Cryptographic Properties of Parastrophic Quasigroup Transformation

V. Dimitrova[1], V. Bakeva[1],
A. Popovska-Mitrovikj[1], and A. Krapež[2]

[1]Faculty of Computer Science and Engineering,
Ss. Cyril and Methodius University, Skopje, Macedonia
[2]Serbian Academy of Sciences and Arts, Beograd, Serbia
vesna.dimitrova@finki.ukim.mk,verica.bakeva@finki.ukim.mk,
aleksandra.popovska.mitrovikj@finki.ukim.mk,sasa@mi.sanu.ac.rs

Abstract. In this paper, we consider cryptographic properties of parastrophic quasigroup transformation defined elsewhere. With that transformation we classify the quasigroups of order 4 in three classes: 1) parastrophic fractal; 2) fractal and parastrophic non-fractal; and 3) non-fractal. We investigate the algebraic properties of the previous classes and present a connection between fractal properties and algebraic properties of quasigroups of order 4. Also, we find a number of different parastrophes of each quasigroup of order 4 and divide the set of all quasigroups of order 4 in 4 classes. Using these classifications the number of quasigroups of order 4 which are suitable for designing of cryptographic primitives is increased.

Keywords: quasigroup, parastrophic quasigroup transformations, cryptographic properties

1 Introduction

Quasigroups and quasigroup transformations are very useful for construction of cryptographic primitives, error detecting and error correcting codes. The reasons for that are the structure of quasigroups, their large number, the properties of quasigroup transformations and so on. The quasigroup string transformations E and their properties were considered in several papers.

A quasigroup $(Q, *)$ is a groupoid (i.e. algebra with one binary operation $*$ on the finite set Q) satisfying the law:

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad (x * u = v \ \& \ u * y = v) \tag{1}$$

In fact, (1) says that a groupoid $(Q, *)$ is a quasigroup if and only if the equations $x * u = v$ and $u * y = v$ have unique solutions x and y for each given $u, v \in Q$. It has been noted that every quasigroup $(Q, *)$ has a set of five quasigroups, called parastrophes denoted with $/, \backslash, \cdot, //, \backslash\backslash$ which are defined in Table 1.

Table 1: Parastrophes of quasigroup operations $*$

Parastrophes operation
$x\backslash y = z \iff x * z = y$
$x/y = z \iff z * y = x$
$x \cdot y = z \iff y * x = z$
$x//y = z \iff y/x = z \iff z * x = y$
$x\backslash\backslash y = z \iff y\backslash x = z \iff y * z = x$

In this paper we use the following notations for parastrophe operations:

$$f_1(x,y) = x * y,\ f_2(x,y) = x\backslash y,\ f_3(x,y) = x/y,$$
$$f_4(x,y) = x \cdot y,\ f_5(x,y) = x//y,\ f_6(x,y) = x\backslash\backslash y.$$

Let $A = \{1, \ldots, s\}$ be an alphabet ($s \geq 2$) and denote by $A^+ = \{x_1 \ldots x_k |\ x_i \in A,\ k \geq 1\}$ the set of all finite strings over A.

Note that $A^+ = \bigcup_{k \geq 1} A^k$, where $A^k = \{x_1 \ldots x_k |\ x_i \in A\}$. Assuming that (A, f_i) is a given quasigroup, for a fixed letter $l \in A$ (called leader) we define transformation $E = E_{f_i,l} : A^+ \to A^+$ by

$$E_{f_i,l}(x_1 \ldots x_k) = y_1 \ldots y_k \Leftrightarrow \begin{cases} y_1 = f_i(l, x_1), \\ y_j = f_i(y_{j-1}, x_j), \quad j = 2, \ldots, k. \end{cases} \tag{2}$$

In section 2 we give the new parastrophic quasigroup transformation and we analyze the application of that transformation in cryptography. Using the new transformation and the number of different parastrophes we make several classifications of quasigroups of order 4 presented in section 3. In addition, in section 4 we consider some algebraic properties of parastrophic fractal quasigroups and we propose a mathematical model for parastrophic fractality.

