On Quasigroup Pseudo Random Sequence Generators

V. Dimitrova, J. Markovski

Institute of Informatics, Faculty of Natural Sciences and Mathematics
Ss Cyril and Methodius University, 1000 Skopje, FYRO Macedonia
Email: {vesnap, jasen}@ii.edu.mk

Abstract. Pseudo random sequence generators (PRSG) produce sequences of elements that imitate natural random behavior. They have extensive use in (1) scientific experiments as input sequences for different kinds of simulators, (2) cryptography for preparation of keys and establishing communication and (3) authentication for preparation of identification numbers, smart cards, serial numbers, etc. However, widely available PRSGs have limited periods (for example, 264) which means that the pseudo random sequences start repeating the same elements (after at most 264 elements). This makes them inappropriate for large scale scientific experiments, cryptography and authentication. In this paper we investigate the properties of a new type of PRSG which overcomes these difficulties. The PRSG is designed using quasigroup processing. We show that the quasigroup PRSG is highly scalable and with arbitrary large period. Also we present experimental results on some properties of the quasigroups which make them appropriate for implementation of PRSG.

1 Introduction

Many scientific experiments require large amounts of random input data in order to simulate some process. Random sequences are inevitable in many fields like cryptography, authentication, cryptanalysis etc. For this reason the field of pseudo random generators is widely exploited.

In this paper we present an implementation of a new type of PRSG [3, 5]. This generator is designed using quasigroup processing and it is both highly scalable and not predictable.

In the beginning we give a brief introduction to the notion of PRSG and quasigroup processing. Afterwards, we give theory background of PRSG and quasigroup processing and describe one possible implementation of a Quasigroup PRSG (QPRSG). Next, we introduce new property of the quasigroups called coefficient of period growth. We investigate further this property and present statistical results from which we draw conclusions about the period of the QPRSG. We finish with conclusion about a possible approximation to the ideal random sequence generator.

2 Pseudo Random Sequence Generators

PRSG are deterministic algorithms that produce seemingly random sequences of elements. A PRSG starts with some random sequence of elements. Usually, that is a short random sequence known as seed. The output is much longer pseudo random sequence of elements [2, 8, 9].

Since PRSGs are deterministic algorithms, there is no guaranty that a theoretically ideal random sequence can be produced. Thus, only pseudo random sequence can be produced. Every PRSG has its deficiencies and there are not many all purpose PRSGs. For example, lots of widely available PRSGs are inappropriate for cryptography and authentication, because they produce predictable pseudo random output sequence that start repeating after relatively short time of usage [2, 8, 9].

Secure PRSGs produce unpredictable sequences of elements and have seemingly infinite period [7]. For example, it is possible to build next bit predictors for the linear congruence generators using several schemes. These predictors provide the next pseudo random bit if they have sufficiently many consecutive bits of the pseudo random sequence [8].

Every PRSG has a period. It represents the distance between two sequential appearances of the same pseudo random sequence. This means that the sequence of pseudo random elements will eventually start to repeat. Obviously, the ideal random generator has a period of infinite length. Most widely available PRSGs have limited periods (up to 2^{64}) which means that the pseudo random sequences start repeating the same elements after at most 2^{64} elements [2, 8]. This is not enough for high scale scientific experiments or authentication purposes.

There are two big families of PRSGs: (1) linear PRSGs, which rely on linear congruence functions and (2) nonlinear PRSGs, which are built using some other method. The best-known and most widely available implementations of linear PRSGs are linear congruence functions and linear feedback shift registers. They have relatively small periods, but are also highly predictable which makes them inappropriate for cryptography and authentication. However the production of the pseudo random sequences is relatively fast and that is why they have extended use in scientific experiments (like Monte Carlo simulations) [9]. The QPRSG is a nonlinear PRSG with arbitrary large period.

3 Quasigroups and simple operations

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

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

In other words the equations $x * u = v$, $u * y = v$ for each given $u, v \in Q$ have unique solutions x, y [1].

