Large Quasigroups in Cryptography and their Properties Testing

Jiří Dvorský, Eliška Ochodková, Václav Snášel
Department of Computer Science,
VŠB - Technical University of Ostrava
17. listopadu 15, 708 33
Ostrava-Poruba, Czech Republic
{jiri.dvorsky,eliska.ochodkova,vaclav.snasel}@vsb.cz

Ajith Abraham
Center of Excellence for Quantifiable
Quality of Service, Norwegian
University of Science and Technology
O.S. Bragstads plass 2E,
N-7491 Trondheim, Norway
ajith.abraham@ieee.org

***Abstract*—One of the current trends in cryptography is to search for new approaches to the cryptographic algorithms design. One such possibility is to use the other algebraic structures, such as a quasigroup, rather than the traditional. Quasigroups are equivalent to more familiar Latin squares. One of quasigroups' important properties is that all possible elements of certain quasigroup occur with equal probability. Testing properties of quasigroups of a large order isn't trivial, effective methods are necessary. There are described statistical experiments on various types of data, on various types of guasigroups in this paper; experiments were done within a framework of a simple quasigorup hash function. The distribution of hash value's changes, for given quasigroup and for given testing data, with respect to bit change in them and with respect to the positions of changed bits were measured.**

I. Introduction

Quasigroups, or more famous Latin squares, are well known combinatorial designs with a lot of theoretical results concerning them. Researchers have focused in quasigroups usage in the cryptography more seriously from the beginning of century, e.g. [1], [7], [10]. There were published many cryptographic algorithms based on quasigroups primitives, from simple till more ambitious ones.

For cryptographic purposes quasigroups have to be of a good quality. By a quasigroup of a high cryptographic quality we mean foremost a non-commutative, non-associative, nonidempotent quasigroup without right or left units and without proper sub-quasigroups. Such a quasigroup is named as shapeless quasigroup in [5], where the length of period of obatined word generated by so called quasigroup string transformation is tested.

Various approaches are used for the good quality quasigroup generation. It is possible to use quasigroups of a small order represented as a look-up table only, whose properties may by verified by the exhaustive search. There is proposed stream cipher Edon80 [8] as an eSTREAM[1] candidate. The cipher Edon80 uses quasigroup of order 4. Principle of the selection appropriate quasigroups of order 4 is described in [11].

One common way of creating quasigroups is through isotopies. We can imagine an isotopism of quasigroups as a permutation of rows and columns of quasigroups multiplication table. Permutations used in the concept of isotopism may be done in many ways. Authors of NISTs SHA-3 competition[2] candidate, hash function Edon$\mathcal{R}$, have used high-quality Latin squares of order 8 for constructing the permutations on 256-bit words and these permutations are then used for the quasigroup of order 2^{256} construction [6].

The goal of this paper is to introduce a method for huge quasigroups properties testing. What is meant about quasigroups of large order depends mainly on cryptographic algorithm and its other memory requirements. We present statistical tests, which should reflect algebraic properties of the tested quasigroups. We are not engaged in resistance against differential or linear cryptanalysis. Previous experiments were published in [15], [13]. There were used two types of quasigroups, the table quasigroup and analytic one; their properties were tested by analyzing values of a simple hash function based on quasigroup operation. We have conducted the same experiments with additive group $(\mathbb{Z}_n, +)$.

The organization of the paper is as follows: in section 2 we give brief introduction to the math concepts used in the paper. Experiments, tested data and quasigroups are presented in section 3. In section 4 we describe experiments results. Finally in last section we give conclusions and future research directions.

II. Mathematical background

Definition 2.1: A grupoid $(Q, *)$ is said to be a quasigroup (i.e. algebra with one binary operation $(*)$ on the set Q) satisfying the law:

$$\forall(u, v \in Q)(\exists! x, y \in Q)(u * x = v \wedge y * u = v).$$

This implies:

1) $x * y = x * z \vee y * x = z * x \Rightarrow y = z$
2) The equations $a * x = b, y * a = b$ have an unique solutions x, y for each $a, b \in Q$.

Quasigroups are equivalent to the well known Latin

[1] http://www.ecrypt.eu.org/stream/

[2] http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

978-1-4244-5612-3/09/$26.00 ©2009 IEEE

squares[3]. The multiplication table of a quasigroup of order n is a Latin square of order n, and conversely every Latin square of order n is the multiplication table of a quasigroup of order n [4]. However, in general, the operation $(*)$ is neither a commutative nor an associative operation. As is known, every quasigroup satisfying the associative law has an identity element and is, hence, a group, e.g. a group is, by definition, an associative loop.

