THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 18, Special Issue 2017, pp. 381-388

NEW RESULTS CONCERNING THE POWER OF NIST RANDOMNESS TESTS

Carmina GEORGESCU, Emil SIMION

University Politehnica from Bucharest, Department of Mathematical Methods and Models, Romania
E-mail: emil.simion@upb.ro

Abstract. In this paper we study the probability of false acceptance regarding the statistical tests specified by NIST SP 800-22. Based on the central limit theorem, we compute the probability of accepting a false hypothesis and carry out experimental results for the following NIST tests: frequency, block frequency, runs, Fourier discrete (spectral) and serial test.

Key words: statistical testing, random bit generators.

1. INTRODUCTION AND MOTIVATION

Statistical hypothesis testing is a mathematical technique, based on sample data and used for supporting the decision making-process on the theoretical distribution of a population. In the case of statistical analysis of a cryptographic algorithm, the sample is the output of the algorithm from different inputs for the key and plain text. Because we deal with sample data from the population, the decision process of the population's probability distribution is prone to errors. To meet this challenge, we model the decision making-process with the aid of two statistical hypotheses: the null hypothesis denoted by H_0 - in this case, the sample does not indicate any deviation from the theoretical distribution - and the alternative hypothesis H_A - when the sample indicates a deviation from the theoretical distribution. There can be three types of errors:

- first type error (also known as the significance level), which is the probability of rejecting the null hypothesis when it is true: $\alpha = P(\text{reject } H_0 | H_0 \text{ is true})$; it is recommended that the level α be selected in the range [0.001,0.01];
- second type error, which represents the probability of failing to reject the null hypothesis when it is false: $\beta = P(\text{accept } H_0 | H_0 \text{ is false})$; the complementary value of β, that is $1-\beta = P(\text{reject } H_0 | H_0 \text{ is false})$ represents the test's power;

Table 1

Relation between the truth of the null hypothesis and outcomes of the test

Conclusion	Real situation	
	H_0 is true	H_0 is false
Reject H_0	α (false positive result)	$1-\beta$ (true positive result)
Accept H_0	$1-\alpha$ (true negative result)	β (false negative result)

- third type error happens when we ask a wrong question and use the wrong null hypothesis. This error is less analytical and requires more care before starting our analysis.

Notice that the two errors α and β can't be minimized simultaneously since the risk β increases as the risk α decreases and vice-versa. Therefore, one solution is to have the value of α under control and to compute the error β. Table I presents the relation between the truth of the null hypothesis and outcomes of the test.

From cryptographic point of view, statistical tests are useful in estimating the entropy which is a measure of the amount of information needed for an attacker to find the encryption key or to predict the nonce values. If one statistical test finds some predictable information in the analyzed sample, then it will reject the null hypothesis.

The pseudorandom bit generators (PRBGs) are considered cryptographically secure if they pass the next-bit test. This test states that no polynomial time algorithm, when given the first l-bits of the output, can predict the l+1 bit with a probability significantly greater than 0.5. Moreover, if part of the PRBG is compromised, it should be impossible to reconstruct the stream of random bits prior to the compromise. Andrew C. Yao [17] proved that a PRBG passes the next-bit test only if it passes every polynomial time statistical test. Because this isn't feasible, a representative polynomial time statistical testing suite is necessary. Representative examples of such suites are Crypt-XS , DIEHARD, STS SP 800-22 and TestU01 statistical tests. Because STS SP 800-22 is a standard, we shall focus on it rather than others tests suites.

In order to reduce the second type errors in NIST SP800-22 suite, Y.Wang ([11]) proposed statistical distance based testing techniques and LIL based testing techniques for (pseudo) random generators.

The analysis plan of the statistical test includes decision rules for rejecting the null hypothesis. These rules can be described in two ways:

Decision based on *P*-value. In this case, we will consider f to be the value of the test function and will compare the P-value, defined as $P(X < f)$, with the value α and will decide on the null hypothesis if P-value is greater than α.

The "critical region" of a statistical test is the set which causes the null hypothesis to be rejected; the complementary set is called the "acceptance region". In the acceptance region, we shall find the ideal results of the statistical test.

Because for each statistical test the rejection rate α is a probability, which is "approximated" from the sample data, we need to compute the minimum sample size necessary to achieve the desired rejection rate α. Also, the sample must be independent and governed by the same distribution. In Figure 1, we present the graphical interpretation related to the errors of a statistical test in case of testing the null hypothesis H_0 against the alternative one, H_1. The reference distribution in this case is the normal one.

