ON SOME KNOWN POSSIBLE APPLICATIONS OF QUASIGROUPS IN CRYPTOLOGY

Victor Shcherbacov

Abstract. It is surveyed known (published) possible application of binary and n-ary quasigroups in cryptology.

Mathematics Subject Classification: 20N05, 94A60.

Key words and phrases: Cryptology, cryptography, cipher, key, quasigroup, n-ary quasigroup.

Introduction

Almost all results obtained in branch of application of quasigroups in cryptology and coding theory to the end of eighties years of the XX-th century are described in [20, 21]. In the present survey the main attention is devoted more late articles in this direction.

Basic facts on quasigroup theory it is possible to find in [5, 6, 7, 64]. Information on basic fact in cryptology it is possible to find in many books see, for example, [3, 11, 60, 54].

Cryptology is a science that consists form two parts: cryptography and cryptanalysis. Cryptography is a science on methods of transformation (ciphering) of information with the purpose of a protection this information from an unlawful user. Cryptanalysis is a science on methods and ways of breaking down of ciphers ([32]).

In some sense cryptography is a "defense", i.e. this is a science on construction of new ciphers, but cryptanalysis is an "attack", i.e. this is a science and some kind "art", a set of methods on breaking of ciphers. This situation is similar to situation with intelligence and contr-intelligence.

These two objects (cryptography and cryptanalysis) are very closed and there does not exist a good cryptographer that do not know methods of cryptanalysis.

It is clear, that cryptology depends from a level of development of a society and a level of development of technology.

We recall, a cipher is a way (a method, an algorithm) of a transformation of information with purpose of its defense. A key is some hidden part (a little bit, usually) or parameter of a cipher.

Steganography is a set of means and methods of hiddenness of a fact of sending (or passing) of information, for example, a communication or a letter. Now there exist methods of hiddenness of a fact of sending information by usual post, by e-mail post and so on.

© VICTOR SHCHERBACOV, 2003

Acknowledgment. The author wishes to thank Czech Grant Agency for the award of grant which provided the author to visit the Czech Republic and to work at Charles University.

In this survey Coding Theory (Code Theory) will be meant a science on defense of information from accidental errors by transformation and sending (passing) this information.

By sending of important and confidential information, as it seems us, there exists a sense to use methods of Code Theory, Cryptology, and Steganography all together.

In cryptology often one uses the following Kerkhoff's (1835-1903) rule: an opponent (an unlawful user) knows all ciphering procedure (sometimes a part of plaintext or ciphertext) with exception of a key.

Many authors of books devoted cryptology divide this science (sometimes and do not taking for attention this fact) on two parts: before article of Diffie and Hellman ([30]) (so-called cryptology with non-public (symmetric) key) and past this work (a cryptology with public or non-symmetric key). Especially fast development of the second part of cryptology is connected with very fast development of Personal Computers and Nets of Personal Computers, other electronics technical devices in the end of XX-th century. Many new mathematical, cryptographical problems are appeared in this direction and some of them have not solved. Solving of these problems have big importance for practice.

Almost all known construction of error detecting and error correcting codes, cryptographic algorithms and enciphering systems have made use of associative algebraic structures such as groups and fields, see, for example, [55]. There exists a possibility to use such non-associative structures as quasigroups and neo-fields in almost all branches of coding theory, and especially in cryptology.

Codes and ciphers based on non-associative systems show better possibilities than known codes and ciphers based on associative systems [22, 51].

There is a sense to notice that in the last years the quantum code theory and quantum cryptology ([68, 39, 71]) have been developed intensively.

Efficacy of applications of quasigroups in cryptology is based on the fact that quasigroups are "generalized permutations" of some kind and the number of quasigroups of order n is larger than $n! \cdot (n-1)! \cdot ... \cdot 2! \cdot 1!$ ([20]).

It is worth noting that several of the early professional cryptographers, in particular, A.A. Albert, A. Drisko, J.B. Rosser, E. Schönhardt, C.I. Mendeson, R. Schaufler, M.M. Gluhov were connected with the development of Quasigroup Theory. The main known "applicants" of quasigroups in cryptology were and are J.Denes and A.D. Keedwell [20, 21, 22].

Of course, one of the most effective cipher methods is to use unknown, non-standard or very rare language. Probably the best enciphering method was and is to have a good agent (a good spy).

Some problems of cryptology for computer systems

Recall some problems of protection information in computer systems ([31]). At construction of protected computer systems (PCS) the role of cryptographic methods for the decision of various problems of information safety is difficult for overestimating. Cryptographic methods now are base for maintenance reliable authentication schemes by an information exchange, for protection of the information in transport subsystem, in PCS, for acknowledgement (confirmation) of integrity of objects of PCS, etc.

Cryptographic protection information concern to means equipment rooms, hardware, hardware-software and the software realizing cryptographic algorithms of transformation of the information with the purpose:

protection of the information at its processing, storage and transfer in transport environment of Computer systems;

maintenance of reliability and integrity of the information (including with use of algorithms of electronic digital signature) at its processing, storage and transfer in transport environment of Computer systems;

manufactures of the information used for identification and authentication of subjects, users and devices;

manufactures of the information used for protection of authenticating elements of PCS at their development (manufacture), snore, processing and transfer.

It is supposed, that Means of Computer Protection of Information (MCPI) are used also to some computer system (in a number of sources such that information - telecommunication system or communication networks), together with mechanisms of realization and warranting of some politics of safety.