Definition 2.2: A loop is a quasigroup $(Q, *)$ with an identity element $e \in Q$ such that:

$$(\exists e \in Q)(\forall x \in Q)(x * e = x = e * x).$$

While some Latin squares do represent associative operations and can form a group, most Latin squares do not. For example, at order 4 there are 576 Latin squares, but only 16 are associative (about 2.8 percent). So non-associative (and thus non-group) squares dominate heavily, and are desirable for cryptography anyway [4]. Also quasigroups with various identities seem to be problematic structures. Ideally, for cryptographic purposes quasigroup should be a shapeless quasigroup [5].

Definition 2.3: A quasigroup $(Q, \circ)$ of order n is said to be shapeless if it is non-commutative, non-associative, it does not have neither left nor right unit, it does not contain proper sub-quasigroups, and there is no $k < 2n$ for which are satisfied the identities of the kinds:

$$\underbrace{x \circ (\ldots (x}_{k} \circ y)) = y \quad \text{and} \quad y = ((y \circ \underbrace{x) \circ \ldots) \circ x}_{k}$$

If we work with quasigroups of large order, it is computationally infeasible (both in terms of space and in terms of time) to store the entire quasigroup and perform multiplication by a table lookup. This implies that we need to find a more efficient method for representing quasigroups of large order and performing multiplication within these quasigroups. One common way of creating quasigroups is through isotopism [4].

Definition 2.4: Let $(Q_1, \cdot)$ and $(Q_2, \circ)$ be two quasigroups with $|Q_1| = |Q_2|$. An ordered triple (α, β, γ) of one-to-one mappings α, β, γ of the set Q_1 onto the set Q_2 is called an isotopism of Q_1 upon Q_2 if

$$\alpha(x) \circ \beta(y) = \gamma(x \cdot y) \tag{1}$$

for all $x, y \in G$.

It is also said that Q_2 is an isotope of a primary quasigroup Q_1. One can prove that the set of all isotopisms of a quasigroup of order n forms a group of order $(n!)^3$.

[3]Latin square is an $n \times n$ matrix filled with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column

It should be noted that the mapping γ permutes the elements in the table of operations in a quasigroup Q_1, while α and β operate on the elements of the row and column borders of this table, respectively. It simply means that the Cayley table of the quasigroup $(Q_2, \circ)$ can be obtained from the Cayley table of the quasigroup $(Q_1, \cdot)$, resp. vice versa, simply by rearranging rows, columns, and renaming elements. From (1) it follows that

$$x \circ y = \gamma^{-1}(\alpha(x) \cdot \beta(y)) \tag{2}$$

for all $x, y \in Q_2$.

There are several special quasigroups, where the quasigroup operation can be speciffied using common arithmetic operations. One such an example is the quasigroup of modular subtraction $(Q, \circ_{ms})$, which was propsed in [14]. The operation $\circ_{ms}$ on Q is defined as easy to evaluate expression:

$$x \circ_{ms} y = x + (n - y) \; mod \; n, \; n = |Q|. \tag{3}$$

This allows us to use quasigroups with a very large number of elements without necessity of their storage. Generally, if isotopies are used to create a quasigroup, the only information that needs to be stored are the permutations α, β and γ along with the group that is used to generate the quasigroup $(Q, \circ)$.

The quasigroups isotopic to groups (to abelian groups) form an important class of quasigroups. The well known subclasses of such quasigroups are medial quasigroups and T-quasigroups. Any commutative quasigroup is trivially a medial quasigroup. A nontrivial class of examples are T-quasigroups [2], [12].

Definition 2.5: A medial quasigroup is a quasigroup such that, for any choice of four elements $a, b, c, d \in Q$, one has $(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$.

Definition 2.6: A quasigroup $(Q, \circ)$ defined over an abelian group $(Q, +)$ by $x \circ y = \alpha(x) + \beta(y) + c$, where c is a fixed element of Q, α and β are both automorphisms of the group $(Q, +)$, is called a T-quasigroup.

By Toyoda theorem (T-theorem) [17] every medial quasigroup $(Q, \circ)$ is a T-quasigroup with additional condition that automorphisms α, β commute.

Testing properties of the large qausigroups is done through a simple hash function defined below.

Definition 2.7: Let $(Q, *)$ be a quasigroup and Q^+ be a set of all nonempty words formed by the elements $q_i \in Q$, $1 \leq i \leq n$. For a fixed $a \in Q$ let the hash function $h_a : Q \times Q^+ \to Q^+$ be defined as

$$h_a(q_1 q_2 \ldots q_n) = ((a * q_1) * q_2 * \ldots) * q_n.$$

III. The experiments

The aim of our experiments was to check empirically the characteristics of quasigroups by valuing the hash function based on the table quasigroups and on quasigroups defined

analytically. This experiments are an extension of published works [15], [13], where distribution of hash values, for given quasigroup and for given testing data were tested. The experiments are divided into following groups:

1) distribution of hash value's changes, for given quasigroup and for given testing data, with respect to single bit change in them,
2) distribution of positions of hash value's changes, for given quasigroup and for given testing data, with respect to single bit change in them.

