Resistance to Statistical Attacks of Parastrophic Quasigroup Transformation

Verica Bakeva, Aleksandra Popovska-Mitrovikj and Vesna Dimitrova
University "Ss Cyril and Methodius" - Skopje,
Faculty of Computer Science and Engineering,
P.O. Box 393 1000 Skopje,
Republic of Macedonia

***Abstract*—The resistance to statistical kind of attacks of encrypted messages is a very important property for designing cryptographic primitives. In this paper, the parastrophic quasigroup PE-transformation, proposed elsewhere, is considered and the proof that it has this cryptographic property is given. Namely, it is proven that if PE-transformation is used for design of an encryption function then after n applications of it on arbitrary message the distribution of m-tuples ($m = 1, 2, \ldots, n$) is uniform. These uniform distributions imply the resistance to statistical attack of the encrypted messages. For illustration of theoretical results, some experimental results are presented as well.**

***Keywords*—uniform distribution; cryptographic properties; statistical attack; encrypted message; quasigroup; parastrophic quasigroup transformation**

I. 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:

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

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 $u, v \in Q$.

In the sequel, let $A = \{1, \ldots, a\}$ be an alphabet of integers ($a \geq 2$) 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 $(A, *)$ is a given quasigroup, for any letter $l \in A$ (called leader), Markovski and al. (see [5]) defined the transformation $E = E_l^{(1)} : A^+ \to A^+$ by

$$E(x_1 \ldots x_k) = y_1 \ldots y_k \Leftrightarrow \begin{cases} y_1 = l * x_1, \\ y_i = y_{i-1} * x_i, \quad i = 2, \ldots, k \end{cases} \qquad (2)$$

where $x_i, y_i \in A$. Then, for given quasigroup operations $*_1, *_2, \ldots, *_n$ on the set A, we can define mappings $E_1, E_2, \ldots, E_n$, in the same manner as previous by choosing fixed elements $l_1, l_2, \ldots, l_n \in A$ (such that E_i is corresponding to $*_i$ and l_i). Let

$$E^{(n)} = E^{(n)}_{l_n, \ldots, l_1} = E_n \circ E_{n-1} \circ \cdots \circ E_1,$$

where $\circ$ is the usual composition of mappings ($n \geq 1$). It is easy to check that the mappings E is a bijection. In the same paper, authors proposed a transformation $E^{(n)}$ as an encryption function and proved the following theorem.

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

Also, in Theorem 2 in [1], Bakeva and Dimitrova proved that the probabilities of $(n+1)$-tuples in $\beta = E^{(n)}(\alpha)$ are divided in a classes where $a = |A|$, if $(p_1, p_2, \ldots, p_a)$ is the distribution of letters in an input string and $p_1, p_2, \ldots, p_a$ are distinct probabilities, i.e., $p_i \neq p_j$ for $i \neq j$. Each class contains a^n elements with the same probabilities and the probability of each $(n+1)$-tuple in i-th class is $\frac{1}{a^n} p_i$, for $i = 1, 2, \ldots, a$. If $p_{i_1} = p_{i_2} = \cdots = p_{i_\nu}$ for some $1 \leq i_1 < \cdots < i_\nu \leq a$, then the classes with probabilities $\frac{1}{a^n} p_{i_1} = \frac{1}{a^n} p_{i_2} = \cdots = \frac{1}{a^n} p_{i_\nu}$ will be merged in one class with νa^n elements. Using these results, the authors proposed an algorithm for cryptanalysis.

In paper [4], Krapez gave an idea for a new quasigroup string transformation based on parastrophes of quasigroups. A modification of this quasigroup transformation is defined in [2]. In [3], authors showed that the parastrophic quasigroup transformation has good properties for application in cryptography. Namely, using that transformation the number of quasigroups of order 4 useful in cryptography is increased. To complete the proof of goodness of parastrophic quasigroup transformation for cryptography, it is needed to prove that Theorem 1 holds for that transformation, too. It will guarantee that message encrypted by the parastrophic quasigroup transformation will be resistant to a statistical kind of attacks.