We recall that the most important functions required by the test suite are the gamma function, the incomplete gamma function, the standard normal (cumulative distribution) function, the complementary error function and the chi-square distribution.

The gamma function is given by

$$\Gamma(a) = \int_0^\infty e^{-t} \cdot t^{a-1} \mathrm{d}t, \quad a > 0 .$$

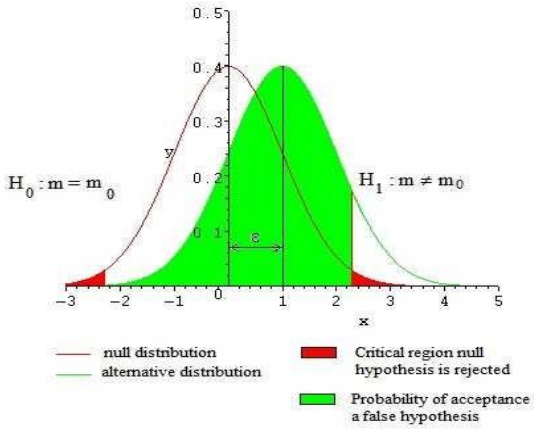


Fig. 1 – Critical region of a statistical test at 0.01 level of significance.

The formula for the incomplete gamma function is:

$$igamma(a,x) = \frac{1}{\Gamma(a)} \int_0^x e^{-t} \cdot t^{a-1} \mathrm{d}t, \quad a, x > 0$$

,

with the limiting values $igamma(a,0) = 0$ and $igamma(a,\infty) = 1$. The standard normal distribution is defined as follows

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} \mathrm{d}t.$$

A special case of the incomplete gamma function is the complementary error function:

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} \mathrm{d}t.$$

The chi-square distribution with v degrees of freedom, widely used in inferential statistics such as hypothesis testing, results when v mutually independent standard normal random variables are squared and summed. Its probability density function is defined by

$$f(x) = \frac{e^{-\frac{x}{2}} x^{\frac{\nu}{2}-1}}{\Gamma\left(\frac{\nu}{2}\right) 2^{\frac{\nu}{2}}}, \quad x \geq 0$$

The cumulative distribution function of a chi-square random variable is $\chi^2(x,\nu) = igamma\left(\frac{\nu}{2}, \frac{x}{2}\right)$

Based on the above special functions, in Table II we can see the reference distribution of some NIST statistical tests to be approached in the sequel.

The fundamental theorem of statistics, also known as the strong law of large numbers, can be stated in two different ways:

1) the first form is derived from Liapounoff-Lindeberg's theorem and states that if (f_n) is a sequence of independent random variables with the same distribution (expectation m and variance σ) then, for large n, one has:

$$P\left(a < \sum_{i=1,n} f_i < b\right) \simeq \Phi\left(\frac{b - nm + 0.5}{\sigma\sqrt{n}}\right) - \Phi\left(\frac{a - nm - 0.5}{\sigma\sqrt{n}}\right)$$

Table 2

The reference distribution of five NIST statistical tests

Test	Distribution	Parameters
Frequency (monobit) test	half normal	n = the length of bit stream
Frequency Test within a Block	$\chi^2(N)$	n = the length of bit stream M = the length of each block
Runs Test	normal	n = the length of bit stream
Discrete Fourier Transform (Spectral) Test	normal	n = the length of bit stream
Serial Test	$\chi^2(2^m - 1)$	n = the length of bit stream m = the length of each block

2) the second form is derived from De Moivre's theorem and states that if (f_n) is a sequence of independent Bernoulli random variables with $P(X = 1) = p$ and $P(X = 0) = 1 - p$ then, for large n, one has:

$$P\left(a < \sum_{i=1,n} f_i < b\right) \simeq \Phi\left(\frac{b - nm + 0.5}{\sqrt{np(1-p)}}\right) - \Phi\left(\frac{a - nm - 0.5}{\sqrt{np(1-p)}}\right).$$

The De Moivre form is usually used for randomness testing of binary sequences. Even in the case when we have small values of n and a and b are very close one to another, the above formulas are still good estimations.