Historical digression to a problem of synthesis of means of cryptographic protection of information on the basis of computer systems allows to speak about that, complexity a safety with help of MCPI grows with growth of complexity of a communication facility and information technologies.

The basic difficulties are connected to the following factors:

means of realization of cryptographic algorithm in computer system represents equal in rights with other a resource (is the program and uses the data of computer system);

key information of MCPI is the data of computer system with an opportunity of access on the part of other programs and with passage at processing also through a number (a line) external in relation to MCPI program modules;

functioning MCPI occurs not independently, and is carried out under the control of operational system and various programs - intermediaries who at desire can deform any way entered and deduced (removed) MCPI the information;

the program environment in which works MCPI is arranged hierarchically, i.e. for performance of typical functions all programs use the same fragments of a code and the data;

work MCPI is connected to occurrence of erroneous situations in the hardware and program environment of computer system.

The described complexities are aggravated also with that many countries now are not engaged in development of own hardware decisions in the field of modern computer facilities (excluding a special chips) and program decisions in the field of operational systems and the basic functional appendices.

In this connection for good safety in modern information-telecommunication systems (ITS) based on advanced information technologies, it is necessary to solve information effectively a circle of complex (difficult) scientific and technical problems, namely:

to provide optimum, formally checked realization of cryptographic algorithms (further - cryptographic algorithms) within the framework of maintained in ITS program and hardware platforms;

to provide at designing MCPI of a measure of maintenance of fault tolerance, protection against failures and distortions of an equipment room components;

to provide security MCPI and its resources (the key information and other) from the non-authorized access on the part of other programs;

to guarantee quality of management MCPI on the part of operational system of the programs - intermediaries developed by foreign firms, including in conditions of erroneous and deliberate actions of users.

It is necessary to notice, that component of scientific and technical activity no to all specified directions development of requirements, classifications, techniques, working and educational technical materials, recommendations of the instructions for use concerning development, manufacture, operation MCPI is important.

It is necessary to note also, that realization MCPI in complex universal operational environments such as Windows or Unix demands carrying out of significant volumes of basic researches for definition of points of embedding MCPI in operational system and maintenance of a correctness of their work.

Application of quasigroups in "classical" cryptology

There exist two main elementary methods by ciphering of information.

(i). Symbols in a plaintext (or in its piece (its bit)) are permuted by some law. The first known cipher of such kind is cipher "Scital" (Sparta, 2500 years ago).

(ii). All symbols in a fixed alphabet are changed by a law on other letters of this alphabet. One of the first ciphers of such kind was Cezar's cipher ($x \to x + 3$ for any letter of Latin alphabet, for example $a \to d, b \to d$ and so on).

In many contemporary ciphers (DES, Russian GOST, Blowfish ([60, 31])) are used methods (i) and (ii) with some modifications.

Trithemius cipher makes use of 26×26 square array containing the 26 letters of alphabet (assuming that the language is English) arranged in a Latin square. Different rows of this square array are used for enciphering the various letters of the plaintext in a manner prescribed by the keyword or key-phrase ([3, 44]). Since a Latin square is the multiplication table of a quasigroup, this may be regarded as the earliest use of a non-associative algebraic structure in cryptology. There exists a possibility to develop this direction using quasigroup approach, in particular, using orthogonal systems of binary or n-ary quasigroups.

R. Schaufler in his Ph.D. dissertation ([66]) of 1948 discussed the minimum amount of plaintext and corresponding ciphertext which would be required to break the Vigenere cipher (i.e. Trithemius cipher). That is, he considered the minimum member of entries of particular Latin square which would determine the square completely.

Recently this problem has re-arisen as the problem of determining so-called critical sets in Latin squares, see [47, 16, 17, 18, 19], and, possibly, future A.D. Keedwell's survey on BCC'03. See, also, articles, devoted Latin trades, for example, [4].

More recent enciphering systems which may be regarded as extension of Vigenere's idea are mechanical machines such as Jefferson's wheel and the M-209 Converter (used by U.S.Army until the early 1950's) and the electronically produced stream ciphers of the present day ([50, 60]). We recall, a cipher is called a stream cipher, if by ciphering of a block (a letter) B_i of a plaintext is used the previous ciphered block C_{i-1}.

In [50] (see also [51, 52]) C.Koscielny has shown how quasigroups/neofields-based stream ciphers may be produced which are both more efficient and more secure than those based on groups/fields.

Eliska Ochodkova and Vaclav Snasel ([63]) proposed to use quasigroups for secure encoding of file system.

It is well known that a quasigroup $(Q, \cdot)$ and its (23)-parastroph $(Q, \star)$ $(x \cdot y = z \Leftrightarrow x \star z = y)$ for all $x, y, z \in Q$ satisfies the following identities $x \star (x \cdot y) = y,\ x \cdot (x \star y) = y$. The authors propose to use this property of the quasigroups to construct a stream cipher.

Definition. Let A be a non-empty alphabet, k be a natural number, $u_i, v_i \in A$, $i \in \{1, ..., k\}$. A fixed element l $(l \in A)$ is called leader. Then $f(u_1 u_2 ... u_k) = v_1 v_2 ... v_k \Leftrightarrow v_1 = l \cdot u_1, v_{i+1} = v_i \cdot u_{i+1}, i = 1, 2, ..., k-1$ is an ciphering algorithm.