In Section II, we briefly repeat the construction of parastrophic quasigroup transformation given in [2]. In Section III, we give the theoretical proofs that PE-transformation guaranties a resistance to statistical kind of attacks. Some experimental results (in order to illustrate the theoretical results) are presented in Section IV. In Section V, we make

some conclusions about the goodness of PE-transformation for application in cryptography.

II. Parastrophic transformation

Recall 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 I: Parastrophes of quasigroup operations $*$

Parastrophe operations				
$x\backslash y = z$	$\Longleftrightarrow$	$x * z = y$		
$x/y = z$	$\Longleftrightarrow$	$z * y = x$		
$x \cdot y = z$	$\Longleftrightarrow$	$y * x = z$		
$x//y = z$	$\Longleftrightarrow$	$y/x = z$	$\Longleftrightarrow$	$z * x = y$
$x\backslash\backslash y = z$	$\Longleftrightarrow$	$y\backslash x = z$	$\Longleftrightarrow$	$y * z = x$

In this paper the following notations for parastrophe operations is used:

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

Let $M = x_1x_2 \dots x_k$ be an input message. Let d_1 be an random integer such that $(2 \leq d_1 < k)$ and l be random chosen element (leader) from A. Also, let $(A, *)$ be a quasigroup and f_1, ..., f_6 be its parastrophe operations.

Using previous transformation E, for chosen l, d_1 and quasigroup $(A, *)$ we define a parastrophic transformation $PE = PE_{l,d_1} : A^+ \to A^+$ as follows.

At first, let $q_1 = d_1$ be the length of the first block, i.e., $M_1 = x_1x_2 \dots x_{q_1}$. Let $s_1 = (d_1 \bmod 6) + 1$. Applying the transformation E on the block M_1 with leader l and quasigroup operation f_{s_1}, the following encrypted block is obtained.

$$C_1 = y_1y_2 \dots y_{q_1-1}y_{q_1} = E_{f_{s_1},l}(x_1x_2 \dots x_{q_1-1}x_{q_1}).$$

Further on, using last two symbols in C_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 $M_2 = x_{q_1+1} \dots x_{q_2-1}x_{q_2}$. After applying $E_{f_{s_2},y_{q_1}}$, the encrypted block C_2 is

$$C_2 = y_{q_1+1} \dots y_{q_2-1}y_{q_2} = E_{f_{s_2},y_{q_1}}(x_{q_1+1} \dots x_{q_2-1}x_{q_2}).$$

In general case, for given i, let the encrypted blocks $C_1, \dots, C_{i-1}$ be obtained and d_i be calculated using the last two symbols in C_{i-1}, i.e., $d_i = 4y_{q_{i-1}-1} + y_{q_{i-1}}$. Let $q_i = q_{i-1} + d_i$, $s_i = (d_i \bmod 6)+1$ and $M_i = x_{q_{i-1}+1} \dots x_{q_i-1}x_{q_i}$. Applying the transformation $E_{f_{s_i},y_{q_{i-1}}}$ on the block M_i the obtained encrypted block is

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

Now, the parastrophic transformation is defined as

$$PE_{l,d_1}(M) = PE_{l,d_1}(x_1x_2 \dots x_n) = C_1||C_2|| \dots ||C_r, \quad (3)$$

where $||$ is a concatenation of blocks. Note that the length of the last block M_r may be shorter than d_r (depends on the number of letters in the input message). The transformation PE is schematically presented in Figure 1.