2.EVALUATING THE SECOND TYPE ERROR

Suppose that we are given a binary sequence produced by a random Bernoulli variable X such that $P(X = 1) = p$ and $P(X = 0) = q = 1 - p$. Using the strong law of large numbers, we test the null hypothesis $H_0 : p = p_0$ against the alternative hypothesis $H_1 : p = p_1$, with $p_1 \neq p_0$. In what follows, we derive analytical formulas which compute the probability β for the following tests: a) frequency monobit test, b) frequency test within a block, c) runs test, d) discrete Fourier transform (spectral) test and e) serial test.

Suppose that the bit stream has the length n and let $q_0 = 1 - p_0$ and $q_1 = 1 - p_1$. For each of the above mentioned tests we give an estimation of the second error β.

a) Frequency (monobits) test. This test investigates whether the frequency of ones in a sequence of length n is approximatively $n/2$, as would be expected under an assumption of randomness. For this test, the second error probability β has been computed in [9] and is as follows:

$$\beta\ (p_1) = \Phi\left(\sqrt{\frac{p_0q_0}{p_1q_1}}\left(u_{1-\frac{\alpha}{2}} - \frac{n(p_1-p_0)}{\sqrt{np_0q_0}}\right)\right) - \Phi\left(\sqrt{\frac{p_0q_0}{p_1q_1}}\left(u_{\frac{\alpha}{2}} - \frac{n(p_1-p_0)}{\sqrt{np_0q_0}}\right)\right),$$

where $u_{1-\frac{\alpha}{2}}$ and $u_{\frac{\alpha}{2}}$ stand for quantiles of the standard normal distribution.

b) Frequency test within a block. This test is a generalization of the first one, where the number of blocks is one. The test determines if the number of ones and zeroes in an $M-$ bit block are about the same. For any block $i = \overline{1,[n/M]}$, the proportion π_i of ones is computed by means of a chi-square statistics. As specified in [6], the block size M and the number of blocks N should be selected such that $M \geq 20$ and $MN \leq n < 100M$.

$$\beta\ (p_1) = P\left(\frac{M}{p_0q_0}\sum_{i=1}^{N}(\pi_i - p_0)^2 \leq \chi^2_{1-\alpha}\middle| p = p_1\right) =$$

$$= P\left(\frac{M}{p_1q_1}\sum_{i=1}^{N}(\pi_i - p_1 + p_1 - p_0)^2 \leq \frac{p_0q_0}{p_1q_1}\chi^2_{1-\alpha}\middle| p = p_1\right) =$$

$$= P\left(\frac{M}{p_1q_1}\sum_{i=1}^{N}(\pi_i - p_1)^2 \leq \frac{p_0q_0}{p_1q_1}\chi^2_{1-\alpha} - \frac{M(p_1-p_0)}{p_1q_1}\left(2\sum_{i=1}^{N}\pi_i - 2Np_1 + N(p_1-p_0)\right)\middle| p = p_1\right) =$$

$$\simeq P\left(\frac{M}{p_1q_1}\sum_{i=1}^{N}(\pi_i - p_1)^2 \leq \frac{p_0q_0}{p_1q_1}\chi^2_{1-\alpha} - \frac{MN(p_1-p_0)^2}{p_1q_1}\right) \simeq \chi^2\left(\frac{p_0q_0\chi^2_{1-\alpha} - MN(p_1-p_0)^2}{p_1q_1}, N\right),$$

where M is the length of a block, $\chi^2_{1-\alpha}$ stands for quantile of the chi-square distribution with $N=\left[\frac{n}{M}\right]$ degrees of freedom.

c) Runs test. The runs test is based on the distribution of the total number of runs, defined as uninterrupted substrings of consecutive 1's (one-runs) or consecutive 0's (zero-runs) and denoted by V_n. The test also measures the oscillation speed between zeros and ones. Let π be the proportion of ones across all n bits of the sequence. Then the distribution of $\frac{V_n - 2n\Pi(1-\Pi)}{2\sqrt{2n}\Pi(1-\Pi)}$ can be approximated by the standard normal distribution. The runs test is applicable provided that $|\Pi - 0.5| \leq 2/\sqrt{n}$.

