**Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 5, Issue 15, pages 1-6, 2019**

# A Systematic Approach of NIST Statistical Tests Dependencies

Paul Burciu
PhD. Electronics Engineering
Military Technical Academy
Bucharest, Romania
pburciu@yahoo.com

Emil Simion
PhD. Mathematics
University Politehnica of Bucharest
Bucharest, Romania
emil.simion@upb.ro

***Abstract* – In order to evaluate binary strings generated by cryptographic applications, for randomness and unpredictability, an instrument may be the statistical tests. Because in terms of probability it cannot be assumed that these statistical tests are completely reliable/effective, they must be tested for uniformity, scalability, and consistency, searching for any kind of correlation that might affect their desired properties and their results. In this paper we proposed a systematic approach of testing and analyzing results concerning the NIST statistical test suite, determining dependencies between tests, and finding patterns for the evolution of these dependencies according to specific factors, such as binary string length.**

***Keywords-Statistical Test, Correlation Coefficient, Sample Length***

## I. Introduction

As the National Institute of Standards and Technology, NIST, asserts in the argument for its statistical test suite ([1], [2]), there is a “need for random and pseudorandom numbers”, and this need “arises in many cryptographic applications”, that is, in cryptographic keys or protocols, in digital signatures, or in authentication protocols.

In order to evaluate binary strings generated by cryptographic applications, for randomness and unpredictability, an instrument may be the statistical tests. Because in terms of probability it cannot be assumed that these statistical tests are completely reliable/effective, they must be tested for uniformity, scalability, and consistency, searching for any kind of correlation that might affect their desired properties and their results. This study started from the idea of doing randomness testing of cryptographic algorithms by using NIST statistical test suite more:

- Reliable/Effective
- Practical/Efficient.

Accordingly, the goal was searching for any correlation that might exist between the NIST tests. The experimental procedure implied all 15 tests (being aware of the criticisms given by [3] to [6], especially about the Discrete Fourier Transform Test) contained by this suite.

The overall investigation consisted of two phases:

- A systematic application of NIST tests to pseudorandom binary strings, previously generated by using a well-known cryptographic algorithm such as AES
- A statistical evaluation of the results based on Galton-Pearson formula [7], in order to find any mathematical relationship between NIST tests.

Finally, all experiments and analysis were resumed by this paper which essentially contains 4 sections as follows: Section 1 is for an introduction to the topics, Section 2 makes a brief presentation of the theoretical basis, Section 3 details the experimental procedure, and Section 4 is for conclusions and future topics of our research on the field.

## II. Theoretical Basis

### A. *Correlation evaluation*

The result of the statistical tests, denoted as P-value, is a measure of randomness which ranges between [0,1], and is calculated by a specific formula given for each test by NIST’s specification. With a P-value close to 1, we have a high level of randomness.

The Galton-Pearson “product-moment correlation coefficient” [7], calculated by formula (1), evaluates pairs of P-values, that is, X and Y, and produces a result which ranges between [-1, 1]. A correlation of +1 means that there is a perfect positive linear relationship between variables, or a direct proportion, while a correlation of -1 means that there is a perfect negative linear relationship between them, or an inverse pro-portion. With a correlation which is close to the absolute value of 1, we have a strong relationship between the variables. In case of a correlation close to 0, the variables are independent. The reciprocal is not always true [8].

$$r = \frac{\Sigma\left(X_i - \overline{X}\right)\Sigma\left(Y_i - \overline{Y}\right)}{\sqrt{\left(X_i - \overline{X}\right)^2\left(Y_i - \overline{Y}\right)^2}} =$$

$$= \frac{N\sum X_iY_i - (\sum X_i)(\sum Y_i)}{\sqrt{[N\sum X_i^2 - (\sum X_i)^2][N\sum Y_i^2 - (\sum Y_i)^2]}} \qquad (1)$$

### B. *Other approaches*

In literature, there are a few works regarding correlation between NIST statistical tests. Especially [3] has the same approach as ours, but also some other by the same authors ([9] and [10]) studied this correlation with focus on the proportion of regions in which P-values are lower than 0.01 for each test, or defining correlation by examining the distribution of a test's results on a region where another test's results are lower than 0.01.