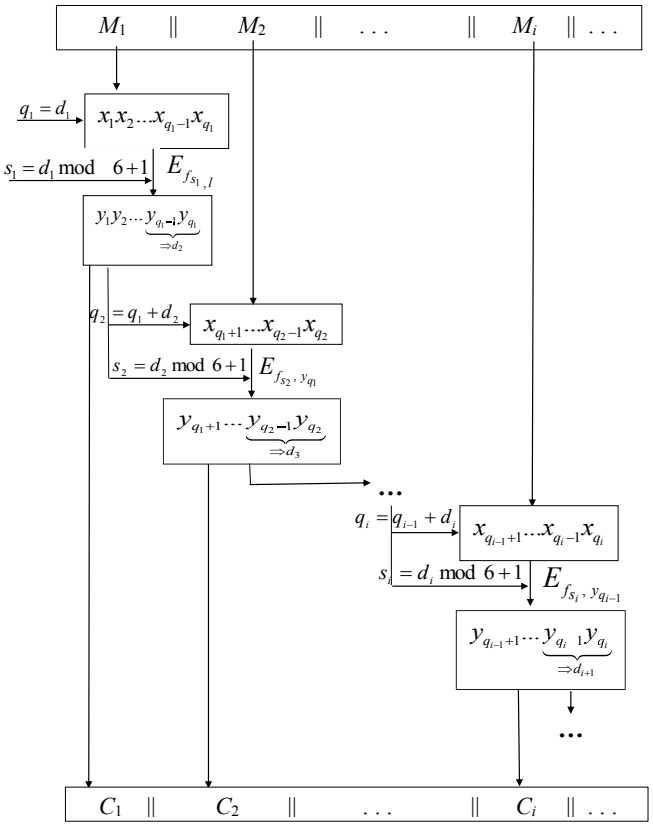

Fig. 1: Parastrophic transformation PE

For arbitrary quasigroup on a set A, random leaders $l_1, \dots l_n$ and random lengths $d_1^{(1)}, \dots, d_1^{(n)}$, we define mappings PE_1, PE_2, ..., PE_n as in (3) such that PE_i is corresponding to $d_1^{(i)}$ and l_i. Using them, we define the transformation $PE^{(n)}$ as follows:

$$PE^{(n)} = PE^{(n)}_{(l_n,d_1^{(n)}),\dots,(l_1,d_1^{(1)})} = PE_n \circ PE_{n-1} \circ \dots \circ PE_1,$$

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

III. Theoretical proof for resistance to statistical kind of attacks

Let the alphabet A be as above. A randomly chosen element of the set A^k can be considered as a random vector $(X_1, X_2, \dots, X_k)$, where A is the range of X_i, $i = 1, \dots, k$. Let consider these vectors as input messages. The transformation $PE = PE_{l,d_1} : A^+ \to A^+$ can be defined as:

$$PE_{l,d_1}(X_1,\dots,X_k)=(Y_1,\dots,Y_k)\Leftrightarrow$$

$$\Leftrightarrow\begin{cases} Y_1=f_{s_1}(l,X_1),\\ Y_j=f_{s_1}(Y_{j-1},X_j),\ j=2,\dots,d_1,\\ \\ Y_{q_i+j}=f_{s_{i+1}}(Y_{q_i+j-1},X_{q_i+j}),\ \begin{matrix} i=1,\dots,r-1,\\ j=1,\dots,d_{i+1}\end{matrix}\end{cases} \tag{4}$$

Let $(p_1,p_2,...,p_a)$ be the probability distribution of the letters $1,...,a$ in an input message. That implies $p_i>0$ for each $i=1,2,...,a$ and $\sum_{i=1}^{a}p_i=1$.

An important property of one transformation for application in cryptography is the uniform distribution of the substrings in the output message $(Y_1,\dots,Y_k)$. This property guarantee the resistance to statistical attack. Therefore, we investigate the distribution of substrings in the output message obtained using PE-transformation. At first we will prove that after applying the transformation $PE^{(1)}$ on an input message α, the letters in transformed message are uniformly distributed.

Theorem 2. *The letter Y_t has uniform distribution on the set $A=\{1,\dots,a\}$, i.e., $Y_t\sim U(\{1,\dots,a\})$ for each t ($t=1,2,\dots,k$).*

Proof. In this proof we use the same notations as in construction of parastrophic quasigroup transformation given in the previous section.

At first, note that the leader l can be consider as uniformly distributed random variables on the set A since it is randomly chosen from the set A. Therefore, $l\sim U(\{1,\dots,a\})$, i.e.,

$$P\{l=i\}=\frac{1}{a},\qquad \text{for each } i\in A.$$

Also, leader l is independent of each letter X_i in the input message.