$$\beta\ \ (p_1) = P\left(u_{\frac{\alpha}{2}} \le \frac{V_n - \frac{n\pi(1-\pi)}{\sqrt{p_0q_0}}}{\sqrt{\frac{n}{p_0q_0\sqrt{p_0q_0}}\,\pi(1-\pi)}} \le u_{1-\frac{\alpha}{2}} \middle| p = p_1 \right) =$$

$$= P\left(u_{\frac{\alpha}{2}} \sqrt{\frac{n}{p_0q_0\sqrt{p_0q_0}}}\, p_1q_1 + \frac{np_1q_1}{\sqrt{p_0q_0}} \le V_n \le u_{1-\frac{\alpha}{2}} \sqrt{\frac{n}{p_0q_0\sqrt{p_0q_0}}}\, p_1q_1 + \frac{np_1q_1}{\sqrt{p_0q_0}} \right) =$$

$$= P\left(\frac{u_{\frac{\alpha}{2}} \frac{\sqrt{n}p_1q_1}{\sqrt{p_0q_0\sqrt{p_0q_0}}} + \frac{np_1q_1}{\sqrt{p_0q_0}} - n\sqrt{p_1q_1}}{\sqrt{n}\sqrt[4]{p_1q_1}} \le \frac{V_n - n\sqrt{p_1q_1}}{\sqrt{n}\sqrt[4]{p_1q_1}} \le \frac{u_{1-\frac{\alpha}{2}} \frac{\sqrt{n}p_1q_1}{\sqrt{p_0q_0\sqrt{p_0q_0}}} + \frac{np_1q_1}{\sqrt{p_0q_0}} - n\sqrt{p_1q_1}}{\sqrt{n}\sqrt[4]{p_1q_1}} \right) =$$

$$\simeq \Phi\left(\sqrt[4]{p_1q_1} \left(u_{1-\frac{\alpha}{2}} \frac{\sqrt{p_1q_1}}{\sqrt{p_0q_0\sqrt{p_0q_0}}} + \frac{\sqrt{np_1q_1}}{\sqrt{p_0q_0}} - \sqrt{n} \right) \right) -$$

$$-\Phi\left(\sqrt[4]{p_1q_1} \left(u_{\frac{\alpha}{2}} \frac{\sqrt{p_1q_1}}{\sqrt{p_0q_0\sqrt{p_0q_0}}} + \frac{\sqrt{np_1q_1}}{\sqrt{p_0q_0}} - \sqrt{n} \right) \right),$$

Where $u_{1-\frac{\alpha}{2}}$ and $u_{\frac{\alpha}{2}}$ stand for quantiles of the standard normal distribution.

d) Discrete Fourier transform (spectral) test. Based on a spectral method, this test is looking for the peak heights in the sequence of the discrete Fourier Transform images associated to the bit stream. Under an assumption of randomness, the values obtained from the test should not exceed the threshold value $T = 0.95$. The algorithm computes the number N_1 of peaks in the subsequence given by the first half of the sequence, that are less than T.

$$\beta\ \ (p_1) = P\left(u_{\frac{\alpha}{2}} \le \frac{N_1 - 0.95 \cdot np_0}{\sqrt{np_0q_0 \cdot 0.95 \cdot 0.05}} \le u_{1-\frac{\alpha}{2}} \middle| p = p_1 \right) =$$

$$= P\left(u_{\frac{\alpha}{2}} \sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \le \frac{N_1 - 0.95 \cdot np_1}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \le u_{1-\frac{\alpha}{2}} \sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \right)$$

$$\simeq \Phi\left(u_{1-\frac{\alpha}{2}} \sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \right) - \Phi\left(u_{\frac{\alpha}{2}} \sqrt{\frac{p_0q_0}{p_1q_1}} + \frac{0.95 \cdot n(p_0 - p_1)}{\sqrt{np_1q_1 \cdot 0.95 \cdot 0.05}} \right)$$

e) Serial test. The serial test with the parameter m, verifies the uniformity of distributions of patterns of given length m.

The input size recommended in [7] should verify $m < [log_2 n] - 2$.

In what follows we are concerned with a version of this test, that presented by Maurer in [14].

Consider the set of integers $0 \le i \le 2^m - 1$ and for any i, let n_i be the number of occurrences of the binary representation of i.