Let Q be a set of elements ($|Q\,| \geq 2$). We denote by $Q^{+} = \{x_1 x_2 \ldots x_k \mid x_i \in Q,, k \geq 2\}$ the set of all finite sequences with elements of Q. Assuming that $(Q\ , *)$ is a given quasigroup, for a fixed element a$\in Q$, we define transformation $E_a^{(1)}$: $Q^{+} \rightarrow Q^{+}$ on the quasigroup as follows [5]:

$$E_a^{(1)}(x_1 x_2 \ldots x_k) = y_1 y_2 \ldots y_k \Leftrightarrow \begin{cases} y_1 = a * x_1 \\ y_{i+1} = y_i * x_{i+1} \end{cases} . \tag{2}$$

Also, we define $E_a^{(s)} = E_a^{(1)} \circ E_a^{(1)} \circ \ldots \circ E_a^{(1)}$ (s times) [3] to be

$$E_a^{(s)} (a_1a_2...a_k) = a_1^{(s)} a_2^{(s)} \ldots a_k^{(s)}.$$

(3)The following theorem proved in [5] provides the backbone for the QPRSG.

Theorem 1: Let $1 \le l \le n$, $\alpha = a_1a_2...a_k \in Q^+$ and $\beta = E^{(n)}(\alpha)$. Then the distribution of subsequences of β of length l is uniform. ■

The theorem states that if we have arbitrary sequence of sufficiently large length and if we apply n times the transformation E on the sequence, then every subsequence of length not greater than n will have uniform distribution in the resulting sequence. This provides a natural behavior of the pseudo random subsequences of length not greater than n. However, subsequences of length greater than n must not necessarily be uniformly distributed.

This means, that we can apply the transformation E sufficiently many times on a large sequence of elements and we can expect QPRSG with a suitable period to be produced. We will present experimental data that shows the growth of the period of the QPRSG depending on the quasigroup and the times of application of transformation E.

4 Pseudo Random Sequence Generator Using Quasigroup Processing

One possible implementation of the QPRSG is shown on Figure 1.

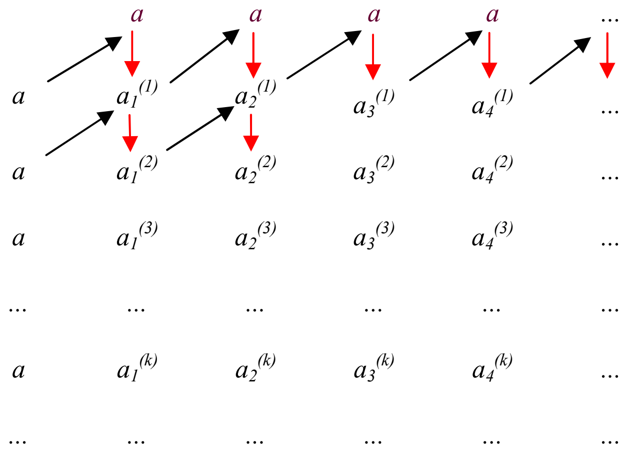

a a a a ...
a $a_1^{(1)}$ $a_2^{(1)}$ $a_3^{(1)}$ $a_4^{(1)}$ ...
a $a_1^{(2)}$ $a_2^{(2)}$ $a_3^{(2)}$ $a_4^{(2)}$ ...
a $a_1^{(3)}$ $a_2^{(3)}$ $a_3^{(3)}$ $a_4^{(3)}$ ...
... ...
a $a_1^{(k)}$ $a_2^{(k)}$ $a_3^{(k)}$ $a_4^{(k)}$ ...
... ...

Figure 1: Implementation of a PRSG using quasigroup processing

The element a is an arbitrary element of the quasigroup Q such that $a*a \neq a$. The sequence $a_1^{(1)} a_2^{(1)} a_3^{(1)} \ldots$ is obtained as $E_a (aaa\ldots)$. The sequence $a_1^{(p+1)} a_2^{(p+1)} a_3^{(p+1)} \ldots$ is obtained as

$$E_a^{(p+1)}\ (aaa...) = E_a\ (a_1^{(p)}\ a_2^{(p)}\ a_3^{(p)}...)\ . \qquad (4)$$

The pseudo random sequence is $a_1^{(k)}a_2^{(k)}a_3^{(k)}...$, where k is large enough.

The following theorem proved in [3] shows the relation between the times of application of the transformation E and the period growth of the QPRSG.

Theorem 2: Let α be a sequence of k elements. If the period of $E_a(\alpha)$ is p_0, then the sequences $E_a^{(s)}(\alpha)$ are periodical with periods p_{s-1} correspondingly, all of which are multiples of p_0. The periods satisfy the law $p_{p_{s-1}} > p_{s-1}$ for each s ≥ 1. ■

Thus, it is reasonable to expect that not all quasigroups provide the same period of the QPRSG. According to the theorem we can easily observe that the period growth of the QPRSG is at least linear.

