Development and Justification of Techniques for Periodic Quality Control of Random/Pseudorandom Number Generators for Cryptographic Applications

Lyudmila Kovalchuk[1,†], Oleksii Bespalov[1,†] and Hanna Nelasa[1,*,†]

[1] G.E. Pukhov Institute for Modelling in Energy Engineering, General Naumov Str. 15, Kyiv, 03164, Ukraine

Abstract

The use of random/pseudorandom number generators with good cryptographic properties is critical for cryptographic applications, especially when these generators are used to generate key data. Using a generator whose outputs do not form a "perfect" random sequence significantly reduces the cryptographic properties of a cryptosystem. Specifically, the system becomes vulnerable to a directed brute-force attack, which allows one to recover the most probable key of a cryptographic algorithm, based on deviation of equiprobable distribution. However, developers of such generators typically focus on engineering, analytical, and statistical quality checks of the proposed generator, and pay virtually no attention to developing effective quality control methods for the generator throughout its lifecycle. This paper aims to fill this gap. Its goal is to develop and validate an effective (in terms of speed and quality) periodic verification of the correct operation of a random/pseudorandom number generator, ensuring its cryptographic properties are preserved. Such testing is necessary for the timely detection of generator operational deviations at the early stages of their occurrence, before their impact becomes critical. This paper develops a periodic generator quality check procedure, called "the second-level verification" (the first-level verification is performed upon generator adoption). A set of statistical tests for performing this verification is proposed; it is shown that these tests identify various types of generator operational deviations and are independent. It also shows how the results of applying these tests to generator outputs should be processed. As an example of the use of a second-level verification, the results of its application to a standardized generator based on DSTU 7624:2014 "Kalina" are presented.

Keywords

random/pseudorandom number generator, random sequences, statistical tests, key data generation

1. Introduction

The NIST STS [1] statistical test suite, designed to verify the cryptographic qualities of random/pseudo-random number generators (RNGs/PRNGs), is a powerful and extremely important tool. It is mandatory when verifying a newly developed generator before its adoption, or after a major overhaul of a hardware generator [2].

However, in addition to a one-time inspection upon adoption, hardware generators require additional periodic control. Hardware RNG testing requires more complex approach than others classes of digital devices. This is due to the following factors.

Information Technology and Implementation (IT&I-2025), November 20-21, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
lusi.kovalchuk@gmail.com (L. Kovalchuk); annanelasa@gmail.com (H. Nelasa); alexb5dh@gmail.com (O. Bespalov).
0000-0003-2874-7950 (L. Kovalchuk); 0000-0002-3708-0089 (H. Nelasa); 0000-0001-7126-6752 (O. Bespalov).

1. In contrast to traditional approach to functionality verification, for hardware RNG it is impossible to organize verification according to the black box approach [3], or using known test input-output values, or like that.

2. The occurrence of a failure in hardware RNG functioning, causing incorrect output sequences, usually will not be immediately detected.

3. Hardware generators are significantly vulnerable to misuse or to use in inappropriate physical conditions [4], or to the deterioration of the quality of the physical source of randomness [5].

Thus, for hardware generation of random/pseudo-random sequences with a given level of security, it is necessary to perform periodic (once a day, a week, etc.) verifications of the correctness of its functioning, assessing the quality of the output sequences.

At the same time, periodic checking should not be as complicated and resource-consuming as the verification upon adoption. This is due to the fact that periodic checking is applied to such a RNG/PRNG, which, firstly, has good cryptographic properties, and secondly, has passed preliminary engineering checks for reliability of functioning. In addition, periodic checking should be applied to a working RNG/PRNG without stopping it, therefore it should occur almost in real time.

Summarizing the above, we conclude that it is necessary to develop a "lightweight" analogue of the RNG/PRNG Verification Strategy defined in [1] and improved in [6]. As in lightweight cryptology, this analogue should, on the one hand, require significantly less time, and on the other hand, perform less detailed verification.

The structure of the article is the follows. In Section 2 we consider articles on the topic, analyze directions of their investigations. In the Section 3 the main results are given, namely: detailed description of tests proposed for second-level verification; justification of the tests independence; application of proposed second-level verification for standardized PRNG. We conclude with Section 4, summarizing the usage of our results and describing the possible direction of future investigations.

2. Related work

The vast majority of contemporary works, devoted to issues related to RNG/PRNG, can be divided into the following clusters by topic.

2.1. The methods of RNG/PRNG creation or improvement

Thus, in [7] a number of methods for constructing high-quality RNG by harnessing the inherent noise properties of multistage ring oscillators and using fast Fourier transformation-based noise are proposed. The authors verify the statistical properties of their proposed RNG using a test suite [1] and obtain results confirming its cryptographic qualities.

