Math. Maced.
Vol. 8 (2010)
47-52

AN APPLICATION OF QUASIGROUPS IN CRYPTOLOGY

ALEKSANDAR KRAPEŽ*

Dedicated to Academician Ǵorǵi Čupona

Abstract. Quasigroup string processing of S. Markovski and colaborators is one of interesting and recently reported methods for encryption. We propose an alternative encryption method using parastrophes of a single quasigroup to encrypt blocks of the plaintext of various sizes. The proposed method has potential to provide an enhanced security and an increased memory efficiency in comparison to the Quasigroup string processing.

1. Introduction

0

As an algebraic structure the quasigroups are the product of the XX senctury. However, as their combinatorial equivalent - latin squares - they enjoy a much longer existence. Even in antiquity, the permutatins were used to encode texts, and permutations are the essence of quasigroups. Namely, both left and right translations in quasigroups are permutations and quasigroups are characterized by this property.

In cryptography, the use of groups is much more popular but we think that quasigroups provide an interesting approach for design of certain encryption techniques. Even in a group case in a number of instantiations, we actually use groups to make quasigroups and do the encrypting with these quasigroups. The main reason for the popularity of groups is that they are more regular as they satisfy associativity and are therefore easier to implement. However, the quasigroups offer a potential for an enhanced security and high speed of modern day computers compensate the implementation advantages implied by the regularity of groups.

In the first section of the paper, we give some basic facts on quasigroups. In the next sections we describe, the method of Quasigroup string processing of Markovski et al. first and then propose our method called Quasigroup encrypton with parastrophes. We briefly compare these two similar methods.

Date: August 8, 2010.
2010 *Mathematics Subject Classification.* Primary 94A60; Secondary 20N05.
Key words and phrases. encryption, quasigroup, parastrophe, quasigroup string processing.
0* Supported by the Ministry of Science and Technology of Serbia, grants 174008, 174026

2. Quasigroups

A quasigroup is a natural generalization of the concept of a group. Quasigroups differ from groups in that they need not be associative.

We say that a groupoid $(A;\cdot)$ is a *quasigroup* if for all a, b from A there are unique solutions x, y from A to the equations $x \cdot a = b$ and $a \cdot y = b$. An associative quasigroup is a *group*.

Quasigroups are important algebraic (combinatorial, geometric) structures which arise in various areas of mathematics and other disciplines. We mention just a few of their applications:

- in combinatorics (as latin squares, see [1])
- in geometry (as nets/webs, see [1] and [2])
- in statistics (see [3] and [1])
- in special theory of relativity (see [4]),
  and, of particular importance for our topic,
- in coding theory and cryptography ([1] and [5]).

As usual, whenever unambiguous, a term like $x \cdot y$ is shortened to xy. The word 'iff' stands for 'if and only if'.

A quasigroup operation $\cdot$ is often considered together with its *inverse operations*: left ($\backslash$) and right ($/$) division. The inverse operations are defined by: $xy = z$ iff $x\backslash z = y$ iff $z/y = x$. Both of the inverse operations are also quasigroups. However, the inverse operations of a group operation need not produce a group.

It is often convenient to say that the operation $\cdot$ itself is a quasigroup, assuming the underlying base set A and the division operations.

Theorem 1 (Evans)**.** *A groupoid with three operations $\cdot, \backslash, /$ is a quasigroup iff it satisfies:*

$$x\backslash xy = y \tag{2.1}$$
$$x(x\backslash y) = y \tag{2.2}$$
$$xy/y = x \tag{2.3}$$
$$(x/y)y = x \tag{2.4}$$

The dual operations of $\cdot, \backslash, /$ are defined as follows:

$$x * y = yx$$
$$x \backslash\backslash y = y\backslash x$$
$$x /\!/ y = y/x$$

These are also quasigroup operations, and the six operations $\cdot, \backslash, /, *, \backslash\backslash, /\!/$ are said to be *parastrophes* (or *conjugates*) of each other.

By considering formulas 2.1 and 2.2 we see that operations $\cdot$ and $\backslash$ are left inverse operations to each other. Similarly, from the formulas:

$$x/(y\backslash x) = y \tag{2.5}$$
$$(x/y)\backslash x = y \tag{2.6}$$

which are also true in all quasigroups, we conclude that the operations / and $\backslash\backslash$ are left inverses of each other. Finally, $*$ and $/\!/$ are also left inverses of each other as follows from 2.3 and 2.4.