However, experimental results show that exist quasigroups which increase the period of the QPRSG with each application of the transformation E. Hence, we can obtain exponential period growth of the QPRSG using these quasigroups.

5 Choosing Suitable Quasigroups

We have experimentally discovered that the choice of the quasigroup has a great effect on the performance of the QPRSG. Every quasigroup has a coefficient of period growth, which represents how many times the period has grown (in average) after one application of the transformation E. It is obvious that the ideal coefficient of period growth is at most the order of the quasigroup. Thus, ideally, if we apply the transformation $E^{(k)}$ on the quasigroup of order n, then the pseudo random sequence will have a period n^k. This implies that we can obtain a PRSG with arbitrary period by choosing suitable k [3].

For example, if the quasigroup has order 10 and the transformation is applied 100 times, then a PRSG with a period of 10^{100} can be obtained in the ideal case. We measured the average of the coefficient of period growth for quasigroups of orders 5, 6, 7, 8, 9 and 10. The values of the coefficients of period growth were grouped into 20 equal intervals as presented on Figure 2.

We used 2^{16} randomly chosen quasigroups for each order and the average of the coefficient of period growth was measured from seven consecutive applications of the transformation E. None of the quasigroups satisfies the equation $a*a=a$, which means that we have reduced the number of all possible quasigroups by a fraction reversely proportional to the order of the quasigroup. For example, 20% of the quasigroups of order 5 are eliminated, but only 10% of the quasigroups of order 10. The elements of a quasigroup of order n are in the set {0, 1, …, n-1}. We take a = 0 for all statistics and the starting array is $aaa...$ = 000….

The observed statistics are quite optimistic. Over 50% of the quasigroups have coefficient of period growth greater than half of their order. Although the fraction of quasigroups with almost ideal coefficient of period growth is relatively small, the fact that such quasigroups do exist provides good background for a QPRSG that has large periods for relatively small number of applications of the transformation E.

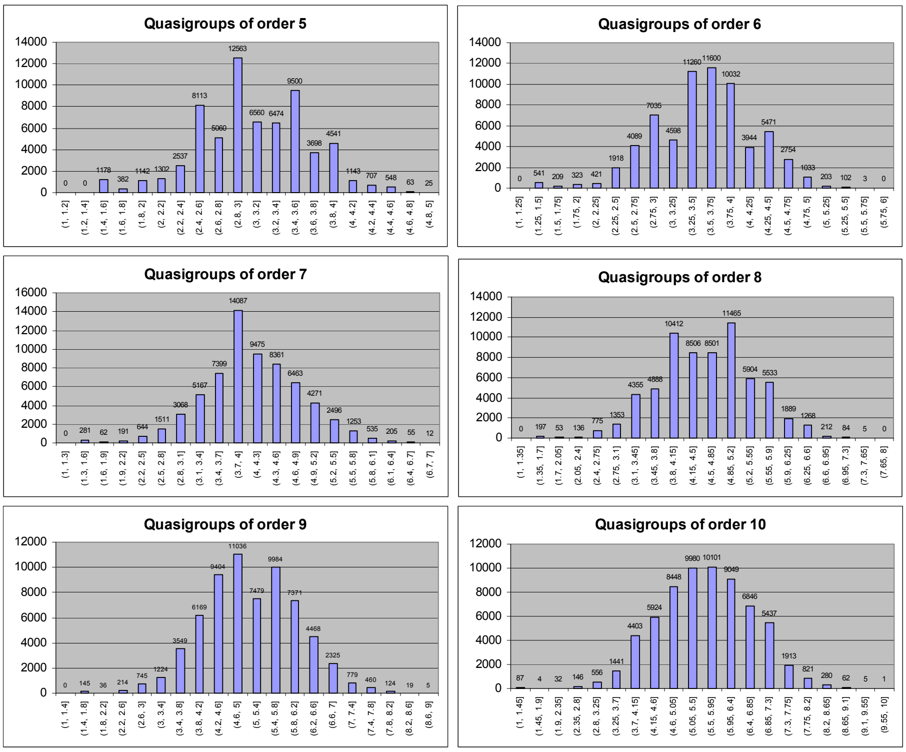


Figure 2: Distribution of the coefficient of growth for quasigroups of various orders

We notice big difference in the number of quasigroups with high coefficient of period growth. For example, we obtained 25 quasigroups of order 5 that have coefficient of period growth between 4.8 and 5, but only 6 quasigroups of order 10 whose coefficient of period growth is between 9.1 and 10. The main reason for this behavior is the number of quasigroups of different order.