Let $t=1$. Using the equation (4) and total probability theorem, for distribution of Y_1, we obtain

$$\begin{aligned} P\{Y_1=j\} &= P\{f_{s_1}(l,X_1)=j\}\\ &= \sum_{i=1}^{a}P\{l=i\}P\{f_{s_1}(l,X_1)=j|l=i\}\\ &= \sum_{i=1}^{a}\frac{1}{a}P\{f_{s_1}(l,X_1)=j|l=i\}\\ &= \sum_{i=1}^{a}\frac{1}{a}P\{f_{s_1}(i,X_1)=j\}\\ &= \frac{1}{a}\sum_{i=1}^{a}P\{X_1=f'_{s_1}(i,j)\}\end{aligned}$$

Here, f'_{s_1} is the inverse quasigroup transformation of f_{s_1}, i.e., if $f_{s_1}(u,x)=v$, then $f'_{s_1}(u,v)=x$. Note that if i runs over all values of A then for fixed j, the expression $X_1=f'_{s_1}(i,j)$ runs over all values of A, too. Therefore,

$$P\{Y_1=j\}=\frac{1}{a}\sum_{i=1}^{a}P\{X_1=f'_{s_1}(i,j)\}=\frac{1}{a}\sum_{i=1}^{a}p_i=\frac{1}{a},$$

i.e., $Y_1\sim U(\{1,\dots,a\})$.

The proof is proceed by induction. Let suppose that $Y_r\sim U(\{1,2,\dots,a\})$. Similarly as previous, using that $f_{s_{r+1}}$ is the parastrophe operation applied in $(r+1)^{th}$ step we compute the distribution of Y_{r+1} as follows.

$$\begin{aligned} P\{Y_{r+1}=j\} &= P\{f_{s_{r+1}}(Y_r,X_{r+1})=j\}\\ &= \sum_{i=1}^{a}P\{Y_r=i\}P\{f_{s_{r+1}}(Y_r,X_{r+1})=j|Y_r=i\}\\ &= \sum_{i=1}^{a}\frac{1}{a}P\{f_{s_{r+1}}(i,X_{r+1})=j|Y_r=i\}\end{aligned}$$

According to definition of parastrophic operation given with (4), one can conclude that the random variables X_{r+1} and Y_r are independent. Applying that in previous equation, we obtain

$$\begin{aligned} P\{Y_{r+1}=j\} &= \sum_{i=1}^{a}\frac{1}{a}P\{f_{s_{r+1}}(i,X_{r+1})=j\}\\ &= \frac{1}{a}\sum_{i=1}^{a}P\{X_{r+1}=f'_{s_{r+1}}(i,j)\}\\ &= \frac{1}{a}.\end{aligned}$$

As previous, $f'_{s_{r+1}}$ is the inverse quasigroup transformation of $f_{s_{r+1}}$. In the last equation, we use that $X_{r+1}=f'_{s_{r+1}}(i,j)$ runs over all values of A when j is fixed and i runs over all values of A, i.e.

$$\sum_{i=1}^{a}P\{X_{r+1}=f'_{s_{r+1}}(i,j)\}=\sum_{i=1}^{a}p_i=1.$$

On this way, we proved that Y_t has uniform distribution on the set A, for each $t\geq 1$.

From the Theorem 2 the following can be concluded. If $M\in A^k$ and $C=PE_{l,d_1}(M)$ then the letters in the message C are uniformly distributed, i.e., the probability of the appearance of a letter i at the arbitrary place of the string C is $\frac{1}{a}$, for each $i\in A$.

