European Information Technologies Certification Institute
Avenue des Saisons 100-102, 1050 Brussels, Belgium, EU
Web: https://www.eitci.org, E-mail: info@eitci.org
Phone: +32 2 588 73 51, Fax: +32 2 588 73 52

Reference Standard

RS-EITCI-QSG-EQRNG-TESTING-STD-VER-1.0

Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Testing and Verification Schemes including Sustaining Secrecy

EITCI INSTITUTE QUANTUM STANDARDS GROUP

EITCI-EQRNG-QSG

Brussels, 22nd December 2019
Version: 1.0

Table of contents

1. Randomness testing and verification

1.1. Hypothesis testing and verification

The model of statistical testing of quantum randomness in its computational implementation constitutes area of application of the hypothesis testing. Hypothesis testing is a strict mathematical approach for verifying assumptions about the general population or statistical populations, i.e. sets of items subject to statistical testing. This verification concerns the answer to the question whether the supposition (hypothesis) is justified and requires determination of the content of the hypothesis, which in the case of randomness testing is defined as a statement that a given element of the statistical population (random sequence) is significantly random (or truly random in respect to pre-defined statistical parameters). Mathematical verification of the strict hypothesis that the sequence is truly random is not possible in mathematical terms.

The hypothesis about the randomness of a given numerical sequence (e.g. a binary sequence) can be verified only in the convention of randomness in relation to the sequences in which the lack of this randomness can be demonstrated. This means that the tested hypothesis is not in fact the hypothesis of true randomness of the statistical series, but only a conventional definition of randomness functioning as a failure to show a randomness of fracture (constituting a certain minimal level bar, which, however, can be arbitrarily raised by parameterizing tests, which in turn, however, involves the cost of computing resources predisposed to implement the testing and the verification of randomness beyond the capacities of the system of randomness generation, which in the essential part of the standardized EQRNG architecture involves quantum randomness verification model associated with the concept of public proving randomness without revealing its form in the quantum entanglement regime).

As indicated above, the computational testing is only a negative criterion, and the proof of true quantum randomness should be based on the laws of quantum mechanics in terms of randomness generation. Here, a quantitative entanglement introduces a significant qualitative advantage over the classical randomness generation, where the fundamentally non-classical correlations in the measurement results allow at the level of physics laws to guarantee the randomness of sources by breaking the classical correlations imposed by locality.

The calculation model of statistical randomness testing can be used to confirm that a quantum random string was not generated in the event of any implementation irregularity in a way that distorts its randomness (introducing repeatability or predictability resulting from classical processes that undesirably occur in incorrect implementation of the quantum process). However, this is all that such a model can offer. In particular, this type of a model cannot guarantee that a given random sequence is truly random (and states, at the most, that there are no deviations in the specified random distribution from the random distribution defined in this distribution, or verified deterministic patterns of given lengths and forms). However, the fact that the sequence is truly random can only be guaranteed by the process of its generation, in which there is no fundamental predictability, i.e. the quantum-mechanical process, in which only the laws of nature guarantee non-determinism. In connection with the problems of qualitative and quantitative verification of true randomness discussed in the research results, quantum physics based technology becomes the only adequate instrument to prove true randomness by determining the influence of classical factors on the quantum system, which is referred to as the decoherence in the field of quantum mechanics.

The coherent quantum system is subject to unitary evolution in which the degrees of freedom of the quantum system do not get entangled with the degrees of freedom of the macroscopic environment of the system. Imperfect isolation of the quantum system from its surroundings leads to the process of quantum decoherence, i.e. the system drops a coherent state through non-uniform evolution, i.e.

getting entangled in the sense of quantum entanglement of the degrees of freedom of the environment (the dynamics of the quantum decoherence process depends on the physical system, and the process of getting around the degrees of freedom of the environment is associated with the difficulty of isolating the interaction of the system with its surroundings).

Therefore, in foundational terms of the true randomness generation, the physical side of this process is of a key importance, including the implementation of quantum dynamics in a random source and the study of decoherence occurring under physical interactions at the quantum level. Nevertheless, the complementary role of statistics is a supportive criterion, however, all its limitations in relation to quantum randomness testing should be emphasized as meeting minimum industrial standardization of random generation, i.e. ensuring that the technically generated quantum randomness is definitely not classic and the classical errors have not crept in the process, which would be verified by the computational model.

In accordance with this goal of the quantum randomness verification model in its computational part of statistical testing methods, the reference standard presents below its statistical characteristics.

1.2. Statistical testing of randomness

Here, the central concept is the concept of a statistical test, which was adopted to be called a specific mathematical function that allows estimating the probability value of a certain statistical hypothesis in a population based on a random sample from that population.

Statistical tests against the application criterion can generally be divided into parametric and non-parametric.

The first group, parametric tests, are used to verify parametric hypotheses, i.e. referring to the parameters of statistical distribution of the examined feature in the general population. Most often, parametric statistical tests verify hypotheses about population parameters such as arithmetic mean, variance, or structure index (fraction, i.e. the ratio of the number of distinguished elements to the number of all elements of the sample or population - hypotheses regarding the value of fraction / proportion in the general population or comparing their values in two or more populations). In addition, parametric tests are defined and used with a significant assumption of knowledge of the general form of the cumulative distribution function in the population whose statistical hypotheses are the subject of research. In parametric tests (e.g. average values, proportions or variances), the random sample parameters are compared with hypotheses regarding the values of these parameters.

As mentioned above, parametric tests can also be carried out in two or more populations in which the parametric properties of these populations are compared. In turn, nonparametric tests are used to verify unparametrized hypotheses, for example in terms of compliance of the distribution of the trait in the general population with a specific theoretical statistical distribution, as well as e.g. compliance of the distributions in two or more populations, or the randomness of the examined sample of the general population, which concerns this discussion in the field of testing the randomness of generation of numerical sequences.

Regarding applications, nonparametric tests are usually divided into two basic groups for testing the properties of one-dimensional populations (relevant in this case, random string tests) and for comparing the properties of two or more populations. In the first group can be distinguished as the most important nonparametric tests, the so-called compliance tests: chi-square and lambda (Kolmogorov-Smirnov), i.e. tests verifying whether the distribution in a given population for a given random variable corresponds to the assumed theoretical distribution when a statistical sample is

available (finite number of random variable observations), also working comparatively for two populations, as well as series tests (sample randomness, i.e. Stevens and Wald-Wolfowitz tests).

A special case of compliance tests are normality tests, the best of which according to Monto-Carlo analyzes is the Shapiro-Wilk normality test (testing the compliance of the distribution in the studied statistical population with the normal distribution). It can be mentioned here that compliance tests (e.g. the lambda Kolmogorov-Smirnov test) can be tests of normality if the theoretical distribution adopted is a normal distribution (Gaussian distribution), although their effectiveness is less than the Shapiro-Wilk test. Non-parametric tests, the configuration of which is to enable comparative testing of the properties of two populations, include: Kolmogorov-Smirnov test, chi-square homogeneity test, as well as median, series, character tests, etc.

The role of these tests is to verify the compatibility of two (or more through comparisons) of statistical empirical distributions generated from independent samples (applies to Kolmogorov-Smirnov tests, chi-square homogeneity, median and series) or generated in combined samples. Almost all nonparametric tests are equivalent to the relevant parametric tests.

1.2.1. Mathematical definitions for statistical testing of randomness

As regards the description of the randomness testing statistical model, reference should also be made to the basic mathematical concepts that formalize the discussion in the field of statistics, i.e. to the basic definitions within the theory of statistics. First of all, therefore, in the discussed hypothesis testing model, it should be clarified that the null hypothesis is the hypothesis subject to verification, i.e. in the case of randomness testing, the hypothesis about string randomness.

The alternative hypothesis is, in turn, the opposite hypothesis, in this case concerning the lack of randomness in the string. Random sequences constituting the general population or the statistical population are the subject of the abovementioned statistical tests, which correspond to testing of sources of randomness generation, as the strings from these sources reflect the characteristics of randomness of the sources, with the parameterization of randomness testing being the length of the strings and the subject of statistical tests. Elements of the statistical population (individual random strings from given sources of randomness generation) are contained in large size strings, constituting their substrings. Another concept is test statistics (a mathematical method of searching for static deviations from randomness), which is a type of statistics adopted in a given mathematical method.

Most randomization generation tests are based on the chi-square statistical distribution (the distribution of a random variable defined as the sum of squares of independent random variables with a normal distribution), which is also the most commonly used statistical test for hypothesis verification. Another important concept is the level of significance (usually denoted by alpha) defining the maximum allowable probability of a type 1 error (otherwise it is the maximum risk of error that can be accepted in a given problem). The choice of the alpha value depends on the definition of the problem of the level of accuracy at which the statistical test is to verify the assumed hypotheses. The commonly adopted parameterization is alpha = 0.05, 0.03, 0.01 or even 0.001 (in the parameterization of the calculation model of the quantum random verification, the parameter alpha is as large as 0.1, i.e. 10 %).