The test function in this case deals with the normalized variable

$$\frac{m}{np_0^m} \sum_{i=0}^{2^m-1} (n_i - \frac{np_0^m}{m})^2$$

which is for large n very well approximated by the χ^2 distribution with $2^m - 1$ degrees of freedom. We have the following estimations:

$$\beta\ (p_1) = P\left(\frac{m}{np_0^m}\sum_{i=1}^{2^m-1}\left(n_i - \frac{np_0^m}{m}\right)^2 \le \chi^2_{1-\alpha}(2^m-1)\middle| p = p_1\right) =$$

$$= P\left(\frac{m}{np_1^m}\sum_{i=1}^{2^m-1}\left(n_i - \frac{np_0^m}{m}\right)^2 \le \left(\frac{p_0}{p_1}\right)^m \chi^2_{1-\alpha}(2^m-1)\right) =$$

$$= P\left(\frac{m}{np_1^m}\sum_{i=1}^{2^m-1}\left(n_i - \frac{np_1^m}{m} + \frac{n}{m}(p_1^m - p_0^m)\right)^2 \le \left(\frac{p_0}{p_1}\right)^m \chi^2_{1-\alpha}(2^m-1)\right) \simeq$$

$$\simeq P\left(\frac{m}{np_1^m}\sum_{i=1}^{2^m-1}\left(n_i - \frac{np_1^m}{m}\right)^2 + \frac{2^m n}{mp_1^m}(p_1^m - p_0^m)^2 + \frac{2(p_1^m - p_0^m)}{p_1^m}\left(\frac{n}{m} - \frac{n}{m}p_1^m 2^m\right) \le \left(\frac{p_0}{p_1}\right)^m \chi^2_{1-\alpha}(2^m-1)\right)$$

$$= P\left(\frac{m}{np_1^m}\sum_{i=1}^{2^m-1}\left(n_i - \frac{np_1^m}{m}\right)^2 \le \left(\frac{p_0}{p_1}\right)^m \chi^2_{1-\alpha}(2^m-1) - \frac{n(p_1^m - p_0^m)}{mp_1^m}\left(2^m p_1^m + 1 - 2^{m+1}p_1^m\right)\right) \simeq$$

$$\simeq \chi^2\left(\left(\frac{p_0}{p_1}\right)^m \chi^2_{1-\alpha}(2^m-1) + \frac{n}{m}\frac{(p_0^m - p_1^m)^2}{p_0^m p_1^m}, 2^m - 1\right).$$

3. EXPERIMENTAL RESULTS AND DISCUSSION

In this section we study the variation of the second order error β with respect to p_1 and the length n of the bit stream.

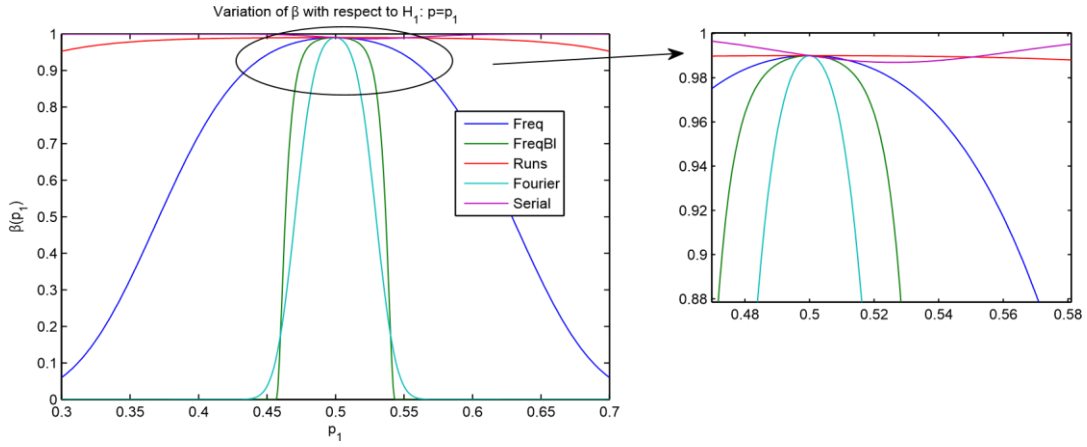
Figure 2 compares the different values of β obtained for the above tests in the following cases: a) $n = 100$, p_1 in the range [0.3,0.7], $M = 20$ in the frequency test within a block and $m = 2$ in the serial test; b) $n = 6724$, p_1 in the range [0.48,0.52], $M = 100$ in the frequency test within a block and $m = 8$ in the serial test; c) $n \in [6724,9604]$ and $p_1 \in [0.48,0.52]$.