Theorem 3. *Let $M\in A^+$ be an arbitrary string and $C=PE^{(n)}(M)$. Then the m-tuples in C are uniformly distributed for $m\leq n$.*

Proof. Let $(Y_1^{(n)},Y_2^{(n)},\dots,Y_k^{(n)})=PE^{(n)}(X_1,X_2,\dots,X_k)$. This theorem will be proved by induction. For $n=1$, the statement is satisfied according to Theorem 2. Let suppose that the statement is satisfied for $n=r$, i.e., $(Y_{t+1}^{(r)},Y_{t+2}^{(r)}\dots Y_{t+m}^{(r)})\sim U(\{1,2,\dots,a\}^m)$ for each $1\leq m\leq r$ and each $t\geq 0$. Now, let $n=r+1$. We consider the distribution of $(Y_{t+1}^{(r+1)},Y_{t+2}^{(r+1)}\dots Y_{t+m}^{(r+1)})$ for each $1\leq m\leq r+1$ and arbitrary t.

$$P\{Y_{t+1}^{(r+1)}=y_{t+1}^{(r+1)},Y_{t+2}^{(r+1)}=y_{t+2}^{(r+1)},\dots,Y_{t+m}^{(r+1)}=y_{t+m}^{(r+1)}\}$$

$$=P\{Y_{t+1}^{(r+1)}=y_{t+1}^{(r+1)},f_{s_{t+2}}(Y_{t+1}^{(r+1)},Y_{t+2}^{(r)})=y_{t+2}^{(r+1)},\dots$$

$$\dots,f_{s_{t+m}}(Y_{t+m-1}^{(r+1)},Y_{t+m}^{(r)})=y_{t+m}^{(r+1)}\},$$

where f_{s_j} is the parastrophe operation applied in the step j and f'_{s_j} is its inverse transformation, $j = t+2, \ldots, t+m$. Now,

$$P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} = y_{t+2}^{(r+1)}, \ldots, Y_{t+m}^{(r+1)} = y_{t+m}^{(r+1)}\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, f_{s_{t+2}}(y_{t+1}^{(r+1)}, Y_{t+2}^{(r)}) = y_{t+2}^{(r+1)}, \ldots \\ \ldots, f_{s_{t+m}}(y_{t+m-1}^{(r+1)}, Y_{t+m}^{(r)}) = y_{t+m}^{(r+1)}\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r)} = f'_{s_{t+2}}(y_{t+1}^{(r+1)}, y_{t+2}^{(r+1)}), \ldots \\ \ldots, Y_{t+m}^{(r)} = f'_{s_{t+m}}(y_{t+m-1}^{(r+1)}, y_{t+m}^{(r+1)})\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}\} P\{Y_{t+2}^{(r)} = f'_{s_{t+2}}(y_{t+1}^{(r+1)}, y_{t+2}^{(r+1)}), \ldots \\ \ldots, Y_{t+m}^{(r)} = f'_{s_{t+m}}(y_{t+m-1}^{(r+1)}, y_{t+m}^{(r+1)})\}.$$

The last equality is obtained by using the fact that $Y_{t+1}^{(r+1)}$ is independent of the vector $(Y_{t+2}^{(r)}, \ldots, Y_{t+m}^{(r)})$, since $Y_{t+2}^{(r)}, \ldots, Y_{t+m}^{(r)}$ are not used for obtaining $Y_{t+1}^{(r+1)}$.

Using the inductive hypothesis $(Y_{t+2}^{(r)}, \ldots, Y_{t+m}^{(r)}) \sim U(\{1, 2, \ldots, a\}^{m-1})$, $Y_{t+1}^{(r+1)} \sim U(\{1, 2, \ldots, a\})$ and from previous expression we obtain that

$$P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} = y_{t+2}^{(r+1)}, \ldots, Y_{t+m}^{(r+1)} = y_{t+m}^{(r+1)}\}$$

$$= \frac{1}{a} \cdot \frac{1}{a^{m-1}} = \frac{1}{a^m}.$$

So, we have proved that $(Y_{t+1}^{(n)}, Y_{t+2}^{(n)} \ldots Y_{t+m}^{(n)}) \sim U(\{1, 2, \ldots, a\}^m)$ for each $m \leq n$ and each $t \geq 0$.

IV. Experimental results

We made many experiments in order to illustrate our theoretical results. Here an example is given. We have randomly chosen a message M with 1,000,000 letters of the alphabet $A = \{1, 2, 3, 4\}$ with the distribution of letters given in the Table II .