A. Data used in test

There is need to select input data to perform experiments. Selected input data should have certain characteristics. Therefore, we have selected three types of input data, three files:

- *Words extracted from text*. Words were extracted from a .GOV collection of web pages WebTREC [9]. The original text size was approximately 18 gigabytes. The dictionary was drawn up from this text. The dictionary contains a total of 4319200 unique words. In following text, this file is referred as `webtrec`. This file is used to simulate hashing of text messages.
- *Random data*. As a source of random data have served first million digits of number π. This file was acquired from the Canterbury Compression Corpus [3]. In following text, this file is referred as `pi`. Changes of the whole file's hash value, when single bit was changed, will be examined on this file.
- *Completely regular data*. Here we have again used a file from Canterbury Compression Corpus. This file contains one hundred thousand characters 'a'. In following text, this file is referred as `aaa`. The file will be used in the same manner as `pi`.

B. Quasigroups used in tests

- *"Table quasigroup"* that comes from the quasigroup isotopic of quasigroup of modular subtraction (2) was the first type of quasigroup used in tests. The multiplication in such an isotopic quasigroup is defined through (3) as follows [15]:
$$a \circ b = \pi((\omega(a) + n - \rho(b)) \bmod n).$$
- *"Analytic quasigroup"* was the second quasigroup type. The operation $\circ$ in analytic quasigorup is defined as $x \circ y = (ax + by + c) \bmod n$, where $n = |Q|$ and $\gcd(a, n) = 1 = \gcd(b, n)$, a, b and c are integers (where $\gcd$ denotes a greatest common divisor). Then $Q_m = (\mathbb{Z}_n, \circ)$ is T-quasigroup over $\mathbb{Z}_n$ [16].

Quasigroups of following orders were used in our experiments:

- quasigroup of order 5003 defined by table and analytically,
- quasigroup of order 2^{16} defined analytically,
- quasigroup of order 2^{32} defined analytically[4].
- The (associative) additive group $(\mathbb{Z}_n, +)$, rather group $(\mathbb{Z}_{5003}, +)$ was used for comparison in test too. The additive group of integers $\bmod n$ satisfies Latin square law.

To compare properties of table quasigroups and analytic quasigroups, quasigroups of order 5003 were used. Simultaneously these quasigroups are used for testing quasigroups of prime order. Quasigroups of this order can be used as base of hash functions for hash table data structure. Quasigroups of order $64K$ and $4G$ were used to test large quasigroup with order equal to power of 2. These quasigroups are intended rather for the area of cryptography.

IV. Results of experiments

A. Changes of hash values – The number of changed bits

The first part of our experiment was to monitor changes in the hash values for the given hash function – quasigroup. The `webtrec` was used as input data in this case. The experiment was as follows:

1) Initialize of quasigroup[5] Q of order k.
2) For each input word w compute hash value $h_a(w)$.
3) Assume that binary representation of word w has l bits. Create l words w_i from word w such that i-th bit in word w is changed.
4) For each word w_i compute hash value $h_a(w_i)$ and measure Hamming distance between $h_a(w)$ and $h_a(w_i)$.

In the case of `pi` and `aaa` files, the whole file was considered as word w.

1) Ideal results: The ideal result of this experiment is to change half of bits in hash values when one bit is changed in the input. Histogram of Hamming distances in this case should copy the normal distribution.

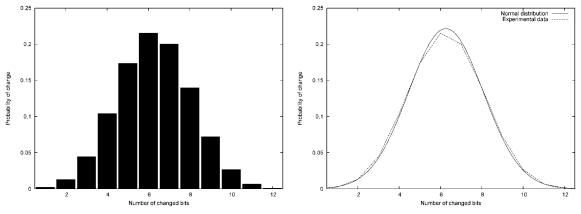
2) Experimental results: Charts in Figures 1, 3, and 5 show histograms of Hamming distances between original word hash value and hash value of word with one bit changed. X-axis represents the number of changed bits; y-axis represents the probability (relative frequency) of change of given number of bits.