Notice that for each case, the necessary condition in the runs test is verified: a) $|\Pi - 0.5| \le 0.2 < 2/\sqrt{n}$, b) and c) $|\Pi - 0.5| \le 0.02 < 2/\sqrt{n} \approx 0{,}204$, so the test is applicable.

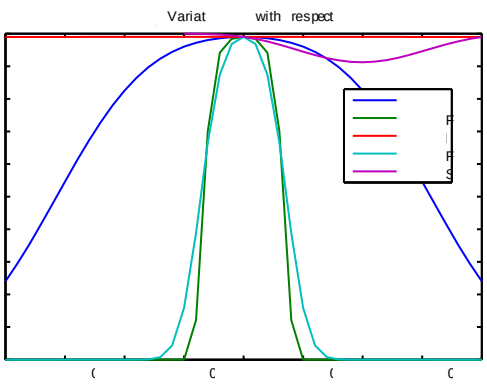
Our analysis suggests that, in some local situations, some tests dominate others tests. Therefore, the second type error for the statistical tests suite, expressed by

$$\beta(p_1) = \max_{i=1,15} \beta_i\,(p_1)$$

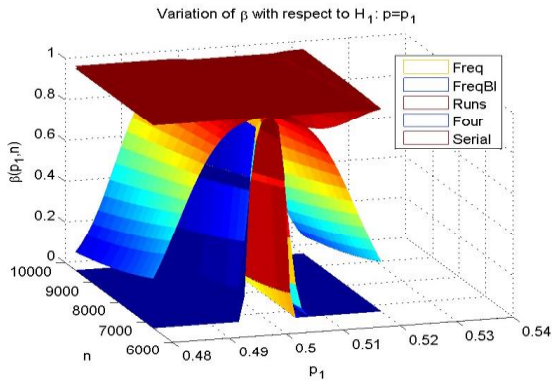
has a complicated form.



a) $n = 100$.



b) $n = 6724$.



c) $6724 \leq n \leq 9604$.

Fig. 2 – Comparative view of β function in case of frequency, block frequency, runs, Fourier discrete and serial test.

4. CONCLUSIONS

In this paper we obtained estimations of the second error probability for five NIST tests and we showed that it is feasible to derive analytical formulas for computing the probability of accepting a false hypothesis. The next step in our future work will be to solve equations of the following form

$$\beta(p_i) = \beta(p_j)$$

and compare the theoretical results with the simulations suggested in [1]: associate with each test i, a Bernoulli random variable T_i (which will take the value 1 for the samples that pass the test i and 0 otherwise), estimate the value of $p_{ij} = P(T_i \cap T_j) - P(T_i) \cdot P(T_j)$ and find the highest value p_{ij} for $i, j = \overline{1,15}$.

A full computation of the second error probability for all NIST tests is a pressing open problem that remains to be addressed. Some examples of applying statistical tests are in automated key and nonce values generation used in cryptographic protocols (nonce values are used to avoid the possibility of a replay attack as challenges in cryptographic protocols and shall not be repeated until authentication keys are changed). Practical examples are for Digital Identity Guidelines (see [8]). Automated key and nonce values generation is made usually by RBG (random bit generators implemented by hardware devices) or PRBG (implemented by software/firmware devices).