Coming from the same authors, the study of [11] examines dependencies of 9 statistical tests included in the NIST test suite and found the same dependencies as for [3].

Another approach is [12] where P-values are calculated by using 2 different sets and for each sequence the difference between 2 P-values corresponding to 2 different tests is calculated and found according to the distribution of difference correlation.

Two of our preceding papers, [13] and [14], investigated and proposed numerical methods for solving three open problems regarding the NIST statistical test suite:

- Estimating and deriving analytical formulas for computing the probability of accepting a false hypothesis for five of the NIST tests (i.e. Frequency Test, Frequency Test within a Block, Runs Test, Discrete Fourier Transform (Spectral), and Serial Test)
- Finding the number of minimum sample size to achieve a given probability error
- The (in)dependence of statistical tests.

This paper continues our studies from [13] and [14], approaching systematically the (in)dependence of statistical tests.

## III. Experimental work

### A. *Experimental method*

For the evaluation of correlation between statistical test results, the chosen method was Galton-Pearson formula [7], that is, the correlation coefficient. In order to produce reliable/effective results and conclusions, this was done by calculating and analyzing 4 sets of coefficients corresponding to the application of NIST statistical tests over 100 binary samples of different lengths (i.e. 1, 2, 5, 6 million bits) (see Appendix A).

The number of samples was chosen according to NIST's specifications (see Appendix A) where the only value of minimum 200, that is, for Linear Complexity Test, was intentionally unaccomplished due to the fact that this test works with a fixed number of 500 substrings. Hence, this limit in fact was accomplished.

As asserted in Section 1, a pseudorandom binary string of approximately 1 billion bits was previously generated by using an FPGA loop implementation of AES-128 encryption [15], a well-known symmetrical cryptographic algorithm, with a “1h” (i.e. hex value) unique key. On the loop, every encrypted output binary sequence was taken and applied as an input to the next encryption. Knowing that for one encryption simulation, that is, for 128 bits, it took 240 ns, we had to run a 1.875 s simulation (i.e. 7,812,500 iterations) in order to produce a 1-billion-bits binary string. This simulation was done by using Xilinx ISE Design Suite (shareware version 14.7) and one of the authors previous hardware implementation of AES-128 [16], on a Xilinx Spartan-6 FPGA platform (Fig. 1).

Figure 1. Xilinx Spartan-6 FPGA platform

With the intention to make experiments practical/efficient, the NIST test suite (version 2.1.2) was implemented according to NIST's specifications on five Linux OS (Ubuntu version 18.04.1 Desktop 64-bit) virtual machines (4 processors, 4 GB of RAM), all running on a single physical desktop PC (Intel I7 Quad Core, 16 GB of RAM). The virtual machines were created with the VMWare Workstation software (shareware version 12.5.5).

All 15 tests were used, 3 of them being treated like double tests as follows:

- Cumulative Test, denoted as T3, consists of Forward (T3F) and Reverse (T3R) tests;
- Non Periodic Template Matchings Test, denoted as T8, was approached as for 2 binary sequences, “ 000000001 ” (T8.1) and “ 111111110” (T8.2), respectively;
- Serial Test, denoted as T14, was treated like 2 tests (T14.1 and T14.2) corresponding to 2 P-values produced by this test.

Therefore, instead of 15, we considered 18 individual tests listed by Table I.

As mentioned before, we chose to use samples of 4 different lengths in order to check any possible dependence between correlation coefficients and the sample length. Moreover, the option of using 100, as a unique number of samples, was motivated by the necessity of having uniform results, such that they could be compared. In case we did not comply with this requirement, the comparison would not be possible.

