Tatra Mt. Math. Publ. **45** (2010), 27–36
DOI: 10.2478/v10127-010-0003-z

TATRA MOUNTAINS
Mathematical Publications

ISOTOPY OF LATIN SQUARES IN CRYPTOGRAPHY

Otokar Grošek — Marek Sýs

ABSTRACT. We present a new algorithm for a decision problem if two Latin squares are isotopic. Our modification has the same complexity as Miller's algorithm, but in many practical situations is much faster. Based on our results we study also a zero–knowledge protocol suggested in [3]. From our results it follows that there are some problems in practical application of this protocol.

1. Introduction

Throughout this paper we use a common notation for the symmetric group of elements from a set X as $\mathrm{Sym}(X)$. Especially, the symmetric group over the symbol set $I_n = \{1, \ldots, n\}$ will be denoted by S_n. Also $\mathcal{L}(n)$ will denote the set of all Latin squares over I_n. We will understand the Cayley table of a quasigroup $(S, *)$ over the symbol set I_n as a Latin square $L = L(\ell_{ij}) \in \mathcal{L}(n)$ with $\ell_{ij} = i * j$. Therefore the notions of a quasigroup and a Latin square will be freely interchanged in the paper. Since it is more natural and handy to express definitions and results concerning the topic in the language of Latin squares, the notion of a quasigroup will be used only sporadically.

A Latin square was regarded by Euler as a square matrix with n^2 entries of n different elements, none of them occurring twice within any row or column of the matrix:

1	2	3	4	5
2	4	1	5	3
3	5	2	1	4
4	3	5	2	1
5	1	4	3	2

. Latin squares as a basic core for cryptographic systems go approximately 20 years back although, there were some systems where they played a marginal role. In 1941 A. Adrian Albert has written

2010 Mathematics Subject Classification: 20N05, 94A60.
Keywords: Latin squares, isotopy of quasigroups, zero–knowledge protocol.
Supported by the grant NIL-I-004 from Iceland, Lichtenstein and Norway through the EEA Financial Mechanism and the Norwegian Financial Mechanism.

that (quote [12]) "... various algebraic structures can be used for ciphering". The first serious usage of Latin squares in Block ciphers with detailed analysis is connected with the cipher IDEA [14]. In this paper authors used the concept of non-isotopic quasigroups. Since that time plenty of papers has been published, some of them are mentioned in [19]. It is customary to mention

- Block ciphers (Lai, Massey IDEA 1990, [14]).
- (Almost) public key cryptography (Koscielny and Mullen 1999 [13], Markovski, Gligoroski, Stojcevska 2000 [15]).
- S-box theory (Grošek, Satko, Nemoga 2000 [9], [10], Grošek, Horák, Tran 2004 [11]).
- Stream ciphers (Gligoroski, Markovski, Kocarev, Gusev: Edon80 2005 [6])
- Hash functions and MAC's (Gligoroski, Odegard, Mihova, Knapskog, Kocarev, Drápal: EDON-R 2009 [7]).

From such a brief list one can see a large potential of Latin squares for cryptography along with their analysis as a part of cryptanalysis. One of the basic properties of Latin squares is their membership to an isotopy class. These are precisely Latin squares which differ in the row, column or element permutation, respectively. We say that they are in some sense similar. Such Latin squares are used in the stream cipher EDON 80, and in [22] authors analyzed the influence of isotopic Latin squares to the security of this cipher. Their analysis by exhaustive search was possible because of the small size of them, namely 4×4. Nowadays ciphers, like EdonR [7] which is a candidate for the new standard SHA3, use much larger quasigroups. Thus a natural task arises: to develop a strong toolkit for the decision problem if two Latin squares are isotopic.

In Miller's paper [16] one can find an $\mathcal{O}(n^{\log_2 n})$ algorithm based on a previous work of Tarjan [17]. Obviously this algorithm is impossible to use for EdonR analysis. In some other papers authors used a graph representation of Latin squares, and the problem is converted to finding isomorphisms of strongly regular graphs. Complexity of such algorithms is of the order $\mathcal{O}(n^{n^{1/3} \log_2 n})$, and hence they are, in general, slower than Miller's algorithm.

2. Isotopy problem of two Latin squares

For convenience of a reader we briefly recall some basic definitions.

Definition 1 ([2]). Two Latin squares of order n are said to be isotopic if one can be transformed into other by rearranging rows, rearranging columns, and

renaming elements, that is, if the quasigroups whose multiplication tables they represent are isotopic.

