Bulletin of the *Transilvania* University of Braşov • Vol 2(51) - 2009
Series III: Mathematics, Informatics, Physics, 93-106

# WALSH-HADAMARD RANDOMNESS TEST AND NEW METHODS OF TEST RESULTS INTEGRATION

**Andrei-George OPRINA** [1] **, Adrian POPESCU** [2]**, Emil SIMION** [1] **and Gheorghe SIMION** [3]

Communicated to:
*9-ème Colloque franco-roumain de math. appl., 28 août-2 sept. 2008, Braşov, Romania*

**Abstract**

We present a new statistical randomness test based on Walsh-Hadamard transform. This test is a extension of frequency and autocorrelation tests and can detect a general class of defects which can appear in (pseudo)random generators. The test is based on the probability distribution of the Walsh-Hadamard transform. NIST Special Publication 800-22 [10] present two methods of integrating the results of one or more tests based on proportion of passing tests and uniformity of the corresponding $P-$values. This paper will introduce another two methods of integration of test results based on maximum test statistics and sum of squares test statistics. The integration of test results are independent from the proposed test and may be used by all the statistical tests based on confidence intervals. Some of the applications of the Walsh-Hadamard statistical test and decision procedures are in the following areas: (pseudo)randomness testing, cryptanalytic area and steganographic detection.

2000 *Mathematics Subject Classification*: 94A60.

## 1 Introduction

Some of the most used mathematical transformations used in *IT technology* (and also in cryptography and steganography) are *Discrete Fourier transform* (signal processing), *Walsh-Hadamard transform* (algorithmic processing) and *Discrete Cosine Transform* (image processing). In many scientific areas we need to test, from statistical point of view the randomness of a sequence. This paper focus on testing randomness of binary sequences using the Walsh-Hadamard transform and propose some new methods of integrating the results of one or more test results. This test detects a general class of randomness failure such as: frequency and autocorrelations failure. Another goal of this test is to answer to the question if the tested sequence is produced by some binary function (it is known that Berlekamp-Massey test may detect the sequences produced by linear functions). Walsh

[1]Institute of Mathematics "Simion Stoilow" of the Romanian Academy
[2]Millitary Technical Academy
[3]University Politehnica of Bucharest

Hadamard transform is used in testing several cryptographic criteria like: correlation immunity, balance and strict avalanche (described in detail in *Forré* [2], *Massey* [9], *Preneel* [14] and [15]). The Walsh-Hadamard is also used in fast correlation attack for a general class of cryptosystems (a correlation attack assume the existence of correlations between linear combinations of internal and output bits, see for details *Gólic* [3], *Siegenthaler* [17] and *Zhang* [18] and fast correlation which is based on precomputing data).

We remember that a *cipher system* (see *Schneier* [16])is composed from three principal elements:

- the cipher algorithm;
- the key generator algorithm;
- the key agreement protocol.

Let us denote by $\mathbf{m}$ the plain text and by $\mathbf{k}_t$ the ciphering key at time $t$ and with $\mathbf{c}$ the encrypted message (bold letters will denote vectors and the normal letters denotes scalar elements). Therefore we have the connection written in vectorial form:

$$\mathbf{c} = \mathbf{f}(\mathbf{m}; \mathbf{k}_t) \tag{1}$$

where $\mathbf{f}$ is the encryption operator.

If $\mathbf{k}_t = \mathbf{k}$ for every $t \in T$ ($T$ is the ciphering time period which is a finite set) then we can rewrite the above

$$\mathbf{c} = \mathbf{f}(\mathbf{m}; \mathbf{k}) \tag{2}$$

where $\mathbf{f}$ is the encryption operator. In this case we say that we have a codification of the information (the role of the coding theory is to protect the information from errors which can appear in the communication channel; the role of the cryptography is to protect the information from the eavesdropper).