The level of significance is sometimes called simply the size of the statistical test. The value of the assumed significance level is compared to the one calculated from the statistical test.

The p value (P-value) is the test probability (sometimes the test statistic values are immediately compared with the value corresponding to a given level of significance). If the P-value is greater than alpha, it means that there is no reason to reject the so-called the null H_0 hypothesis, which usually states that the tested distribution is random (hypotheses defined in this way have the statistical, computational randomness tests discussed below).

The p value is therefore a statistically crucial measure of the strength of evidence provided by statistically analyzed data providing a hypothesis. In terms of the concepts of error in testing hypotheses, two types are distinguished. A type 1 error applies to the rejection of a random string that was generated by a random generator and was, however, incorrectly assessed as a supposed non-random string as a result of the test (this type of error can be defined otherwise as incorrect rejection). In turn, a type II error relates to a situation in which the tested random sequence is incorrectly accepted as random, despite the fact that it was generated by a non-random generator (incorrect acceptance). The confidence interval (with a confidence factor of 1 - alpha) is, in turn, assumed to be the range which, with a certain level of certainty, contains the value of the given estimated parameter.

In the basic course of the model statistical test, certain statistics are determined as a function of the results of the random sample, and then its statistical distribution is determined, assuming that the null hypothesis is true (this statistics is marked as W and is called the test statistics or test function).

After determining the test function (in the case of testing the null hypothesis, the randomness of the sequence is also the most often used statistical distribution is chi-square), the level of significance alpha is selected, which is the maximum probability of the first type of error acceptable in the test (i.e. rejection of the null hypothesis despite that it is true, i.e. in the case of testing the randomness of rejection as a non-random sequence actually random). As indicated above, the alpha values should be close to zero to minimize the risk of a first (false positive) error, but a higher significance level increases the sensitivity of the test.

The next step is to determine the critical test area, i.e. the area located at the ends of the distribution. If the value of the calculated statistics is in this area, then the null hypothesis is rejected.

The critical area of the test (sometimes also called the critical set) is formally a set of values of the distribution of the test function in the relevant statistical test, whose occurrence due to the assumption of the null hypothesis is unlikely enough (according to the assumed level of significance) that the actual implementation of the random variable in the critical area allows to reject this hypothesis. In other words, the critical area calculated from data statistics is assumed to be unlikely if the null hypothesis is true. Critical values are called critical area boundary values and the relationship between the critical area (denoted by C) and the significance level alpha expresses the size of the critical area, i.e. its probability integral, which is equal to alpha.

In other words, the alpha significance level means the probability of realizing a random variable in the critical range provided that the null hypothesis is true. For example, the critical area alpha = 0.1 is the same as the 10% probability of statistics in this range assuming the null hypothesis is true.

The free choice of alpha significance level means that the data, subject to verification, statistical hypotheses are qualified as significant or irrelevant only depending on the chosen alpha value. Therefore, often instead of determining the level of significance alpha and alternatively determining the significance of the hypothesis at a specific level of the significance level factor alpha, simply p-value (test probability) is given as the result of the statistical test, i.e. the probability of receiving under the assumption that the null hypothesis is true of the value of the test statistics corresponding to the empirically obtained reference to the specific value of the significance level of the relevant hypothesis (which releases the dependence of the hypothesis testing result on the arbitrariness of the selection of the significance level).

1.3. Summary of the statistical testing of randomness

To summarize, the size of the critical area (located at the ends of the distribution) defines the level of significance alpha and its location is determined by the alternative hypothesis (the critical area of the

test is separated from the remaining distribution of statistics by so-called critical values denoted as alpha, i.e. values read from the distribution of statistics at a certain level of significance alpha with the fulfillment of the relationship depending on how the alternative hypothesis is defined. In further steps of the test there are run calculations of statistics from the sample (by assigning appropriate mathematical functions on the results of the sample in accordance with the mathematical definition of the statistical test) and to make a decision by reference to the statistical value obtained from the sample, i.e. the p value with the critical value of the test. If the p value is found in the critical area of the test, the null hypothesis is rejected in favor of the alternative hypothesis. Otherwise, there are no grounds to reject the null hypothesis, which means that the null hypothesis may not necessarily be true. The test probability, i.e. the p-value does not contain information about the truth of the null hypothesis. It authorizes only to reject the null hypothesis if the abovementioned condition is met (finding the p-value in the critical area of the test). Otherwise, it is not an important criterion for verifying the statistical properties of the sample tested. An important criterion for using statistical tests in hypothesis verification is the repeatability of empirical results, which in this case boils down to the implementation of a series of tests on large samples of random strings.

1.4. The standardized set of the randomness statistical tests

The list of statistical tests in the quantum randomness verification model along with their relevant parameterization for the verification of random quantum sequences in the reference standard is following below.

The reference standard model for verification of quantum randomness in the statistical and classical computational approach is based on the statistical tests by Marsaglia (Diehard) and by Lecuyer (U01).

This model extends the NIST (National Institute of Standardization and Technology in the US).

The basic configuration of the tests as part of the NIST requirements is not very extensive and refers to the certification of the classical Pseudo-Random Numbers Generators (PRNG). Parameterization of the Diehard and U01 statistical tests implementing the scope of the NIST standard, but in advanced configuration for quantum randomization verification requires vast computing resources, mainly through exponentially scalable computational complexity searching for patterns of increasing sizes.

The implementation of all tests in the computational model of quantum randomness verification according to the present reference standard was carried out on the basis of literature specifications of individual tests and their mathematical procedures with the parameterization of tests based on the empirical studies to verify quantum randomness in relation to the practicality of consumed computational resources.

1.5. List of the randomness statistical tests included in the reference standard

- One-bit frequency test (Frequency, monobit) – sstring_HammingWeight2 test of the U01 set - significance level alpha = 0.1 and the minimum string length n > 10^6
    - Kai Lai Chung, Elementary Probability Theory with Stochastic Processes. New York: SpringerVerlag, 1979 (pp. 210-217)
    - Jim Pitman, Probability. New York: Springer-Verlag, 1993 (pp. 93-108)

- Block Frequency Test - sstring_HammingWeight2 test of the U01 set - alpha = 0.1, n> 10^6, block length M = 100, number of blocks N = 10,000 up to M = 10,000, N = 100
    - Nick Maclaren, "Cryptographic Pseudo-random Numbers in Simulation," Cambridge Security Workshop on Fast Software Encryption. Dec. 1993. Cambridge, U.K .: R. Anderson, pp. 185-190

- Donald E. Knuth, The Art of Computer Programming. Vol 2: Seminumerical Algorithms. 3rd ed. Reading, Mass: Addison-Wesley, 1998 (pp. 42-47)
- Milton Abramowitz, Irene Stegun, Handbook of Mathematical Functions: NBS Applied Mathematics Series 55. Washington, D.C .: U.S. Government Printing Office, 1967

- Runs test – sstring_Run test of the U01 set and also the Runs test of the Diehard set -alpha = 0.1, n> 10^6
  - Jean D. Gibbons, Nonparametric Statistical Inference, 2nd ed. New York: Marcel Dekker, 1985 (pp. 50-58)
  - Anant P. Godbole, Stavros G. Papastavridis, (ed), Runs and patterns in probability: Selected papers. Dordrecht: Kluwer Academic, 1994

- Test of the longest run in the block (Longest Run) - sstring_LongestHeadRun test of the set U01 - alpha = 0.1, n> 10^6, block length M = 10000
  - F. N. David, D. E. Barton, Combinatorial Chance. New York: Hafner Publishing Co., 1962, p. 230
  - Anant P. Godbole, Stavros G. Papastavridis (ed), Runs and Patterns in Probability: Selected Papers. Dordrecht: Kluwer Academic, 1994
  - Pal Revesz, Random Walk in Random and Non-Random Environments. Singapore: World Scientific, 1990

- Binary matrix rank test (Rank) - smars_MatrixRank test of the U01 set and Binary Rank Tests for Matrices of the Diehard set - alpha = 0.1, n> 10^6, number of rows and columns Q = 168, M = 168
  - George Marsaglia, DIEHARD: a battery of tests of randomness, http: //www.stat.fsu.edu/pub/diehard/
  - I. N. Kovalenko (1972), "Distribution of the linear rank of a random matrix," Theory of Probability and its Applications. 17, pp. 342-346
  - G. Marsaglia, L. H. Tsay (1985), "Matrices and the structure of random number sequences," Linear Algebra and its Applications. Vol. 67, pp. 147-156