TABLE I. USED TESTS LIST

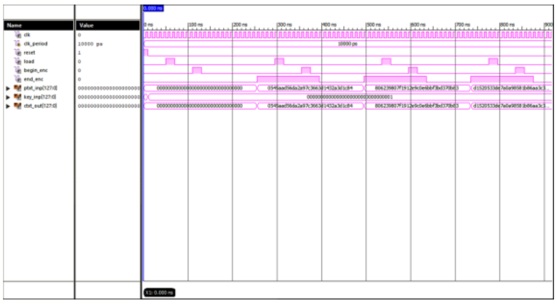
| Test No. | Test Name | Test Variants |
|---|---|---|
| T1 | Frequency (Monobit) | |
| T2 | Frequency Test within a Block | |
| T3 | Cumulative Sums (Cusums) | T3F; T3R |
| T4 | Runs | |
| T5 | Longest-Run-of-Ones in a Block | |
| T6 | Binary Matrix Rank | |
| T7 | Discrete Fourier Transform (Spectral) | |
| T8 | Non-overlapping Template Matching | T8.1; T8.2 |
| T9 | Overlapping Template Matching | |
| T10 | Maurer's “Universal Statistical” | |
| T11 | Approximate Entropy | |
| T12 | Random Excursions | |
| T13 | Random Excursions Variant | |
| T14 | Serial | T14.1; T14.2 |
| T15 | Linear Complexity | |

In order to relieve certain correlations between the results of statistical tests and to give reliable/effective conclusions, we only took into consideration correlation coefficients greater than or equal to 0.5 (similarly to [3]), avoiding to set too high limits and to neglect any dependencies with lower coefficients that might occur.

### *B. Experimental results*

The correlation coefficients resulted from the application of NIST statistical tests on the FPGA loop implementation (Fig. 2), following the procedure described by the preceding subsection, are contained by Table II, III, IV, and V (with a minimized form that shows only actual correlations between tests, all other values being irrelevant, showing weak or no dependencies between tests), for a sample length of 1, 2, 5, and 6 million bits.

Figure 2. FPGA loop implementation of AES-128



The table cells that are filled with grey color contain correlation coefficients with values that exceed 0.5, showing dependence (correlation) between a test situated on the horizontal line and one on the vertical.

For Table II (M = 1,000,000 bits) we found (2):

$$\begin{gathered} \text{T1-T3F} = 0.738; \\ \text{T1-T3R} = 0.722; \\ \text{T3F-T3R} = 0.765; \\ \text{T12-T13} = 0.725; \\ \text{T14.1-T14.2} = 0.690. \end{gathered} \tag{2}$$

For Table III (M = 2,000,000 bits) we found (3):

$$\begin{gathered} \text{T1-T3F} = 0.790; \\ \text{T1-T3R} = 0.767; \\ \text{T3F-T3R} = 0.705; \\ \text{T12-T13} = 0.623; \\ \text{T14.1-T14.2} = 0.690. \end{gathered} \tag{3}$$

For Table IV (M = 5,000,000 bits) we found (4):

$$\begin{gathered} \text{T1-T3F} = 0.716; \\ \text{T1-T3R} = 0.733; \\ \text{T3F-T3R} = 0.637; \\ \text{T14.1-T14.2} = 0.746. \end{gathered} \tag{4}$$

For Table V (M = 6,000,000 bits) we found (5):

$$\begin{gathered} \text{T1-T3F} = 0.745; \\ \text{T1-T3R} = 0.753; \\ \text{T3F-T3R} = 0.711; \\ \text{T14.1-T14.2} = 0.679. \end{gathered} \tag{5}$$

TABLE II. CORRELATION COEFFICIENTS FOR M = 1,000,000 BITS

| Tests | T1 | T3F | T3R | T12 | T13 | T14.1 | T14.2 |
|---|---|---|---|---|---|---|---|
| **T1** | 1 | 0.738 | 0.722 | 0.287 | 0.248 | 0.031 | -0.002 |
| **T3F** | 0.738 | 1 | 0.765 | 0.371 | 0.313 | -0.087 | -0.245 |
| **T3R** | 0.722 | 0.765 | 1 | 0.235 | 0.180 | -0.049 | -0.149 |
| **T12** | 0.287 | 0.371 | 0.235 | 1 | 0.725 | -0.010 | -0.037 |
| **T13** | 0.248 | 0.313 | 0.180 | 0.725 | 1 | -0.011 | -0.079 |
| **T14.1** | 0.031 | -0.087 | -0.049 | -0.010 | -0.011 | 1 | 0.690 |
| **T14.2** | -0.002 | -0.245 | -0.149 | -0.037 | -0.079 | 0.690 | 1 |