In the codification case, after solving some nonlinear system, we can write

$$\mathbf{m} = \mathbf{h}(\mathbf{c}; \mathbf{k}) \tag{3}$$

Thus the knowledge of $\mathbf{f}(.;.)$ allows us to find $\mathbf{m}$ from $\mathbf{c}$. The system 1, which is a stochastic system, is much difficult to solve then the system 2, which is a deterministic system, because the time parameter $t$ is involved. Thus the solution of system 2, given by 3, is a particular solution of the system 1 in the case $\mathbf{k}_t = \mathbf{k}$.

Many times we have the encryption function $\mathbf{f}$ given in scalar form like

$$c_i = f(m_i, k_i), \text{ for every i}$$

where $k_i$ is the $i^{th}$ key derived from base key $\mathbf{k}_t$.

If $f$ can be factorized like

$$f(m_i, k_i) = m_i \oplus g(k_i),$$

then the encryption scheme is called *stream encryption* and we call the function $g$ *(pseudo) random generator*. Because this encryption scheme is very fast it is wide spread use in

on line communications security, speech and data transmission. In this case the cracking difficulty is due to the prediction or finding the function $g$ (or some others functions which give the same output). The problem is quite similar to the reverse engineering methods. The techniques used to recover function $g$, analyze its properties and recovering plain text are based on Walsh-Hadamard transform.

Random number generators are an important link in the computer security chain. They are very important in the construction of encryption keys and other cryptographic algorithm parameters.

In this paper, we have introduced new metrics, which may be employed to investigate the randomness of cryptographic RNGs and thus gain additional confidence that random number generators are acceptable from a statistical point of view.

As we saw in the above presentation, we need to develop dynamically statistical tools for testing the degree of randomness of binary sequences. Such tools exist in the field of public cryptography area:

- NIST 800-22 [10] is a publication of sixteen statistical tests, which can be founded at the Internet page of Computer Security Research Center (http://csrc.nist.gov/) among with an implementation of this tool. We must remark the fact that NIST 800-22 was one of the cryptographic tools which which were involved in evaluation of the candidates for Advanced Encryption Standard (FIPS PUB 197);

- In Donald Knuth's book [5], The Art of Computer Programming, Seminumerical Algorithms, Volume 2, he describes several empirical tests which include the: frequency, serial, gap, poker, coupon collector's, permutation, run, maximum-of-t, collision, birthday spacings, and serial correlation. For further information, visit http://www-cs-faculty.stanford.edu/ knuth/taocp
.html;

- The Crypt-XS suite of statistical tests was developed by researchers at the Information Security Research Centre at Queensland University of Technology in Australia. Crypt- XS tests include the frequency, binary derivative, change point, runs, sequence complexity and linear complexity. For additional information visit http://www.isrc.qut.edu.au/cryptx/index.html.

- The DIEHARD suite of statistical tests developed by George Marsaglia [7] consists of fifteen tests, namely the: birthday spacings, overlapping permutations, ranks of 31x31 and 32x32 matrices, ranks of 6x8 matrices, monkey tests on 20-bit Words, monkey tests OPSO (Overlapping-Pairs-Sparse-Occupancy), OQSO (Overlapping-Quadruples-Sparse-Occupancy), DNA,
count the 1's in a stream of bytes, count the 1's in specific bytes, parking lot, minimum distance, random spheres, squeeze, overlapping sums, runs, and craps. Additional information may be found at http://stat.fsu.edu/ geo/diehard.html.

National Institute of Standards and Technologies, update the statistically test periodically, at this time they have more then 200 statistical tests for randomness.

Another problem is to integrate the results of one or more different tests, applied on several sequences produced by the same (pseudo)generator and to give a unique answer at the question of the randomness of the tested sequences. This is a hard problem because the statistical test are not quite independent.

Another application is the steganographic one: we can detect with some probability if in a given message (text, image, audio, video etc.) there is a hidden foreign message. *Steganography* is used to hide the occurrence of communication. Recent suggestions in US newspaper (*Kelly* [4]) indicates that terrorist use steganography to communicate in secret with their accomplices. In particular, images on the Internet were mentioned as the communication medium.

In general, the information hiding process consist of the following steps:

1. Identification of redundant bits in a *cover medium* (*trash message).* Redundant bits are those that can be modified without degrading the quality of the cover medium.