An enciphering algorithm is constructed in the following way: $f^{\star}(v_1 v_2 ... v_k) = u_1 u_2 ... v_k \Leftrightarrow u_1 = l \star v_1, u_{i+1} = v_i \star v_{i+1}, i = 1, 2, ..., k-1$.

Authors say that this cipher is resist to the brute force attack and to the statistical attack.

Example.

Table 1. Let quasigroups $(A, \cdot)$ and $(A, \star)$ are defined by following Cayley tables

$\cdot$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$\star$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

Let $l = a$ and $u = b\,b\,c\,a\,a\,c\,b\,a$. Then the cipher text is $v = c\,b\,b\,c\,a\,a\,c\,a$. Applying of decoding function on v we get $b\,b\,c\,a\,a\,c\,b\,a = u$.

Remark. There exists a sense to study possibilities of use an n-ary quasigroup and its parastrophes in Ochodkova-Snasel construction.

In [56] the authors introduce a stream cipher with almost public key, based on quasigroups for defining suitable encryption and decryption. They consider the security of this method. It is shown that the key (quasigroups) can be public and still having sufficient security. A software implementation is also given.

In [53] a public-key cryptosystem, using generalized quasigroup-based streamciphers is presented. It is shown that such a cryptosystem allows one to transmit securely both a cryptogram and a secret portion of the enciphering key using the same insecure channel. The system is illustrated by means of a simple, but nontrivial, example.

During the second World War R.Shauffler while working for the German Cryptography service, developed a method of error detection based on the use of generalized identities (as they were later called by V.D. Belousov) in which the check digits are calculated by means of an associative system of quasigroups (see also [14]). He pointed out that the resulting message would be more difficult to decode by unauthorized receiver than is the case when a single associative operation is used for calculation ([67]).

Therefore it is possible to assume that information on systems of quasigroups with generalized identities (see, for example, works of Yu. Movsisyan ([61]) may be applied in cryptography of the present day.

Definition. A bijective mapping $\varphi : g \rightarrowtail \varphi(g)$ of a finite group $(G, \cdot)$ onto itself is called an orthomorphism if the mapping $\theta : g \rightarrowtail \theta(g)$ where $\theta(g) = g^{-1}\varphi(g)$ is again a bijective mapping of G onto itself. The orthomorphism is said to be in canonical form if $\varphi(1) = 1$ where 1 is the identity element of $(G, \cdot)$.

A direct application of group orthomorphisms to cryptography is described in [58, 59].

"Neo-classic" cryptology and quasigroups

In [22] some applications of CI-quasigroups in cryptology with non-symmetric key are described.

Definition. Suppose that there exists a permutation J of the elements of a quasigroup $(Q, \circ)$ such that, for all $x, y \in Q$ $J^r(x \circ y) \circ J^s x = J^t y$, where r, s, t are integers. Then $(Q, \circ)$ is called an (r, s, t)-inverse quasigroup ([48]).

In the special case when $r = t = 0$, $s = 1$, we have a definition of CI-quasigroup.

Example ([22, 46]). A CI-quasigroup can be used to provide a one-time pad for key exchange (without the intervention of a key distributing centre).

The sender S selects arbitrary (using a physical random number generator (see [51] on random number generator based on quasigroups) an element $c^{(u)}$ of the CI-quasigroup $(Q, \circ)$ and sends both $c^{(u)}$ and enciphered key (message) $c^{(u)} \circ m$. The receiver R uses this knowledge of the algorithm for obtaining $Jc^{(u)} = c^{(u+1)}$ from $c^{(u)}$ and hence he computes $(c^{(u)} \circ m) \circ c^{(u+1)} = m$.

Remark. In previous example Kerkhof's rule is not fulfilled, so, this example need to be improved. Maybe there exists a sense to use in this example, as and in the next example rst-inverse quasigroups.

Example ([22]). A CI-quasigroup with a long inverse cycle $(c\,c'\,c'' \dots c^{t-1})$ of length t and suppose that all the users U_i $(i = 1, 2, \dots)$ are provided with apparatus (for example, a chip card) which will compute $a \circ b$ for any given $a, b \in Q$. We assume that only the key distributing centre has a knowledge of the long inverse cycle which serves as a look-up table for keys.

Each user U_i has a public key $u_i \in Q$ and a private key Ju_i, both supplied in advance by the key distributing centre. User U_s wishes to send a message m to user U_t. He uses U_t's public key u_t to compute $u_t \circ m$ and sends that to U_t. U_t computes $(u_t \circ m) \circ Ju_t = m$.

Remark. It is not very difficult to understand that opponent which knows the permutation J may decipher a message encrypted by this method.

Secret sharing systems

Definition ([54]). A critical set C in a Latin square L of order n is a set $C = \{(i; j; k) \mid i, j, k \in \{1, 2, \dots, n\}\}$ with the following two properties:

(1) L is the only Latin square of order n which has symbols k in cell (i, j) for each $(i; j; k) \in C$;

(2) no proper subset of C has property (1).

A critical set is called minimal if it is a critical set of smallest possible cardinality for L. In other words a critical set is a partial Latin square which is uniquely completable to a Latin square of order n.

If the scheme has k participants, a (t, k)-secret sharing scheme is a system where k pieces of information called shares or shadows of a secret key K are distributed so that each participant has a share such that

(1) the key K can be reconstructed from knowledge of any t or more shares;

(2) the key K cannot be reconstructed from knowledge of fewer than t shares.