TABLE III. CORRELATION COEFFICIENTS FOR M = 2,000,000 BITS

| Tests | T1 | T3F | T3R | T12 | T13 | T14.1 | T14.2 |
|---|---|---|---|---|---|---|---|
| **T1** | 1 | 0.790 | 0.767 | 0.286 | 0.324 | 0.022 | -0.052 |
| **T3F** | 0.790 | 1 | 0.705 | 0.421 | 0.348 | -0.092 | -0.116 |
| **T3R** | 0.767 | 0.705 | 1 | 0.236 | 0.201 | -0.043 | 0.033 |
| **T12** | 0.286 | 0.421 | 0.236 | 1 | 0.623 | 0.128 | 0.036 |
| **T13** | 0.324 | 0.348 | 0.201 | 0.623 | 1 | 0.049 | -0.098 |
| **T14.1** | 0.022 | -0.092 | -0.043 | 0.128 | 0.049 | 1 | 0.690 |
| **T14.2** | -0.052 | -0.116 | 0.033 | 0.036 | -0.098 | 0.690 | 1 |

TABLE IV. CORRELATION COEFFICIENTS FOR M = 5,000,000 BITS

| Tests | T1 | T3F | T3R | T12 | T13 | T14.1 | T14.2 |
|---|---|---|---|---|---|---|---|
| **T1** | 1 | 0.716 | 0.733 | 0.199 | 0.139 | -0.123 | -0.111 |
| **T3F** | 0.716 | 1 | 0.637 | 0.267 | 0.099 | -0.107 | -0.117 |
| **T3R** | 0.733 | 0.637 | 1 | 0.086 | 0.014 | -0.164 | -0.106 |
| **T12** | 0.199 | 0.267 | 0.086 | 1 | 0.498 | -0.056 | -0.135 |
| **T13** | 0.139 | 0.099 | 0.014 | 0.498 | 1 | -0.013 | -0.023 |
| **T14.1** | -0.123 | -0.107 | -0.164 | -0.056 | -0.013 | 1 | 0.746 |
| **T14.2** | -0.111 | -0.117 | -0.106 | -0.135 | -0.023 | 0.746 | 1 |

TABLE V. CORRELATION COEFFICIENTS FOR M = 6,000,000 BITS

| Tests | T1 | T3F | T3R | T12 | T13 | T14.1 | T14.2 |
|---|---|---|---|---|---|---|---|
| **T1** | 1 | 0.745 | 0.753 | 0.193 | 0.372 | 0.03 | -0.018 |
| **T3F** | 0.745 | 1 | 0.711 | 0.166 | 0.329 | 0.089 | 0.08 |
| **T3R** | 0.753 | 0.711 | 1 | 0.003 | 0.226 | 0.085 | 0.084 |
| **T12** | 0.193 | 0.166 | 0.003 | 1 | 0.474 | -0.08 | -0.119 |
| **T13** | 0.372 | 0.329 | 0.226 | 0.474 | 1 | 0.03 | -0.007 |
| **T14.1** | 0.03 | 0.089 | 0.085 | -0.08 | 0.03 | 1 | 0.679 |
| **T14.2** | -0.018 | 0.08 | 0.084 | -0.119 | -0.007 | 0.679 | 1 |

Looking at the correlation coefficients, concerning only the presumed dependencies (correlations), we found different patterns of variation depending on the sample length, expressed by (6), (7). (8), (9), (10), as follows:

- Oscillation pattern

  T1-T3F: 0.738 ↗ 0.790 ↘ 0.716 ↗ 0.745 (6)

- Oscillation pattern

  T1-T3R: 0.722 ↗ 0.767 ↘ 0.733 ↗ 0.753 (7)

- Large Oscillation pattern

  T3F-T3R: 0.765 ↘ 0.705 ↘ 0.637 ↗ 0.711 (8)

- Decrease pattern

  T12-T13: 0.725 ↘ 0.623 ↘ 0.498 ↘ 0.474 (9)

- Large Oscillation pattern

  T14.1- T14.2: 0.690 ↗ 0.690 ↗ 0.746 ↘ 0.679 (10)

Therefore, we could remark an oscillation pattern in 4 cases and a decrease pattern in a single case. Except the decrease tendency for T12-T13, which is still present, all other patterns are oscillations. These results will be object of further investigations on our future work.