2. Selection of a subset of the redundant bits to be replaced with data from a secret message (*information message*). The *stego medium* (*mixed message*) is created by replacing the selected redundant bits with message bits.

The modification of redundant bits can change the statistical properties of the cover medium. As a result, statistical analysis may reveal the hidden content. The test we present in this paper is a generalized autocorrelations test and can detect the most significant generalized autocorrelations.

The statistical steganographic procedure for detecting message insertion is at follows:

-elaborate a mathematical model (this step includes also the design of a statistical testing procedure);

-determine the test value for a pure class message (message with no hidden insertion);

-compute the test statistics for the analyzed message;

-decide if in the tested message there is something hidden;

-determine the hidden message (if it exists).

If the hidden technique is interleaving with a constant step: read $m-$bits from original, insert $n-$bits from message etc., then the autocorrelation tests (if the message source and hidden source are stochastically different) will detect the value $m+n$. Exhaustive searching algorithm is required to detect the exact values of $m$ and $n$. The complexity of this technique is $O(n^2)$ (the brute force attack has the complexity $O(n^3)$). Of course the possibility of a false detection is present. The presented test can detect a more generally hidden technique: the algorithmic techniques where the mixing technique is made via a boolean function. The mathematical model is a boolean function $\mathbf{f} : \mathbf{Z}_2^m \times \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^p$. Let us denote by $\mathbf{x}$ the cover medium $\mathbf{y}$ the message to be hidden and $\mathbf{z}$ the stego medium. Suppose that we know the bit probability of trash message equal with $\Pr(X = 1)$. The eavesdropper does not know the values $m, n, p$ and function $\mathbf{f}$, trash message $\mathbf{x}$ and information message $\mathbf{y}$. Of course after the steganographic step is made we can encrypt the result (the mixed sequence can be easy detect in the communication channel because the bit probability of mixed message $\Pr(Z = 1) = 0.5$) or we can encrypt the text before the steganographic step (in this case the bit probability of information message is $\Pr(Y = 1) = 0.5$). A statistical survey of probabilistic and statistic techniques used in steganographic detection is made in *Povros* [13]. The *stego basic principle* is the following: hide message in cover medium in such way cover medium doesn't change statistical properties, visual properties etc.

Therefore, for the reason presented above, we have the following abordation:

In section 2 of this paper we introduce the Walsh-Hadamard transform and present its properties.

In section 3 we focus on Walsh-Hadamard statistical test presenting the concept of statistical test, the test function and practical implementations. In fact there are done a class of autocorrelation tests with the correlation mask given by the rows of Hadamard matrix.

Finally another focus of this paper is to give some new methods of integrating the results of one or more tests. NIST Special Publication 800-22 [10] gives two methods of integrating the results of one or more results of the same statistical tests by terms of the corresponding $P-$values:

-proportion of the sequences passing a given test;

-uniformity of the $P-$values.

We propose another two methods, based on confidence intervals, namely the *maximum value test* and a *sum of square test*, which can detects a more general failure in the random and pseudorandom generators.

Thus focus of this paper was to design a new statistical test (which includes also decisions rules) which is suitable for different purposes:
(pseudo)randomness testing, cryptographic design, cryptanalysis techniques and steganographic detection.

## 2 Review of Walsh-Hadamard transform

### 2.1 Definition of Walsh-Hadamard transform

Let us consider the binary function $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ written in algebraic normal form. We define $\overset{\wedge}{f}$ transform by the formula

$$\overset{\wedge}{f}(\mathbf{x}) = 1 - 2f(\mathbf{x}) = (-1)^{f(x)},$$

thus $\overset{\wedge}{f}$: $\mathbf{Z}_2^n \to \{-1, 1\}$.

For a binary sequence $\mathbf{x}$ define the transformation $\overset{\wedge}{\mathbf{x}}$ by a similar formula:

$$\overset{\wedge}{x}_i = 1 - 2x_i = (-1)^{x_i} \text{ for every } i.$$

The *Hadamard matrix* of order $n = 2^m$ is defined recursively by the formula

$$H_{2^m} = \begin{pmatrix} H_{2^{m-1}} & H_{2^{m-1}} \\ H_{2^{m-1}} & -H_{2^{m-1}} \end{pmatrix}$$

with

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The Hadamard matrix is symmetric and its inverse is $\frac{1}{2^m} H_n$.