TABLE II: The distribution of the letters in the input message

1	2	3	4
0.70	0.15	0.10	0.05

The quasigroup (5) and its parastrophes are used.

$*$	1	2	3	4
1	1	2	4	3
2	3	4	2	1
3	4	3	1	2
4	2	1	3	4

(5)

After applying $PE^{(3)}$ on M, the encrypted message $C = PE^{(3)}(M)$ is obtained. In each PE-transformation, we chose the length of the first block $d_1 = 3$ and the initial leader $l_1 = 4$.

The distribution of letters in the output C is given in the Table III.

TABLE III: The distribution of the letters in the output message

1	2	3	4
0.2501	0.2393	0.2576	0.2530

It is obvious that the distribution of letters in the output message C is uniform.

The distribution of pairs, triplets and 4-tuples of letters in C are given on the Figure 2, Figure 3 and Figure 4. On the Figure 2, the pairs are presented on the x-axis in the lexicographic order ($'11' \to 1$, $'12' \to 2$, …, $'44' \to 16$). On the similar way, the triplets and 4-tuples are presented on Figure 3 and Figure 4.

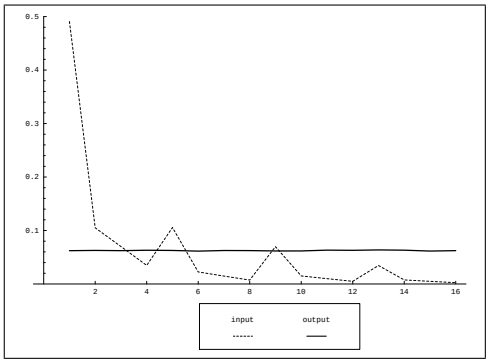

Fig. 2: The distribution of the pairs in the input message and the output message

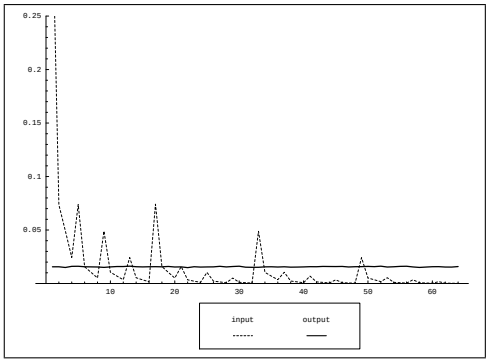

Fig. 3: The distribution of the triplets in the input message and the output message

One can see on Figure 2 and Figure 3 that after three applications of PE-transformations, the pairs and triplets are also uniformly distributed as we proved in Theorem 3. Also, the distribution of the 4-tuples in C is not uniform, but that distribution is closer to the uniform distribution than the distribution of 4-tuples in the input message (see Figure 4).

Next, we check whether Theorem 2 in [1] is satisfied when PE-transformation is applied. The distribution of pairs after one application of PE-transformation is presented on Figure 5. On Figure 6, the distribution of pairs after one application of

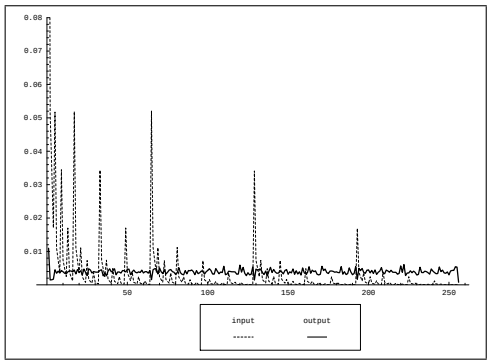

Fig. 4: The distribution of the 4-tuples in the input message and the output message

E-transformation is given. From Figure 6 it can be noticed that probabilities of pairs are divided in 4 classes, as the Theorem 2 in [1] claims. But we cannot distinguish any classes for probabilities on Figure 5. This means that the algorithm for cryptanalysis proposed in [1] cannot be applied when an input message is encrypted by PE-transformation. Therefore encryption by PE-transformation is more resistant to statistical kind of attacks.