2 Parastrophic transformation and its cryptographic properties

In [4], using quasigroup parastrophes, Krapež gives an idea for quasigroup string transformation which can be applied in cryptography. A modification of this quasigroup transformation is defined in [2]. Here we describe that quasigroup transformation called parastrophic quasigroup transformation and futher on, we consider its cryptographic properties.

Let p be a positive integer and $x_1 x_2 \ldots x_n$ be an input message. Using previous transformation E, we define a parastrophic transformation $PE = PE_{l,p} : A^+ \to A^+$ as follows.

At first, let $d_1 = p$, $q_1 = d_1$, $s_1 = (d_1 \bmod 6) + 1$ and $A_1 = x_1 x_2 \dots x_{q_1}$. Applying the transformation $E_{f_{s_1},l}$ on the block A_1, we obtain the encrypted block

$$B_1 = y_1 y_2 \dots y_{q_1-2} y_{q_1-1} y_{q_1} = E_{f_{s_1},l}(x_1 x_2 \dots x_{q_1}).$$

Further on, using last two symbols in B_1 we calculate the number $d_2 = 4y_{q_1-1} + y_{q_1}$ which determines the length of the next block. Let $q_2 = q_1 + d_2$, $s_2 = (d_2 \bmod 6) + 1$ and $A_2 = x_{q_1+1} \dots x_{q_2-1} x_{q_2}$. After applying $E_{f_{s_2},y_{q_1}}$, the encrypted block B_2 is

$$\begin{aligned} B_2 &= y_{q_1+1} \dots y_{q_2-2} y_{q_2-1} y_{q_2} = \\ &= E_{f_{s_2},y_{q_1}}(x_{q_1+1} \dots x_{q_2-2} x_{q_2-1} x_{q_2}). \end{aligned}$$

In general case, for given i, let the encrypted blocks $B_1, \dots, B_{i-1}$ be obtained and d_i be calculated using the last two symbols in B_{i-1} as previous. Let $q_i = q_{i-1} + d_i$, $s_i = (d_i \bmod 6) + 1$ and $A_i = x_{q_{i-1}+1} \dots x_{q_i-1} x_{q_i}$. We apply the transformation $E_{f_{s_i},y_{q_{i-1}}}$ on the block A_i and obtain the encrypted block

$$B_i = E_{f_{s_i},y_{q_{i-1}}}(x_{q_{i-1}+1} \dots x_{q_i}).$$

Now, the parastrophic transformation is defined as

$$PE_{l,p}(x_1 x_2 \dots x_n) = B_1 || B_2 || \dots || B_r. \tag{3}$$

Note that the length of the last block A_r may be shorter than d_r (depends on the number of letters in input message). The transformation PE is schematically presented in Figure 1.

For arbitrary quasigroup on a set A and for given $l_1, \dots l_n$ and $p_1, \dots, p_n$, we define mappings PE_1, PE_2, ..., PE_n as in (3) such that PE_i is corresponding to p_i and l_i. Using them, we define the transformation $PE^{(n)}$ as follows:

$$PE^{(n)} = PE^{(n)}_{(l_n,p_n),\dots,(l_1,p_1)} = PE_n \circ PE_{n-1} \circ \dots \circ PE_1,$$

where $\circ$ is the usual composition of mappings.

We make experiments with PE-transformation for different ways for determine the length of the next block and the quasigroup operation, in each iteration. Analyzing the results from our experiments, we obtain that we have the best results if we take the last two symbols for computing the length of the next block and corresponding quasigroup operation. Namely, if we take one symbol then we can obtain only 4 values for choosing the quasigroup operations, but we have 6 parastrophes. On the other side, when we take more the 2 symbols for computing the length of the next block and corresponding quasigroup operation, we conclude that the parastrophes are not changing very often. Therefore, in these cases we obtain worse results in terms of fractality, i.e., we have not increased the number of quasigroups suitable for cryptography.