**Definition 1.** *For a function* $\overset{\wedge}{f}\colon \mathbf{Z}_2^n \to \{-1,1\}$ *we define the Walsh-Hadamard transform* $\overset{\wedge}{F}$ *by the formula*

$$\overset{\wedge}{F}(\omega) = \sum_{\mathbf{x}\in\mathbf{Z}_2^n} \overset{\wedge}{f}(\mathbf{x})(-1)^{\omega.\mathbf{x}} \text{ for every } \omega$$

*where* $\omega.\mathbf{x}$ *is the scalar product of* $\omega$ *and* $\mathbf{x}$*. Note that the Walsh Hadamard transform can be defined for any real function.*

**Definition 2.** *For a binary sequence* $\overset{\wedge}{\mathbf{x}}$ *we define the Walsh-Hadamard transform by the formula*

$$\overset{\wedge}{\omega}_i = \sum_{j=0}^{2^{m-1}} \overset{\wedge}{x}_j (-1)^{i.j} \text{ for every } i$$

*where* $i.j$ *is the scalar product of the binary representation of* $i$ *and* $j$*.*

**Remark 1.** *It is easy to see that the Walsh-Hadamard transform of a function* $\overset{\wedge}{f}$ *can be written like the matricial product*

$$\overset{\wedge}{F} = H \overset{\wedge}{f}.$$

*Similar relation for the Walsh-Hadamard transform for sequences.*

**Remark 2.** *The general term of the Hadamard matrix is* $h_{ij} = (-1)^{\mathbf{i.j}}$ *where* $\mathbf{i.j}$ *represent the scalar product of the binary representations of numbers* $i$ *and* $j$*.*

**Remark 3.** *The inverse of* $H$ *is* $\frac{1}{2^m}H$ *and it follows that*

$$\overset{\wedge}{f} = \frac{1}{2^m} H \overset{\wedge}{F}.$$

## 2.2 Properties of Walsh-Hadamard transform

We present the main properties for the Walsh-Hadamard transform for a function $\overset{\wedge}{f}$. The results for the Walsh-Hadamard transform for sequences have similar properties.

**Theorem 1.** *The operator* $\wedge$ *defined for real functions is linear. The fixed point of the Walsh-Hadamard transform is* $\mathbf{0}$*.*

**Theorem 2.** *The inverse Walsh-Hadamard transform of the function* $\overset{\wedge}{f}\colon \mathbf{Z}_2^n \to \{-1,1\}$ *is given by the formula:*

$$\overset{\wedge}{f}(\mathbf{x}) = \frac{1}{2^n} \sum_{\omega\in\mathbf{Z}_2^n} \overset{\wedge}{F}(\omega).$$

**Theorem 3.** *For a function* $\overset{\wedge}{f}\colon \mathbf{Z}_2^n \to \{-1,1\}$ *we have the following property regarding the sum of values of Walsh-Hadamard transform:*

$$\sum_{\omega\in\mathbf{Z}_2^n} \overset{\wedge}{F}(\omega) = 2^n \overset{\wedge}{f}(\mathbf{0}).$$

**Theorem 4.** *If variable* $x_j$ *is idle (does not appear in the algebraic normal form:* $f(x_1,\ldots,x_i,\ldots,x_n) = f(x_1,\ldots,\bar{x}_i,\ldots,x_n)$*) then*

$$\overset{\wedge}{F}(\omega) = 0 \text{ for every } \omega:\ \omega_i = 1.$$

**Remark 4.** *i) The Walsh-Hadamard transform of the function* $\overset{\wedge}{f}(\mathbf{x})$ *defined by the function* $f(x) = c$ *(constant function) is equal with the vector* $(2^n(1-2c),0,\ldots,0)^t$.