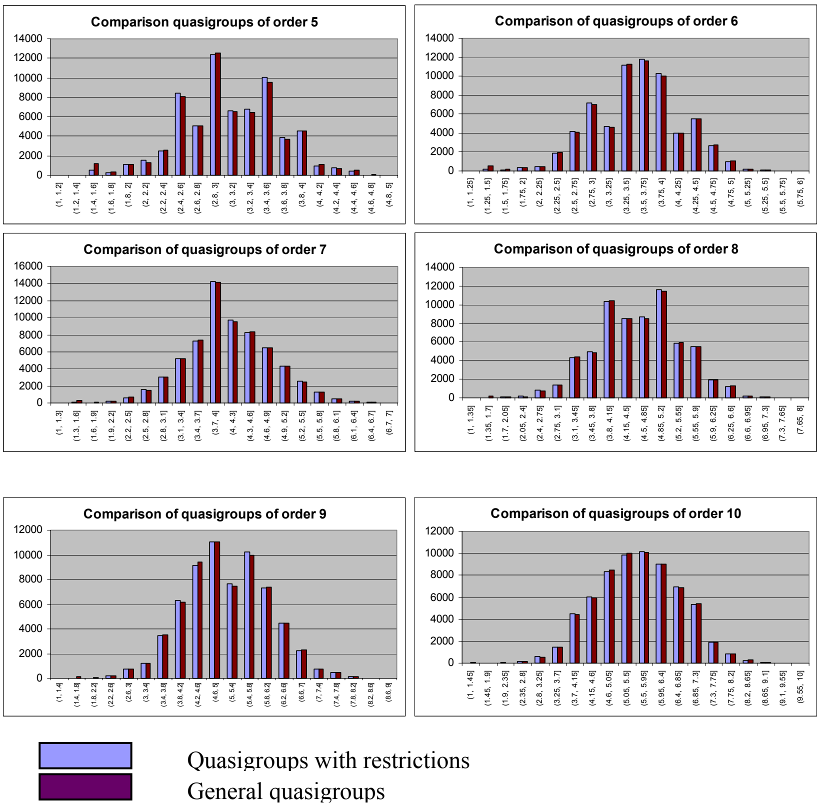
For example, there are about 160000 quasigroups of order 5, and over 10^{30} quasigroups of order 10, but we took equal samples of 2^{16} quasigroup of order 5 and 10. Obtaining proportional samples was computationally infeasible.

We may argue that a relatively small percentage (less than 0.00001%) of the quasigroups has almost ideal coefficient of period growth (i.e. less than 5% of the ideal coefficient). However, this is enough if we consider that the number of quasigroups increases with great speed as the order of the quasigroup increases. If we consider the previous example, the number of quasigroups increased more than 10^{24} times (from 160000 to 10^{30}) and the order of the quasigroup increased only 2 times (from 5 to 10).

In order to approve the coefficient of period growth of the quasigroups we introduced the following restrictions on the quasigroups:

$$(\forall u, v \in Q)\,(u * u \neq u \quad \& \quad u * v \neq u \quad \& \quad u * v \neq v)\,. \tag{6}$$

After gathering statistical data in the same manner as before we compared the new results with the previous as presented on Figure 3.


Comparison quasigroups of order 5

Comparison of quasigroups of order 6

Comparison of quasigroups of order 7

Comparison of quasigroups of order 8

Comparison of quasigroups of order 9

Comparison of quasigroups of order 10

Figure 3: Comparison of the coefficients of period growth between general quasigroups and quasigroups with restrictions.

We observe that the behavior of the coefficients of the period growth has not changed significantly. Some improvements can be noticed in the manner of reduced number of quasigroups with very low coefficient of period growth. This is noticeable for the quasigroups with low orders.

However, there is no considerable gain by applying the suggested restrictions on the quasigroups. Future work may suggest better classification of the quasigroups which may improve the coefficient of period growth.

6 Examples of Quasigroups with High Coefficient of Period Growth

The quasigroups presented on Figure 4 have almost ideal coefficient of period growth after 7 consecutive applications of the transformation E. Note that this results are obtained for seven consecutive applications of the transformation E. By further application of the transformation the coefficient of period growth will change.