5. APPENDIX

In this appendix, very simple code fragments implementing the probability functions described in the section [2] are provided.

```
% matlab script for Frequency test
function [betap] = betaFreq(p1,n)
p0=0.5; q0=0.5; q1=1-p1; alf=0.01;
x1=sqrt(p0*q0./(p1.*q1)).*(norminv(1-alf/2,0,1)-n.*(p1-p0)./sqrt(n.*p0*q0));
x2=sqrt(p0*q0./(p1.*q1)).*(norminv(alf/2,0,1)-n.*(p1-p0)./sqrt(n.*p0*q0));
betap=cdf('Normal',x1,0,1)-cdf('Normal',x2,0,1);
end

% matlab script for Block Frequency test
function [betap] = betaFreqBl(p1,n,m)
```

```
p0=0.5; q0=0.5; q1=1-p1; alf=0.01;
glib=floor(n/m)
x=(p0*q0*chi2inv(1-alf,glib)-m*n.*(p1-p0).*(2*p1-p1-p0)./(p1.*q1);
betap=chi2cdf(x,glib);
end

% matlab script for Serial test
function [betap] = betaSerial(p1,n,m)
p0=0.5; alf=0.01;
glib=2^m-1;
v=p0^m./(p1.^m);
x=v.*chi2inv(1-alf,glib)+n/m*(p0^m-p1.^m).^2./(p0^m)./(p1.^m);
betap=chi2cdf(x,glib);
end

% plotting the output
n=6724; p1=0.48:0.001:0.52;  % 2Dplot

b1=betaFreq(p1,n);
b2=betaFreqBl(p1,n,100);
b3=betaRuns(p1,n);
b4=betaFour(p1,n);
b5=betaSerial(p1,n,10);
plot(p1,b1,p1,b2,p1,b3,p1,b4,p1,b5);
legend('Freq','FreqBl','Runs','Fourier','Serial');

n=6724:10:9604;%3Dplot
p1=0.48:0.001:0.52;  [p1,n]=meshgrid(p1,n);
mesh(p1,n,b1); hold on
mesh(p1,n,b2);
mesh(p1,n,b3);
mesh(p1,n,b4);
mesh(p1,n,b5);
```

REFERENCES

1. C. GEORGESCU, A. PETRESCU-NITA, E. SIMION, A. TOMA, *A View On NIST Randomness Tests (In)Dependence*, ECAI 2017 – International Conference – 9th Edition Electronics, Computers and Artificial Intelligence, to be published.
2. A.P. GODBOLE, S.G. PAPASTAVRIDIS, *Runs and patterns in probability: Selected papers*, Dordrecht, Kluwer Academic, 1994.
3. W. KILLMAN, J. SCHTH, W. THUMSER, I. ULUDAG, *A Note Concerning the DFT Test in NIST Special Publication 800-22*, T-Systems, Systems Integration, 2004.
4. S. KIM, K, UMENO, A. HASEGAWA, *Corrections of the NIST Statistical Test Suite for Randomness*, Cryptology ePrint Archive, Report 2004/018, 2004.
5. I. J. GOOD, *The serial test for sampling numbers and other tests for randomness*, Proc. Cambridge Philos. Soc., **47**, pp. 276-284, 1953.
6. M. KIMBERLEY, *Comparison of two statistical tests for keystream sequences*, Electronics Letters, **23**, pp. 365-366, 1987.
7. NIST standards: http://www.nist.gov/, http://www.csrc.nist.gov/.
8. https://pages.nist.gov/800-63-3/sp800-63-3.html.
9. M. ABRAMOWITZ, I. STEGUN, *Handbook of Mathematical Functions*, Applied Mathematics Series, **55**, Washington, National Bureau of Standards, 1964; reprinted by Dover Publications, New York, 1968.
10. A. OPRINA, A. POPESCU, E. SIMION, GH. SIMION, *Walsh-Hadamard Randomness Test and New Methods of Test Results Integration*, Bulletin of Transilvania University of Brasov, **2** *(51)*, pp. 93-106, Series III-2009.
11. D. MAIMUT, A. PATRASCU, E. SIMION, *The Relevance of Second Error Probability in Modern Statistical Analysis*, Proc. of 6-th International Conference on Electronics, Computers and Artificial Intelligence ECAI 2014, Bucharest, **6**, *2*, pp. 91-94, 2014.
12. Y. WANG, *On the design of LIL Tests for (pseudo) random generators and some experimental results*, IACR Cryptology ePrint Archive, 2014.
13. E. BARKER, J. KELSEY, *NIST SP 800-90A: Recommendation for random number generation using deterministic random bit generators*, NIST, 2012.
14. A. RUKHIN, J. SOTO, J. NECHVATAL, M. SMID, E. BARKER, S. LEIGH, M. LEVENSON, M. VANGEL, D. BANKS, A. HECKERT, J. DRAY, S. VO, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST SP 800-22, 2010.
15. U.M. MAURER, *A universal statistical test for random bit generators*, J. of Cryptology, **5**, *2*, pp. 89-105, 1992.
16. E. SIMION, *The Relevance of Statistical Tests in Cryptography, IEEE Security & Privacy* **13** (*1*), 66-70, 2015.
17. A.C. YAO, *Theory and Applications of Trapdoor Functions*, Proc. 23rd IEEE Symp. Foundations of Computer Science, pp. 80-91, 1982.