*ii) The Walsh-Hadamard transform of the function* $\overset{\wedge}{f}(\mathbf{x})$ *defined by the function* $f(x) = c + x_i$ *(*$i^{th}$ *projection function) is equal with* $(0,\ldots,2^n(1-2c),\ldots,0)^t$, *with the non zero factor on position* $2^{i-1}$.

*iii) From the above remarks we can see that the free term c has influence on the sign of non zero factor of Walsh-Hadamard transform.*

# 3 Walsh-Hadamard statistical test

## 3.1 The concept of statistical test

The concept of statistical testing can be found in every statistical book. Statistical testing in cryptography can be found in *Maurer* [8]. Here we have two statistical hypothesis regarding the binary sequence which is under test:

$H_0$ : the sequence $\mathbf{x}$ is produced by a binary memory less source: $Pr(X=1) = p_0$ and $Pr(X=0) = 1-p_0$, (in this case we say that the sequence does not present any predictable component)

and the alternative:

$H_1$ : the sequence $\mathbf{x}$ is produced by a binary memory less source: $Pr(X=1) = p_1$ and $Pr(X=0) = 1-p_1$ with $p_1 \neq p_0$,(in this case we say that the sequence present a predictable component regarding the probability $p$).

In statistical testing there are two kinds of errors: the first order error denoted by $\alpha$ (also called level of significance, it is the probability of occurrence of a false positive result) and second order of error denoted by $\beta$ (is the probability of the occurrence of a false negative result). This errors have the following interpretation:

$$\alpha = \Pr(\text{reject } H_0 | H_0 \text{ is true}) = 1 - \Pr(\text{accept } H_0 | H_0 \text{ is true})$$

and

$$\beta = \Pr(\text{accept } H_0 | H_0 \text{ is false}) = 1 - \Pr(\text{reject } H_0 | H_0 \text{ is false}).$$

This two errors can't be minimized simultaneous (Neymann-Pearson tests minimize the value of $\beta$ for a given $\alpha$). The testing procedure we present here is the following: for a fixed value of $\alpha$ we find a confidence region for the test statistic and check if the statistical test value is in the confidence region. The confidence region is computed using the quantiles of order $\frac{\alpha}{2}$ and $1-\frac{\alpha}{2}$. (For example the quantile $u_\alpha$ of order $\alpha$ is defined by $Pr(X < u_\alpha) = \alpha$.) Let us denote $f_{test}$ the value of test function. Another equivalent method is to compare the $P - value = Pr(X < f_{test})$ with $\alpha$ and decide the randomness if $P - value \geq \alpha$.

### 3.2 Test function

To define the test statistics for the Walsh-Hadamard test we start with some results.

Let be $\mathbf{x}$ the binary sequence under the test definite above. Suppose that the length of $\mathbf{x}$ is $n = 2^m$. We construct the transformed sequence $\hat{\mathbf{x}}$ and the Walsh-Hadamard transform of it denoted by $\hat{\omega}$ .

**Theorem 5.** *For the first component $\hat{\omega}_0$ of the Walsh-Hadamard we have the following:*

*i) the mean value of $\hat{\omega}_0$ is $m_0 = 2^m(1-2p)$.*

*ii) the variance of $\hat{\omega}_0$ is $\sigma_0^2 = 2^{m+2}p(1-p)$.*

*iii) the distribution of $\frac{\hat{\omega}_0 - m_0}{\sigma_0}$ is well approximated (for $m \geq 7$) by the normal distribution $N(0,1)$.*

**Theorem 6.** *For the $i^{th}$ component $\hat{\omega}_i$ $(i \geq 1)$ of the Walsh-Hadamard we have the following:*

*i) the mean value of $\hat{\omega}_i$ is $m_i = 0$.*

*ii) the variance of $\hat{\omega}_i$ is $\sigma_i^2 = 2^{m+2}p(1-p)$.*

*iii) the distribution of $\frac{\hat{\omega}_i - m_i}{\sigma_i}$ is well approximated (for $m \geq 7$) by the normal distribution $N(0,1)$.*

**Remark 5.** *For $p = 0.5$ (symmetric source) the mean value of $\hat{\omega}_i$ is equal with 0, for every $i$. The random variables $\omega_i$ have the same distribution.*

**Theorem 7.** *For symmetric source the vector $\hat{\omega}$ has a normal multidimensional distribution.*

The statistical test is done using the above test functions. In fact when we test a binary sequence of length $2^m$ using the above procedures we perform $2^m$ tests. This test is a basic test for the $2^{2^m}$ tests (we do not perform all tests).