- Discrete Fourier Transform Test, spectral test (FFT) - sspectral_Fourier1 test of the U01 set - alpha = 0.1, n> 10^6
  - R. N. Bracewell, The Fourier Transform and Its Applications. New York: McGraw-Hill, 1986

- Nonoverlapping template) - smars_CATBits test of the U01 set - alpha = 0.1, n> 10^6, pattern length m> 15
  - A. D. Barbour, L. Holst, S. Janson, Poisson Approximation (1992), Oxford: Clarendon Press (Section 8.4 and Section 10.4)

- Overlapping template - smultin_MultinomialBitsOver test subclass of set U01 - alpha = 0.1, n> 10^6, m> 15
  - O. Chrysaphinou, S. Papastavridis, "A Limit Theorem on the Number of Overlapping Appearances of a Pattern in a Sequence of Independent Trials." Probability Theory and Related Fields, Vol. 79 (1988), pp. 129-143
  - N.J. Johnson, S. Kotz, A. Kemp, Discrete Distributions. John Wiley, 2nd ed. New York, 1996 (pp. 378-379)

- Universal Maurer test (Universal Maurer test) - svaria_AppearanceSpacings test of the U01 set - alpha = 0.1, n> 10^6, block length L = 6, parameter Q = 640 which gives the minimum number bits equal to 387 840 within the accepted limit of 1 million bits
    - Ueli M. Maurer, "A Universal Statistical Test for Random Bit Generators," Journal of Cryptology. Vol. 5, No. 2, 1992, pp. 89-105
    - J-S Coron, D. Naccache, "An Accurate Evaluation of Maurer's Universal Test," Proceedings of SAC '98 (Lecture Notes in Computer Science). Berlin: Springer-Verlag, 1998
    - J. Ziv, "Compression, tests for randomness and estimating the statistical model of an individual sequence," Sequences (ed. R.M. Capocelli). Berlin: Springer-Verlag, 1990
    - J. Ziv, A. Lempel, A universal algorithm for sequential data compression, Transactions on Information Theory. Vol. 23, pp. 337-343

- Linear complexity test - scomp_LinearComp test of set U01 - alpha = 0.1, n > 10^6, block length M = 5000, number of blocks N = 200
    - H. Gustafson, E. Dawson, L. Nielsen, W. Caelli, "A computer package for measuring the strength of encryption algorithms," Computers & Security. 13 (1994), pp. 687-697
    - A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997
    - R.A. Rueppel, Analysis and Design of Stream Ciphers. New York: Springer, 1986

- Serial test - smultin_MultinomialBitsOver test (with parameter delta = 1) of set U01 - alpha = 0.1, n> 10^6
    - I. J. Good (1953), "The serial test for sampling numbers and other tests for randomness," Proc. Cambridge Philos. Soc. 47, pp. 276-284
    - M. Kimberley (1987), "Comparison of two statistical tests for keystream sequences," Electronics Letters. 23, pp. 365-366
    - D. E. Knuth (1998), The Art of Computer Programming. Vol. 2, 3rd ed. Reading: AddisonWesley, Inc., pp. 61-80
    - A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997

- Approximate entropy) - sentrop_EntropyDiscOver test of set U01 - alpha = 0.1, n > 10^6
    - S. Pincus, B. H. Singer, "Randomness and degrees of irregularity," Proc. Natl. Acad. Sci. USA. Vol. 93, March 1996, pp. 2083-2088
    - S. Pincus, R. E. Kalman, "Not all (possibly)" random "sequences are created equal," Proc. Natl. Acad. Sci. USA. Vol. 94, April 1997, pp. 3513-3518
    - A. Rukhin (2000), "Approximate entropy for testing randomness," Journal of Applied Probability. Vol. 37, 2000

- Cumulative sums test - swalk_RandomWalk1 test (for M statistics) of the U01 set and also in connection with the Overlapping Sums test of the Diehard set - alpha = 0.1, n> 10^6
    - Frank Spitzer, Principles of Random Walk. Princeton: Van Nostrand, 1964 (p. 269)
    - Pal Revesz, Random Walk in Random And Non-Random Environments. Singapore: World Scientific, 1990

- Random trip test - swalk_RandomWalk1 test of the U01 set - alpha = 0.1, n> 10^6
    - M. Baron, A. L. Rukhin, "Distribution of the Number of Visits For a Random Walk," Communications in Statistics: Stochastic Models. Vol. 15, 1999, pp. 593-597

- Pal Revesz, Random Walk in Random and Non-random Environments. Singapore: World Scientific, 1990
- Frank Spitzer, Principles of Random Walk. Princeton: Van Nostrand, 1964, (p. 269)

- Variant test of random trips - swalk_RandomWalk1 test of the U01 set - alpha = 0.1, n> 10^6
  - M. Baron, A. L. Rukhin, "Distribution of the Number of Visits For a Random Walk," Communications in Statistics: Stochastic Models. Vol. 15, 1999
  - Pal Revesz, Random Walk in Random and Non-random Environments. Singapore: World Scientific, 1990
  - Frank Spitzer, Principles of Random Walk. Princeton: Van Nostrand, 1964, (p. 269)

In a shortened list form:

1. Single-bit frequency test (Frequency, monobit) - sstring_HammingWeight2 of set U01 - significance level alpha = 0.1 and minimum string length n> 10^6
2. Block Frequency Test - sstring_HammingWeight2 of the U01 set - alpha = 0.1, n> 10^6, block length M = 100, number of blocks N = 10000 to M = 10,000, N = 100
3. Runs test - sstring_Run of the U01 set and also the Runs test of the Diehard set - alpha = 0.1, n> 10^6
4. Test of the longest run in the block (Longest Run) - test sstring_LongestHeadRun of the set U01 - alpha = 0.1, n> 10^6 block length M = 10000
5. Binary matrix rank test (Rank) - smars_MatrixRank of the U01 set and Binary Rank Tests for Matrices of the Diehard set - alpha = 0.1, n> 10^6, number of rows and columns Q = 168, M = 168
6. Discrete Fourier Transform Test, spectral test (FFT) - sspectral_Fourier1 test of the U01 set - alpha = 0.1, n> 10^6
7. Nonoverlapping template) - smars_CATBits set U01 - alpha = 0.1, n> 10^6, pattern length m> 15
8. Overlapping template) - smultin_MultinomialBitsOver test subclass of U01 - alpha = 0.1, n> 10^6, m> 15
9. Universal Maurer test (Universal Maurer test) - svaria_AppearanceSpacings test set U01 - alpha = 0.1, n> 10^6, block length L = 6, parameter Q = 640 which gives the minimum number of bits equal to 387 840 within the accepted limit of 1 million bits
10. Linear complexity test - scomp_LinearComp test of the U01 set - alpha = 0.1, n> 10^6, block length M = 5000, number of blocks N = 200
11. Serial test - smultin_MultinomialBitsOver test (with parameter delta = 1) of set U01 - alpha = 0.1, n> 10^6
12. Approximate entropy) - sentrop_EntropyDiscOver of set U01 - alpha = 0.1, n> 10^6
13. Cumulative sums test - swalk_RandomWalk1 test (for statistics M) of the U01 set and also in connection with the Overlapping Sums test of the Diehard set - alpha = 0.1, n> 10^6
14. Random trip test - swalk_RandomWalk1 test of the U01 set - alpha = 0.1, n> 10^6
15. Variant test of random trips - swalk_RandomWalk1 test of U01 set - alpha = 0.1, n> 10^6

1.6. Application of the randomness statistical tests

The goal of the application of the randomness statistical tests is to allow verification of the stationarity and ergodicity of the process of stochastic generation of a bit random sequence (constant average values, variances and autocorrelation functions). This verification is ensured by the following statistical methods included in the model: single-bit and block frequency tests, waveform tests (straight and longest waveform in a block) as well as binary matrix rows test. In addition, it is to enable searching for repetitive substrings, which constitute recognizable patterns. The theory of randomness, developed as a mathematical field of basic research, defines a whole series of statistical

tests allowing to measure the level of randomness of bit strings. Classical RNGs that use deterministic physical processes (e.g. electronic noise class) for the genes of random strings introduce predictable patterns (e.g. associated with periodicity of wave properties in electrodynamics) that have low Kolmogorov complexity, and in Shannon's information theory reveal the possibility of lossless compression. The search for repetitive substrings constituting recognizable patterns is carried out by the following statistical methods: tests of discrete Fourier transform / spectral (FFT), universal Maurer test (Universal Maurer test), serial (Serial) and entropy estimation (Approximate entropy). Finally, the model should also allow mapping the physical structure of the generation process mechanism in bit values in a random sequence. This is important because even if the random sequence is stationary, ergodic and does not contain repetitive substrings, if it is based on a deterministic process, then the simulation of such a process (even approximate) allows you to reproduce a largely convergent bit sequence (entropy fast). bit positions is less than the value of 1 for a recipient who has premises for the process). The search for unique substrings that are recognizable patterns is carried out by statistical tests: the occurrence of non-overlapping patterns (Nonoverlapping template) and overlapping patterns (Overlapping template).

