, for example, [16], [17]. Following Markovski, Gligoroski, and Kocarev [9], [10], we name such hybrid as a cryptcode.

Author chooses "example" style for this paper in order to make it accessible for engineers and students.

Definition 1. *A T-quasigroup (Q, A) is a quasigroup of the form $A(x, y) = \varphi x + \psi y + c$, where $(Q, +)$ is an abelian group, φ, ψ are some fixed automorphisms of this group, c is a fixed element of the set Q [8], [15].*

Theorem 1. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \alpha x + \beta y + c$ and a T-quasigroup $(Q, \circ)$ of the form $x \circ y = \gamma x + \delta y + d$, both over a group $(Q, +)$, are orthogonal if and only if the map $\alpha^{-1}\beta - \gamma^{-1}\delta$ is an automorphism of the group $(Q, +)$ [14].*

Denote elements of the group $Z_2 \oplus Z_2$ as follows: $\{(0; 0), (1; 0), (0; 1), (1; 1)\}$. The group $Aut(Z_2 \oplus Z_2)$ consists of the following automorphisms:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Denote these automorphisms by the letters $\varepsilon, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$, respectively.

Notice that $\varphi_2^2 = \varphi_3^2 = \varphi_4^2 = \varepsilon, \varphi_5^2 = \varphi_6, \varphi_6^2 = \varphi_5$. It is known that $Aut(Z_2 \oplus Z_2) \cong S_3$ [6], [7].

For convenience we give Cayley table of the group $Aut(Z_2 \oplus Z_2)$.

$\cdot$	ε	φ_2	φ_3	φ_4	φ_5	φ_6
ε	ε	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	ε	φ_5	φ_6	φ_3	φ_4
φ_3	φ_3	φ_6	ε	φ_5	φ_4	φ_2
φ_4	φ_4	φ_5	φ_6	ε	φ_2	φ_3
φ_5	φ_5	φ_4	φ_2	φ_3	φ_6	ε
φ_6	φ_6	φ_3	φ_4	φ_2	ε	φ_5

Information on codes can be found in [4].

2 Construction

Code part. We shall use a code given in [13, Example 19]. Let's suppose that the symbols x, y are informational symbols, and the symbol z is a check symbol. Remember $x, y, z \in (Z_2 \oplus Z_2)$. We propose the following check equation $x + \varphi_5 y + \varphi_6 z = (0;0)$, i.e., we set the following formula to find the element z:

$$z = \varphi_5 x + \varphi_6 y \tag{1}$$

Recall, statistical investigations of J. Verhoeff [19] and D.F. Beckley [2] have shown that the most frequent errors made by human operators during data transmission are single errors (i.e. errors in exactly one component), adjacent transpositions (in other words errors made by interchanging adjacent digits, i.e. errors of the form $ab \to ba$), and insertion or deletion errors. If all codewords are of equal length, insertion and deletion errors can be detected easily.

Twin error is an error of the form $(aa \to bb)$. In [13] it is proved the following

Theorem 2. *Any $(n-1)$-T-quasigroup code (Q, g) with check equation*

$$d(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

detects:

- *any transposition error on the place $(i, i+k), (i \in \overline{1, n-k},\ k \in \overline{1, n-i},\ i+k \leq n)$ if and only if the mapping $\alpha_i - \alpha_{i+k}$ is an automorphism of the group $(Q, +)$;*
- *any twin error on the place $(i, i+k)$, $(i \in \overline{1, n-k},\ k \in \overline{1, n-i},\ i+k \leq n)$ if and only if the mapping $\alpha_i + \alpha_{i+k}$ is an automorphism of the group $(Q, +)$.*

From Theorem 2 follows that the proposed code detects any transposition and twin error. The proposed code is quasigroup code, therefore it detects any single error [12], [13].

Suppose we have a word of the form ab, $a, b \in Z_2 \oplus Z_2$. There exist $3 \cdot 3 = 9$ double errors that can be done in this word. It is easy to see that given code detects 6 errors and it cannot detect 3 double errors.

Thus this code detects 12 from theoretically possible 15 errors in any word of the form ab, $a, b \in Z_2 \oplus Z_2$, i.e., it detects 80% errors in information symbols by supposition that the check symbol was transmitted without error.