Basic statistical results of this experiment are shown in Table I. Tables II, III, and IV show, that distribution of bit changes corresponds to 68-95-99.7 rule (three-sigma rule), with some exception in $[-\sigma, +\sigma]$ interval. Distribution of Hamming distances can be considered as normal distribution. From these tables, it is clear that table and analytic quasigroups of order 5003 provides almost identical results. The parameters μ and σ were used for normal distribution curve $N(\mu, \sigma^2)$ construction. We can graphically compare experimentally measured distribution curve and normal distribution curve $N(\mu, \sigma^2)$ in the charts 1. In all cases, we can see very good agreement between experiment and the ideal results, the theoretical results.

Completely different situation arises for the additive group $(\mathbb{Z}_{5003}, +)$. In the case of the file `webtrec` is the following

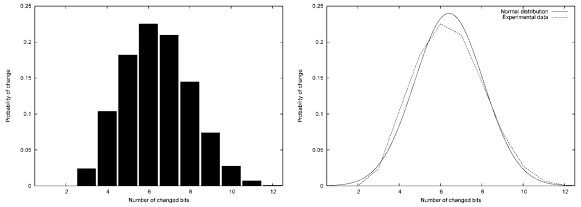
[4]Orders of these qusigroups will be referred as $64K$ and $4G$ in following text.

[5]In the case of the experiment with the group, create a group instead of quasigroup.



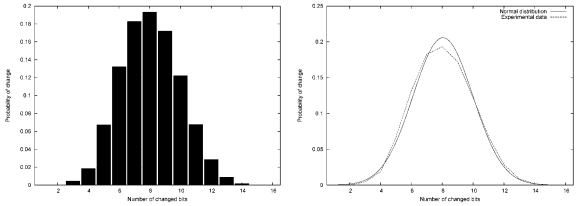
(a) Table quasigroup, order 5003

(b) Table quasigroup, order 5003



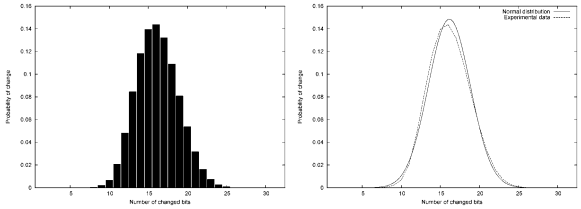
(c) Analytic quasigroup, order 5003

(d) Analytic quasigroup, order 5003



(e) Analytic quasigroup, order 64K

(f) Analytic quasigroup, order 64K



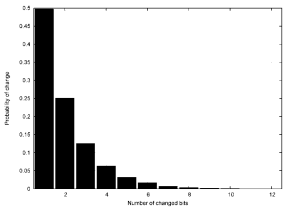
(g) Analytic quasigroup, order 4G

(h) Analytic quasigroup, order 4G

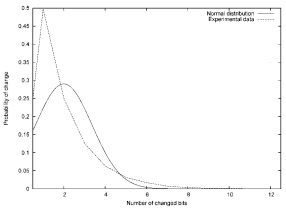
Fig. 1. Histogram of Hamming Distances – `webtrec`

situation. It hasn't good avalanche effect (when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip)). From the histogram 2(a) is quite clear that in half of the cases changed only one bit, in the quarter of the cases, only two bits. This illustrates the mean number of changed bits in Table I(a). Comparison with the normal distribution curve is shown in Figure 2(b). A significant deformation of distribution of changed bits can be seen there. Avalanche effect

A similar distortion of the histogram can be seen in the chart 4 for file `aaa`. From this chart it is clear that the hash value changed in the 25 % of cases either one or three bits. In the remaining 50 % of cases have changed exactly two bits. This is a substantial difference to the expected half of bits. In even 60 % of cases there has changed only one bit in the file `pi`, see Figure 6.

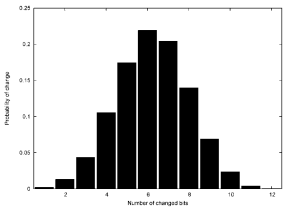


(a) Group $(\mathbb{Z}_{5003}, +)$

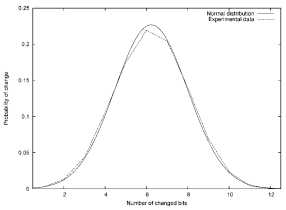


(b) Group $(\mathbb{Z}_{5003}, +)$

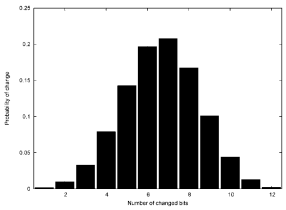
Fig. 2. Histogram of Hamming Distances – `webtrec`