Below is a detailed discussion on the parameterization of statistical tests under the reference standard model to adapt it to verify quantum randomness. This parameterization boils down to the task of correspondingly higher sensitivity of statistical tests to find deterministic classic deviations from randomness than conventionally required to verify the unpredictability of pseudo-random strings. The overall research result, however, is demonstrating, as discussed in the R-1 report, that statistical classical models cannot prove quantum randomness, at most increasing the minimum bar for detecting classical deviations. True quantum randomness cannot include any (even the smallest) classical deviations and its proving can take place only within physics (i.e. description of the evolution of the system occurring in a coherent quantum regime confirmed experimentally, e.g. in the verification of the violation of the Bell inequalities by quantum correlations in the results of entangled quantum state measurements). Thus, the quantum randomness is demonstrated in the area of quantum decoherence, and classical statistical models can only serve as an auxiliary criteria for the negative detection of classical deviations that may exist in systems due to implementation imperfections, introducing processes in accordance with the laws of classical physics. The arbitrarily high-level parameterization of the statistical tests allows for the detection of ever smaller potential classic deviations in the tested random sequences, but is associated with increasing computational complexity. Therefore, the reference standard parameterizes the statistical tests towards maximized sensitivities (meeting the contractual criteria in terms of information entropy between the sequences generated in classical and quantum processes - here it should be noted that contractual because for truly random quantum sequences entropy on each the next bit position of the string should be equal to 1 and not even arbitrarily close to 1). The parameterization of the model in terms of its optimal sensitivity for the verification of quantum sources (in the sense of the criterion of negative detection or potentially existing very small deterministic classic deviations) boils down to empirical testing of parametric values of selected statistical methods in relation to the limits of computational resources, so that verification remains practical (parameterization of this primarily applies to the input lengths of random strings as the minimum sample sizes - the larger, the better enabling detection of small deviations from randomness in the form of long-range correlations, as well as the length of operating blocks in the search for aperiodic patterns, which can also be large in size, and the search for the increasing sizes of all possible aperiodic patterns causes an exponential increase in the computational complexity). Qualifying studies underlying the present reference standard of the parameterized model for verifying quantum randomness therefore relate to the optimization of its sensitivity (in accordance with the minimum requirements for verification of quantum randomness, especially in terms of entropy, as explained in the discussion below) in relation to the costs in the form of the necessary computational resources (translating into verification time, which should be rational).

1.7. Quantum randomness statistical tests empirical qualification

The present reference standard in quantum randomness testing was developed upon an empirical analysis concerning quantum-generated random sequences (the results are presented in the XXX resource appendix).

Each of the empirically tested sequences obtained in the laboratory from experimentally verified quantum processes contained a sequence of 800 million bits (4000 million bits or 4 Gbits in total):

- cs_100mb_1.dat - first part; continuous generation, generation process: current fluctuations based on white noise on a cluster of semiconductor transistors (effect empirically verified as a quantum in connection with tunneling of electrons in the semiconductor diode connector)
- cs_100mb_2.dat - part two; continuous generation, generation process: tangle-free quantum optics system (attenuated low intensity multiphoton source; beam splitter; low sensitivity photon detectors for recording strongly suppressed pulses with statistical distribution of average values of individual photons in the pulse - in polarization regime, as well as in quantum phase properties) light, i.e. in the phase shift regime in the range of recorded photons using Mach-Zehnder interferometer systems)
- cs_100mb_3.dat - part three; continuous generation, generation process: tangled optical system (source of entanglement - birefringent BBO crystal separating the beam as a result of the SPDC process, pairs of polarized tangled photon pairs occur at the intersection points of the beam; 50/50 beam splitters; high sensitivity detectors, single-photon avalanche diodes, cooled piezoelectrically - a separate demonstration of fractures of the Bell inequality
- cs_100mb_4.dat - part four; mosaic time scale with an hour period (acquisition of 10 parts); process as sample \ _1
- cs_100mb_5.dat - part five; time-scale mosaic sample and source mosaic of sources _1 _2 and _3
- cs_100mb_1-5.dat - concatenation of parts _1 to _5 into one string of 4000 million bits.

The main element of calculations in the verification of randomness are P-values of statistical tests (the so-called test probabilities), which can be interpreted as the probabilities that the observed phenomena in the statistical sample from the general population may have occurred accidentally due to random variability of the statistical samples, even if in the population of the phenomenon they do not occur at all. As part of the formal definition, the P-value is the increasing probability of random sampling similar to that observed with the assumption that the null hypothesis is met. This is the basic parameter of inference in the form of hypothesis verification in the statistical frequency approach. The main purpose of calculating the P-value is negative inference, i.e. if the P-value is lower than the statistical significance level adopted in advance, it should be concluded that the null hypothesis is false. Hence, an important parameterization of the test sensitivity towards configuring known statistical methods to verify quantum randomness is to increase the significance factor (alpha).

Of course, increasing the level of significance increases the risk of type I error (false positive, i.e. rejection of the null hypothesis despite its undetected truthfulness). It should be emphasized that this is an important consequence of the basic approach to increasing the sensitivity of test parameterization for the verification of quantum randomness, but increasing the likelihood of false positive errors. This is not a problem, however, if the generator is actually quantum, then it should not return P-values below, even a high confidence factor in randomness tests (and if this is the case, it means that in the implementation of the quantum generator the classic deviation of randomness is detected). An important aspect of the correct use of the statistically calculated P-value in frequency inference as part of hypothesis verification is repeatability. The single P-value obtained from the test is only for the basic control of errors (type I) and does not allow for making further conclusions. Only

the high repeatability of the calculated P-value in a series of tests for a given random sample allows to increase its probative value.

1.8. Quantum randomness statistical testing non-definite result remarks

It should be emphasized that in the present context of the reference standard for the statistical true quantum randomness testing and verification, one cannot speak of its proving due to fundamental non-determinism. At most, the P-value is intended to demonstrate the rejection of the null hypothesis of true randomness by detecting deviations of the nature of classical determinism (hence testing quantum randomness is only a negative criterion, a certain minimal-level bar, which can be raised by an adequately sensitive parameterization in relation to the limitations on computational resources in in the complexity of searching for growing classic patterns - every quantum generator must pass this bar - but this still does not mean proof of its quantumness).

Evidence of quantumness, according to the presented reference standard, is provided only by the empirically verified evolution regime under the quantum laws of nature, which are, however, beyond the reach of classical statistics (what's more, it can be shown that in purely quantum effects, without classic equivalents, such as quantum entanglement, correlations of measurement results completely violate limitations of the classical statistics - which is well known in terms of the first experimentally confirmed in 1981 by Aspect of the violation of the Bell inequalities and concerns the so-called Einstein-Podolski-Rosen paradox in quantum mechanics). The empirical demonstration of the quantum phenomenon (e.g. by violating the Bell inequalities) and the empirical and theoretical verification of decoherence in the system are appropriate instruments for proving quantum randomness in the prototype systems of quantum randomization generators, which is the subject of work under stage 2 of the project - while classic statistical tests even parameterized for verification of quantum randomness, they can only be used as a classic supportive tool for the negative criterion: i.e. detection of any classical deviations in the quantum process and demonstrating statistical regularities of a deterministic nature that should not be present at all in a (quantum) random distribution.

The normalized P-value is also of a significant nature in simplifying statistical methods (without losing their generality) in terms of their universal applicability to various theoretical statistical distributions, including in particular the most important of them allowing the best possible theoretical modeling of random sequences, as used in the Diehard and U01 tests, i.e. statistics from the chi-square and Kolmogorov-Smirnov, creating possibility of a direct comparison of the measure of unexpectedness of statistical empirical results assuming the truth of the null hypothesis (i.e. true randomness of the sequence).