3. Quasigroup string processing

V. Shcherbacov gave in [5] an overview of possible applications of quasigroups in cryptography. One of the successfull methods is the Quasigroup string processing of S. Markovski et al. [6, 7]. We give a short description of their method.

Let $A = \{a_1, \dots a_n\}$ $(n > 1)$ be an *alphabet*, and let $(A; \cdot)$ be a quasigroup as in the previous section. Denote by A^+ the set of all nonempty words over A. Take an element a from A and define a unary operation F on A^+, as follows:

$$F(u_1, \dots, u_k) = v_1, \dots, v_k, \quad k > 0$$

where

$$v_1 = a \cdot u_1,$$
$$v_i = v_{i-1} \cdot u_i, \quad 1 < i \leq k.$$

Also

$$G(v_1, \dots, v_k) = u_1, \dots, u_k, \quad k > 0.$$

where

$$u_1 = a \backslash v_1,$$
$$u_i = v_{i-1} \backslash v_i, \quad 1 < i \leq k.$$

The set A, the operations $\cdot$ and $\backslash$ (i.e. the quasigroup $(A; \cdot)$), the *leader* a and functions F and G define a *cipher* over the alphabet A.

The most important property of this cipher is:

$$F \circ G = \mathrm{Id}$$

i.e. the function G decrypts the text encrypted by the function F. The other interesting properties of this cipher are:

- the cipher text is the same length as the plain text
- the cipher could be considered as a stream cipher
- the cipher can detect errors
- as there are more than $n!(n-1)! \cdots 2!1!$ of quasigroups of order n , the brute force attack on the cipher appears as not feasible, assuming n large enough
- for 'well chosen' quasigroups, the cipher provides good statistical properties of its output
- the cipher provides a potential for an enhanced resistance against cryptanalysis even when both plain text and the corresponding cipher text are known.

The liability of the method is that we have to choose a quasigroup carefully. Any kind of internal symmetry, such as commutativity $(xy = yx)$, associativity $(x \cdot yz = xy \cdot z)$, left symmetry $(x \cdot xy = y)$, total symmetry (both commutativity and left symmetry) etc., would weaken the resistance to attacks.

Gligoroski et al. in [8] experimentaly concluded that out of existing 576 quasigroups of order four, only 192 are suitable for employment in the cipher. However, for an alphabet with 256 letters (a more realistic case), there are more than 10^{58000} candidate quasigroups for selection ([6]).

A variant of the method has also been reported where a sequence of quasigroups (and leaders) is employed for multiple re-encryptions. This considerably improves resistance against a number of attaking approaches as the weaknesses of one quasigroup are cancelled out by other quasigroups. However, the price to be paid is in the employed memory size for the cipher implementation. For example, we need 64KB of memory to store a quasigroup of order 256.

4. Quasigroup encryption with parastrophes

We propose a new method of ciphering based on the same principle as Quasigroup string processing but with modifications which provide potential for an increased security, and at the same time reduces the implementation requirements for memory size.

The proposed method splits the plain text into blocks of various sizes and encrypts it employing various parastrophes of a single quasigroup.

The method is based on the following: We select a leader a and a key, i.e. a quasigroup $(A;\cdot)$, over an alphabet A and a computable function of natural numbers with values (b_j). We employ $\cdot, \backslash, /, *, \backslash\backslash, //$ for the operation $\bullet_n$ and $n = 0,1,2,3,4,5$, and $\backslash, \cdot, \backslash\backslash, //, /, *$ for the operation $\diamond_n$ and $n = 0,1,2,3,4,5$. Accordingly, we define a unary operation F on A^+ :

$$F(u_1,\dots,u_k) = v_1,\dots,v_k, \quad k>0$$

where

$$v_1 = a \bullet_{b_0(mod6)} u_1,$$

$$v_i = v_{i-1} \bullet_{b_0(mod6)} u_i, \quad 1 < i \le b_0,$$

$$v_i = v_{i-1} \bullet_{b_j(mod6)} u_i, \quad b_0+\dots+b_{j-1} < i \le b_0+\dots+b_j$$

for values of j big enough so that $k \le b_0+\dots+b_j$. Also

$$G(v_1,\dots,v_k) = u_1,\dots,u_k, \quad k>0$$

where

$$u_1 = a \diamond_{b_0(mod6)} v_1,$$

$$u_i = v_{i-1} \diamond_{b_0(mod6)} v_i, \quad 1 < i \le b_0,$$

$$u_i = v_{i-1} \diamond_{b_j(mod6)} v_i, \quad b_0+\dots+b_{j-1} < i \le b_0+\dots+b_j$$

for the same values of j as above.