Such systems were first studied in 1979. Simmons ([69]) surveyed various secret sharing schemes. Secret sharing schemes based on critical sets in Latin squares are studied in [12]. We note, critical sets of Latin squares give rise possibilities to construct secret-sharing systems.

Critical sets of Latin squares were studied in sufficiently big number of articles. We survey results from some of these articles. The paper ([30]) gives constructive proofs that critical sets exist for all sizes between $[n^2/4]$ and $[(n^2 - n)/2]$, with the exception of size $n^2/4 + 1$ for n even.

In the paper [16] presents a solution to the interesting combinatorial problem of finding a minimal number of elements in a given Latin square of odd order n by which one may restore the initial form of this square. In particular, it is proved that in every cyclic Latin square of odd order n the minimal number of elements equals $n(n - 1)/2$.

The paper [17] contains lists of (a) theorems on the possible sizes of critical sets in Latin squares of order less than 11, (b) publications, where these theorems are proved, (c) concrete examples of such type of critical sets. In [18] an algorithm for writing any Latin interchange as a sum of intercalates is corrected.

Remark. See also Introduction for other application of critical sets of Latin squares in cryptology.

Some secret-sharing systems are pointed in [21]. One of such systems is the Reed-Solomon code over a Galois field $GF[q]$ with generating matrix $C(a_{ij})$ of size $k \times (q - 1)$, $k \leq q - 1$. The determinant formed by any k columns of G is a non-zero element of $GF[q]$. The Hamming distance d of this code is maximal $(d = q - k)$ and any k from $q - 1$ keys unlock the secret.

In [8] an approach to some Reed-Solomon codes as a some kind of orthogonal systems of n-ary operations is developed.

There exist generalizations of notion of orthogonality in some directions. We recall that in [9, 21] notion of partial orthogonality for binary quasigroups is studied. On application of this notion in code theory see [20]. Notion of partial orthogonality has good perspectives in cryptology (private communication from Russian mathematicians).

Cryptosystems based on power sets of Latin squares and on row-Latin squares

A Latin square is an arrangement of m symbols $x_1, x_2, \dots, x_m$ into m rows and m columns such that no row and no column contains any of the symbols $x_1, x_2, \dots, x_m$ twice. It is well known that Cayley table of any finite quasigroup is a Latin square ([20]).

Two Latin squares are called orthogonal if when one is superimposed upon the other every ordered pair of symbols $x_1, x_2, \dots, x_m$ occurs once in the resulting square.

Each row and column of a Latin square L of order m can be thought of as a permutation of the elements of an m-set. The product of two Latin squares L_1 and L_2 of order m is an $m \times m$ matrix whose ith row is the composition of the permutations comprising the ith rows of L_1 and L_2. Pick the smallest positive m such that $L^{m+1} = L$.

In general product of two Latin squares is row Latin square since in row-Latin square only rows are permutations of the set $x_1, x_2, \dots, x_m$. If $L, L^2, \dots, L^{m-1}$ are all Latin squares, then they form a set called a Latin power set. D. A. Norton ([62]) has shown that the Latin squares in a Latin power set are mutually orthogonal.

Power sets of Latin squares were studied in [26], [10].

The authors of article [26] conjecture that if $n \neq 2$ or 6 then there exists a Latin power set consisting of at least two Latin squares of order n. This would provide another disproof of the Euler conjecture that a pair of orthogonal Latin squares fails to exist for orders $n \equiv 2 \pmod 4$. The authors use resolvable Mendelsohn triple systems to establish their conjecture if $n \geq 7$ and $n \equiv 0, 1 (\text{mod } 3)$. The authors also discuss some related conjectures.

A possible application in cryptology of Latin power sets is proposed in [25].

In [29] an encrypting device is described, based on row-Latin squares with maximal period equal to the Mangoldt function.

In our opinion big perspectives has an application of row-Latin squares in various branches of contemporary cryptology ("neo-cryptology"). In [54] it is proposed to use row-Latin squares to generate an open key, a conventional system for transmission of a message that is the form of a Latin square, row-Latin square analogue of the RSA system and on row-Latin squares based procedure of digital signature.

Example.

Let

$$L = \begin{matrix} 2 & 3 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 4 & 3 & 1 & 2 \end{matrix}.$$

Then

$$L^7 = \begin{matrix} 4 & 1 & 2 & 3 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 3 & 4 & 2 & 1 \end{matrix},$$

$$L^3 = \begin{matrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{matrix}.$$

Then

$$L^{21} = \begin{matrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{matrix}$$

is a common key for a user A with the key L^3 and a user B with key L^7.

NLPN sequences over GF[q]

Non-binary pseudo-random sequences over GF[q] of length $q^m - 1$ called PN sequences have been known for a long time ([41]). PN sequences over a finite field GF[q] are unsuitable directly for cryptology because of their strong linear structure ([51]). Usually PN sequences are defined over a finite field and often it is used an irreducible polynomial for their generation.

In article [51] definition of PN sequence was generalized with the purpose to use this sequences in cryptology.

We notice, in some sense ciphering is making a "pseudo-random sequence" from a plaintext, and cryptanalysis is a science how to reduce a check of all possible variants (cases) by deciphering of some ciphertext.