Cryptographical part. We construct cryptographical part of the proposed cryptcode. For this aim we take three T-quasigroups over the group $Z_2 \oplus Z_2$:
$(Z_2 \oplus Z_2, D)$ with the form $D(x, y) = \varphi_3 x + \varphi_6 y + a_1$;
$(Z_2 \oplus Z_2, E)$ with the form $E(x, y) = \varphi_2 x + \varphi_5 y + a_2$;
$(Z_2 \oplus Z_2, F)$ with the form $F(x, y) = \varphi_3 x + \varphi_5 y + a_3$.

Lemma 1. *The quasigroups $(Z_2 \oplus Z_2, D)$, $(Z_2 \oplus Z_2, E)$, and $(Z_2 \oplus Z_2, F)$ are orthogonal in pairs.*

Proof. We can use Theorem 1 and Cayley table of the group $Aut(Z_2 \oplus Z_2)$.

Define three ternary operations:

$$\begin{aligned} K_1(D(x, y), z) &= D(x, y) + z \\ K_2(E(x, y), z) &= E(x, y) + z \\ K_3(F(x, y), z) &= F(x, y) + z \end{aligned}$$

It is clear that these operations can be replaced by a more complex system of operations.

Lemma 2. *The triple of ternary operations $K_1(x, y, z), K_2(x, y, z), K_3(x, y, z)$ forms an orthogonal system of operation.*

Proof. We solve the following system of equations

$$\begin{cases} \varphi_3 x + \varphi_6 y + a_1 + z = b_1 \\ \varphi_2 x + \varphi_5 y + a_2 + z = b_2 \\ \varphi_3 x + \varphi_5 y + a_3 + z = b_3 \end{cases} \tag{2}$$

where b_1, b_2, b_3 are fixed elements of the set $Z_2 \oplus Z_2$.
We use properties of the groups $(Z_2 \oplus Z_2)$ and $Aut(Z_2 \oplus Z_2)$:

$$\begin{cases} \varphi_3 x + \varphi_6 y + z = b_1 + a_1 \\ \varphi_2 x + \varphi_5 y + z = b_2 + a_2 \\ \varphi_3 x + \varphi_5 y + z = b_3 + a_3 \end{cases} \tag{3}$$

We do the following transformations of the system (3): (first row + third row) $\rightarrow$ first row; (second row + third row) $\rightarrow$ second row; and obtain the system:

$$\begin{cases} y = b_1 + a_1 + b_3 + a_3 \\ x = \varphi_4(b_2 + a_2 + b_3 + b_4) \\ \varphi_3 x + \varphi_5 y + z = b_3 + a_3 \end{cases} \tag{4}$$

In the third equation of the system (4) we replace x by $\varphi_4(b_2 + a_2 + b_3 + b_4)$ and y by $b_1 + a_1 + b_3 + a_3$, obtaining:

$$\begin{cases} x = \varphi_4(b_2 + a_2 + b_3 + a_3) \\ y = b_1 + a_1 + b_3 + a_3 \\ z = b_3 + a_3 + \varphi_5(b_1 + a_1 + b_2 + a_2) \end{cases} \tag{5}$$

Therefore, the system (2) has a unique solution for any fixed elements $b_1, b_2, b_3 \in (Z_2 \oplus Z_2)$, operations $K_1(x, y, z), K_2(x, y, z), K_3(x, y, z)$ are orthogonal.

Triplets of orthogonal operations $K_1(x, y, z), K_2(x, y, z), K_3(x, y, z)$ (by $a_1 = a_2 = a_3 = (0; 0)$) define on the set Q^3 permutation with the following cycle type: $1^2 2^1 4^1 7^2 14^1 28^1$, i.e., this permutation contains two cycles of order 1, one cycle of order 2, and so on. Denote this permutation by the letter K.

The order of permutation K is equal to 28. Notice that using isotopy [3], [11] or generalized isotopy [14] it is possible to change the order of permutation K.

We shall use the system of three ternary orthogonal groupoids (Q, A), (Q, B), (Q, C) of order 4 from [5].

In these tables $A(0, 1, 2) = A_0(1, 2) = 3$, $C(2, 3, 2) = C_2(3, 2) = 2$, and so on.