The use of P-values in the manner described above is standard in classic randomness tests, including the statistical methods of the present reference standard, on which the calculation model of quantum randomness verification is based: the Diehard and U01 tests. NIST's reference requirements for certification of randomness generation based on these tests (which must also be met in terms of all individual tests of the developed quantum randomness generator) are parameterized for the purposes of verification of classical randomness. Parameterization takes into account, for example, relatively low significance factors alpha = 0.01 (i.e. 1%). In the parameterization of the computational model for the verification of quantum randomness in the present reference standard, the significance factor was assumed at a level of a higher order, i.e. alpha = 0.1 (10%), which means, on the one hand, a proportional increase in the sensitivity of detecting deterministic classic deviations from true randomness, and on the other hand, increases the risk of errors of the first kind (rejecting null hypotheses despite their truthfulness, i.e. rejections of truly random strings). However, for true quantum generators, such rejections (false positive errors), despite the fact that one order more likely, should still not occur anyway, which is the subject of empirical qualification of the present reference standard statistical testing model on random data

from empirically verified processes as truly quantum and laboratory-generated (also in terms of generation of physically verified quantum entanglement violating Bell inequalities and thus violating the local-realism).

1.9. Quantum randomness statistical testing parametrization remarks

An important aspect of the parameterization of the computational statistical model for quantum randomization verification is the consideration of checking the properties of low entropy deviation from maximum values at individual bit positions, of the order of 2^{-64} i.e. circa 5 times 10^{-20}. This value determining the optimal boundary with respect to computational resources for the distinction (in a conventional way, based on the classical statistical with all of its limitations, i.e. without the possibility of taking into account arbitrarily long deterministic patterns) of pseudo-random sequences from truly random (quantum) is verified in the calculation model using corresponding to the entropy estimation test configured for this value (sentrop_EntropyDiscOver test of the set U01). Entropy is estimated on a 1 bit string with the increasing length of the disposable block tested. The results of the model qualification in relation to that assumed in the present reference standard, the entropy limit value (adopted for theoretical quantum generated random sequences) conducted on physically (i.e. empirically in the field of quantum mechanics experiment) confirmed as quantum, i.e. truly non-deterministic random sequences – were positive and the present reference standard model was thus empirically qualified. The model is able to detect deviations from entropy of 2^{-64} – 5 times 10^{-20} magnitude, and qualification tests conducted on laboratory quantum randomized sequences exceed this entropy approach limit to 1 (i.e. they do not fall into the area critical test and do not demonstrate any classic randomness deviations or biases). According to the suppositions of the present reference standard, the main risk (of a technological nature) lies in the possible difficulties in modeling measures for parameterization of very small deviations from truly random, i.e. fully non-deterministic sequence. Currently widely described and available classical models and parametric randomness tests are adequate for pseudo-random strings. According to the discussion presented, their extreme configuration for verifying negatively anything not arbitrarily close enough to the perfect, i.e. truly quantum randomness is paid for by increasing the computational complexity. The assessment of the quality of the randomness of a bit string depends on the measures of deviation from the maximum binary entropy of 1 at each bit position. In this regard, a successful qualification of the parameterized standard model meeting the detectability of limit values of deviations from entropy equal to 1 on subsequent bits of a truly (i.e. quantum) random sequence assumed as stated above and declared in the present reference standard.

1.10. Quantum randomness statistical testing versus mathematical determinism limitations

According to the definite conclusion, as noted by von Neumann (1963), no mathematical calculation process can lead to true randomness because it is deterministic (due to mathematical axioms). If the pseudo-random string is generated using programming algorithms, it cannot be a truly random string for these very reasons. As indicated in the design application, e.g. a linear congruence generator is commonly used (based on a previous state, and 3 constant parameters, a new state in the modular algebra is calculated, saved for the next iteration, where it will be used as the input state), the deviation from true randomness is significant (moreover, if the initiation vector of such an algorithm - i.e. the abovementioned constants, will be invariant, then the strings generated by the algorithm will be identical). A similar situation occurs when using more complex algorithms based e.g. on register shifts and delayed Fibonacci recursions, or iterative hash functions (MD-5 / SHA-1) - random IV vectors are critical here (but even with their full randomness, deviations from algorithm-expanded pseudo-random nondeterminism are significant). This means that the classical entropy of random sequences is low compared to quantum entropy (based on non-deterministic quantum effects, which, however, due to the imperfection of the technical implementation of QRNG may introduce

some deviations). Thus, the proper parameterization of the quantum randomness verification model based on statistical tests constitutes an important part of the present reference standard, while in view of the problem of increasing computational complexity the standard proposes a new concept of shifting of the quantum randomness verification outside of the generator in a public manner while maintaining the secrecy of the random sequence, which is essential for cryptographic applications.

The parameterization for quantum verification of individual randomness tests upon the present reference standard is summarized below, while the elaborations of statistical test descriptions compiled into a quantum verification model based on the Marsaglia and Lecuyer testing sets are presented in the appendix. XXX

1.11. Quantum randomness statistical testing detailed parametrization

One-bit frequency test (Frequency, monobit) - configuration for quantum randomness verification:

Significance level adopted at the level of alpha = 0.1 (10%), government above the NIST recommendations requirements in the field of Diehard and U01 methods. Minimum bit string length n = 1 million bits (10^6), i.e. 5 rows above the minimum NIST recommendation (standard NIST recommendations point to parameterization of the test with random strings of at least 100 bits, i.e. n geq 100) . In the case of verification of the randomness of quantum sequences, it should be assumed that the test should detect even very small classical deviations in the quantum process, which may introduce frequency disturbances only in much longer sequences. Testing longer strings increases the computational complexity, but due to the low complexity of the subject test algorithm, you can successfully perform practical tests for string lengths exceeding one million bits, which in five orders of magnitude increase the level of sensitivity by applying one more order to increase the sensitivity of rejection of non-random string within significance level alpha = 0.1.

Block Frequency Test - configuration for quantum randomization verification:

The level of significance adopted at the level of alpha = 0.1 (10%) as for the frequency test, i.e. the order above the NIST recommendations requirements in the scope of Diehard and U01 methods. Also, as in the case of the standard frequency test for verifying the randomness of quantum sequences in a block test, it should be assumed that very small classical deviations in the quantum process should be detected, which may introduce frequency disturbances only in much longer sequences. Testing longer strings increases the computational complexity, but also like the standard frequency test, due to the low complexity of the algorithm, you can successfully perform practical tests for string lengths exceeding one million bits. This was also the minimum criterion in the random quantum verification model, which goes (10,000 times) over the standard NIST recommendations for parameterization of the test with random strings of at least 100 bits (n > 100) for model configuration for optimal verification of randomness quantum. In addition to the parameter M parameter configuration, the minimum block length (in the classic case, at least 20 bits assuming that they are greater than 0.1 minimum string length recommended by NIST, i.e. 100 bits, and that their number is less than 100) within the empirical optimization of this parameterization for verification of quantum randomness in the qualification of the model for large size strings (over 1 million bits), a minimum block length of 100 bits and their maximum number N of 10 thousand were asked (the maximum adequate block lengths established empirically for testing quantum generated strings are 10,000 with a minimum number of blocks of 100).

Runs test - configuration for quantum randomness verification:

Significance level adopted at the level of alpha = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. In addition to changing the level of significance for better verification of the randomness of quantum sequences, it should be

assumed that the test should detect even small classical deviations in the quantum process, which may introduce oscillatory disturbances detectable in much longer sequences. So, as in the case of frequency tests, testing longer strings in terms of sequence occurrence (monovalent waveforms) results in an increase in computational resources used, but due to the low computational complexity of the algorithm, practical tests can be performed for string lengths exceeding one million bits. Hence, in the parameterization of the subject model, the minimum length of the bit string for the waveform test n = 1 million bits.

Longest Run test in the block - configuration for quantum randomness verification:

As in the case of the usual waveform and frequency test, the significance level adopted at the level of alpha = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. As part of the parameterization of the test for quantum random verification, the standard NIST recommendations were raised for a minimum string length of n million bits (from over 6,000, i.e. 3 rows) and in this configuration block lengths of 10,000 bits, i.e. 2 rows over NIST recommendations (which is however, the length can be reduced to the standard NIST 128-bit recommendation to reduce computing resource requirements and randomization verification times.

Binary matrix rank test (Rank) - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. For the verification of quantum randomness, the probabilities were calculated for the quantum randomness selected as the optimal configuration for testing in sufficiently large strings in the 32 x 32 matrix range (M = 32, Q = 32), i.e. 1024 elements, which there are 976 within a million bits. For these matrix configurations were calculated and used in the programming implementation of the model proper statistical probabilities used in the function calculating the P-value of the test in accordance with the guidelines for calculating these values given by Marsaglia. An important requirement to configure the test to detect even small deviations potentially occurring in quantum-generated strings through the influence of classic effects is to assume a minimum random string length of at least 38QM, i.e. 38,912 bits (which means that at least 38 binary matrices can be filled). In the case of scaling the sensitivity of the test to detect even smaller classic deviations potentially occurring in the theoretically non-deterministic sequence of generated quantum randomness, matrix sizes adequate for the minimum string length of one million bits can be assumed, in which case the number of M rows and Q columns are 162 bits (total matrix then contains 28224 bits, and the 38QM parameter is close to the assumed minimum size, i.e. 1 million bits). Such ranges of matrix configuration require the calculation of appropriate probabilities before the test implementation, which was presented in the empirical studies performed in this configuration with a significant (almost by a row) increase in the consumption of computational resources in the test implementation (i.e. calculation time), which particularly justifies its derivation from a random generator in the concept of public verification of quantum randomness while maintaining its secrecy based on quantum entanglement.