The authors of [8] consider memristor TRNGs (True Random Number Generators) obtained using various entropy sources for producing high quality random numbers or sequences, analyze their strengths and weaknesses, and show that memristor TRNGs stand out due their simpler circuits and lower power consumption in comparison with CMOS (Complementary Metal-Oxide-Semiconductor)- based TRNGs.

The work [9] is devoted to the evaluation of the theoretical bound for the min-entropy of the output random sequence through the very efficient entropy accumulation using only bitwise XOR operations, under the condition that the inputs from the entropy source are independent. The obtained theoretical results were applied to the quantum random number generator that uses dark shot noise arising from image sensor pixels as its entropy source.

Chaos Based Cryptography Pseudo-Random Number Generator Template with Dynamic State Change is proposed in [10]. It is also analyzed using NIST STS tests [1]. Obtained results show that

chaotic maps can be successfully used as a building blocks for cryptographic random number generators.

The work [11] deals with the method of Improving the Statistics Qualities of Pseudo Random Number Generators. The authors present a new non-linear filter design of PRNG that improves the output sequences of common pseudo random generators in terms of statistical randomness .

At last, [12] proposes a variety of randomness extraction methods to post-process the output of random number generators and evaluated their impacts on the statistical properties. The findings show that all proposed post-processing methods improved the statistical properties of RNG/PRNG.

2.2. New methods for verifying the cryptographic qualities of a generator or applying known methods to widely used generators

In [13], the use of Neural Networks for the assessment of the quality and hence security of several Random Number Generators is considered. The authors focus both on the vulnerability of classical Pseudo Random Number Generators, such as Linear Congruential Generators and the RC4 algorithm, and extend their analysis to non-conventional data sources, such as Quantum Random Number Generators based on Vertical-Cavity Surface-Emitting Laser. Their findings reveal the potential of NNs to enhance the security of RNGs, along with highlighting the robustness of certain QRNGs, in particular the VCSEL-based (Vertical-Cavity Surface-Emitting Laser) variants.

The work [14] proposes a rough sets based analyzing system to analyze the quality of Pseudorandom Number Generator, while the design of generators is outside the scope of this paper.

The special of RNGs, namely Physical Prime Random Number Generator Based on Quantum Noise is considered in [15]. Such generators have not yet been explored, and in this work the authors experimentally implement and characterize a vacuum-based probabilistic prime number generation scheme with an error probability of about 3.5×10^{-15}.

2.3. Review articles with comprehensive and comparative analysis of different well-known RNG or PRNG

The good example of such articles is [16], which reviews the performance and statistical quality of some well known algorithms for generating pseudo random numbers. For completeness, we should also mention such articles as [17], [18], [19].

However, as the study of these works showed, none of them considers the full process of functioning of the RNG/PRNG during its lifetime, in particular the issue of verifying the cryptographic qualities of the RNG/PRNG at different stages of its functioning.

In [5] and [20], the necessity to use three different types of RNG/PRNG quality verification was justified. The first-level verification is performed during the adoption process. The second-level verification is performed periodically at certain specified intervals to prevent usage of the RNG/PRNG with a slight (but dangerous) degradation of its cryptographic properties and to detect such degradation at an early stage. The third-level verification is a continuous verification aimed at instantly detecting significant failures in operation.

For the first level verification, an Improved Strategy for RNG/PRNG Quality Verification was proposed in [6]. For the third level verification, it's enough to use 2-3 simple tests (like chi-square and maximal series tests) which may detect significant deviations from equiprobable distribution, or significant symbol dependency, or different physical faults. But the question about the second-level (periodic) verification is still opened, and we are going to focus on it in this paper.

3. Our results. Description of criteria and justification for the chosen statistics. P-values calculation

The object of this work is process of random/pseudorandom numbers and sequences generation.

The main purpose of it is to create an efficient second-level verification, which can be periodically applied to RNG/PRNG to verify correctness of its functioning. Here under "sufficient verification" we understand fast procedure, which is able to detect different dangerous deviation in its work on their early stage, while these deviations become essentially dangerous.

For the second-level verification, it is sufficient to use a significantly smaller tests suite than for the first-level one. This is explained by the fact that at this stage it is not necessary to conduct a comprehensive analysis of the RNG/PRNG, but only to make sure that it functions correctly. But the technique for test results processing can be the same as in the Improved Strategy [6].