Definition 2 ([1]). Let Latin squares L and L' be isotopic. Let θ, ψ, φ be bijections such that

$$\psi(\ell_{\theta(i),\varphi(j)}) = \ell'_{i,j}.$$

Then (θ, φ, ψ) is called isotopism of L on L'. If L and L' are identical ($\ell_{ij} = \ell'_{ij}$ for all (i, j), then isotopism is also called autotopism.

Application of an isotopism (θ, φ, ψ) on Latin square L we denote as $L^{(\theta,\varphi,\psi)}$.

Isotopy is an important relation on the set of Latin squares. Even more this is an equivalence relation which divides $\mathcal{L}_n$ on disjoint classes of isotopic squares. And we have a decision problem

INPUT: Latin squares L, M of order n.

DECISION: Are they isotopic?

OUTPUT: YES – NO.

To solve this problem doest not require, in general, to find permutation of rows θ, columns φ and symbols ψ if they are isotopic. One such approach is due to Ferguson [4] which was shown as wrong in [5]. An informal description is as follows:

- Let E be the equivalence relation on $\mathcal{L}_n$ in which L and M, or transpose of M, M^t are isotopic.
- One can assume a Latin square as $n \times n$ matrix, and calculate its determinant.
- It has been shown in [4] that L and M, $n \leq 7$, are isotopic iff they have the same determinant.
- This result is not true for $n = 8$ as shown in [5].

One of the first attempts to use isotopy to evaluate security of a cryptographic system was paper [22]. EDON80, as one of the submissions to the ECRYPT Stream Ciphers Project—eSTREAM that passed to the Phase II, uses so called e-transformers. They consist of four quasigroups of order $n = 4$ in each e-transformer (out of 64 carefully chosen), selected to use by 80 bits key read as two-bits sequences $00, 01, 10, 11$. Vojvoda and Sýs presented at SASC '07 in Bochum that all 64 are isotopic to $(Z_4, +)$. Moreover, they are polynomial [11] over $GF(2^2)$. If L, M are isotopic and L is polynomial, then M is polynomial. Thus one polynomial is enough to describe e-transformers. These two facts may imply a possible weakness, or simplification in hardware.

Another possibility is to use isotopy for a cryptographic primitive. It is known that isotopy problem belongs to the "hard problems" [16]. As we mentioned above the complexity by Miller's algorithm is $\mathcal{O}(n^{\log_2 n})$. Thus this problem can

be (potentially) used in zero–knowledge protocols by Goldreich, Micali, Wigderson theorem which states that all NP problems give to rise to a zero-knowledge proofs.

Theorem 1 (Goldreich-Micali-Wigderson [8]). *Every provable mathematical statement has a zero-knowledge proof.*

We focus on this problem in the Section 4.

3. A new algorithm for isotopy

A well known Cayley theorem [18] states that any group $(G, *)$ is isomorphic to a subgroup $\overline{G}$ of the symmetric group $\mathrm{Sym}(G)$. This isomorphism is known as a regular representation of G. Elements of $\overline{G}$ can be represented by left translations of G. Translation by $a \in G$ is denoted by L_a, $L_a : G \mapsto G$, defined for $x \in G$ as $L_a(x) = a * x$. Hence a group G is represented by the set of its translations $L_G \subseteq \mathrm{Sym}(G)$.

For a quasigroup Q we can similarly consider the set of left translations although in this case L_Q is not the isomorphic image of Q. The quasigroup is defined by L_Q uniquely. Next theorem states relation between translations and isotopy of two quasigroups.

Theorem 2. *Let (θ, φ, ψ) be isotopism of two quasigroups $Q_1 = (Q, *_1)$ and $Q_2 = (Q, *_2)$. Then for the set of left translations L_{Q_1}, L_{Q_2} it is valid*

$$L_{Q_2} = \psi L_{Q_1} \varphi^{-1}. \tag{1}$$

From Theorem 2 we have a straightforward method how to find an isotopism for two quasigroups Q_1, Q_2: For all $\varphi, \psi \in \mathrm{Sym}(Q)$ verify (1). This approach has obviously a very high complexity. The next theorem is more practical for such purposes.