Theorem 2.

$$F \circ G = \mathrm{Id}.$$

The proof is based on examination of all cases. If, for example, $b_j(mod6) = 4$ then $x \diamond_4 (x \bullet_4 y) = x/(x\backslash\backslash y) = x/(y\backslash x) = y$ and in a similar way in other cases.

The above theorem implies feasibility of encryption and decryption, i.e. that we can decrypt ciphertext back to plaintext.

Assume that all numbers from the sequence (b_j) are divisible by 6. Then all quasigroups used for encrypting are the same parastrophe of $\cdot$ – the quasigroup $\cdot$ itself. Accordingly, the method obviously reduces to Quasigroup string processing with a single quasigroup. Therefore we have the following statement:

Theorem 3. *The Quasigroup encoding with parastrophes generalizes the Quasigroup string processing.*

The proposed method of ciphering has the following desirable properties:

- the cipher text is the same length as the plain text
- the cipher could be considered as a stream cipher
- the cipher can detect errors
- the brute force attack appears as even more complex compared to related previously reported methods
- for 'well chosen' quasigroups and a sequence (b_j), the cipher provides good statistical properties of its output
- the cipher provides a potential for an enhanced resistance against cryptanalysis even when both plain text and the corresponding cipher text are known.

The liability of the method is that we have to choose a quasigroup even more carefully than in the case of Quasigroup string processing. The method is sensitive to any kind of internal symmetry which is reflected in properties of parastrophes of the given quasigroup. We also have to be careful when we choose the sequence (b_j). The distribution of residuals $mod6$ should be close to uniform to make the best effects of the method. On the other hand, the splitting of plain text into blocks is orthogonal to quasigroup encryption and yields potential for an increased resistance against a number of attacks.

The method uses a single quasigroup to produce six different quasigroups for encryption without the additional requirements for memory. The amount of time needed to find products of elements in parastrophes in terms of original quasigroup is at most quadratic as it is the use of original quasigroup, so it doesn't increase the order of magnitude of the algorithm.

Finally note that, if appropriate, we can also introduce new quasigroups and their parastrophes for building a cipher based on the re-encryption in the same manner as Markovski et al. have reported. The advantage of novel re-encryption approach is that the number of new quasigroups can be an order of magnitude smaller and at the same time yielding a potential for higher level of security.

Acknowledgement

We thank Verica Bakeva who noticed an error in a previous version of the paper.

References

[1] J. Dénes, A. D. Keedwell, *Latin squares and their applications*, Acadmiai Kiadó, Budapest, (1974).
[2] V. D. Belousov, *Configurations in algebraic nets* (Russian), Shtiinca, Kishinev, (1979).
[3] R. A. Fisher, *The design of experiments* (8th edition), Oliver & Boyd, Edinburgh, (1966).
[4] A. Ungar, *Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession - The Theory of Gyrogroups and Gyrovector Spaces*, Kluwer Academic Publishers, Dordrecht, Boston, London, (2001).
[5] V. Shcherbacov, *On some known possible applications of quasigroups in cryptology*, manuscript, (2003), http://www.karlin.mff.cuni.cz/˜drapal/krypto.pdf .
[6] S. Markovski, D. Gligoroski and S. Andova, *Using quasigroups for one-one secure encoding*, in *Proceedings of VIII-th Conference for Logic and Computing - LIRA'97, September 1997*, Novi Sad, (1997).
[7] S. Markovski, D. Gligoroski and V. Bakeva, *Quasigroup String Processing: Part 1*, Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. **XX 1-2**, (1999).
[8] D. Gligoroski and S. Markovski, *Cryptographic Potentials of Quasigroup Transformations*, manuscript, (2003).

Mathematical Institute of the Serbian Academy of Science and Arts,
Knez Mihailova 36, Belgrade, Serbia
E-mail address: sasa@mi.sanu.ac.rs