The requirements for the tests suite for the second level verification are as follows:

- tests should be independent;
- tests must be selected in a such way, that the obtained set contains tests that can check all major types of deviations from randomness, such as: violation of symbol equiprobability; presence of dependencies between symbols; presence of a symbol's dependence on its place in the sequence; etc.;
- tests should be quick and easy to perform;
- the number of tests should be as minimal as possible.

Based on the above requirements, a set of statistical tests will be proposed below, their choice will be justified, and what deviations each test detects will be shown. We will call this set of tests OPTIMA-5 according to the number of tests in the set. In order to make it possible to apply the Improved Strategy to the test results, an appropriate algorithm for calculating the P-value corresponding to the obtained statistic will be given for each test.

In what follows, we will use the hypothesis H_0, which is formulated as "the sequence obtained from the RNG/PRNG is an implementation of a true random sequence, i.e. sequence of equiprobable, independent, identically distributed bitwise random variables". The alternative hypothesis H_1 is complex and may be formulated as "H_0 is not true". The tests given below are aimed at testing the hypothesis H_0.

3.1. Monobit χ^2 -test

Let $\{\xi_i\}_{i=1}^n$ be a sequence of independent random variables, equiprobably distributed on the alphabet $A=\{a_1,...,a_N\}$ of the size N.

Then the random variable

$$\chi^2=\sum_{i=1}^{N}\frac{(M_i-np_i)^2}{np_i}=\sum_{i=1}^{N}\frac{M_i^2}{np_i}-n,$$

where $p_i=P\{\xi_l=a_i\}$, $i\in[N]$, $l\in[n]$, M_i is the number of symbols a_i in the sequence $\{\xi_i\}_{i=1}^n$, will asymptotically have a χ 2 -distribution with N-1 degrees of freedom.

Under the condition of equiprobable distribution of variables ξ_i (according to H_0), we have $p_i=\frac{1}{N}$ and

$$\chi^2=\frac{N}{n}\sum_{i=1}^{N}M_i^2-n. \qquad (1)$$

If N-1≤30, then the limit value of the statistic χ_α^2 for a given significance level α is calculated from the formula $F(\chi_\alpha^2)=1-\alpha$, where $F(x)$ is a χ2 -distribution function with N-1 degrees of freedom (the value of the distribution function is tabulated, see, for example, [21]).

If N-1 >30, then the distribution $\sqrt{2\chi^2}$ approaches normal distribution with parameters $N(x;\sqrt{2(N-1)+1},1)$, and the limit value of the statistic χ^2_α for a given significance level α may be found from the formula $\chi^2_\alpha=\frac{1}{2}\left(\sqrt{2(N-1)-1}+z_\alpha\right)^2$, where $\Phi(z_\alpha)=1-\alpha$ and $\Phi(x)$ is the standard normal distribution function (the value of the distribution function is tabulated, see for example [22].

For example, for N = 16 and α=0.001, we have χ^2_α=37.7; for $N=2$ and α=0.01, we have χ^2_α = 10.83.

A sequence passed the test with a significance level α if $\chi^2<\chi^2_\alpha$.

P-value calculation.

If $N-1<30$, then the P-value corresponding to the calculated value of the statistic $\chi^2=\frac{N}{n}\sum_{i=1}^{N}M_i^2-n$ is calculated as $P_{\chi^2}=1-F(\chi^2)$, where $F(x)$ is χ^2-distribution function with N-1 degrees of freedom.

If $N-1\geq 30$, then the P-value corresponding to the calculated value of the statistic $\chi^2=\frac{N}{n}\sum_{i=1}^{N}M_i^2-n$ is calculated with the next steps:

- calculate the value $z=\sqrt{2\chi^2}-\sqrt{2(N-1)-1}$;

- calculate the P-value from the equation $P_{\chi^2}=1-\Phi(z)$, where $\Phi(x)$ is the standard normal distribution function (the value of the distribution function is tabulated, see [22]).

3.2. Bigram χ^2-test

Let $\{\xi_i\}_{i=1}^{n}$ be a sequence of independent random variables, equiprobably distributed on the alphabet $A=\{a_1,\ldots,a_N\}$ of the size N.

Then the sequence $\nu=\{\nu_j\}_{j=1}^{n/2}$, where $\nu_j=(\xi_{2j-1},\xi_{2j})$, consisting of non-overlapping bigrams, is a sequence of independent random variables that take values in the alphabet A ×A of size N^2. Then the random variable

$$\mathrm{X}^2=\sum_{i,j=1}^{N}\frac{(M_{ij}-kp_{ij})^2}{kp_{ij}}=\sum_{i,j=1}^{N}\frac{M_{ij}^2}{kp_{ij}}-k, \qquad (2)$$

where $p_{ij}=P\{\nu_l=(a_i,a_j)\}$, $k=\frac{n}{2}$, M_{ij} is the number of all bigrams $(a_i,a_j)\in A\times A$ in the sequence ν, will asymptotically have a χ 2 -distribution with N^2-1 degrees of freedom.