Theorem 3. *Let $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ be two quasigroups and $p_2 \in L_{Q_2}$. Then Q_1, Q_2 are isotopic iff there exist $p_1 \in L_{Q_1}$, $p \in \mathrm{Sym}(Q)$ such that*

$$L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}. \tag{2}$$

An algorithm based on Theorem 3 is much more effective than that based on Theorem 2. It is enough to find for a fixed $p_2 \in L_{Q_2}$ permutations $p_1 \in L_{Q_1}$, $p \in \mathrm{Sym}(Q)$ such that $L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}$. Since the sets of permutations $L_{Q_2} p_2^{-1}, L_{Q_1} p_1^{-1}$ are conjugate by p, and thus they possess the same cycle structure. This fact allows to modify the set of permutations p from the search space. The cycle structure of $g, h \in S_n$ directly leads to the set $C_n(g, h) = \{p |\ pgp^{-1} = h\}$. The cardinality of this set is given by the structure

of permutations g, h. The cycle structure of $p \in S_n$ is a vector of the numbers $(a_1, \cdots, a_n)$, of disjoint cycles of p. More precisely, p possesses a_i cycles of the length i. For two conjugate permutations g, h, of the type $(a_1, \cdots, a_n)$ we have [21] $|C_n(g,h)| = \prod_{i=1}^{n} a_i! i^{a_i}$.

Another improvement for the isotopy algorithm is based on generators for the conjugate sets $G, H \subseteq S_n$ with $C_n(G,H) = \{p|\ pGp^{-1} = H\}$.

Definition 3. We say that $G' \subseteq G$ generates $G \subseteq S_n$, if for each $\tau \in G$ there exists a sequence of permutations $\{g'_n\}_{j=1}^{k}$ from G' such that for the permutation $\tau = \prod_{j=1}^{k} g'_j$.

A pseudocode of the algorithm to find $C_n(G,H)$ is as follows:

Algorithm 1. Input: Set $G, H \subseteq S_n$ Output: Set $C_n(G,H)$

(1) Divide $g_i \in G$ to cycles and find the smallest set $G' = \{\overline{g_1}, \cdots, \overline{g_m}\}$ of generators of G. Let $|G'| = m$.
(2) Divide to cycles permutations $h_i \in H$.
(3) For each m-subset H' of $\overline{h_1}, \cdots, \overline{h_m}$ such that H' is of the same type as G', and H' generates H do:
   (a) for each $P_j \in I_m$ such that $\overline{g_i}$ and $\overline{h_{P_j(i)}}$ are of the same type, find $p \in S_n$ such that $pG'p^{-1} = H'$.
   (b) If $pGp^{-1} = H$ add p to $C_n(G,H)$.
(4) Return $C_n(G,H)$.

We will use Algorithm 1 in the next one to find for two quasigroups G, H the set of their isotopisms $Is(G,H)$. To speed up this algorithm there was proven in [21] a new necessary condition for the existence of an isotopism. The condition is based on Theorem 4 and its Corollary.

Definition 4 ([1])**.** Let $(Q, *)$ be a quasigroup and define new binary operations $*_{(1,2,3)}, *_{(1,3,2)}, *_{(2,1,3)}, *_{(2,3,1)}, *_{(3,1,2)}, *_{(3,2,1)}$ on Q as follows: relation $a * b = c$ is valid if and only if

$$a *_{(1,2,3)} b = c, a *_{(1,3,2)} c = b, b *_{(2,1,3)} a = c,$$
$$b *_{(2,3,1)} c = a, c *_{(3,1,2)} a = b, c *_{(3,2,1)} b = a.$$

Then we say that $\left(Q, *_{(i,j,k)}\right)$ are conjugate with $(Q, *)$.

Recall that all such quasigroups $\left(Q, *_{(i,j,k)}\right)$ are also conjugate each other, and thus this is an equivalence relation on $\mathcal{L}_n$.

Theorem 4. *Let $Q = (Q, *)$ be a quasigroup. If quasigroups $Q_1 = \left(Q, *_{(i,j,k)}\right)$, $Q_2 = \left(Q, *_{(i,k,j)}\right)$ are conjugate with Q, then $L_{Q_1} = \{q^{-1} | q \in L_{Q_2}\}$.*

Let $L_{Q_1} = \{g_1, \cdots, g_n\}, L_{Q_2} = \{h_1, \cdots, h_n\}$. Next we simplify notation of $L_{Q_1} g_i^{-1}$ as $L^i_{Q_1}$ and $L_{Q_2} h_i^{-1} = L^i_{Q_2}$, respectively.