An important property of one transformation for application in cryptography is the uniform distribution of the substrings in the output message. This property

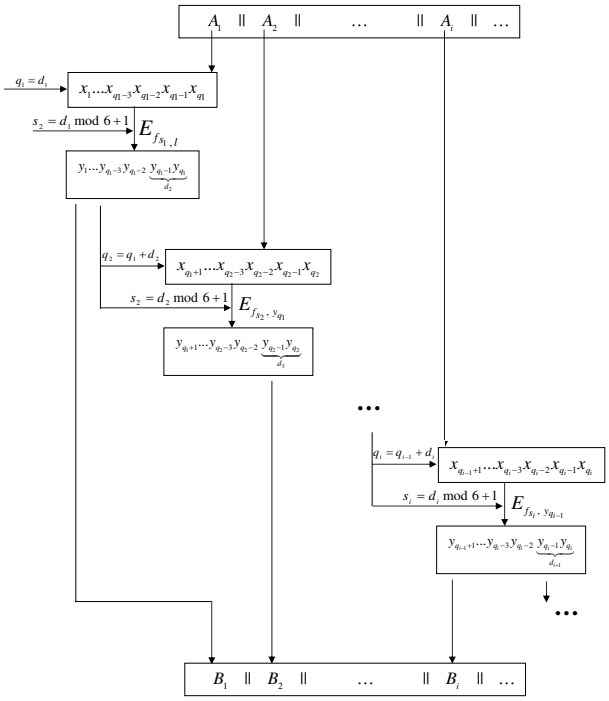


Fig. 1. Parastrophic transformation PE

is useful for proving the resistance of statistical attack. Therefore, we investigate the uniformity of the output message obtained after using PE-transformation and experimentally, we proved the following result.

Proposition 1. *Let $\alpha \in A^+$ be an arbitrary string and $\beta = PE^{(n)}(\alpha)$. Then the m-tuples in β are uniformly distributed for $m \leq n$.*

The theoretical prof of this result is in progress.

3 Classifications of quasigroups of order 4 useful in cryptography

In [3], using image pattern, Dimitrova and Markovski give a classification of quasigroups of order 4 as fractal and non-fractal. This classification is made on the following way. The authors start with a periodical sequence 123412341... with length 100 and apply 100 times the E-transformation given in (2) with given leaders. They present the transformed sequences visually using different color for each symbol 1,2,3,4. On this way, they obtain an image pattern for each quasigroup and then analyze the structure of this patterns. If the pattern has a fractal structure, the suitable quasigroup is called fractal. In opposite case, the quasigroup is called non-fractal. The number of fractal quasigroups of order

4 is 192 and the number of non-fractal quasigroups is 384. Fractal quasigroups are not good for designing of cryptographic primitives since they give a regular structures.

In order to increase the number of quasigroups suitable for application in cryptography, we give new classifications of quasigroups of order 4:

- classification by number of different parastrophes;
- classification by PE-transformation.

3.1 Classification by number of different parastrophes

We consider all 576 quasigroups of order 4 and for each quasigroup we find the set of all parastrophes. The cardinality of each of these sets is less or equal to 6, i.e., not all parastrophes of a quasigroup are different.

Using the number of different parastrophes of each quasigroup we divide the set of all quasigroups of order 4 in 4 classes. The number of quasigroups in each of these classes are given in Table 1.

Table 1. Cardinality of classes by number of different parastrophes

No. parastrophes	No. quasigroups
1	16
2	2
3	240
6	318
Total	576

In Table 2 we give a sub-classification of the previous one. Namely, according to number of different parastrophes we classify separately, the fractal and non-fractal quasigroups of order 4.

Table 2. Cardinality of subclasses by number of different parastrophes

No. parastrophes	No. fractal quasigroups	No. non-fractal quasigroups
1	16	0
2	2	0
3	96	144
6	78	240
Total	192	384

From Table 2, we can note that the class of fractal quasigroups of order 4 is divided in 4 subclasses, and the class of non-fractal quasigroups is divided

in just 2 subclasses. Comparing Table 1 and Table 2 we can conclude that all quasigroups with 1 or 2 parastrophes are fractal. Quasigroups with 3 and 6 parastrophes can be fractal or non-fractal.