### 3.3 The randomness test

The test purpose is to detect autocorrelation patterns in the tested sequence.

**Inputs:**

-Binary sequence $\mathbf{x}$ of length $n$;

-Block size of length $2^m$;

-Rejection limit $\alpha$;

-Number of classes $K$ for Goodness-of-Fit Distributional Test.

- $p$ the probability of occurrence of the symbol 1.

**Output:** Decision regarding the randomness at level of significance $\alpha$ regarding $i^{th}$ test function (also called $i^{th}$ type autocorrelation).

**Step 1.** Transform the binary sequence $\mathbf{x}$ in a sequence of 1 or $-1$: $\overset{\wedge}{\mathbf{x}} = 1 - 2\mathbf{x}$.

**Step 2.** Compute lower and upper rejection limits of the test $u_{\frac{\alpha}{2}}$ and $u_{1-\frac{\alpha}{2}}$.

**Step 3**. Compute the number of blocks to be processed $\left[\frac{n}{2^m}\right]$. Split the sequence $\overset{\wedge}{\mathbf{x}}$ into $\left[\frac{n}{2^m}\right]$ adjacent blocks.

**Step 4.** For $j = 0$ to $\left[\frac{n}{2^m}\right] - 1$ do

For $i = 0$ to $2^m - 1$ do

Compute the $i^{th}$ test statistic

$$t_{ij} = \frac{\overset{\wedge}{\omega}_{ij} - m_i}{\sigma_i},$$

where $\overset{\wedge}{\omega}_{ij}$ is the $i^{th}$ Walsh-Hadamard transform component of the block $j$; values $m_i$ and $\sigma_i$ are given by theorems 3.1 and 3.2. For every $t_{ij}$ we can compute the $P-$values $P_{ij} = \Pr(X < t_{ij})$. Decision rules can be made by apartanance of $t_{ij}$ at a confidence interval or by comparing $P_{ij}$ with value $\alpha$ (given in NIST 800-22 [10] specifications).

**Step 5.** For $i = 0$ to $2^m - 1$ take the decision regarding $i^{th}$ type autocorrelation

i) *Majority decision* also named crude decision, based on confidence interval*:* if there is a value

$$t_{ij} \notin [u_{\frac{\alpha}{2}}; u_{1-\frac{\alpha}{2}}],$$

($u_\alpha$ is the quantile of order $\alpha$ of the normal distribution) then reject the hypothesis of randomness (regarding $i^{th}$ test function) of sequence $\mathbf{x}$ at significance level $\alpha$ and display the values of $i$ and $j$. This decision rule is suitable for small values of integer $j \leq \frac{1}{\alpha}$. Equivalent, in terms of $P-$value, the randomness is decided if $P - value \geq \alpha$.

ii) *Proportion of passing test rule* (see NIST 800-22 [10]), based on $P-$value: when value $j$ is increasing we have naturally a failure given in majority decision rule. Therefore it is suitable to use the statistics given by the numbers of test failures (a integer between 0 and $\frac{n}{2^m}$). Using the confidence interval defined by the quantiles of normal distribution:

$$\left[\alpha\frac{n}{2^m} + \sqrt{\frac{n}{2^m}\alpha(1-\alpha)}u_{\frac{\alpha}{2}};\ \alpha\frac{n}{2^m} + \sqrt{\frac{n}{2^m}\alpha(1-\alpha)}u_{1-\frac{\alpha}{2}}\right].$$

If the number of test falls outside this interval, then there is evidence that the data is nonrandom. Note that other standard deviation values could be used. The confidence interval was calculated using a normal distribution as an approximation to the binomial distribution, which is reasonably accurate for large sample sizes (e.g., $n = 1000$).