Corollary 5. *Let $Q = (Q, *)$ be a quasigroup of order n. For conjugate quasigroups $Q_1 = \big(Q, *_{(i,j,k)}\big)$, $Q_2 = \big(Q, *_{(i,k,j)}\big)$ with Q there exists $P \in S_n$ such that $L^1_{Q_1}, L^{P(1)}_{Q_2}$ contain the same number of permutations with the same cyclic structure, i.e., are of the same type.*

Finally, using the necessary condition in the Algorithm 1 we get our new algorithm for finding isotopisms of two quasigroups.

Algorithm 2. Input: Quasigroups G, H of order n. Output: The set of their isotopisms $Is(G, H)$.

(1) Find conjugate quasigroups
$G_1 = G = G_{(1,2,3)}, G_2 = G_{(2,1,3)}, G_3 = G_{(3,1,2)}$ and $H_1 = H = H_{(1,2,3)}$, $H_2 = H_{(2,1,3)}, H_3 = H_{(3,1,2)}$.

(2) Find permutations $P_1, P_2, P_3 \in S_n$ such that the sets $L^i_{G_j}$ a $L^{P_j(i)}_{H_j}$ are of the same type for all $i, j \in I_n \times I_3$. If such a triplet does not exist, then Stop algorithm and Return $Is(G, H) = \emptyset$.

(3) For all $j \in I_n$, such that L^1_G, L^j_H are of the same type do:
   (a) By Algorithm 1 find sets $C_n(L^1_G, L^j_H)$.
   (b) Compute for all $p \in C_n(L^1_G, L^j_H)$ two permutations $\varphi = h_j^{-1} p g_1$, $\psi = p$. Find θ and Store in $Is(G, H)$ isotopism (θ, φ, ψ).

(4) Return $Is(G, H)$.

This algorithm has the same worst case complexity $\mathcal{O}(n^{\log_2 n})$ as the Miller's algorithm [16]. Our contribution is in the step with necessary condition step (2) which can distinguish non isotopic quasigroups of order $n \leq 8$ in majority cases.

Probability for non isotopic quasigroups to pass step (2) is for orders $6, 7, 8$ lower than $4.3 * 10^{-3}, 3.15 * 10^{-5}, 3.0 * 10^{-10}$, respectively. If this was the case for higher orders, too, then we would have a very strong probabilistic toolkit to verify isotopy of two Latin squares. Its complexity is $\mathcal{O}(n^3)$ only, and thus for quasigroups of order $n > 9$ would be faster than Miller's algorithm.

Based on our algorithm we can sharpen estimation of S a d e [20] for the cardinality of autotopisms $AUT(Q)$ of a quasigroup Q, which is $n \times n!$.

Theorem 6. *Let M be the set of permutations from S_n, where $n \geq 5$ consisting from cycles of the length 2 and 3 only. Then cardinality of their stabilizer in the action of conjugacy $|St_{S_n}(p)|$, except of $n = 9$, is maximal if it possesses maximum of 2-cycles. For $n = 9$ the stabilizer is maximal if the permutation consists of 3-cycles only.*

Corollary 7. *Let Q be a quasigroup of order $n > 5$. If n is even, then*

$$|AUT(Q)| \leq n(n-1)(n/2)!2^{n/2}.$$

For n odd, except of $n = 9$,

$$|AUT(Q)| \leq n(n-1)3((n-3)/2)!2^{(n-3)/2}.$$

For $n = 9$ we have

$$|Aut(Q)| \leq 9(9-1)3!3^3 = 11664.$$

4. Zero knowledge protocol and isotopy

As we mentioned above due to theorem Goldreich-Micali-Wigderson any hard problem can be used in zero–knowledge protocols. Probably, led by this idea, authors of [3] published their zero–knowledge protocol. In the protocol we have two participants u_i, u_j, and public as well as secret parameters distributed as follows:

- Public parameters of u_i: isotopic Latin squares L, L'.
- Secret parameters of u_i: $I = (\theta_i, \varphi_i, \psi_i)$.
- Aim of u_i: to prove u_j knowledge of I without revealing I itself.

The Protocol is based on public keys L, L' and a secret key $I = (\theta_i, \varphi_i, \psi_i)$, respectively. Realization of the protocol supposes the following steps:

(1) u_i randomly permutes L to produce another Latin square, say H.