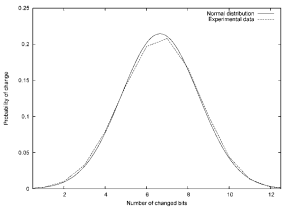
(a) Table quasigroup, order 5003



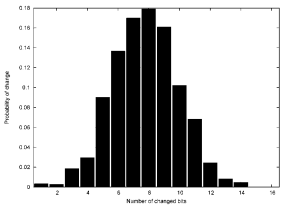
(b) Table quasigroup, order 5003



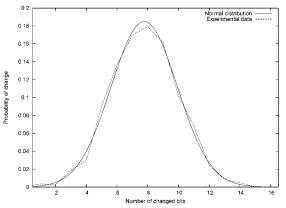
(c) Analytic quasigroup, order 5003



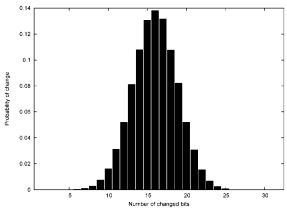
(d) Analytic quasigroup, order 5003



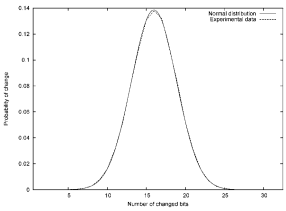
(e) Analytic quasigroup, order 64K



(f) Analytic quasigroup, order 64K

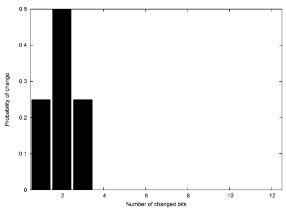


(g) Analytic quasigroup, order 4G

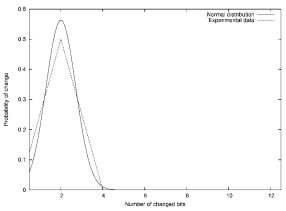


(h) Analytic quasigroup, order 4G

Fig. 3. Histogram of Hamming Distances – `aaa`



(a) Group $(\mathbb{Z}_{5003}, +)$



(b) Group $(\mathbb{Z}_{5003}, +)$

Fig. 4. Histogram of Hamming Distances – `aaa`

TABLE I
HAMMING DISTANCES — STATISTICAL EVALUATION

(a) webtrec

Quasigroup	Order	μ	σ
Table quasigroup	5003	6.263	1.800
Analytic quasigroup	5003	6.414	1.662
Analytic quasigroup	64K	8.043	1.938
Analytic quasigroup	4G	16.163	2.684
Group $(\mathbb{Z}_{5003}, +)$	5003	1.996	1.374

(b) aaa

Quasigroup	Order	μ	σ
Table quasigroup	5003	6.226	1.758
Analytic quasigroup	5003	6.654	1.859
Analytic quasigroup	64K	7.771	2.156
Analytic quasigroup	4G	15.979	2.877
Group $(\mathbb{Z}_{5003}, +)$	5003	2.000	0.707

(c) pi

Quasigroup	Order	μ	σ
Table quasigroup	5003	6.197	1.756
Analytic quasigroup	5003	6.150	1.722
Analytic quasigroup	64K	7.692	2.065
Group $(\mathbb{Z}_{5003}, +)$	5003	1.925	1.243

TABLE II
CONFIDENCE INTERVALS, WEBTREC

(a) Table quasigroup, 5003

Confidence interval	Percentage
$[-\sigma, \sigma]$	72.895
$[-2\sigma, 2\sigma]$	94.986
$[-3\sigma, 3\sigma]$	99.888

(b) Analytic quasigroup, 5003

Confidence interval	Percentage
$[-\sigma, +\sigma]$	76.205
$[-2\sigma, +2\sigma]$	94.006
$[-3\sigma, +3\sigma]$	99.882

(c) Analytic quasigroup, 64K

Confidence interval	Percentage
$[-\sigma, +\sigma]$	54.818
$[-2\sigma, +2\sigma]$	93.738
$[-3\sigma, +3\sigma]$	99.781

(d) Analytic quasigroup, 4G

Confidence interval	Percentage
$[-\sigma, +\sigma]$	64.292
$[-2\sigma, +2\sigma]$	96.286
$[-3\sigma, +3\sigma]$	99.824

(e) Group $(\mathbb{Z}_{5003}, +)$

Confidence interval	Percentage
$[-\sigma, +\sigma]$	87.386
$[-2\sigma, +2\sigma]$	93.752
$[-3\sigma, +3\sigma]$	98.676

TABLE III
CONFIDENCE INTERVALS, AAA

(a) Table quasigroup, 5003

Confidence interval	Percentage
$[-\sigma, \sigma]$	59.825
$[-2\sigma, 2\sigma]$	95.629
$[-3\sigma, 3\sigma]$	99.957