Under the condition of equiprobable distribution of variables ξ_i, the corresponding bigrams will also have equiprobable distribution, i.e. $p_{ij}=\frac{1}{N^2}$, therefore

$$\mathrm{X}^2=\frac{N^2}{k}\sum_{i,j=1}^{N}M_{ij}^2-k.$$

If $N-1<30$, then the limit value of the statistic X^2_α for a given significance level α is calculated from the formula $F(\mathrm{X}^2_\alpha)=1-\alpha$, where $F(x)$ is a χ^2-distribution function with N^2-1 degrees of freedom.

If $N^2-1\geq 30$, then the distribution $\sqrt{2\chi^2}$ approaches normal $N(x;\sqrt{2(N^2-1)+1},1)$, and the limit value of the statistic X_α^2 for a given significance level α may be found from the formula $\mathrm{X}_\alpha^2=\frac{1}{2}\left(\sqrt{2(N^2-1)-1}+z_\alpha\right)^2$, where $\Phi(z_\alpha)=1-\alpha$ and $\Phi(x)$ is the standard normal distribution function.

For example, for $N=16$ and $\alpha=0.01$ we have X_α^2 = 309.781; for $N=2$ and α=0.01, we have X_α^2 = 6.63.

A sequence passed the test with a significance level α if $X^2<X_\alpha^2$.

P-value calculation.

If $N-1<30$, then the P-value corresponding to the calculated value of the statistic $\mathrm{X}^2=\frac{N^2}{k}\sum_{i,j=1}^{N}M_{ij}^2-k$ is calculated as $P_{\mathrm{X}^2}=1-F(\mathrm{X}^2)$, where $F\left(x\right)$ is χ^2-distribution function with N^2-1 degrees of freedom.

If $N-1\geq 30$, then the P-value corresponding to the calculated value of the statistic $\chi^2=\frac{N}{n}\sum_{i=1}^{N}M_i^2-n$ is calculated with the next steps:

- calculate the value $Z=\sqrt{2\cdot\mathrm{X}^2}-\sqrt{2(N^2-1)-1}$;

- calculate the P-value from the equation $P_{\chi^2}=1-\Phi(Z)$, where $\Phi(x)$ is the standard normal distribution function (the value of the distribution function is tabulated, [22]).

The two tests described above check the equiprobability of distributions of symbols and bigrams. Note that the combination of these tests also checks pairwise symbol dependencies.

3.3. Number of runs test

Let $\{\xi_i\}_{i=1}^n$ be a sequence of independent random variables, equiprobably distributed on the alphabet A of the size *N*.

Define a random variable $G_n=\sum_{i=1}^{n-1}I(\xi_{i+1}\neq\xi_i)+1$ (the number of series in the sequence $\{\xi_i\}_{i=1}^n$). Then

$$MG_n=\sum_{i=1}^{n-1}MI+1=(n-1)(1-\frac{1}{N})+1;\ DG_n=\sum_{i=1}^{n-1}DI=(n-1)(\frac{N-1}{N^2}).$$

Since G_n is a sum of identically distributed, independent random variables, the random variable

$$G=\frac{G_n-MG_n}{\sqrt{DG_n}} \tag{3}$$

has asymptotically the standard normal distribution, i.e. $\frac{G_n-MG_n}{\sqrt{DG_n}}\to N(0,1)$ when $n\to\infty$.

Therefore, for the chosen significance level α obtain:

$$\alpha=P\left(\left|\frac{G_n-MG_n}{\sqrt{DG_n}}\right|>G_\alpha\right)=P(G>G_\alpha\vee G<-G_\alpha)=P(G>G_\alpha)+P(G<-G_\alpha)=$$
$$=1-F(G_\alpha)+F(-G_\alpha)=1-F(G_\alpha)+1-F(G_\alpha)=2-2F(G_\alpha),$$

where $F(x)$ is the standard normal distribution function.

A sequence passed the test with a significance level α if

$$\left|\frac{G_n - MG_n}{\sqrt{DG_n}}\right| < G_\alpha,$$

where G_α is calculated from the equation $F(G_\alpha) = 1 - \frac{\alpha}{2}$.

For example, for α=0.01 we have G_α =2.58.

P-value calculation.