A_0	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

A_1	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

A_2	0	1	2	3
0	2	3	0	1
1	3	0	1	2
2	0	1	2	3
3	1	2	3	0

A_3	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

B_0	0	1	2	3
0	3	0	1	3
1	0	2	3	0
2	1	2	1	3
3	1	1	2	2

B_1	0	1	2	3
0	2	1	1	0
1	2	3	3	0
2	0	2	1	3
3	0	0	3	1

B_2	0	1	2	3
0	1	2	0	0
1	2	0	3	1
2	0	2	3	2
3	3	2	1	1

B_3	0	1	2	3
0	3	3	2	2
1	0	1	2	1
2	0	2	0	3
3	3	1	0	3

C_0	0	1	2	3
0	3	1	2	0
1	2	1	1	2
2	0	1	0	1
3	3	1	2	3

C_1	0	1	2	3
0	1	2	1	3
1	1	2	3	1
2	0	2	2	0
3	1	3	1	1

C_2	0	1	2	3
0	3	3	0	0
1	2	1	0	1
2	3	3	2	0
3	3	0	2	3

C_3	0	1	2	3
0	2	1	0	0
1	2	0	2	3
2	3	3	2	0
3	2	0	0	3

Denote permutation that defines this system of three ternary orthogonal groupoids by the letter M, $M = M(A(x, y, z), B(x, y, z), C(x, y, z))$. This permutation has the following cycle type: $1^1 17^1 20^1 26^1$. The order of this permutation is equal to $17 \cdot 20 \cdot 13 = 4420$.

In order to use the system of orthogonal groupoids and the system of orthogonal T-quasigroups simultaneously we redefine the basic set of the T-quasigroups in the following (non-unique) way: $(0; 0) \to 0$, $(1; 0) \to 1$, $(0; 1) \to 2$, $(1; 1) \to 3$.

We propose the following cryptographical term (a cryptographical primitive):

$$H(x, y, z) = M^k(K^l(x, y, z)), k, l \in \mathbb{Z} \tag{6}$$

The transformation H is a permutation of the set Q^3. Indeed, this transformation is a composition of two permutations: K^l and M^k.

Remark 1. It is possible to use the following cryptographical procedure:

$$H_1(x, y, z) = K^t(M^k(K^l(x, y, z))), t, k, l \in \mathbb{Z},$$

and so on.

3 Algorithm

We propose the following

Algorithm 1 *1. Take a pair of information symbols $a, b \in (Z_2 \oplus Z_2)$;*
2. using formula (1) (or its analogue), find value of the check symbol c;
3. apply the cryptographical term H to the triple (a, b, c);
4. therefore, we obtain first three elements of the cipher-text;
5. take a pair of information symbols $d, e \in (Z_2 \oplus Z_2)$;
6. using formula (1), find value of the check symbol f;
7. change values of the numbers k, l in the cryptographical term H; also it is possible to change the term H by other term of such or other type;
8. apply the cryptographical term H to the triple (d, e, f);
9. we obtain next three elements of the cipher-text;
10. and so on.

Remark 2. At Step 7 of Algorithm 1 it is possible to use ideas of Feistel schema. Namely, it is possible to calculate the numbers k, l using some bijective functions, where the numbers of triplet $H(a, b, c)$ and previous values of k and l are used as arguments.

Decoding. Using permutations K^{-1} and M^{-1}, we can construct corresponding triplets of orthogonal 3-ary groupoids and so on.

Resistance relative to some possible attacks. Taking into consideration Remark 1, we can estimate the number of possible keys in the presented crypt-code. This number is equal to (64!). Length of any key is equal to $64 \cdot 3 \cdot 2 = 384$ bits.

At each step of the proposed algorithm only three symbols (six bits) are ciphered. Moreover, after any step this key can be changed. Therefore, brute-force attack is difficult.

Statistical attack also seems to be difficult. It is possible to present the following argument: the symmetric group S_{64} acts on the set, which consists from 64 triplets 64-transitively [7].