(b) Analytic quasigroup, 5003

Confidence interval	Percentage
$[-\sigma, +\sigma]$	71.490
$[-2\sigma, +2\sigma]$	97.221
$[-3\sigma, +3\sigma]$	99.780

(c) Analytic quasigroup, 64K

Confidence interval	Percentage
$[-\sigma, +\sigma]$	64.697
$[-2\sigma, +2\sigma]$	96.191
$[-3\sigma, +3\sigma]$	99.659

(d) Analytic quasigroup, 4G

Confidence interval	Percentage
$[-\sigma, +\sigma]$	61.622
$[-2\sigma, +2\sigma]$	94.578
$[-3\sigma, +3\sigma]$	99.707

(e) Group $(\mathbb{Z}_{5003}, +)$

Confidence interval	Percentage
$[-\sigma, +\sigma]$	50.000
$[-2\sigma, +2\sigma]$	100.000
$[-3\sigma, +3\sigma]$	100.000

TABLE IV
CONFIDENCE INTERVALS, PI

(a) Table quasigroup, 5003

Confidence interval	Percentage
$[-\sigma, \sigma]$	60.069
$[-2\sigma, 2\sigma]$	95.733
$[-3\sigma, 3\sigma]$	99.960

(b) Analytic quasigroup, 5003

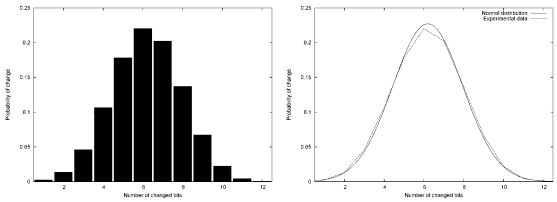
Confidence interval	Percentage
$[-\sigma, +\sigma]$	61.201
$[-2\sigma, +2\sigma]$	96.202
$[-3\sigma, +3\sigma]$	99.980

(c) Analytic quasigroup, 64K

Confidence interval	Percentage
$[-\sigma, +\sigma]$	68.776
$[-2\sigma, +2\sigma]$	95.316
$[-3\sigma, +3\sigma]$	99.442

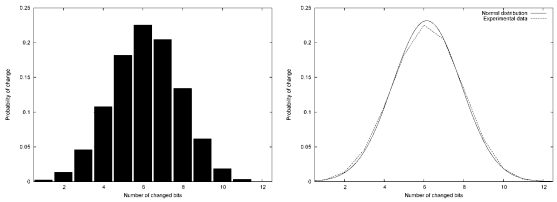
(d) Group $(\mathbb{Z}_{5003}, +)$

Confidence interval	Percentage
$[-\sigma, +\sigma]$	77.501
$[-2\sigma, +2\sigma]$	100.000
$[-3\sigma, +3\sigma]$	100.000



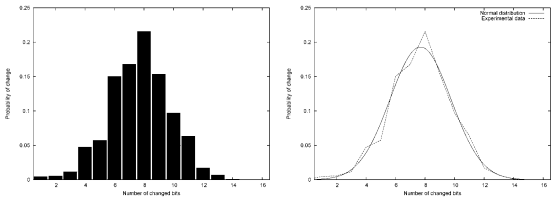
(a) Table quasigroup, order 5003

(b) Table quasigroup, order 5003



(c) Analytic quasigroup, order 5003

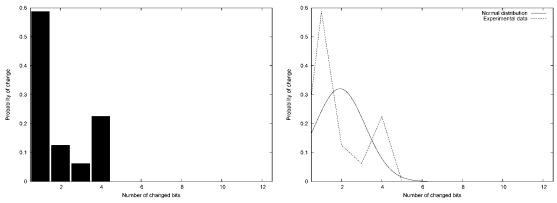
(d) Analytic quasigroup, order 5003



(e) Analytic quasigroup, order 64K

(f) Analytic quasigroup, order 64K

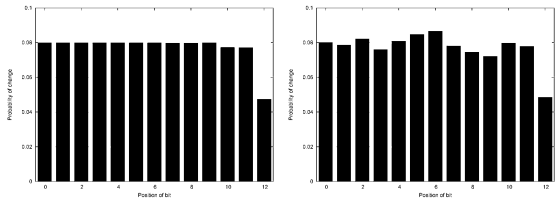
Fig. 5. Histogram of Hamming Distances – `pi`