The P-value corresponding to the calculated value of the statistic $G = \left|\frac{G_n - MG_n}{\sqrt{DG_n}}\right|$ is calculated from the equation $P_G = 2 \cdot (1 - F(G))$, where $F(x)$ is the function of the standard normal distribution.

The number of runs test checks the absence of dependencies between the symbols. For example, if the probability of changing the next symbol is greater than ½, then the number of series will be too large; otherwise, if this probability is small, too long series will appear, and the number of series will be small.

3.4. Places of symbols test

Let $\{\xi_i\}_{i=1}^n$ be a sequence of independent random variables, equiprobably distributed on the alphabet $A = \{a_1, \ldots, a_N\}$ of the size N.

Let us define a random variable $R_\nu = \sum_{i=1}^{n-1} iI(\xi_i = \nu)$ (the sum of the positions of the symbol $\nu \in A$ in the sequence $\{\xi_i\}_{i=1}^n$). Then

$$MR_\nu = \sum_{i=1}^{n} iP(\xi_i = \nu) = \frac{n(n+1)}{2N}, \quad DR_\nu = \sum_{i=1}^{n} i^2 DI(\xi_i = \nu),$$

since $I(\xi_i = \nu)$ are independent random variables with variance

$$DI(\xi_i = \nu) = MI^2(\xi_i = \nu) - (MI(\xi_i = \nu))^2 = MI(\xi_i = \nu) - (MI(\xi_i = \nu))^2 =$$

$$= MI(\xi_i = \nu)(1 - MI(\xi_i = \nu)) = \frac{N-1}{N^2},$$

and for sufficiently large n

$$DR_\nu = \sum_{i=1}^{n} i^2 \frac{N-1}{N^2} = \frac{N-1}{N^2} \cdot \frac{2n^3 + 3n^2 + n}{6} = \frac{N-1}{N^2} \cdot \frac{n(n-1)(2n+1)}{6} \approx \frac{N-1}{N^2} \cdot \frac{n^3}{3}.$$

Then

$$\left(\frac{R_\nu - MR_\nu}{\sqrt{DR_\nu}}\right)^2 = \frac{\left(R_\nu - \frac{n(n+1)}{2N}\right)^2}{\frac{N-1}{N^2} \cdot \frac{n^3}{3}} = \frac{3N^2}{(N-1)n^3}\left(\frac{R_\nu}{n} - \frac{n+1}{2N}\right)^2 n^2 \approx \frac{3N}{n}\left(\frac{R_\nu}{n} - \frac{n+1}{2N}\right)^2.$$

The random variables $R_\nu = \sum_{i=1}^{n-1} iI(\xi_i = \nu)$ ($\nu \in$A) are independent, so (for sufficiently large n) the distribution of the quantity $\frac{R_\nu - MR_\nu}{\sqrt{DR_\nu}}$ can be considered as N(0,1). Therefore, the limiting distribution of the sum of their squares is the χ^2-distribution. Therefore, we can assume that the variable

$$T=\frac{3N}{n}\sum_{\nu=0}^{N-1}\left(\frac{R_\nu}{n}-\frac{n+1}{2N}\right)^2 \qquad (4)$$

has χ^2 -distribution with degrees $N-1$ of freedom and for the chosen significance level α the limit statistics χ^2_α can be calculated as $\alpha=P\left(T>\chi^2_\alpha\right)=1-F(\chi^2_\alpha)$, where $F(x)$ is the χ^2-distribution function with $N-1$ degree of freedom.

A sequence passed the test with a significance level α if $T<\chi^2_\alpha$.

If $N-1<30$, then the limit value of the statistic χ^2_α for a given significance level α is calculated from the formula $F(\chi^2_\alpha)=1-\alpha$, where $F\left(x\right)$ is a χ^2 -distribution function with N-1 degrees of freedom (the value of the distribution function is tabulated).

If N-1 >30, then the distribution $\sqrt{2\chi^2}$ approaches normal $N(x;\sqrt{2(N-1)+1},1)$, and the limiting value of the statistic χ^2_α for a given level of significance αis found from the formula $\chi^2_\alpha=\frac{1}{2}\left(\sqrt{2(N-1)-1}+z_\alpha\right)^2$, where $\Phi(z_\alpha)=1-\alpha$, $\Phi(x)$ is a function of the standard normal distribution.

For example, for $N=16$ and $\alpha=0.01$ we have $\chi^2_\alpha=30.58$; for $N=16$ and α=0.001, we have $\chi^2_\alpha=37.7$

A sequence passed the test with a significance level α if $\chi^2<\chi^2_\alpha$.