Quasigroups with high coefficient of period growth

order 5, coef. per. growth 4.71

	0	1	2	3	4
0	1	0	4	3	2
1	3	2	1	0	4
2	4	3	0	2	1
3	0	1	2	4	3
4	2	4	3	1	0

order 6, coef. per. growth 5.57

	0	1	2	3	4	5
0	1	0	2	4	3	5
1	2	4	0	3	5	1
2	3	1	4	5	2	0
3	4	2	5	0	1	3
4	5	3	1	2	0	4
5	0	5	3	1	4	2

order 7, coef. per. growth 7

	0	1	2	3	4	5	6
0	1	4	5	3	0	2	6
1	4	0	1	2	3	6	5
2	0	3	6	5	1	4	2
3	2	1	3	6	5	0	4
4	3	2	4	0	6	5	1
5	5	6	2	1	4	3	0
6	6	5	0	4	2	1	3

order 8, coef. per. growth 7.57

	0	1	2	3	4	5	6	7
0	3	1	0	4	7	6	5	2
1	5	7	6	2	1	3	4	0
2	2	3	5	6	0	4	1	7
3	7	4	1	0	2	5	3	6
4	0	2	3	5	6	1	7	4
5	1	6	7	3	4	0	2	5
6	6	5	4	7	3	2	0	1
7	4	0	2	1	5	7	6	3

order 9, coef. per. growth 8.86

	0	1	2	3	4	5	6	7	8
0	6	0	8	4	1	5	2	3	7
1	2	3	6	7	5	1	0	8	4
2	5	8	1	2	0	4	3	7	6
3	1	6	2	5	7	0	8	4	3
4	8	7	3	0	6	2	4	1	5
5	7	4	5	1	3	8	6	2	0
6	3	1	4	6	8	7	5	0	2
7	4	5	0	8	2	3	7	6	1
8	0	2	7	3	4	6	1	5	8

order 10, coef. per. growth 9.43

	0	1	2	3	4	5	6	7	8	9
0	1	2	6	5	0	3	8	7	4	9
1	3	0	1	8	5	7	9	4	2	6
2	9	7	4	6	2	8	3	5	0	1
3	6	8	3	4	1	0	7	2	9	5
4	7	1	5	0	8	2	4	9	6	3
5	8	6	0	2	9	1	5	3	7	4
6	2	3	7	9	6	4	0	1	5	8
7	4	9	8	1	7	5	6	0	3	2
8	0	5	9	3	4	6	2	8	1	7
9	5	4	2	7	3	9	1	6	8	0

Figure 4: Examples of quasigroups with very high coefficients of period growth

7 Security and Efficacy of the QPRSG

The QPRSG is cryptographically secure PRSG if the quasigroup used to build the generator remains unknown. This follows from Theorem 2 proved in [5] for finding a quasigroup of a given QPRSG. Namely, one needs to make at last at many trials as there are quasigroups of order n in order to seek out the seed of the generator.

For examples, if QPRSG employs quasigroup of order 10, then more than 10^{30} trials are made to discover the quasigroup, which is a computationally infeasible problem. As an illustration, we may use quasigroups of order 256 (if 10 is not sufficiently large) where the number of trial increases to 10^{60000}. If quasigroup is known, than the PRSG is cryptographically non-secure generator [5].

In order to assess the efficacy of the QPRSG we took two different quasigroups of order 16 as presented on Figure 5. The first quasigroup has a coefficient of period growth about 1.6 and the second quasigroup has a coefficient of period growth about 15.4 for 5 applications of the transformation.

Quasigroup of order 16 with very low coefficient of period growth 1.6 for 5 applications of the transformation															
8	6	14	5	15	7	1	0	13	11	3	9	10	4	2	12
5	7	13	1	0	6	11	4	9	2	10	3	14	15	12	8
3	5	10	2	1	9	14	11	8	12	4	6	7	0	13	15
14	13	4	12	2	10	3	7	5	15	0	11	1	8	6	9
7	1	2	10	12	13	6	9	0	14	15	4	11	3	8	5
6	12	5	7	8	14	4	10	15	1	2	13	0	9	11	3
4	0	1	9	11	8	10	15	2	6	5	12	13	14	3	7
11	4	7	6	5	3	8	2	10	0	13	15	9	12	14	1
0	14	3	15	13	4	2	1	11	9	6	8	12	5	7	10
10	9	6	11	4	5	0	3	14	7	12	1	8	13	15	2
13	15	12	0	10	2	9	14	6	4	8	7	3	1	5	11
2	3	15	13	6	11	5	8	12	10	9	14	4	7	1	0
15	10	8	4	9	12	7	6	1	3	14	2	5	11	0	13
9	2	0	14	7	1	13	12	3	8	11	5	15	10	4	6
1	11	9	8	3	15	12	5	4	13	7	0	2	6	10	14
12	8	11	3	14	0	15	13	7	5	1	10	6	2	9	4