Experimentally, we prove the following proposition.

Proposition 2. *All fractal quasigroups of order* 4 *have fractal parastrophes.*

Consequently, all non-fractal quasigroups of order 4 have non-fractal parastrophes.

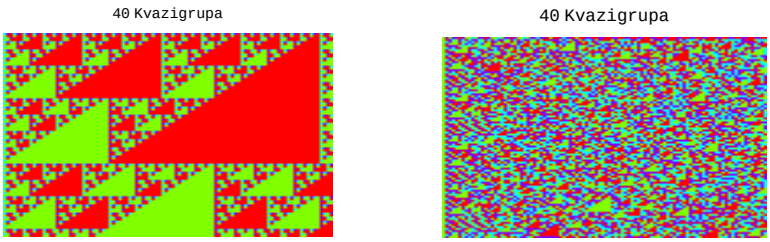
3.2 Classification using PE-transformation

In this paper, using image pattern as in [3], we make a similar classification using new PE-transformation instead of E-transformation. We apply the new transformation $PE^{(n)}$ to the sequence 123412341234... as previous and consider the fractal structure of the obtained image. Depending on that structure we introduce new types of fractal quasigroups.

Definition 1. *Quasigroups with fractal structure obtained after applying of PE-transformation are called* ***parastrophic fractal quasigroups****. In the opposite case, the quasigroup is called* ***parastrophic non-fractal quasigroups****.*

We made experiments with image pattern for all 576 quasigroups of order 4 and we found that 88 are parastrophic fractal and 488 are parastrophic non-fractal. We conclude that all parastrophic fractal quasigroups are in class of fractal quasigroups, but not all fractal quasigroups are parastrophic fractal. This means that the class of all 192 fractal quasigroups is divided in 2 subclasses: 1) parastrophic fractal (88 quasigroups) and 2) fractal, but parastrophic non-fractal (104 quasigroups), called ***fractal parastrophic non-fractal quasigroups***.

In Figure 2, we give the quasigroup with lexicographic number 40 which is fractal (a), but it is not parastrophic fractal (b).



(a) (b)

Fig. 2. Fractal, but parastrophic non-fractal quasigroup

On the other side, the class of all 384 non-fractal quasigroups is completely contained in the class of parastrophic non-fractal quasigroups.

According to the previous, we make a new classification of quasigroups of order 4:

1) class of parastrophic fractal (88 quasigroups);
2) class of fractal parastrophic non-fractal quasigroups (104 quasigroups);
3) class of non-fractal quasigroups (384 quasigroups).

With this classification the number of quasigroups useful in cryptography is increased. Namely, for cryptographic purposes we can use not only quasigroups from class 3, but the quasigroups from class 2, too.

Further on, according to the number of different parastrophes, we find the cardinality of subclasses of parastrophic fractal and fractal parastrophic non-fractal quasigroups, separately. The results are given in Table 3.

Table 3. Cardinality of subclass of fractal quasigroups by number of different parastrophes

No. parastrophes	No. parastrophic fractal	No. fractal parastrophic non-fractal
1	16	0
2	0	2
3	72	24
6	0	78
Total	88	104

Comparing Table 2 and Table 3 we can conclude that all fractal quasigroups with 1 parastrophe are parastrophic fractal, all fractal quasigroups with 2 and 6 different parastrophes are fractal parastrophic non-fractal quasigroups. Only the subclass of fractal quasigroups with 3 different parastrophes contains parastrophic fractal and fractal parastrophic non-fractal quasigroups.