A code-crypt algorithm. Denote the coding procedure from Algorithm 1 as $C(x, y)$ since this procedure is a function of two variables. Therefore, we can describe procedures of coding and enciphering in Algorithm 1 by the following formula:

$$H(x, y, C(x, y)), \tag{7}$$

where H is taken from equation (6). It is possible to construct a code-crypt algorithm by the formula $C_1(H(x, y, z))$ since there exists a possibility to use an analogue of the code C for three information symbols [13, Example 19], i.e., we can transpose the procedures C and H.

Conclusion. Almost all constructions in this paper are performed over the field $GF(2^2)$. An analog of Algorithm 1 can be constructed over a field of the order more than four. Also we can use an alternating more powerful code [1].

Acknowledgment. Author thanks Referees for their helpful comments.

References

1. Bakeva V., Ilievska, N.: A Probabilistic Model of Error-Detecting Codes Based on Quasigroups. Quasigroups Related Systems 17(2), 135–148 (2009).
2. Beckley, D.F.: An Optimum Systems with Modulo 11. The Computer Bulletin 11, 213–215 (1967).
3. Belousov, V.D.: Foundations of the Theory of Quasigroups and Loops. Nauka, Moscow, (1967). (in Russian).
4. Blahut, Richard E.: Theory and Practice of Error Control Codes. Addison-Wesley Publishing Company, Advanced Book Program, Reading (1983).
5. Csorgo, Piroska, Shcherbacov, Victor: On Some Quasigroup Cryptographical Primitives, http://arxiv.org/abs/1110.6591 (2011).
6. Hall, Marshall: The Theory of Groups. The Macmillan Company, New York (1959).
7. Kargapolov, M.I., Merzlyakov, M.Yu.: Foundations of Group Theory. Nauka, Moscow (1977).
8. Kepka T., Němec, P.: T-quasigroups, II. Acta Univ. Carolin. Math. Phys. 12(2), 31–49 (1971).
9. Markovski, S., Gligoroski, D., Kocarev, Lj.: Totally Asynchronous Stream Ciphers + Redundancy = Cryptcoding. In Proceedings of the 2007 International Conference on Security and Management, SAM 2007, June 25-28, 2007, Las Vegas, USA, 446–451, (2007). http://www.informatik.uni-trier.de/ ley/db/conf/csreaSAM/csreaSAM2007.html/.../GligoroskiMK07.
10. Markovski, S., Gligoroski, D., Kocarev, Lj.: Error Correcting Cryptcodes Based on Quasigroups. NATO ARW, October 6-9, 2008, Veliko Tarnovo, Bulgaria, (2008). https://www.cosic.esat.kuleuven.be/.../Markovski_slides_nato08.ppt.
11. Pflugfelder, H.O.: Quasigroups and Loops: Introduction. Heldermann Verlag, Berlin (1990).
12. Mullen, G.L., Shcherbacov, V.A.: Properties of Codes with One Check Symbol from a Quasigroup Point of View. Bul. Acad. Stiinte Repub. Mold., Mat., 2 (48), 71–86 (2002).
13. Mullen, G.L., Shcherbacov, V.A.: n-T-quasigroup Codes with One Check Symbol and Their Error Detection Capabilities. Comment. Math. Univ. Carolin. 45(2), 321–340 (2004).
14. Mullen, G.L., Shcherbacov, V.A.: On Orthogonality of Binary Operations and Squares. Bul. Acad. Stiinte Repub. Mold., Mat., (2 (48)), 3–42 (2005).
15. Němec, P., Kepka, T.: T-quasigroups, I. Acta Univ. Carolin. Math. Phys. 12(1), 39–49 (1971).
16. Shcherbacov, V.A.: Elements of Quasigroup Theory and Some Its Applications in Code Theory, (2003). urls: www.karlin.mff.cuni.cz/drapal/speccurs.pdf; http://de.wikipedia.org/wiki/Quasigruppe
17. Shcherbacov, V.A.: On Some Known Possible Applications of Quasigroups in Cryptology (2003). www.karlin.mff.cuni.cz/drapal/krypto.pdf
18. Shcherbacov, Victor: Quasigroup Based Crypto-Algorithms. arXiv:1110.6591v1 (2012). http://arxiv.org/pdf/1201.3016v1.

19. Verhoeff, J.: Error Detecting Decimal Codes, volume 29. Math. Centrum, Amsterdam (1969).