Discrete Fourier Transform Test, Spectral Test (FFT) - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. In the case of verification of the randomness of quantum sequences, it should be assumed that the test of the discrete Fourier transform should detect even very small classical deviations in the quantum process, which may introduce disturbances in the distribution of spectral image only in much longer sequences. Spectral testing of longer strings increases computational complexity and this situation requires determining the optimal selection of the sample. Current empirical studies have shown that optimal results are obtained for string lengths exceeding one million bits. This was also the minimum criterion in the

random quantum verification model for the test of the discrete Fourier transform. It is a thousand times greater minimum string length than recommended by NIST for a spectral test, i.e. a recommendation of n equal to 1000 bits (increase in the possibility of detecting long-range correlations by 3 orders). Computational complexity in the spectral test despite the FFT algorithm (fast Fourier transform), however, increases logarithmically, i.e. exponentially. Therefore, a particularly important element of the Fourier Quantum Randomization Verification Model is the ability to derive the verification of randomness generation outside the generator itself while maintaining the secrecy of the sequence whose randomness is verified (which is the subject of the proposed proprietary concept using quantum entanglement for the task of implicit correlation between generated random sequences).

Nonoverlapping template test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. It should be emphasized that tests for finding patterns, including non-overlapping (non-overlapping) patterns, are the most important area of statistical verification of quantum randomness, which results from the possibility of masking classical effects in technically imperfect implementation of the quantum process through not necessarily repetitive but deterministic patterns. This means that the patterns do not have to contain statistical repeatability that would be detectable by statistical deviations according to the other standard randomness verification tests (i.e. their statistics do not differ from theoretical randomness expectations), nevertheless these patterns are deterministic and can be reproduced as part of a potential attack randomness in which such deterministic processes (reflected in aperiodic patterns) may have crept in. Therefore, the basic area of definitions of tests aimed at searching for patterns within quantum randomness testing is increasing the size of sought deterministic patterns, which takes place at a significant cost in the area of computational complexity (exponentially increasing with the size of patterns, due to the exponentially growing number of them as combinations in binary sequences). The standard recommendation of NIST is to search for patterns with a length of at least 9 bits (then there are 148 patterns that meet the aperiodicity of the patterns, and so many patterns should be found). Increasing the value of the number of bits in the patterns causes an exponential increase in complexity because so increases the number of possible patterns. As part of empirical research in the field of test parameterization for the quantum randomization verification model, it was possible to achieve the value of 15 bit patterns (among all possible aperiodic forms as many as 8848) with respect to computational practicality. For each of these patterns, a search is performed, which means that it is almost 2 rows more complex than in the case of 9-bit patterns. As regards model qualification, examples of 20 statistical test results out of 8848 completed (for all aperiodic standards) are presented. As in the case of the spectral test, but especially in the case of pattern search tests, a key element of the quantum randomness verification model in the context of exponentially increasing complexity relative to parameterization (in this case, the size of the patterns) is the possibility of deriving the command of randomness generation beyond the generator itself, while maintaining the secrecy of the sequence, which randomness is proved (as part of the EQRNG concept using quantum entanglement to ensure by laws the nature of implicit correlation in generated strings). the nature of the implicit correlation in the generated strings).

Overlapping template test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. As mentioned above, pattern search tests, including non-overlapping patterns, are the most important area of statistical verification of quantum randomness - the discussion of test parameterization in this area is analogous to the test of non-overlapping patterns. Searching for longer patterns paid for by an exponential increase in computational complexity is crucial, as the key part of the developed quantum randomization verification model regarding the use of quantum entanglement to enable previously unattainable

public randomness verification in the absence of computational resource limitations (their scalability in the external center) but maintaining the secrecy generated randomly thrust for applications. Parametric values of the K, M and N tests are selected in such a way that the requirements of the minimum length of 1 million bits of the generated random string, adequate for verification of quantum randomness (small deviations), are met. According to the above notes for verification of quantum randomness are important longer patterns with lengths from m = 15. This configuration of the test was subjected to model qualification on truly random sequences obtained in the laboratory in quantum processes and showed no entry into the critical test area of the calculated P-values for 15-bit standards at the limit of computational practicality.

Universal Maurer test (Universal Maurer test) - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomization verification also includes L values from 6 to 16, due to increasing computational complexity. The expected value for block length L equal to 6 (minimum value of the test run in the established model) is mu (6) = 5.2177052 and sigma variance (6) = 2.954. Combinations of the parameters n, Q for such a configuration (L = 6) are: $Q = 10\ 2^L = 640$ and $n > 387\ 840$, which can be taken as meeting the string length requirements for quantum randomness verification (order of several hundred thousand to million bits, as expected to detect possible long-range correlations showing classical deviations).

Linear complexity test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomization verification also includes, according to the arguments presented earlier, determining the minimum length of a string verified in randomness per million bits. In this situation, empirically confirmed (as part of model qualification) configuration optimization requires determining M (block length) in the range $500 < M < 5000$ and N (number of blocks) in the range $200 < N < 2000$, respectively. This parameterization is optimized for compliance with distribution of chi squate for verification sensitivity requirements for potential small classical deviations in quantum random generation that can be seen in sequences of at least 1 million bits. In the presented samples of the qualification results of the model, the upper limit of the block size M = 5000 was adopted (i.e. the tests worked on the border of practicality with respect to computational complexity, but they qualified the model without detecting in the laboratory random quantum sequences of classical deviations, also with such parameters).

Serial test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum random verification verifies the number n at least with a value of 1 million bits, requiring that the length of the pattern $m < \log_2 n - 2$. An important element of the test optimization for searching for deviations in quantum generated strings is the use of small m (patterns), moving away from the upper border $\log_2 n - 2$ with n equal to one million bits. This is related to increasing logarithmic computational complexity and is an important aspect of the quantum randomness verification model developed during the project through external public command while maintaining the secrecy of the generated random sequence by using quantum entanglement.

Approximate entropy test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomness verification includes a minimum length of the tested string n at least 1 million bits, requiring that the length of the pattern $m < \log_2 n - 2$. As in the case of a serial test, the test configuration for quantum randomness includes the number n at least with a value of 1 million bits, requiring that the pattern length $m < \log_2 n - 2$, which results from the mathematical definition of the test algorithm. An important element of optimization for the search for deviations in quantum-generated strings is the most accurate estimated entropy at small values of m (short pattern lengths), moving away from the upper border $\log_2 n - 2$ towards 1 bit. The accuracy of entropy value estimation is paid for by increasing computational complexity, in which context the important aspect is the model of quantum randomness verification developed by the project through an external public computing center (with scalable resources) while maintaining the secrecy of the generated random sequence, which is possible due to the use of quantum entanglement. As part of the model qualification in the parameterization for quantum random verification, it has been shown to check the properties of low entropy deviation from maximum values at individual bit positions to the value assumed in the project 2^{-64} i.e. 5 times 10^{-20}. This value determining the optimal boundary with respect to computational resources for the distinction (in a contractual manner, based on a classical statistical with all of its limitations, i.e. without the possibility of taking into account arbitrarily long deterministic patterns) of pseudo-random sequences from truly random (quantum) is verified in the calculation model using a configured in the discussed manner of entropy estimation test (test sentrop_EntropyDiscOver of set U01) for the parameter length standard m = 1. This means that entropy is estimated on a substring of 1 bit with the increasing length of the tested one-time block. The results of the model qualification in relation to that assumed in the design application, the entropy limit value (adopted for theoretical quantum generated random sequences) conducted on physically (i.e. empirically in the field of quantum mechanics experiment) confirmed true random sequences as presented in the test analyzes are met - the model is able to detect deviations from entropy of 2^{-64} (5 times 10^{-20}), and qualification tests conducted on laboratory randomized sequences exceed this limit of entropy approach to 1 (i.e. they do not enter the critical area of the test and do not demonstrate classic deviations).

Cumulative sums test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomization verification also includes a minimum length of the tested string n of at least 1 million bits.

Random trip test - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomization verification also includes a minimum length of the tested string n of at least 1 million bits.

Variant test of random trips - configuration for quantum randomization verification:

Significance level adopted at the alpha level = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods. The configuration for quantum randomness verification, similarly to the basic random trip test, includes a minimum length of the tested string n of at least 1 million bits.