Looking at all table values, we concluded that there is a strong correlation between Frequency (Monobit) Test (T1) and both components of Cumulative Sums Test (T3F and T3R), and also between Random Excursions Test (T12) and Random Excursions Variant Test (T13) (both being run with a parameter x = 1), except Table 4 and 5 where T12-T13 = 0.498 and T12-T13 = 0.474 (being under 0.5, there is a weak correlation). In addition, there is a strong correlation between the components of Cumulative Sums Test (T3F and T3R) and also between the components of Serial Test (T14.1 and T14.2).

This result showed some redundancies that existed between different tests, such as between Frequency and Cumulative Sums Test, or between Random Excursions and Random Excursions Variant Test (except for the longest samples, that is, with M = 5,000,000 and 6,000,000), but also between components/variants of a single test, such as Cumulative Sums Test or Serial Test.

In terms of practical/efficient testing, these dependencies could be avoided by using only one of the redundant different tests (e.g. T3) and also by rejecting one of the redundant components of a single test (e.g. T3R and T14.2). This is not the case of Random Excursions and Random Excursions Variant Test, because of the variation of their correlation coefficient depending on the sample length. However, this correlation must be relieved and treated carefully.

In addition, the Cumulative Sums Test is correlated both between its components and with other tests. Hence, for a practical/efficient testing, the Cumulative Sums Test and one of the Serial Test's components could be missed from testing.

From a different perspective of practical/efficient testing, we gathered all information regarding approximate duration of all tests on Table VI. As it clearly appears, all duration values are high, especially for M = 2,000,000, 5,000,000, and 6,000,000. Knowing from [15] that software implementations of cryptographic applications are very slow, by comparison to hardware implementations (in many cases 10 times slower), for our future work we intend to realize efficient hardware implementations of NIST statistical tests.

TABLE VI. APPROXIMATE DURATION OF STATISTICAL TESTS

| **Test No.** | **Test Name** | **Test Duration [h:min]** | | | |
|---|---|---|---|---|---|
| | | ***M = 1 mill.*** | ***M = 2 mill.*** | ***M = 5 mill.*** | ***M = 6 mill*** |
| T1 | Frequency (Monobit) | 08:00 | 20:00 | 48:30 | 58:55 |
| T2 | Frequency Test within a Block | 09:00 | 20:00 | 49:00 | 59:20 |
| T3 | Cumulative Sums (Cusums) | 09:25 | 20:40 | 48:00 | 58:55 |
| T4 | Runs | 10:00 | 19:10 | 48:00 | 59:20 |
| T5 | Longest-Run-of-Ones in a Block | 10:00 | 19:10 | 48:00 | 59:10 |
| T6 | Binary Matrix Rank | 10:00 | 20:00 | 48:35 | 59:20 |
| T7 | Discrete Fourier Transform (Spectral) | 09:30 | 20:00 | 48:35 | 59:20 |
| T8 | Non-overlapping Template Matching | 10:00 | 20:00 | 49:15 | 59:50 |
| T9 | Overlapping Template Matching | 09:50 | 20:00 | 49:00 | 59:45 |
| T10 | Maurer's "Universal Statistical" | 10:00 | 20:00 | 49:15 | 60:00 |
| T11 | Approximate Entropy | 10:00 | 20:00 | 49:15 | 59:45 |
| T12 | Random Excursions | 10:00 | 20:00 | 48:45 | 58:55 |
| T13 | Random Excursions Variant | 10:00 | 20:00 | 41:00 | 58:55 |
| T14 | Serial | 10:00 | 20:40 | 37:50 | 59:05 |
| T15 | Linear Complexity | 10:00 | 20:40 | 40:50 | 59:40 |

## IV. CONCLUSIONS

In this paper we proposed a systematic approach of testing and analyzing results concerning the NIST statistical test suite, determining dependencies between tests, and finding patterns for the evolution of these dependencies according to specific factors, such as binary string length. Our future works will involve a mathematical description of the variance of correlation coefficients and, also, more efficient implementations of the statistical tests, in order to improve our systematic approach.