These new sequences were called NLPN-sequences (non-linear pseudo-noise sequences). C.Koscielny proposed the following method for construction of NLPN-sequences. Let $\overrightarrow{a}$ be a PN sequence of length $q^m - 1$ over GF[q], $q > 2$. Let $\overrightarrow{a}^i$ be its cyclic shift i places to the right. Let $Q = (SQ, \cdot)$ be a quasigroup of order q defined on the set of elements of the field GF[q]. Then $\overrightarrow{b} = \overrightarrow{a} \cdot \overrightarrow{a}^i$, $\overrightarrow{c} = \overrightarrow{a}^i \cdot \overrightarrow{a}$, where $b_j = a_j \cdot a^i_j$, $c_j = a^i_j \cdot a_j$ for any suitable value of index j ($j \in \{1, 2, \dots, q^m - 1\}$) are called NLPN sequences.

NLPN sequences have much more randomness than PN sequences. As notice C.Koscielny the method of construction of NLPN sequences is especially convenient for fast software encryption. It is proposed to use NLPN sequences by generation of keys. See also [49].

Quasigroups and authentication of a message and some other problems

By authentication of message we mean that it is made possible for a receiver of a message to verify that the message has not been modified in transit, so that it is not possible for an interceptor to substitute a false message for a legitimate one.

By identification of a message we mean that it is made possible for the receiver of a message to ascertain its origin, so that it is not possible for an intruder to masquerade as someone else.

By non-repudiation we mean that a sender should not be able later to deny falsely that he had sent a message.

In [22] some quasigroup approaches to problems of identification of a message, problem of non-repudiation of a message, production of dynamic password and to digital fingerprinting are discussed. See also [13].

In [23] authors suggested a new authentication scheme based on quasigroups (Latin squares). See also [21, 22, 15]

In [65] several cryptosystems based on quasigroups upon various combinatorial objects such as orthogonal Latin squares and frequency squares, block designs, and room squares are considered.

Let $2 \leq t < k < v$. A generalized $S(t, k, v)$ Steiner system is a finite block design $(T, \mathcal{B})$ such that (1) $|T| = v$; (2) $\mathcal{B} = \mathcal{B}' \cup \mathcal{B}''$, where any $B' \in \mathcal{B}'$, called a maximal block, has k points and $2 \leq |B''| < k$ for any $B'' \in \mathcal{B}''$, called a small block; (3) for any $B'' \in \mathcal{B}''$ there exists a $B' \in \mathcal{B}'$ such that $B'' \subseteq B'$; (4) every subset of T with t elements not belonging to the same $B'' \in \mathcal{B}''$ is contained in exactly one maximal block.

In [57] (see also [40]) an application of generalized $S(t, k, v)$ Steiner systems in cryptology is proposed, namely, it is introduced a new authentication scheme based on the generalized Steiner systems, and the properties of such scheme are studied in the generalized affine planes. The generalized affine planes are investigated, in particular, it is proved that they are generalized $S(2, n, n^2)$ Steiner systems. Some important cases of generalized Steiner systems are the generalized affine planes considered by the authors.

Hamming distance between quasigroups

Very important by construction of quasigroup based cryptosystems is a question: how big distance is between different binary or n-ary quasigroups? Information on Hamming distance between quasigroup operation there is in the articles [33, 34, 35, 36, 37, 38, 70].

We recall, if α and β are two n-ary operations on a finite set Ω, then the Hamming distance of α and β is defined by $\text{dist}(\alpha, \beta) = |\{(u_1, \dots, u_n) \in \Omega^n : \alpha(u_1, \dots, u_n) \neq \beta(u_1, \dots, u_n)\}|$.

The author in [33] discusses Hamming distances of algebraic objects with binary operations. He also explains how the distance set of two quasigroups yields a 2-complex, and points out a connection with dissections of equilateral triangles.

For a fixed group $G(\circ)$, $\delta(G(\circ))$ is defined to be the minimum of all such distances for $G(\star)$ not equal to $G(\circ)$ and $\nu(G(\circ))$ the minimum for $G(\star)$ not isomorphic to $G(\circ)$.

In [36] it is proved that $\delta(G(\circ))$ is $6n - 18$ if n is odd, $6n - 20$ if $G(\circ)$ is dihedral of twice odd order and $6n - 24$ otherwise for any group $G(\circ)$ of order greater than 50. In [70] it is showed that $\delta(G(\circ)) = 6p - 18$ for $n = p$, a prime, and $p > 7$. In the article [35] are listed a number of group orders for which the distance is less than the value suggested by the above theorems.

New results obtained in this direction there are in [38].

On one-way function

A function $F : X \to Y$ is called one-way function, if the following conditions are fulfilled:

- there exists a polynomial algorithm of calculation of $F(x)$ for any $x \in X$;
- there does not exist a polynomial algorithm of inverting of the function F, i.e. there does not exist any polynomial time algorithm for a solving of equation $F(x) = y$ relatively variable x.

It is proved that the problem of the existence of one-way function is equivalent to well known problem of coincidence of classes P and NP.

One of better candidates to be an one-way function is so-called function of discrete logarithms ([54]).

A neofield $(N, +, \cdot)$ of order n consists of a set N of n symbols on which two binary operations $+$ and $\cdot$ are defined such that $(N, +)$ is a loop with identity element 0 say, $(N\backslash\{0\}, \cdot)$ is a group and $\cdot$ distributes from the left and right over $+$ ([22]).