2. The reference standard quantum QRNG classical statistical testing computational model

Expanded description of individual statistical tests combined into a computational model configured for verification of random sequences generated in quantum sources is presented below.

2.1. One-bit frequency test (Frequency, monobit) - a broader discussion of the test context in the quantum randomness verification model

The idea of a frequency statistical test is to verify the proportion of zeros and ones in a random sequence in order to compare their numbers. In the basic one-bit variant (monobit), this test verifies as a statistical measure of random disruption a deviation from the expected proportion between zeros and ones close to 50%, i.e. the equality of the number of zeros and ones in a random binary sequence. Due to the basic statistical nature of the test, if the random string will not be able to pass it successfully, then it is very likely that it will not pass other randomness tests.

Test parameters and configuration for quantum random verification:

The basic test parameter is n - bit string length. Standard NIST recommendations point to parameterization of the test with random sequences of at least 100 bits (i.e. $n \geq 100$). However, in the case of verification of the randomness of quantum sequences, it should be assumed that the test should detect even very small classical deviations in the quantum process, which may introduce frequency disturbances only in much longer sequences. Testing longer strings increases the computational complexity, but due to the low complexity of the subject test algorithm, you can successfully perform practical tests for string lengths exceeding one million bits. This was also the minimum criterion in the random quantum verification model. Significance level adopted at $\alpha = 0.1$ (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Replace within 0 for -1 and ones for +1 and add their values: where
2. Calculate test statistics
3. Calculate P-value: with *kfb* being a complementary error function.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. The case of a small P-value according to its calculation function is caused by a large value or. Large positive values indicate too many ones in a string, while large negative values confirm too many zeros in a string.

2.2. Block Frequency Test - a broader discussion of the test context in the quantum randomness verification model

This test is a modification of the standard frequency test in the direction of evaluating the proportion of ones in blocks (substrings with lengths of M bits) of the random sequence. As expected due to the randomness of the string in each of the drawn blocks, the number of ones should correspond to the number of zeros and be M / 2. This expectation, however, is not proven and remains in this area of doubt in accordance with the discussion of the issue of evidence of randomness presented in the research report. If the value of the block length M is equal to 1, then this test fully corresponds to the monobit frequency test.

Test parameters and configuration for quantum random verification:

The basic test parameters are M (length of each block) and n (minimum length of the random sequence being tested). As ε, we assume the determination of the bit string generated in the process of randomness generation, subject to the test (with $\varepsilon \geq n$). As with the standard frequency test for verifying the randomness of quantum sequences in a block test, it should be assumed to detect very small classical deviations in the quantum process that can introduce frequency disturbances only in much longer sequences. Testing longer strings increases the computational complexity, but also like the standard frequency test due to the low complexity of the algorithm, you can successfully perform practical tests for string lengths exceeding one million bits. This was also the minimum criterion in the random quantum verification model, which goes (10,000 times) over the standard NIST recommendations for parameterization of the test with random sequences of at least 100 bits ($n \geq 100$). In addition, NIST recommends that M block sizes have a length of at least 20 bits, and that they be larger than 0.1 minimum string length recommended by NIST and that their number be less than 100. After empirical optimization of this parameterization for longer string sizes (over 1 million bits), a minimum block length of 100 bits and their maximum number N of 10,000 was given (the maximum adequate block lengths empirically determined for testing quantum generated strings are 10,000, with a minimum number of blocks equal to 100). Significance level adopted at $\alpha = 0.1$ (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Divide the string into non-overlapping blocks (substrings), bypassing the remaining unused bits.
2. Calculate the proportion of, for $1 \leq i \leq N$.
3. Calculate the distribution
4. Calculate the P-value: where the chi-distribution returns the one-tail probability of the chi-square distribution and determines the number of degrees of freedom (number of blocks minus 1).

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. As in the basic frequency test, small P-values mean large deviations from an equal ratio of ones and zeros in at least one block.

2.3. Runs test - a broader discussion of the test context in the quantum randomness verification model

The idea of the test is to test the number of passes or sequences understood as continuous strings of the same bits (e.g. only zeros or only ones). This test corresponds to a test run from a set of mathematical methods for testing the randomness of Dr. George Marsaglia (Diehard collection).

The length of the sequence (run) equal to k consists of k identical bits appearing one after the other (i.e. preceded and ended with opposite bits). The purpose of this statistical randomness test is to determine whether the number (and length) of such sequences correspond to expectations for randomness. It should be emphasized that the situation in which there are too many bit-identical sequences (substrings) is a similar deviation from randomness as their number is too low (e.g. a string in which zeros and ones always alternate is similarly non-random as a string in which only ones or all zeros). The test is therefore intended to determine whether the bit variability between zeros and ones is adequate (i.e. it is neither too fast nor too slow).

Test parameters and configuration for quantum randomness verification:

The basic test parameter is n - the minimum length of the random sequence being tested. As ε, we assume the determination of the bit string generated in the process of randomness generation, subject to the test (with ε≥*n*). As in the case of frequency tests, the standard NIST recommendations point to parameterization of the test with random sequences of at least 100 bits (i.e. *n*≥100). Here, however, also in the case of verification of the randomness of quantum sequences, it should be assumed that the test should detect even small classical deviations in the quantum process, which may introduce oscillatory disturbances detectable in much longer sequences. Also, as in the case of frequency tests, testing longer strings in the range of sequence results in an increase in computational complexity, but due to the low complexity of the algorithm, practical tests can be performed for string lengths exceeding one million bits. This was also the adopted minimum criterion in the random quantum verification model, which also allows verification of source stability. Significance level adopted at $\alpha = 0.1$ (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Calculate as a pre-test the proportion of π of the ones within:
2. Check that the frequency pre-test is passed: however, if $| \pi - 1/2 | \geq \tau$, then the string fails the frequency test and no sequence test is necessary.
3. Calculate the test statistics, where $r(k) = 0$ if and $r(k) = 1$ otherwise.
4. Calculate P-value.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. Large values indicate too low oscillation, i.e. variation between zeros and ones in a string (e.g. in a 500-bit string, you can imagine a non-random situation of only a few sequences occurring: then the string consists of, for example, a very large number of 0 consecutive, later 1 consecutive, then again zeros etc.). Statistically, one would expect a much larger number of sequences for the 500-bit sequence (in the direction of 250). In turn, too much oscillation results from the fast bit variation that occurs e.g. in the alternating sequence 01010101. For a 500-bit example of such (one-element) sequences there would be as much as 500 which is a deviation from randomness in the opposite direction, also undesirable.

2.4. Test of the longest run in a block (Longest Run) - a broader discussion of the test context in the quantum randomness verification model

The idea of this test is to determine the longest sequence (run) of themselves and immediately following ones (alternatively zeros) in a block (substring) with a length of M bits random order. The purpose of the test is to compare whether the length of the longest sequence found matches the expectations of the random string (and thus is neither too long nor too short). Any irregularity in the length of the longest sequence of ones implies an irregularity in the expected longest sequence of zeros, which means that a single test can be performed (e.g. only for the sequence of ones or for the sequence of zeros).

Test parameters and configuration for quantum random verification:

The basic test parameters are n (minimum length of the random sequence being tested) and M (length of each block). As part of the parameterization of the test for quantum randomness verification, the standard NIST recommendations were raised for a minimum string length of n

million bits and in this configuration block lengths of 10,000 bits (which length, however, can be reduced as assumed to 128 bits). ε is the bit string generated in the randomness generation process, subject to the test (with ε≥*n*). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Divide the random string into blocks (substrings) of length M bits.
2. Categorize the frequencies of the longest sequences of ones in each block in the following categories, specifying the number of sequences of a given length. Individual numbers for and for.
3. Calculate where the values are as follows; and for. The values of K and N are selected in relation to the M parameterization as follows: for M = 128, K = 5 and N = 6, for M = 10000, K = 49 and N = 75.
4. Calculate the P-value.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. Large values mean that the tested string has large sequences of ones.

2.5. Test of binary matrix rows (Rank) - a broader discussion of the test context in the quantum randomness verification model

This test focuses on a row of disjoint sub-matrices of the entire string, and its purpose is to verify the linear relationship between the fixed length of the substrings of the entire random sequence. This test was developed by dr. Georg Marsaglia and included in one of the first sets of statistical tests of randomness verification "Diehard", which Marsaglia published in 1995. This test was also included in the NIST randomness verification standard.