(a) Group $(\mathbb{Z}_{5003}, +)$

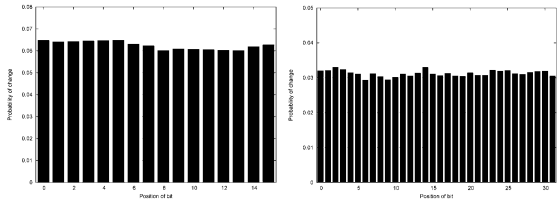
(b) Group $(\mathbb{Z}_{5003}, +)$

Fig. 6. Histogram of Hamming Distances – `pi`



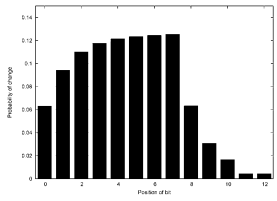
(a) Table quasigroup, order 5003

(b) Analytic quasigroup, order 5003



(c) Analytic quasigroup, order 64K

(d) Analytic quasigroup, order 4G



(e) Group $(\mathbb{Z}_{5003}, +)$

Fig. 7. Histogram of bits' positions changes – `webtrec`

B. Changes of hash values – Positions of changed bits

In the experiment described in section IV-A, Hamming distance was used to measure the change of hash value. In this experiment, we examine changes in individual bit positions of binary representations of hash value. Experiment was the same way, only in the last step positions of changed bits were recorded instead of their number.

1) Ideal results: The ideal result of this experiment is equal probability of bit's change at all positions. Histogram of changed positions should copy the uniform distribution.

2) Experimental results: Charts 7, 8, and 9 show the resulting histograms of the probability of a bit changes between the hash value of the original word and word with the inverted bit. X-axis represents the position of changed bits, while Y-axis represents the probability (relative frequency) of change of bit at given position. All of these charts show good concordance between the results of the experiment and the expected uniform distribution. Anomaly shows only the last bit of quasigroup of order 5003. It is due to the fact that the 12-th bit can change only for hash values greater than $2^{12} = 4096$. When the order of quasigroup is power of 2, this problem does not occur.

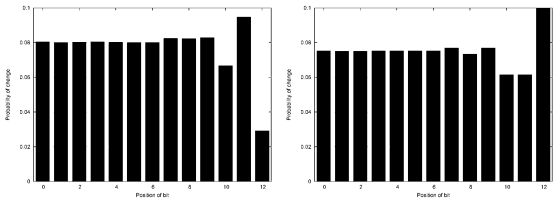
In the case of the file `webtrec`, we tested the group $(\mathbb{Z}_{5003}, +)$. The results are shown in the chart 7(e). It is clearly visible non-uniformity of changes in individual bits from the chart – the bits in the middle of the binary representations of hash values have changed frequently, marginal bits have changed very little.

In the case of the file `aaa` positions of changed bits can be divided into several groups, see chart 8(e). The first group consists of the most frequently changed bit – the 7^{th} is changed with probability 18.75 %. The second group contains bits at positions 1, 2, 3, 5 and 6, probability of change is 12.5 % in this group. Bits 0, 4, and 8 are changed with the smallest probability. Bits at positions 9 to 12 does not change at all!

The situation of the file `pi` is a similar as in the case of file `aaa`. Changed bits' position are spread evenly in this case, see chart 9(d), due to the random nature of the data in this file.

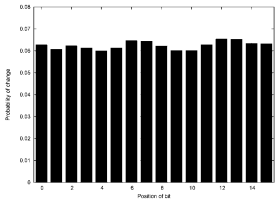
V. Conclusions

Examination various characteristics of small quasigroups, e.g. of order 4, is easy, it can be done by exhaustive search. The goal of our research is to find a way of testing statistical properties of large quasigroups and to explore the interpretation of experimental results. We've reported two types of