Let $(N, +, \cdot)$ be a finite Galois field or a cyclic ($(N\backslash\{0\}, \cdot)$ is a cyclic group) neofield. Then each non-zero element u of the additive group or loop $(N, +)$ can be represented in the form $u = a^{\nu}$, where a is a generator of the multiplication group $(N\backslash\{0\}, \cdot)$. ν is called the discrete logarithm of u to the base a, or, sometimes, the exponent or index of u.

Given ν and a, it is easy to compute u in a finite field, but, if the order of the finite field is a sufficiently large prime p and also is appropriately chosen it is believed to be difficult to compute ν when u (as a residue modulo p) and a are given.

In [22] discrete logarithms are studied over a cyclic neofield whose addition is a CI-loop.

In [54] the discrete logarithm problem for the group RL_n of all row-Latin squares of order n is defined (p.103) and, on pages 138 and 139, some illustrations of applications to cryptography are given.

Zero knowledge protocol and isotopy of quasigroups

In [27] it is proposed to use isotopy of quasigroups in so-called zero knowledge protocol. Quasigroups $(Q, \circ)$ and $(Q, \cdot)$ are called isotopic if there exist bijections α, β, γ of the set Q such that equality $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$ is true for all $x, y \in Q$.

Jean-Jacques Quisquater and Louis Guillou explain zero-knowledge with a story about a cave. The cave, illustrated in Figure 1. has a secret.

Someone who knows the magic words can open the secret door between C and D. To everyone else, both passages lead to dead ends.

Peggy knows the secret of the cave. She wants to prove her knowledge to Victor, but she doesn't want to reveal the magic words. Here's how she convinces him:

(1) Victor stands at point A.

(2) Peggy walks all the way into the cave, either to point C or point D.

(3) After Peggy has disappeared into the cave, Victor walks to point B.

(4) Victor shouts to Peggy, asking her either to:
    (a) come out of the left passage or
    (b) come out of the right passage.
(5) Peggy complies, using the magic words to open the secret door if she has to.
(6) Peggy and Victor repeat steps (1) through (5) n times.

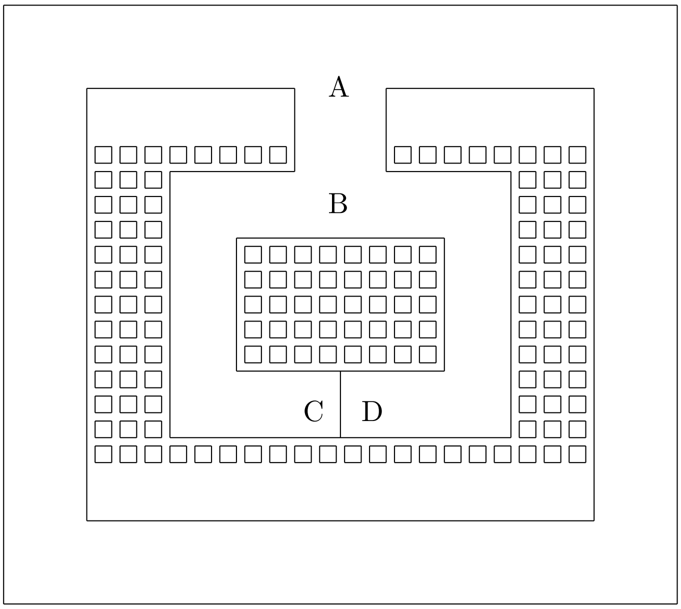

Figure 1.

Assume the users $(u_1, u_2, ..., u_k)$ form a network. u_i has public-key $L_{u_i}, L^{'}_{u_i}$ (denote two isotopic Latin squares at order n and secret-key I_{u_i} (denotes the isotopism of L_{u_i} upon $L^{'}_{u_i}$). u_i wants to prove identity for u_j but he doesn't want to reveal the secret-key (zero-knowledge proof).

1. u_i randomly permutes L_{u_i} to produce another Latin square H.
2. u_i sends H to u_j.
3. u_j asks u_i either to:
   a. prove that H and $L^{'}_{u_i}$ are isotopic,
   b. prove that H and L_{u_i} are isotopic.
4. u_i complies. He either
   a. prove that H and $L^{'}_{u_i}$ are isotopic,
   b. prove that H and L_{u_i} are isotopic.
5. u_i and u_j repeat steps 1. through 4. n times.

Remark. It the last procedure is possible to use even isotopy of n-ary groupoids.

Conclusion remarks

In many cases in cryptography it is possible to change associative systems on non-associative ones and practically in any case this change gives in some sense better results than use of associative systems. Quasigroups in spite of their simplicity, have various applications in cryptology. Many new cryptographical algorithms can be formed on the basis of quasigroups.

References

[1] A.Akritis, *Foundations of Computer Algebra with Applications.* Mir, Moscow, 1994 (in Russian).

[2] M.N. Arshinov, L.E. Sadovskii, *Codes and Mathematics.* Nauka, Moscow, 1983 (in Russian).

[3] H.J. Baker and F.Piper, *Cipher Systems: the Protection of Communications.* Northwood, London, 1982.

[4] R. Bean, D. Donovan, A. Khodkar, A.P. Street, *Steiner trades that give rise to completely decomposable Latin interchanges,* Int. J. Comput. Math. 79, No.12, 2002, 1273-1284.

[5] V.D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, M., Nauka, 1967 (in Russian).

[6] V.D. Belousov, *Elements of the Quasigroup Theory, A Special Course*, Kishinev, 1981 (in Russian).