iii) *Uniformity of $P-$values* (see NIST 800-22 [10]), based on $P-$value: when value $j$ is increasing we have naturally a failure given in majority decision rule. The distribution of $P-$values is examined to ensure uniformity. This may be visually illustrated using a histogram, whereby, the interval between 0 and 1 is divided into $k$ sub-intervals, and the $P-$values that lie within each sub-interval are counted and displayed. Uniformity may also be determined via an application of a $\chi^2$ test and the determination of a $P-$value corresponding to the Goodness-of-Fit Distributional Test on the $P-$values obtained for an arbitrary statistical test (i.e., a $P-$value of the $P-$values).

$$\chi_i^2 = \sum_{j=1}^{K} \frac{\left(F_j - \frac{s}{K}\right)^2}{\frac{s}{K}},$$

where $F_j$ is the number of $P-$values in sub-interval $j$, and $s$ is the sample size. If $\chi_i^2 \notin [0, \chi^2(K-1,\alpha)]$ the reject the hypothesis of randomness (regarding $i^{th}$ test function) of sequence $\mathbf{x}$ at significance level $\alpha$ and display the values of $i$. ($\chi^2(K-1,\alpha)$ is the quantile of order $\alpha$ of the distribution $\chi^2(K-1)$).

iv) *Maximum value decision*, based on confidence interval: compute $T_i = \max_j t_{ij}$, if

$$T_i \notin [u_{(\frac{\alpha}{2})^{\frac{1}{\lceil \frac{n}{2^m} \rceil}}}; u_{(1-\frac{\alpha}{2})^{\frac{1}{\lceil \frac{n}{2^m} \rceil}}}],$$

then reject the hypothesis of randomness (regarding $i^{th}$ test function) of sequence $\mathbf{x}$ at significance level $\alpha$ and display the values of $i$. The test can be modified in terms of using $P-$value.

v) *Sum of square decision*, based on confidence interval: compute

$$C_i = \sum_{j=0}^{\lceil \frac{n}{2^m} \rceil - 1} t_{ij}^2,$$

if $C_i \notin [0, \chi^2(\left\lceil \frac{n}{2^m} \right\rceil, \alpha)]$ the reject the hypothesis of randomness (regarding $i^{th}$ test function) of sequence $\mathbf{x}$ at significance level $\alpha$ and display the values of $i$. ($\chi^2(\left\lceil \frac{n}{2^m} \right\rceil, \alpha)$ is the quantile of order $\alpha$ of the distribution $\chi^2(\left\lceil \frac{n}{2^m} \right\rceil)$). This test is in some connection with the test of uniformity of $P-$values.

**Step 6**. Over all decision: majority decision, proportion of passing test, uniformity of $P-$values, maximum decision or sum of square decision to statistics $t_{ij}$, $T_i$ respectively $C_i$.

**Remark 6.** *Let us note that* $\sum_{i=0}^{2^m-1} t_{ij} = \sum_{i=0}^{2^m-1} \frac{\overset{\wedge}{\omega}_{ij} - m_i}{\sigma_i} = 2^{\frac{m}{2}-1} \frac{(x_0^{(j)} - (1-2p))}{\sqrt{(p(1-p)}}$, *where* $x_0^{(j)}$ *is the first component of the* $j^{th}$ *sequence.*

**Remark 7.** *If almost* $t_{ij} \approx 0$ *(small variance) then proportion of passing test, uniformity of* $P-$*values and sum of square decision does not detect any failure. We can detect if something is wrong with maximum value decision.*

**Remark 8.** *The Walsh-Hadamard randomness statistical test is a collection of* $2^m$ *statistical tests in the following sence: the first test value* $t_{0j}$ *is the test statistics corresponding to frequency test, the second test value* $t_{1j}$ *is the test statistics corresponding to the autocorrelation test at distance* $d = 2$ *(for a definition of frequency test and autocorrelation test at distance* $d$ *the reader may consult Maurer [8]). In fact for every power* $d = 2^p$ $(p \leq m)$ *the Walsh-Hadamard test function have a component which is equivalent with autocorrelation test at distance* $2^p$.