## APPENDIX A - RECOMMENDED AND USED PARAMETERS FOR TESTING

| | Recommended (bits) | | | Used (bits) | | |
|---|---|---|---|---|---|---|
| | ***n*** | ***M/M,Q/Q,K/m*** | ***N/L*** | ***n*** | ***M*** | ***N*** |
| T1 | n≥M*N<br>n≥100 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T2 | n≥M*N<br>n≥100 | M>0,01*n, M≥20 | N<100 | 100,000,000 | 999,936=128*7,812 | 100 |
| | | | | 200,000,000 | 2,000,000=128*15,625 | |
| | | | | 500,000,000 | 4,999,936=128*39,062 | |
| | | | | 600,000,000 | 6,000,000=128*46,875 | |
| T3 | n≥M*N<br>n≥100 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T4 | n≥M*N<br>n≥100 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T5 | n≥128 | M=8 | N=16 | 100,000,000 | 1,000,000=10,000*100 | 100 |
| | n≥6,272 | M=128 | N=49 | 200,000,000 | 2,000,000=10,000*200 | |
| | n≥750,000 | M=10,000 | N=75 | 500,000,000 | 5,000,000=10,000*500 | |
| | | | | 600,000,000 | 6,000,000=10,000*600 | |
| T6 | n≥38M*Q<br>n≥38,912 | M=Q=32 | - | 100,000,000 | 999,424=976*32*32 | 100 |
| | | | | 200,000,000 | 1,999,872=1,953*32*32 | |
| | | | | 500,000,000 | 4,999,168=4,882*32*32 | |
| | | | | 600,000,000 | 5,999,616=5,859*32*32 | |
| T7 | n≥1,000 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T8 | n≥M*N | M>0,01*n, m=9, m=10 | N≤100<br>N=8 | 100,000,000 | 1,000,000=125,000*8, m=9 | 100 |
| | | | | 200,000,000 | 1,000,000=250,000*8, m=9 | |
| | | | | 500,000,000 | 5,000,000=625,000*8, m=9 | |
| | | | | 600,000,000 | 6,000,000=750,000*8, m=9 | |
| T9 | n≥M*N<br>n≥1,000,000 | m≈log2 M, M=1,032 m=9, m=10<br>λ= (M-m+1)/2m ≈2 K≈2*λ, K=5 | N*(min πi)>5<br>N=968 | 100,000,000 | 998,976=1,032*968, m=9, λ=2 | 100 |
| | | | | 200,000,000 | 1,998,984=1,032*1,937, m=9, λ=2 | |
| | | | | 500,000,000 | 4,999,008=1,032*4,944, m=9, λ=2 | |
| | | | | 600,000,000 | 5.999.016=1,032*5,813, m=9, λ=2 | |
| T10 | n≥(Q+K)L | Q=10*2L, 640≤Q≤655,360<br>K≈1000*2L 64,000≤K≤65,536,000 | 6≤L≤16 | 100,000,000 | 999,999=(1,280+141,577)*7 | 100 |
| | | | | 200,000,000 | 1,999,998=(1,280+284,434)*7 | |
| | | | | 500,000,000 | 4,999,995=(5,120+550,435)*9 | |
| | | | | 600,000,000 | 5,999,994=(5,120+661,546)*9 | |
| T11 | n=f(m) | $m<\lfloor \log_2 n \rfloor-5$ | | 100,000,000 | M=1,000,000, m=10 | 100 |
| | | | | 200,000,000 | M=2,000,000, m=10 | |
| | | | | 500,000,000 | M=5,000,000, m=10 | |
| | | | | 600,000,000 | M=6,000,000, m=10 | |
| T12 | n≥1,000,000 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T13 | n≥1,000,000 | - | - | 100,000,000 | 1,000,000 | 100 |
| | | | | 200,000,000 | 2,000,000 | |
| | | | | 500,000,000 | 5,000,000 | |
| | | | | 600,000,000 | 6,000,000 | |
| T14 | n=f(m) | $m=\lfloor \log_2 n \rfloor-2$ | | 100,000,000 | M=1,000,000, m=16 | 100 |
| | | | | 200,000,000 | M=2,000,000, m=16 | |
| | | | | 500,000,000 | M=5,000,000, m=16 | |
| | | | | 600,000,000 | M=6,000,000, m=16 | |
| T15 | n≥1,000,000 | 500≤M≤5,000 | N≥200 | 100,000,000 | 1,000,000=500*2,000 | 100 |
| | | | | 200,000,000 | 2,000,000=500*4,000 | |
| | | | | 500,000,000 | 5,000,000=500*10,000 | |
| | | | | 600,000,000 | 6,000,000=500*12,000 | |

where:

n - The length of the bit string.