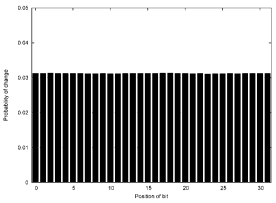


(a) Table quasigroup, order 5003

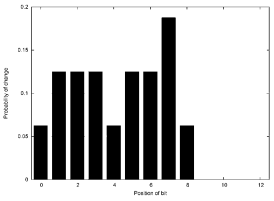
(b) Analytic quasigroup, order 5003



(c) Analytic quasigroup, order 64K

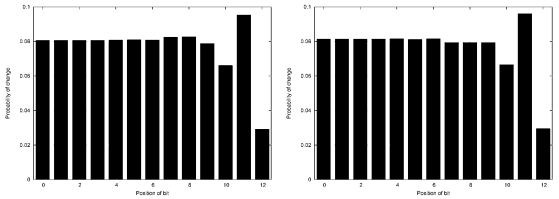


(d) Analytic quasigroup, order 4G



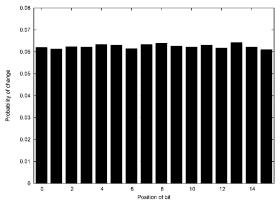
(e) Group $(\mathbb{Z}_{5003}, +)$

Fig. 8. Histogram of bits' positions changes – `aaa`

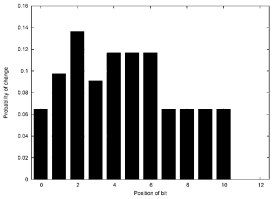


(a) Table quasigroup, order 5003

(b) Analytic quasigroup, order 5003



(c) Analytic quasigroup, order 64K



(d) Group $(\mathbb{Z}_{5003}, +)$

Fig. 9. Histogram of bits' positions changes – `pi`

experiments conducted and their results in this paper – the distribution of hash value's changes, for given quasigroup and for given testing data, with respect to bit change in them and with respect to the positions of changed bits. We try to find the relationship between our results and known algebraic properies of used quasigroups.

Different data sets were chosen for testing, from the regular to random one; we wanted to capture the impact of their structure on the hash function value. Various types of quasigroups were used, quasigroup of prime order 5003 and quasigroups representing the class of quasigroups of order 2^n. Two kinds of quasigroups generation were used, resulting quasigroups were named table and analytical qoausigroup. Results of our experiments are shown in the graphs and tables. We used group $(\mathbb{Z}_{5003}, +)$ for comparison, which represents quasigroup with bad cryptographic quality. The influence of algebraic properties (associativity etc.) of compared group $(\mathbb{Z}_{5003}, +)$ is clearly evident on the charts. The deformations of histograms of bits positions and the deformations of resulting curves representing distributions of hash function value for group are evident, while the results for the quasigroups are close to normal distribution, i.e. are a kind of ideal results.

REFERENCES

[1] L. Bao. Mals: Multiple access scheduling based on latin squares. 1:315–321, 2004.

[2] V. D. Belousov. *Foundations of the Theory of Quasigroups and Loops.* Nauka, , 196.

[3] R. Arnold and T. Bell. A corpus for evaluation of lossless compression algorithms. In *Proceedings Data Compression Conference*, 1997, http://corpus.canterbury.ac.nz

[4] J. Dénes and A. Keedwell. *Latin Squares and their Applications*. Akadémiai Kiadó, Budapest, Academic Press, New York, 1974.

[5] D. Gligoroski, S. Markovski, L. Kocarev. EdonR, An Infinite Family of Cryptographic Hash Functions. *International Journal of Network Security,* Vol. 8 (3) pp. 293-300, 2009

[6] D. Gligoroski and et al. EdonR cryptographic hash function. *Submition to NIST's SHA-3 hash function competition, http://csrc.nist.gov/groups/ST/hash/sha-3/index.html*, 2008.

[7] D. Gligoroski and S. Markovski. Cryptographic potentials of quasigroup transformations. Talk at EIDMA Cryptography Working Group, Utrecht, 2003.

[8] D. Gligoroski, S. Markovski, L. Kocarev, and M. Gusev. Stream cipher edon80. *eSTREAM candidate, http://www.ecrypt.eu.org/stream/*, 2005.

[9] D. Harman, editor. *The Forth REtrieval Conference (TREC-4)*. NIST, 1997.

[10] J. Kong. The role of latin square in cipher systems: Matrix approach to model encryption modes of operation. UCLA Computer Science Department Technical Report CSTR030038, 2008.

[11] S. Markovski, D. Gligoroski, and J. Markovski. Classification of quasigroups by random walk on torus. *Journal of Applied Mathematics and Computing*, 19(1-2):57–75, March 2005.

[12] P. Nemec and T. Kepka. T-quasigroups. Part I. *A*cta Universitatis Carolinae, Math. et Physica, Vol. 12, No. 1, pp. 3949, 1971

[13] E. Ochodková, J. Dvorský and V. Snášel. Testing the Properties of Large Quasigroups. In proceedings ICUMT 2009, http://www.icumt.org/cfp.html.

[14] E. Ochodková, J. Dvorský and V. Snášel. Generation of large quasigroups: An application in cryptography. In *Arbeitstagung Allgemeine Algebra-Workshop on General Algebra*, Olomouc, 2002.

[15] E. Ochodková and V. Snášel. Cryptographic Algorithms with Uniform Statistics. In *NATO Regional Conference on Military Communications and Informations Systems*, pp. 165-172, Zegrze, Poland, 2001.

[16] R. H. Schulz. *Codierungstheorie*. Vieweg Verlag, 1991.

[17] K. Toyoda. On axioms of linear functions. *Proc. Imp. Acad. Tokyo*, 17:221227, 1941.