4 Algebraic properties of parastrophic fractal quasigroups

In [6] using some identities, the authors give a mathematical model of fractality of quasigroups. Our goal is to find similar model, but for parastrophic fractality of quasigroups. For this purpose we investigate the algebraic properties of parastrophic fractal quasigroups. We make a lot of experiments for finding a suitable identities to separate parastrophic fractal quasigroups. We research many identities, especially identities for symmetry. Essential for our model are the following ones given with the corresponding identities: commutativity ($ab = ba$), skew symmetric ($(ab)(ba) = const$), left loops ($ex = x$), right loops ($xe = x$), right symmetric ($(ab)b = a$), left symmetric ($b(ba) = a$), totally symmetric quasigroups (????)

From our experiments we conclude that each parastrophic fractal quasigroup belongs to the set of quasigroups I that satisfies the identity $x(x(x(xy))) = y$ and belongs to one of the following sets of quasigroups:

– Loops (L)
– Totally symmetric quasigroups (TS)
– Left Loops (LL) and Right symmetric quasigroups (RS)
– Right Loops (RL) and Left symmetric quasigroups (LS)
– Left Loops (LL) and Skew symmetric quasigroups (SS)
– Right Loops (RL) and Skew symmetric quasigroups (SS)
– Commutative quasigroups (C) and Skew symmetric quasigroups (SS).

Using the previous notations, we give the following proposition:

Proposition 3. *The class of all parastrophic fractal quasigroups PFQ can be presented as:*

$$PFQ = I \cap [L \cup TS \cup (LL \cap RS) \cup (RL \cap LS) \cup (SS \cap (LL \cup RL \cup C))].$$

In this way, we have the mathematical model for parastrophic fractality and without using image pattern we can check if a given quasigroup is parastrophic fractal.

5 Conclusion

In this paper, we consider the parastrophic quasigroup transformation defined in [2] and using this transformation we define new types of quasigroups depending of parastrophic fractality. We give two new classifications of quasigroups of order 4: 1) classification by number of different parastrophes; and 2) classification by PE-transformation. On this way, we increase the number of quasigroups of order 4 which are suitable for designing of cryptographic primitives. Also, we investigate the algebraic properties of parastrophic fractal quasigroups and we propose a mathematical model for parastrophic fractality.

We give several propositions good for application in cryptography. These propositions are experimentally proved and for some of them the theoretical prof is in progress. At the end, if we summarize the obtained results we can conclude that:

– parastrophic fractal quasigroups should not be used for cryptographic primitives, since they have fractal structure, properties of symmetry and shape;

– we have mathematical model for separating the parastrophic fractal quasigroups;

– the parastrophic tranformation is more suitable for designing of cryptographic primitives, since it increase the number of quasigroups useful in cryptography.

References

1. Bakeva, V., Dimitrova, V.: Some Probabilistic Properties of Quasigroup Processed Strings useful in Cryptanalysis. In: Gusev, M., Mitrevski, P. (eds.) ICT-Innovations 2010, pp. 61-70. Springer (2010)
2. Bakeva,V., Dimitrova, V., Popovska-Mitrovikj, A.: Parastrophic Quasigrouop String Processing. In: Proc. of the 8^{th} Conference on Informatics and Information Technology with International Participants, Macedonia (2011) pp. 19-21.
3. Dimitrova V., Markovski S.: Classification of quasigroups by image patterns. In: Proc. of the Fifth International Conference for Informatics and Information Technology, Macedonia, (2007) pp. 152 - 160.
4. Krapež, A.: An Application Of Quasigroups in Cryptology. In: Math. Maced. Vol. 8 (2010), pp. 47-52.
5. Markovski,S., Gligoroski,D., Bakeva,V.: Quasigrouop string processing: Part 1. In: Contributions, Sec. Math. Tech. Sci., MANU, Vol. XX 1-2 (1999) pp. 13-28.
6. Markovski,S., Dimitrova, V., Samardziska, S.: Identities sieves for quasigroups. In: Quasigroups and Related Systems, Vol. 18, No. 2, (2010) pp. 149-164.
7. Denes J., Keedwell A. D: Latin Squares and their Applications, The English Universities Press Ltd., (1974).