[7] V.D. Belousov, *n-Ary Quasigroups*, Shtiinta, Kishinev, 1972 (in Russian).

[8] G.B. Belyavskaya, *Secret-sharing systems and orthogonal systems of operatins,* Applied and Industrial Mathematics, Abstracts, Chisinau, Moldova, 1995, p. 2.

[9] G.B. Belyavskaya, *On spectrum of partial admissibility of finite quasigroups (Latin squares)*, Matem. Zametki, 32, No. 6, 1982, 777-788.

[10] G.B. Belyavskaya, *Quasigroup power sets and cyclic S-systems*, Quasigroups and Related Systems, 32, V.9, 2002, 1-17.

[11] A. Beutelspacher, *Cryptology: An introduction to the science of encoding, concealing and hiding*, Wiesbaden: Vieweg, 2002, (in German).

[12] J. Cooper, D. Donovan and J. Seberry, *Secret sharing schemes arising from Latin squares*, Bull. Inst. Combin. Appl., 12, 1994, 33-43.

[13] D. Coppersmith, *Weakness in quaternion signatures*, J. Cryptology, 14, 2001, 77-85.

[14] M. Damm, *Prüfziffersysteme über Qasigruppen*, Diplomarbeit, Philipps-Universität Marburg, 1998.

[15] E. Dawson, D. Donowan, A. Offer, *Ouasigroups, isotopisms and authentification schemes*, Australasian J. of Comb., 13, 1996, 75-88.

[16] D. Donowan, *Critical sets for families of Latin squares*, Util. Math. 53, 1998, 3-16.

[17] D. Donowan, *Critical sets in Latin squares of order less than 11*, J. Comb. Math. Comb. Comput. 29, 1999, 223-240.

[18] D. Donowan, E.S. Mahmoodian, *Correction to a paper on critical sets*, Bull. Inst. Comb. Appl. 37, 2003,44.

[19] D. Donowan, A. Howse, *Towards the spectrum of critical sets*, Australasian J. of Comb., 21, 2000, 107-130.

[20] J. Dénes, A. D. Keedwell, *Latin Squares and their Applications*, Académiai Kiadó, Budapest, 1974.

[21] J. Dénes, A. D. Keedwell, *Latin Squares: New Development in the Theory and Applications*, Annals of Discrete Math., v.46, Norht Holland, Amsterdam, 1990.

[22] J. Dénes, A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, PU.M.A. 12, No.2, 2002, 147-195.

[23] J. Dénes, A. D. Keedwell, *A new authentification scheme based on Latin squres*,Discrete Math., 106/107, 1992, 157-161.

[24] J. Dénes, *Latin Squares and non-binary encoding*, Proc. conf. information theory, CNRS, Paris, 1979, 215-221.

[25] J. Dénes, P.Petroczki, *A digital encrypting communication systems*, Hungarian Patent, No. 201437A, 1990.

[26] J. Dénes, G.L. Mullen and S.J.Suchower, *A note on power sets of latin squares*, J. Combin. Math. Combin. Computing, 16, 1994, 27-31.

[27] J. Dénes, T. Dénes, *Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack*, Quasigroups and Related Systems, 8, 2001, 7 - 14.

[28] T. Dénes, *Cardano and the cryptography. Mathematics of the enciphering grill*, (Hungarian), Középiskolai Matematikai és Fizikai Lapok, 6, 2001, 325-335.

[29] J. Dénes, *On Latin squares and a digital encrypting communication system* , PU.M.A., Pure Math. Appl. 11, No.4, 2000, 559-563.

[30] W. Diffie, M.F. Hellman, *New directions in Cryptography*, IEEE, Transactions of Information Theory, IT-22. 1976, 644-654.

[31] V. Domashev, V. Popov, D. Pravikov, I. Prokof'ev, A. Shcherbakov, *Programming of algorithms of defense of information*, Nolidge, Moscow, 2000, (in Russian).

[32] S.A. Dorichenko, V.V. Yashchenko, *25 sketches on ciphers*, Teis, Moscow, 1994, (in Russian).

[33] A. Drapal, *Hamming distances of groups and quasi-groups*, Discrete Math. 235, No. 1-3, 2001, 189-197.

[34] A. Drapal, *On groups that differ in one of four squares*, Eur. J. Comb. 23, No. 8, 2002, 899-918.

[35] A. Drapal, *On distances of multiplication tables of groups*, Campbell, C. M. (ed.) et al., Groups St. Andrews 1997 in Bath. Selected papers of the international conference, Bath, UK, July 26-August 9, 1997. Vol. 1. Cambridge: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 260, 1999, 248-252.

[36] A. Drapal, *How far apart can the group multiplication tables be?*, Eur. J. Comb. 13, No. 5, 1992, 335-343.

[37] A. Drapal, *Non-isomorphic 2-groups Coincide at Most in Three Quartes of their Multiplication Table*, Eur. J. Comb. 21, 2000, 301-321.

[38] A. Drapal, N. Zhukavets, *On multiplication tables of groups that agree on half of the columns and half of the rows*, Glasgow Math. J., 45, 2003, 293-308.

[39] A. Ekert, *From quantum, code-making to quantum code-breaking,* Huggett, S. A. (ed.) et al., The geometric universe: science, geometry, and the work of Roger Penrose. Proceedings of the symposium on geometric issues in the foundations of science, Oxford, UK, June 1996 in honour of Roger Penrose in his 65th year. Oxford: Oxford University Press, 1998, 195-214.