M/m - The length of each block/substring

N - The number of blocks; selected in accordance with the value of M.

M - The number of rows in each matrix. For the test suite, M has been set to 32. If other values of M are used, new approximations need to be computed.

Q - The number of columns in each matrix. For the test suite, Q has been set to 32. If other values of Q are used, new approximations need to be computed.

K - The number of degrees of freedom.

L - The length of each block. Note: the use of L as the block size is not consistent with the block size notation (M) used for the other tests. How-ever, the use of L as the block size was specified in the original source of Maurer's test.

Q - The number of blocks in the first initialization sequence.

K - The number of blocks in the second initialization sequence.

## REFERENCES

[1] NIST, "Special Publication 800-22", 2001.

[2] NIST, "Special Publication 800-22 Revision 1a", 2010.

[3] A. Doğnaksoy, F. Sulak, M. Uğuz, O. Şeker, Z. Akcengiz, "Mutual Correlation of NIST Statistical Randomness Tests and Comparison of Their Sensitivities on Transformed Sequences", Turkish Journal of Electrical Engineering & Computer Sciences, Turkey, 2017

[4] S. Kim, K. Umeno, A. Hasegawa, "On the NIST statistical test suite for randomness", IEICE Technical Report, ISEC 2003-87, Dec. 2003, cited by [3].

[5] S. J. Kim, K. Umeno, A. Hasegawa, "Corrections of the NIST Statistical Test Suite for Randomness", Cryptology ePrint Archive, Tech. Rep. 2004/018, 2004, cited by [3].

[6] H. Okada, K. Umeno, "Randomness Evaluation with the Discrete Fourier Transform Test Based on Exact Analysis of the Reference Distribution", IEEE Transactions on Information Forensics and Security, Volume: 12, Issue: 5, May 2017, cited by [3].

[7] J. L. Rodgers, W. A. Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", The American Statistician, Vol. 42, No. 1, Feb., 1988.

[8] D. S. Moore, W. I. Notz, M. A. Fligner, "The Basic Practice of Statistics - 3rd edition", W. H. Freeman & Co., New York, NY, USA, 2003.

[9] M. S. Turan, A. Doğnaksoy, S. Boztaş, "On independence and sensitivity of statistical randomness tests", International Conference on Sequences and Their Applications (SETA), Lecture Notes in Comput-er Science. Springer, 2008, cited by [3].

[10] A. Doğnaksoy, B. Ege, K. Muş, "Extended Results for Independence and Sensitivity of NIST Randomness Tests", Information Security and Cryptography Conference, ISC Turkey, 2008, cited by [3].

[11] L. Fan, H. Chen, S. Gao, "A general method to evaluate the correlation of randomness tests", Information Security Applications, Lecture Notes in Computer Science, Springer International Publishing, 2014, cited by [3].

[12] F. Sulak, M. Uğuz, O. Koçak, A. Doğnaksoy, "On the independence of statistical randomness tests included in the NIST test suite", Turkish Journal of Electrical Engineering & Computer Sciences, Turkey, 2017.

[13] C. Georgescu, E. Simion, A. Petrescu Nita, A. Toma, "A View On NIST Randomness Tests (In)Dependence", Electronics, Computers and Artificial Intelligence, Pitesti, Romania, 2017.

[14] C. Georgescu, E. Simion, "New Results Concerning the Power of NIST Randomness Tests", Proceedings of The Romanian Academy, Series A, Volume 18, Special Issue 2017, pp. 381-388.

[15] NIST, "FIPS PUB 197, Announcing the Advanced Encryption Standard (AES)", 2001.

[16] P. Burciu, "Design and Optimization Methods for Hardware Implementation of Information Enciphering Algorithms on Digital Communications", PhD Thesis, University of Pitesti, Pitesti, Romania, 2009.