P-value calculation.

If $N-1<30$, then the P-value corresponding to the calculated value of the statistic $T=\frac{3N}{n}\sum_{\nu=0}^{N-1}\left(\frac{R_\nu}{n}-\frac{n+1}{2N}\right)^2$ is calculated as $P_T=1-F(T)$, where $F\left(x\right)$ is χ^2 -distribution function with N-1 degrees of freedom.

If $N-1\geq30$, then the P-value corresponding to the calculated value of the statistic $T=\frac{3N}{n}\sum_{\nu=0}^{N-1}\left(\frac{R_\nu}{n}-\frac{n+1}{2N}\right)^2$ is calculated with the next steps:

- calculate the value $z=\sqrt{2\cdot T}-\sqrt{2(N-1)-1}$;

- calculate the P-value as $P_T=1-\Phi(z)$, where $\Phi(x)$ is the standard normal distribution function (the value of the distribution function is tabulated).

This test checks the dependence of a symbol on its position in a sequence. For example, it can detect any periodic or monotonic trends.

3.5. Test of inversions

Let $\{\xi_i\}_{i=1}^n$ be a sequence of independent random variables, equiprobably distributed on the alphabet A of the size N.

We assume that $n=2l$ (otherwise we discard the last symbol of the sequence).

Build an auxiliary sequence $\zeta_i=I\{\xi_{2i-1}<\xi_{2i}\}$, $i=\overline{1,l}$, and calculate

$$q=P(\zeta_i=0)=\frac{1}{2}+\frac{1}{2N},\quad p=P(\zeta_i=1)=\frac{1}{2}-\frac{1}{2N},$$

$$M\zeta_i=\frac{1}{2}-\frac{1}{2N},\quad D\zeta_i=\frac{1}{4}-\frac{1}{4N^2},\quad \forall i=\overline{1,l}.$$

Define the random variable $I_n = \sum_{i=1}^{l} \zeta_i$ (the number of inversions, without overlapping, in the sequence $\{\xi_i\}_{i=1}^{n}$). Then

$$MI_n = I\left(\frac{1}{2} - \frac{1}{2N}\right), \quad DI_n = I\left(\frac{1}{4} - \frac{1}{4N^2}\right).$$

Since I_n is the sum of identically distributed, independent random variables, then the variable

$$I = \left| \frac{I_n - MI_n}{\sqrt{DI_n}} \right| \tag{5}$$

has asymptotically standard normal distribution. Therefore, for the chosen significance level α the next equality holds:

$$\alpha = P\left(\left| \frac{I_n - MI_n}{\sqrt{DI_n}} \right| > I_\alpha \right) = 2 - 2F(I_\alpha),$$

where $F(x)$ is the standard normal distribution function.

A sequence passed the test with a significance level α if $\left| \frac{I_n - MI_n}{\sqrt{DI_n}} \right| < I_\alpha$, where I_α is calculated from the equation $F(I_\alpha) = 1 - \frac{\alpha}{2}$.

For example, for α=0.01 we have I_α =2.58.

P-value calculation.

The P-value corresponding to the calculated value of the statistic $I = \left| \frac{I_n - MI_n}{\sqrt{DI_n}} \right|$ is calculated as $P_l = 2 \cdot \left(1 - F(I)\right)$, where $F\left(x\right)$ is the function of the standard normal distribution.

Like the series test, this test detects dependencies between symbols, but of a different nature.

It should be noted that, in general situation, a maximum length run test can be added to the above-described set of tests. However, for the second-level verification, it is unnecessary, since such a test is performed continuously according to the third-level verification.

3.6. Independence of tests in the OPTIMA-5 set

To check the independence of the tests of this set, two methods were used: (i) using the normal distribution [23]; (ii) using Chernov's inequality [24], both with the significance level $\alpha = 0.01$. The number of sequences which passed all tests is $T = 296$.

The significance level for checking hypothesis about independence is $A = 0.0001$. The following results were obtained.

Independence verification using normal distribution: credential interval is calculated as $\left[W_1, W_2\right]$, where

$$W_1 = \max\left\{0, \left(1-\alpha\right)^5 - 4 \cdot \sqrt{\frac{\left(1-\alpha\right)^5 \cdot \left(1-\left(1-\alpha\right)^5\right)}{300}}\right\} = 0.9\,,$$

$$W_2 = \min\left\{1, \left(1-\alpha\right)^5 + 4 \cdot \sqrt{\frac{\left(1-\alpha\right)^5 \cdot \left(1-\left(1-\alpha\right)^5\right)}{300}}\right\} = 1\,.$$

As $T \in \left[W_1, W_2\right]$, the hypothesis about tests independence is accepted.