Quasigroup of order 16 with very high coefficient of period growth 15.4 for 5 applications of the transformation															
8	0	3	15	9	14	10	12	11	4	2	7	6	1	5	13
3	8	2	6	14	12	15	9	4	0	5	1	13	7	10	11
0	5	14	8	1	4	2	10	13	11	7	3	9	15	12	6
11	1	12	7	0	10	4	2	6	3	8	15	14	9	13	5
6	10	1	3	12	2	7	15	5	14	9	4	11	13	0	8
4	2	15	1	7	0	3	8	14	9	13	10	5	6	11	12
9	4	11	10	3	6	0	13	15	5	12	8	1	14	7	2
12	6	4	9	2	13	11	5	7	10	1	14	3	0	8	15
5	11	8	2	13	15	6	14	3	12	0	9	7	4	1	10
13	3	9	5	15	8	1	6	2	7	11	0	12	10	4	14
15	9	10	11	6	1	12	7	0	2	14	13	8	5	3	4
7	15	5	13	10	9	8	4	12	1	3	6	2	11	14	0
2	7	13	14	8	3	5	0	9	15	10	11	4	12	6	1
10	14	0	12	11	7	13	1	8	6	4	5	15	3	2	9
1	13	6	4	5	11	14	3	10	8	15	12	0	2	9	7
14	12	7	0	4	5	9	11	1	13	6	2	10	8	15	3

Figure 5 Quasigroups used for the Diehard statistical test for randomness

In order to pass the Diehard statistical tests [10] the QPRSG constructed with the first quasigroup had to perform at least 16 applications of the transformation. The QPRSG that employed the second quasigroup required only 7 applications of the transformation.

The QPRSG obtained with the first quasigroup takes twice more operations than the QPRSG obtained with the second quasigroup. Thus, the efficacy of the QPRSG is greatly affected by the choice of the quasigroup.

8 Conclusion

In this paper we investigated a new type of PRSG [3,5]. We gave the required background and one possible implementation of a QPRSG. The implementation of PRSG using quasigroup processing is highly scalable and fairly unpredictable. It has passed all publicly available random sequence generator tests.

It was shown that the performance of the PRSG depends on the order of the quasigroup used and the number of applications of the quasigroup transformation. We introduced a new property of the quasigroups called coefficient of period growth. The period of the QPRSG depends greatly of this coefficient.

Although we applied some restrictions on the quasigroups, it was not possible to significantly improve the coefficient of period growth. In any case, there is experimental evidence that there exist enough quasigroups that provide exponential growth of the QPRSG. Thus, it is possible to approximate an ideal PRSG with great success, since we can obtain QPRSG with arbitrary large periods.

Acknowledgements

We would like to thank Prof. Smile Markovski for his useful comments and guidelines.

References

[1] Dènes J., Keedwell A.D.: "*Latin Squares and their Applications*", English University Press. (1974)

[2] Knuth D.: "*The Art of Computer Programming, Volume 2*", Addison-Wesley, (1977)

[3] Markovski S.: "Quasigroup String Processing and Applications in Cryptography", *Proceedings 1st Conference of Mathematics and Informatics for Industry*, Thessaloniki, Greece, (2003) 278-290

[4] Markovski S., Gligoroski D., Bakeva V.: "Quasigroup and Hash Functions", In: Discrete Mathematics and Applications, Sl. Shtrakov and K. Denecke (eds.), *Proceedings 6th ICGMA Conference*, Bansko (2001), pp. 43-50

[5] Markovski S., Gligoroski D., Bakeva V.: "Quasigroup String Processing – Part 1", Contributions, *Sec. math. Tech. Sci.,* MANU, XX, 1-2(1999) 13-28

[6] Markovski S., Kusakatov V.: "Quasigroup String Processing – Part 2", Contributions, *Sec. math. Tech. Sci*., MANU, XXI, 1-2 (2000) 15-32

[7] Menezes A., van Oorschot P., Vanstone S.: "*Handbook of Applied Cryptography*", CRC Press, (1996)

[8] Stinson R. D.: "*Cryptography -Theory and Practice*", CRC Press (1995)

[9] http://random.mat.sbg.ac.at : A Server on the Theory and Practice of Random Number Generation

[10] ftp://stat.fsu.edu/pub/diehard