(2) u_i sends H to u_j.

(3) u_j asks u_i either to:
   - prove that H, L are isotopic;
   - prove that H, L' are isotopic.

(4) u_i complies. He either
   - proves that H, L are isotopic;
   - proves that H, L' are isotopic.

(5) u_i, u_j repeat n-times steps (1)–(4) if necessary (i.e., a new H is generated).

In view of our new Algorithm 2, or Miller's algorithm we performed an experiment. To do this we used an equivalent definition of a quasigroup $(Q, *)$:

Definition 5. Let $(Q, *)$ be a set with binary operation satisfying the following conditions: for any $a, b \in Q$ there is a unique solution of the following equations

$$a * b = x_1, \tag{3}$$

$$a * x_2 = b, \tag{4}$$

$$x_3 * a = b. \tag{5}$$

Then $(Q, *)$ is a quasigroup.

This definition leads to a construction of the set of generators of Q. Informally, we can start with two elements of Q, and construct more and more elements x_i by the following iteration: $\{a, b\} \to \{x_1, x_2, x_3\} \cup \{a, b\} \to \ldots$ This leads to the definition.

Definition 6. Let f_1, f_2, f_3 be functions defined as $f_i : Q \times Q \to Q$ such that $f_1(a, b) = x_1$, $f_2(a, b) = x_2$, $f_3(a, b) = x_3$, in accordance with Definition 5 above. Let $G \subsetneq Q$ such that

$$Q = f_1(G, G) \cup f_2(G, G) \cup f_3(G, G) \cup G.$$

Then we call G the set of generators for Q.

Next we recall informally a variation of Miller's Algorithm (or our new algorithm) with generators.

(1) Find generators $\{a_1, \ldots, a_m\}$ for Q_1, $m \leq \log_2 n$.
(2) For each subset $\{b_1, \ldots, b_m\} \subset Q_2$ verify if $\phi(a_j) = b_j$ is an isomorphism $Q_1 \to Q_2$.
(3) If YES, then they are isotopic, otherwise NOT.

Clearly, the complexity of this variation heavily depends on the size of the set of generators of Q_1. Miller [16] proved that $|G| \leq \log_2 n$, and this bound appears in the complexity of his algorithm. Thus a natural question arise: What is the number m_i of non-isotopic quasigroups with $|G| = i$? From our exhaustive computer search for $2 \leq n \leq 8$ we get the results aggregated in the Table 1.

Table 1. Results of the computer search for non isotopic quasigroups with respect of the size of generators m_i.

n	m_1	m_2	m_3	$m = \sum m_i$
2	1	0	0	1
3	1	0	0	1
4	1	1	0	2
5	2	0	0	2
6	21	1	0	22
7	561	3	0	564
8	1676060	206	1	1676267

From this table one can see that:

- There is a limited number of quasigroups with $|G| > 1$;
- For majority of quasigroups complexity of the algorithm is $\mathcal{O}\big(n^{|G|+o(1)}\big) \approx \mathcal{O}\big(n^{1+o(1)}\big)$.

Thus the above mentioned protocol for majority of quasigroups probably faces serious problems.

5. Conclusions

We presented a new algorithm for solving isotopy problem which is of the same worst case complexity as Miller's algorithm but in many practical situations it is much more faster. We also discuss the zero–knowledge protocol introduced in [3]. There are some practical considerations for this protocol in our results.

- The size of the quasigroup Q cannot be too large since $(\theta_i, \varphi_i, \psi_i)$ has to be sent during the protocol;
- Thus our aim is to find a relatively small Q with a large set of generators G. For really "small" n we can use a computer search. But then the protocol is weak;
- Random search is very impractical (see Table 1). For special quasigroups, like $Q = Z_2^n$ we have fast algorithms. The same is true for any group.

Thus we conclude that an applicability of the protocol is really in question.

REFERENCES

[1] COLBOURN, C. J.—DINITZ, J. H., (eds.): *The CRC Handbook of Combinatorial Designs*. in: CRC Press Ser. Discrete Math. Appl., CRC Press, Boca Raton, FL, 1996.

[2] DÉNES, J.—KEEDWELL, A. D.: *Latin Squares and Their Applications*. Academic Press, New York, NY, 1974.

[3] DÉNES, J.—DÉNES, T.: *Non-associative algebraic systems in cryptology. Protection against "meet in the middle" attack*, Quasigroups Related Systems **8** (2001), 7–14.