Independence verification using Chernov's inequality: credential interval is calculated as $[V_1, V_2]$, where

$V_1 = \max\{0,\ \mu - \delta_A\} = 193$ and $V_2 = \min\{1,\ \mu + \delta_A\} = 300$, with $\mu = n \cdot (1-\alpha)^m$, $\delta_A = \sqrt{\frac{3}{\mu} \cdot \ln\frac{2}{A}}$.

As $T \in [V_1, V_2]$, the hypothesis about tests independence is accepted.

Hence, both methods make the same decision and we may consider these tests to be mutually independent.

3.7. Using improved strategy for second-level verification of PRNG, built according to Appendix A of DSTU 9041:2020

It should be noted that, in general situation, a maximum length run test can be added to the above-described set of tests. However, for the second-level verification, it is unnecessary, since such a test is performed continuously according to the third-level verification.

To confirm the practical usage of the Improved Strategy for application in second-level PRNG verification, we applied the verification to the PRNG described in Appendix A of DSTU 9041:2020 [23]. Note that Improved Strategy was described in details in [6], therefore, we only note here that it verifies the following requirements:

- equiprobable distribution of P-values for each test (checked using limit chi-square distribution);
- the proportion of sequences that passed each test (checked using limit normal distribution);
- the number of sequences that passed all tests (checked using limit normal distribution).

All tests from OPTIMA-5 were applied to 300 sequences, obtained from PRNG mentioned above. Then for each test distribution of 300 corresponding P-values was checked using chi-square test with significance level $A = 0.0001$. Next, for each test the proportion of adopted sequences were checked, using limit normal distribution to calculate the edges of credential interval with significance level $A = 0.0001$. At last, the proportion of sequences passed all tests was checked, using limit normal distribution to calculate the edges of credential interval with significance level $A = 0.0001$.

1. Distribution of P-values

In conditions, described above, the limit statistics for chi-square criterion is 33.71995. Based of obtained P-values, the next statistics were calculated (Table 1):

Table 1

Distribution of P-values

Test	P-value	Result
Chi squared test	9.33333	Passed
Chi sq. for bigrams test	11.00000	Passed
Series number test	4.73333	Passed
Sign places test	5.53333	Passed
Inversions test	3.53333	Passed

2. Proportion of accepted sequences

In conditions, described above, the credential interval is [0.96702, 1.00000]. The corresponding proportions are (Table 2).

3. Number of sequences passed all tests:

Here we use approach based on normal distribution instead of approach, based on Chernoff inequality, described in [6].

In conditions, described above, the credential interval is [193, 300].

The number of sequences passed all 5 tests is 296.

Final decision: PRNG from Appendix A of DSTU 9041:2020 is adopted with Improved Strategy.

Table 2
Proportion of accepted sequences

Test	P-value	Result
Chi squared test	0.99667	Passed
Chi sq. for bigrams test	0.99333	Passed
Series number test	0.99667	Passed
Sign places test	0.99667	Passed
Inversions test	0.99667	Passed

4. Conclusion and discussion

The article proposed new technique for second-level verification of the cryptographic quality of RNG/PRNG, intended for key generation. The task of the second-level verification is to detect faults in RNG/PRNG before these faults become critical and dangerous from the cryptographic point of view. This second-level verification consists of 5 tests, which are detailed described in this work. For each test the simple algorithm to calculate corresponding P-value is given, because second-level verification uses the set of obtained P-values to make decision about RNG/PRNG quality. As part of justification of the set of tests, chosen for this verification, we proved that these tests are in dependent using two different methods: one is based on limit normal distribution, the second is based on Chernoff inequality. Both methods made decision about tests mutual independence.

To demonstrate practical usage of the second-level verification, we applied it to standardized PRNG, and obtained the expected result: PRNG was accepted.

As the follow direction of investigation, we consider justification of the value of time interval between second-level verifications, based on the nature of the generator, its characteristics, supposed variant of application and other factors.