[40] F. Eugeni, A. Maturo, *A new authentication system based on the generalized affine planes*, J. Inf. Optimization Sci. 13, No.2, 1992,183-193.

[41] S.W. Golomb, *Shift Register Sequences,* San Francisco, Holden Day,1967.

[42] S.W. Golomb, R.E. Peile, H. Taylor, *Nonlinear shift registers that produce all vectors of weight* $\leq t$*,* IEEE Trans. Inf. Theory 38, No.3, 1992, 1181-1183.

[43] D.F. Hsu, *Cyclic neofields and combinatorial designs,* Lectures Notes in Mathematics, 824, Springer, Berlin, 1980.

[44] D. Kahn, *The codebreakers: the story of secret writing,* Wiedenfield and Nicolson, London, 1967.

[45] M.I. Kargapolov and Yu.I. Merzlyakov, *Foundations of Group Theory,* Moscow, Nauka, 1977, (in Russian).

[46] A. D. Keedwell, *Crossed inverse quasigroups with long inverse cycles and applications to cryptography*, Australasian J.of Comb., 20, 1999, 241-250.

[47] A. D. Keedwell, *Critical sets for Latin Squares, graphs and block designs: a survey*, Congressus Numeratium, 113, 1996, 231-245.

[48] A.D. Keedwell and V. Shcherbacov, *Construction and properties of (r,s,t)-inverse quasigroups, I,* Discrete Math., 266, 2003, 275-291.

[49] A. Klapper, *On the existence of secure keystream generators*, J. Cryptology, 14, 2001, 1-15.

[50] C. Koscielny, *A method of constructing quasigroup-based stream ciphers*, Appl. Math. and Comp. Sci. 6, 1996, 109-121.

[51] C. Koscielny, *NLPN Sequences over GF(q)*, Quasigroups and Related Systems, v.4, 1997, 89-102.

[52] C. Koscielny, *Generating quasigroups for cryptographic applications*, Int. J. Appl. Math. Comput. Sci. 12, No.4, 2002, 559-569.

[53] C. Koscielny, G.L. Mullen *A quasigroup-based public-key cryptosystem*, Int. J. Appl. Math. Comput. Sci. 9, No.4, 1999, 955-963.

[54] Charles F. Laywine and Gary L. Mullen, *Discrete Mathematics Using Latin Squares,* New York, John Wiley & Sons, Inc., 1998.

[55] S.S. Magliveras, D.R. Stinson, Tran van Trung, *New approach to designing public key cryptosystems using one-way function and trapdoors in finite groups,* J.Cryptology, 15, 2002, 285-297.

[56] S. Markovski, D. Gligoroski, B. Stojcevska, *Secure two-way on-line communication by using quasigroup enciphering with almost public key,* Novi Sad J. Math. 30, No.2, 2000,43-49.

[57] Antonio Maturo and Mauro Zannetti, *Redei blocking sets with two Redei lines and quasigroups,* J. Discrete Math. Sci. Cryptography 5, No.1, 2002, 51-62.

[58] L. Mittenhal, *Block substitutions using orthomorphic mappings,* Advances in Applied Mathematics, 16, 1995, 59-71.

[59] L. Mittenhal, *A source of cryptographically strong permutations for use in block ciphers,* Proc. IEEE, International Sympos. on Information Theory, 1993, IEEE, New York, 17-22.

[60] N.A. Moldovyan, *Problems and methods of cryptology,* S.-Peterburg, S.-Peterburg University Press, 1998 (in Russian).

[61] Yu. Movsisyan, *Hyperidentities in algebras and varieties,* Russ. Math. Surv. 53, No.1, 1998, 57-108.

[62] D. A. Norton, Pac. J. Math. 2, 1952, 335-341.

[63] E. Ochadkova, V. Snasel, *Using quasigroups for secure encoding of file system*, Abstract of Talk on Conference "Security and Protection of information", Brno, Czech Republic, 9-11.05.2001, 24 pages.

[64] H.O. Pflugfelder, *Quasigroups and loops: Introduction,* Berlin, Heldermann Verlag, 1990.

[65] D.G. Sarvate and J. Seberry, *Encryption methods based on combinatorial designs,* Ars Combinatoria, 21A, 1986, 237-246.

[66] R. Schauffler, *Eine Anwendung zyklischer Permutationen und ihre Theorie*, Ph.D. Thesis, Marburg University, 1948.

[67] R. Schauffler, *Über die Bildung von Codewörter*, Arch. Elektr. Übertragung, 10, 1956, 303-314.

[68] P.W. Shor, *Quantum computing*, Proc. Intern. Congress of Mathematicians, Berlin, v.1, 1998, 467-486.

[69] G.J. Simmons (ed.), *Contemporary Cryptology - The Science of Information Integrity*, IEEE Press, New York, 1992.

[70] P. Vojtechovsky, *Distances of groups of prime order*, Contrib. Gen. Algebra 11, 1999, 225-231.

[71] H. Zbingen, N. Gisin, B. Huttner, A. Muller and W. Tittel, *Practical aspects of quantum cryptographical key distributions*, J. Cryptology, 13, 2000, 207-220.

Victor Shcherbacov
Institute of Mathematics
and Computer Science
Academy of Sciences of Moldova
str. Academiei 5, MD-2028
Chisinau, Moldova
E-mail: scerb@math.md

Received October 8, 2003