**Remark 9.** *The decision procedures also called linking procedures and are suitable when we have many results of the same test statistics.*

## 4 Practical implementation

In practical situation of testing there are some tricks for optimizing the implementation. First of all let us notice that computing the Walsh-Hadamard transform of a binary sequence of length $2^m$ needs $2^m$ output cells of memory and the number of elementary operations (additions and multiplications by $-1$) are $2^{2m}$ additions and $2^{2m-2}$ multiplications by $-1$. Dynamic allocation data is required. Some time if the size of the tested sequence is large we perform test on smaller size by sliding technique (see above). After we slide with a window all the sequence we can perform an over all test routine such for example majority decision, maximum of $t$ decision or chi-square decision. The spikes in the test functions indicates us a failure at the null hypothesis: the sequence is obtained using a binary recurrence of level $m$. This test is usually applied on decimated sequences, decimation factor depends on codification of trash message (8 or 16 on *.wav files, 24 on *.bmp files etc.). An additional factor may be involved: the position from which the insertion of information message will be done. The *stego detection basic principle* is the following: for the codification element (which is on $m$-bits) there is a control equation $p_0 = f(p_1, \ldots, p_{m-1})$ which holds in probability. A more exactly analysis can be made if our model will be a Markov process.

## 5 Conclusions

This paper presented a new randomness test based on Walsh-Hadamard transform and new methods of integrating the test results. The test statistics may detect possible nonlinearity patterns present in (pseudo)random generators. Thus the focus of this paper is to design a statistical test which is suitable for different purposes: pseudo-randomness

testing, cryptographic design, cryptanalysis techniques, steganographic detection, data classification etc.

## References

[1] Feldman F., *Fast spectral tests of measuring nonrandomness and the DES*, Lecture Notes in Computer Science, Advances in Cryptology - CRYPTO **87**, pp. 243-254.

[2] Forré R., *The strict avalanche criterion: spectral properties of boolean functions and an extended definition*, Lecture Notes in Computer Science, Advances in Cryptology - CRYPTO **88**, pp. 450-468.

[3] Gólic J., *F*ast correlation Attacks on the summation generator, Journal of Cryptology, Vol. **13** (2000), pp. 245-262.

[4] Kelly J., *Terror groups hide behind Wed encryption*, USA Today, February 2001.

[5] Knuth D., *The Art of Computer Programming, Seminumerical Algorithms*, Volume **2**, 3rd edition, Addison Wesley, Reading, Massachusetts, 1998.

[6] Menezes A., et. al., *Handbook of Applied Cryptography*, CRC Press, 1997.

[7] Marsaglia G., *DIEHARD Statistical Tests*: http://stat.fsu.edu/ geo/diehard.html.

[8] Maurer U., *Universal randomness test*, Journal of Cryptology, 1992.

[9] Massey J., *A Spectral characterization of correlation-immune combining functions*, IEEE Transactions on Information Theory, 1988, Vol. **34**, Issue 3.

[10] NIST Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2001.

[11] Pichler F., *On the Walsh-Fourier analysis of correlation-immune switching functions*, Lecture Notes in Computer Science, Advances in Cryptology - EUROCRYPT **88**, 1988.

[12] Pieprzyk J., *Non-linearity of exponent permutations*, Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, 1990, pp. 80-92.

[13] Povros N., *Defending Against Statistical Steganalysis, Proceedings of the 10th USENIX Security Symposium*, 323-335, August 2001.

[14] Preneel B., *Propagation characteristic of boolean functions*, Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, 1991, pp. 161-173.

[15] Preneel B., *Boolean functions satisfying high order propagation criteria*, Advances in Cryptology - EUROCRYPT **'91**, 1991, pp. 141-152.

[16] Schneier B., *Applied Cryptography with source code C*, Addison-Wesley, Second Ed., 1996.

[17] Siegenthaler T., *Cryptanalyst representation of nonlinear filtered ML-sequences*, Advances in Cryptology - EUROCRYPT **'85**, 1985, pp. 103-110.

[18] Zhang M., *Maximum correlation analysis of nonlinear combining functions in stream ciphers*, Journal of Cryptology, Volume **13**, Number 3, 2000, pp. 301-314.