[4] FERGUSON, M.: *The Determinants of Latin Squares of Order 7*. Honours Undergraduate Thesis, Iowa State University, 1989.

[5] FORD, W.—JOHNSON, K. W.: *Determinants of latin squares of order 8*, Experiment. Math. **5** (1996), 317–325.

[6] GLIGOROSKI, D.—MARKOVSKI, S.—KOCAREV, L.—GUSEV, M.: *eSTREAM, ECRYPT Stream Cipher Project, Report 2005/007, 2005*, `http://www.ecrypt.eu.org/stream`.

[7] GLIGOROSKI, D.—ODEGARD, R. S.—MIHOVA, M.—KNAPSKOG, S. J.—KOCAREV, L.— DRÁPAL, A.: *Cryptographic Hash Function EDON-R*, `http://people.item.ntnu.no/đanilog/Hash/Edon-R/Supporting_Documentation/ /EdonRDocumentation.pdf`.

[8] GOLDREICH, O.—MICALI, S.—WIGDERSON, A.: *Proofs that yield nothing but their validity or all languages in NP have zero–knowledge proofs systems*, J. Assoc. Comput. Mach. **38** (1991), 691–729.

[9] GROŠEK, O.—SATKO, L.—NEMOGA, K.: *Ideal difference tables from an algebraic point of view*, in: Cryptology and Information Security, Proc. of VI RECSI, Teneriffe, Spain, 2000, pp. 51–58; Ammendment to Criptología y Seguridad de la Información (P. Caballero-Gil, C. Hernández-Goya), RA-MA, Madrid, 2000, pp. 453–454.

[10] GROŠEK, O.—SATKO, L.—NEMOGA, K.: *Generalized perfectly nonlinear functions*, Tatra Mt. Math. Publ. **20** (2000), 121-131.

[11] GROŠEK, O.—HORÁK, P.—TRUNG VAN TRAN: *On non-polynomial Latin squares*, Des. Codes Cryptogr. **32**, (2004), 217–226.

[12] KAPLANSKY, I.: *Abraham Adrian Albert. A biographical memoir*, `http://citeseerx.ist.psu.edu/`

[13] KOŚCIELNY, C.—MULLEN, G. L.: *A quasigroup-based public-key cryptosystem*, Int. J. Appl. Math. Comp. Sci. **9** (1999), 955–963.

[14] LAI, X.—MASSEY, J. L.: *A proposal for a new block encryption standard*, in: Advances in Cryptology—EUROCRYPT '90, Aarhaus, Denmark, 1990 (I. B. Damgård, ed.), Lecture Notes in Comput. Sci., Vol. 473, Springer-Verlag, Berlin, 1991, pp. 389–404.

[15] MARKOVSKI, S.—GLIGOROSKI, D.—STOJCEVSKA, B.: *Secure two way on-line communication by using quasigroups enciphering with almost public key*, Novi Sad J. Math. **30** (2000), 43–49.

[16] MILLER, G. L.: *On the $n \log n$ isomorphism technique*, in: Proc. 10th Annual ACM Symposium on Theory of Computing—STOC '78, San Diego, California, 1978, ACM, New York, NY, 1978, pp. 51–58.

[17] Miller's private communication with Tarjan.

[18] ROBINSON, D. J. S.: *An Introduction to Abstract Algebra*. in: de Gruyter Textbook, Berlin, 2003.

[19] SHCHERBACOV, V.: *On some known possible applications of quasigroups in cryptology*, `http://www.karlin.mff.cuni.cz/~drapal/krypto.pdf`.

[20] SADE, A.: *Autotopies des quasigroupes et des systmes associatifs*, Arch. Math. (Brno) **4** (1968), 1–23.

[21] SÝS, M.: *Latin Squares in Cryptography*. Honours PhD Thesis, Slovak Technical University, Bratislava, 2009.

[22] VOJVODA, M.—SÝS, M.—JÓKAY, M.: *A Note on Algebraic Properties of Quasigroups in Edon80*, in: The State of the Art of Stream Ciphers—SASC '07, ECRYPT Network of Excelence in Cryptology, Bochum, Germany, 2007, pp. 307–315.

Received April 30, 2010

Department of Applied Informatics
Information Technology
Slovak University of Technology
SK–812-19 Bratislava
SLOVAKIA
E-mail: otokar.grosek@stuba.sk
marek.sys@stuba.sk