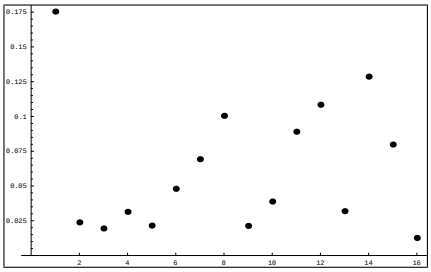

Fig. 5: The distributions of the pairs in output messages obtained by PE-transformation

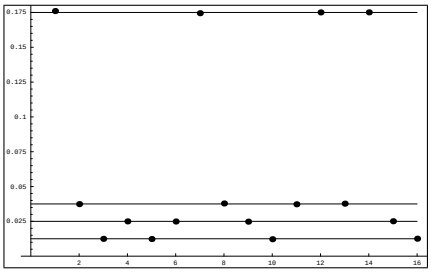

Fig. 6: The distributions of the pairs in output messages obtained by E-transformation

Note that for relevant statistical analyses, it is important to have enough large input message. Namely, in experiments, the probabilities of n-tuples are computed as relative frequencies. So, a relative frequency of an event tends to probability only if we have enough large sample. The relevant statistical analyses cannot be done for shorter message. Therefore, statistical kind of attack is impossible on not enough large input message. Note that if an intruder catches and concatenates a lot of short messages encrypted by the same $PE^{(n)}$-transformation, it will obtain a long message and it can apply a statistical attack. But, the attack will be impossible if quasigroups used in encryption $PE^{(n)}$-transformation is changed more often.

V. Conclusion

In this paper we proved that after n applications of PE-transformation on an arbitrary message the distribution of m-tuples ($m = 1, \ldots, n$) is uniform and we cannot distinguish classes of probabilities in the distribution of $(n+1)$-tuples. This means that if PE-transformation is used as encryption function the obtained cipher messages are resistant to statistical kind of attacks when the number n of applications of PE-transformation is enough large.

In [5], the authors concluded that E-transformation can be applied in cryptography as encryption function since the number of quasigroups is huge one (there are more than 10^{58000} quasigroups when $|A| = 256$) and the brute force attack is not reasonable.

If PE-transformation is used in encryption algorithm then the secret key will be a triplet $(*, l, d_1)$. In that case, the brute force attack also is not possible since except the quasigroup operation $*$ and leader l, the key contains the length of the first block d_1 which has influence of the dynamic of changing of parastrophes.

At the end, in [3] authors proved that PE-transformation has better cryptographic properties than E-transformation for quasigroups of order 4. Namely, some of fractal quasigroups of order 4 become parastrophic non-fractal and they can be used for designing of cryptographic primitives. An investigation for quasigroups of larger order cannot be done in real time since their number is very large.

Finally, from all results we can conclude that PE-transformation is better for design of an encryption function than E-transformation.

Acknowledgment

This research was partially supported by Faculty of Computer Science and Engineering at the University "Ss Cyril and Methodius" in Skopje.

References

[1] V. Bakeva, V. Dimitrova, Some Probabilistic Properties of Quasigroup Processed Strings useful in Cryptanalysis, In: M. Gusev, P. Mitrevski (Eds.) ICT-Innovations 2010, Springer, 2010, pp. 61-70.

[2] V. Bakeva, V. Dimitrova, A.Popovska-Mitrovikj, Parastrophic Quasigrouop String Processing, Proceedings of the 8^{th} Conference on Informatics and Information Technology with International Participants, Macedonia, 2011, pp. 19-21.

[3] V. Dimitrova, V. Bakeva, A.Popovska-Mitrovikj, A.Krapež, Cryptographic Properties of Parastrophic Quasigroup Transformation, In: S. Markovski, M. Gusev (Eds.) ICT-Innovations 2012, Springer, 2012, pp. 221-230.

[4] A. Krapež, An Application Of Quasigroups in Cryptology, Mathematica Macedonica **8**, 2010, pp. 47-52.

[5] S. Markovski, D. Gligoroski, V. Bakeva, Quasigrouop string processing: Part 1, Contributions, Sec. Math. Tech. Sci., MANU, **XX 1-2**, 1999, pp. 13-28.