Acknowledgements

The results of this work were obtained within the project 2023.04/0020 Development of methods and layout of the "DEMETRA" ARM for constant and periodic control of the functioning of cryptographic applications using statistical methods.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] L.E. Bassham III, A.L. Rukhin, J. Soto, J.R. Nechvatal, M.E. Smid, E.B. Barker and others. "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication 800-22, Revision 1a, (2010). URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

[2] Company "IIT". Information protection. Complexes and mechanism of information protection. Hardware RNG "Gryada-3" https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=47

[3] Black box. https://en.wikipedia.org/wiki/Black_box

[4] Lucian Constantin. "IoT devices have serious security deficiencies due to bad random number generation" (2021) https://www.csoonline.com/article/571183/iot-devices-have-serious-security-deficiencies-due-to-bad-random-number-generation.html

[5] Rui Wang, Georgios Selimis, Roel Maes, Sven Goossens. "Long-term continuous assessment of SRAM PUF and source of random numbers" Cryptography and Security (cs.CR)(2020) https://doi.org/10.48550/arXiv.2007.15909

[6] Kovalchuk, L., Nelasa, H., Rodinko, M., Bespalov, O. "A new extended strategy of processing of statistical testing results" CEUR Workshop Proceedings, 2024, 3933, pp. 158–167, ISSN 16130073 Publisher CEUR-WS https://ceur-ws.org/Vol-3933/Paper_12.pdf
[7] Singh V, Hasan MS, Azeemuddin S. "A High-Quality Random Number Generator Using Multistage Ring Oscillators and Fast Fourier Transform-Based Noise Extraction" Eng. 2024; 5(1):433-446. https://doi.org/10.3390/eng5010023
[8] Zhao X, Chen L-W, Li K, Schmidt H, Polian I, Du N. "Memristive True Random Number Generator for Security Applications" Sensors, 2024; 24(15):5001. https://doi.org/10.3390/s24155001
[9] Choi Y, Yeom Y, Kang J-S. Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources. Entropy. 2023; 25(7):1056. https://doi.org/10.3390/e25071056
[10] Datcu O, Macovei C, Hobincu R. Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change. Applied Sciences. 2020; 10(2):451. https://doi.org/10.3390/app10020451
[11] Álvarez, Rafael, Francisco Martínez, and Antonio Zamora. "Improving the Statistical Qualities of Pseudo Random Number Generators" Symmetry 14 (2022), no. 2: 269. https://doi.org/10.3390/sym14020269
[12] Foreman C, Yeung R, Curchod FJ. "Statistical Testing of Random Number Generators and Their Improvement Using Randomness Extraction" Entropy. 2024; 26(12):1053. https://doi.org/10.3390/e26121053
[13] Luis Crespo, José and González-Villa, Javier and Gutiérrez, Jaime and Valle, Angel. "Assessing the quality of random number generators through neural networks" Machine Learning: Science and Technology, IOP Publishing, volume 5 (2), (2024), https://dx.doi.org/10.1088/2632-2153/ad56fb
[14] Aye Myat Nyo et al., "Quality analysis of Pseudorandom Number Generator using rough sets," 2010 2nd International Conference on Education Technology and Computer, Shanghai, China, (2010):V2-338-V2-342, doi: 10.1109/ICETC.2010.5529372.
[15] Ferreira MJ, Silva NA, Pinto AN, Muga NJ. Statistical Validation of a Physical Prime Random Number Generator Based on Quantum Noise. Applied Sciences. 2023, 13(23):12619. https://doi.org/10.3390/app132312619
[16] Preez V., Johnson M., Leist A., Hawick Ken. "Performance and Quality of Random Number Generators." Technical Report CSTN-122 (2011).
[17] Deshmukh Shrutika, Damle Bhagyashree, Kottur Suhasini. "Review of Random Number Generation." International Journal of Current Trends in Engineering & Research (IJCTER) (2017) https://doi.org/10.13140/RG.2.2.21227.62248.
[18] Crocetti, Luca, Pietro Nannipieri, Stefano Di Matteo, Luca Fanucci, and Sergio Saponara. "Review of Methodologies and Metrics for Assessing the Quality of Random Number Generators." Electronics 12, no. 3(2023): 723. https://doi.org/10.3390/electronics12030723
[19] Priyanka, Hussain Imran, Khalique Aqeel. "Random Number Generators and their Applications: A Review". IJRECE VOL 7 (2019): 1777-1781.
[20] Bespalov O., Kovalchuk L., Klimenko T., "New methods for testing random/pseudo-random sequence generators at different stages of their functioning" Èlektron. model. 2025, (5).
[21] Chi-Square (X^2) Table | Examples & Downloadable Table Published on May 31, 2022 by Shaun Turney. Revised on June 21, (2023). URL: https://www.scribbr.com/statistics/chi-square-distribution-table/
[22] Standard Normal Distribution Table. Copyright © 2023 Rod Pierce URL: https://mathsisfun.com/data/standard-normal-distribution-table.html
[23] DSTU 9041:2020 Information technologies. Cryptographic information security. Short message encryption algorithm based on twisted Edwards elliptic curves, 2020. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90523