Test parameters and configuration for quantum random verification:

The basic test parameters are n (minimum length of the random string being tested), M (in this case the number of rows of each matrix) and Q (the number of columns in each matrix). ε is the bit string generated in the randomness generation process, subject to the test (with ε≥*n*). The probabilities were calculated for the quantum randomness testing selected as optimal configuration in suitably large strings in the 32 x 32 matrix range (M = 32, Q = 32), i.e. 1024 element, which there are 976 within a million bits. For these matrix configurations were calculated and appropriate statistical probabilities used in the function calculating the P-value of the test in accordance with the Marsaglia guidelines used in the programming implementation of the model. Other ranges of matrix configuration require the calculation of appropriate probabilities before the test implementation. An important requirement for configuring the test to detect even small deviations potentially occurring in quantum-generated strings through the influence of classic effects is to assume a minimum random string length of at least 38QM, i.e. 38,912 bits (which means that at least 38 binary matrices can be filled). In the case of further scaling of the test sensitivity to detect even smaller classic deviations potentially occurring in the theoretically non-deterministic sequence of generated quantum randomness, matrix sizes adequate for the minimum string length of one million bits can be assumed, in which case the number of M rows and Q columns are 162 bits. Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Sequentially split the test string into M x Q bit separable blocks (substrings). The division will lead to such blocks. Discard the bits that will and will not be enough to create a full M x Q matrix. Each row of the matrix is filled with consecutive Q-blocks of the original random sequence ε (which means that the string is written from left to right by rows in subsequent matrices).
2. Calculate the each row of the binary matrix where *l*= 1, ...,N.
3. Accept: the number of matrices of the order (full row); number of matrices of the order (full order - 1); number of remaining matrices.
4. Calculate, the chi-distribution returns the one-tailed probability of the chi-square distribution and determines the number of degrees of freedom (in this case 2).

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. Large values (and therefore low P-values) indicate deviations in the empirical distribution of matrix rows from the theoretical distribution corresponding to randomness.

2.6. Test of the discrete Fourier transform, spectral test (FFT) - a broader discussion of the test context in the quantum randomness verification model

The idea of the test is to verify the height of the peaks in the spectral image of the discrete Fourier transform of the tested random sequence. The purpose of the test is to detect periodic properties (repetitive patterns) that may be in the sequence and thus prove its deviations from randomness. In quantitative statistics, the test is designed to detect if the number of peaks (vertices in the Fourier transform image) exceeding 95% of the threshold is significantly different from 5%.

Test parameters and configuration for quantum randomness verification:

The basic test parameter is n - the minimum length of the random sequence being tested. ε is the bit string generated in the randomness generation process, subject to the test (with ε≥*n*). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. In the case of verification of the randomness of quantum sequences, it should be assumed that the test of the discrete Fourier transform should detect even very small classical deviations in the quantum process, which may introduce disturbances in the distribution of spectral image only in much longer sequences. Spectral testing of longer strings increases computational complexity and this situation requires determining the optimal selection of the sample. Current empirical studies have shown that optimal results are obtained for string lengths exceeding one million bits. This was also the minimum criterion in the random quantum verification model for the test of the discrete Fourier transform. This is a thousand times greater minimum string length than recommended by NIST for the spectral test, i.e. a recommendation of n equal to 1000 bits. Computational complexity in the spectral test despite the FFT algorithm (fast Fourier transform) increases logarithmically, i.e. exponentially. Therefore, a particularly important element of the model of quantum randomization verification by the Fourier test is the ability to lead the proof of randomness generation outside the generator itself while maintaining the secrecy of the sequence whose randomness is proved (which is the subject of the proposed concept using quantum entanglement for the task of implicit correlation between generated random sequences).

Mathematical test procedure:

1. In the tested random sequence ε change zeros to -1 and ones to +1 creating a string.

2. Apply a discrete Fourier transform on the string X to get: S = DFT (X). A complex string of variables is created that represents the periodic components of the random bit string being tested at different frequencies.
3. Calculate *M*=*mod*(*S*'), |*S*'|, where *S*' is a substring consisting of the first half of the elements in S (n / 2 elements), and the module function returns a string of peak heights.
4. Calculate the 95% peak height threshold. Assuming the randomness of the test string, 95% of the peaks obtained under the test should not exceed the T threshold.
5. Calculate the expected theoretical (95%) number of peaks below the T threshold (assuming the randomness of the test string).
6. Calculate = actual (empirical) number of peaks in M that are below threshold T.
7. Calculate the P-value.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum random verification) , then the tested string is not random. Otherwise, the string passed the randomness test. Obtaining a low d value means too few peaks below the T threshold (less than 95%) and thus too many peaks above the T threshold (more than 5%).

2.7. Nonoverlapping template - a broader discussion of the test context in the quantum randomness verification model

The purpose of this statistical test is to analyze the number of occurrences of specific (predefined) bit patterns. Its primary task is therefore to detect whether the randomness generator is not producing too much of a specific aperiodic pattern. As part of this test, the tested random string is searched with a frame (substring) with a length of m bits containing subsequent tested m-bit patterns. If a given pattern is not found in the tested random string, the search frame moves by the next position in the string (by 1 bit). If the pattern being found is found in the frame, the position of the frame is set to the next bit after the detected substring containing that pattern (i.e. it is moved in the tested sequence of om bits), and the search is resumed. The test allows you to search for any number of patterns, which means that in each search run in the test frame, many searches for subsequent patterns are performed.

Test parameters and configuration for quantum random verification:

The main test parameters include: n (minimum length of the random string being tested), m (bit length of the patterns sought), B specific bit pattern with length m bits (specific binary string), M (predefined length value initial substring of the entire ε string generated in the process of randomness generation, to which substring is limited the search for patterns, adopted at a level less than the length n, e.g. 500,000, only for additional control - limiting - the requirements of test computing resources) and N (the number of independent blocks used in the definition of the test procedure). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. It should be noted that tests for finding patterns, including non-overlapping (non-overlapping) patterns, are the most important area of statistical verification of quantum randomness, which results from the possibility of masking classic effects in technically imperfect implementation of the quantum process through not necessarily repetitive but deterministic patterns. This means that the patterns do not have to contain statistical repeatability that would be detectable by statistical deviations according to the other standard randomness verification tests (i.e. their statistics do not differ from theoretical randomness expectations), nevertheless these patterns are deterministic and can be reproduced as part of a potential attack on randomness in which such deterministic processes (reflected in aperiodic patterns) could sneak in. Therefore, the basic area of definitions of tests aimed at searching for patterns within quantum

randomness testing is increasing the size of sought deterministic patterns, which takes place at a significant cost in the area of computational complexity (exponentially increasing with the size of patterns, due to the exponentially growing number of them as combinations in binary sequences). The standard recommendation of NIST is to search for patterns with a length of at least 9 bits (then there are 148 patterns that meet the aperiedic conditions of the pattern and so many patterns should be found). Increasing the value of the number of bits in the patterns causes an exponential increase in complexity because so increases the number of possible patterns. As part of empirical research in the field of parameterization of the test for the quantum randomization verification model, it was possible to achieve the value of 15 bit patterns (among all possible aperiodic forms as many as 8848) with respect to computational practicality. For each of these patterns, a search is carried out, which means that it is almost 2 rows more complex than in the case of 9-bit patterns. In the scope of model qualification, examples of 20 statistical results of tests out of 8848 completed (for all aperiodic standards) are presented. As in the case of the spectral test, but especially in the case of pattern search tests, a key element of the quantum randomness verification model in the context of exponentially increasing complexity relative to parameterization (in this case, the size of the patterns) is the possibility of deriving the command of randomness generation beyond the generator itself, while maintaining the secrecy of the sequence, which randomness is proved (as part of the EQRNG concept using quantum entanglement to ensure by laws the nature of implicit correlation in generated strings).

Mathematical test procedure:

1. Divide the string into N independent blocks (substrings) of length m, discarding the remaining bits that are not enough to create the last complete block.
2. Assume as the number of occurrences of pattern B in block number j. Patterns are searched for by creating a frame with the length of m bits shifted by the tested string, whose content is compared in successive shifts with subsequent patterns. In case if no match (pattern not found), the frame moves by another position of 1 bit. If, however, one of the searched patterns occurs in the frame, then the frame is moved to the bit position next to the end of the pattern.
3. Calculate the theoretical mean value μ (expected value) and variance assuming randomness.
4. Calculate the empirical distribution.
5. Calculate where the chi-distribution returns the one-tail probability of the chi-square distribution and determines the number of degrees of freedom. A set of P-values will be calculated for all of the sought standards (each pattern will have a corresponding P-value). For example, for the parameter m = 15 specifying the 15-bit length of aperiodic patterns, 8848 P-values (corresponding to individual patterns) will be calculated. This number increases exponentially with the length of the patterns, which is associated with the exponential increase in computational complexity for searching for complex patterns (as indicated above).

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. If the obtained P-value is small, there are non-random patterns in the tested string, which in the context of quantum generation may indicate implementation imperfections and classic effects.

2.8. Overlapping template - a broader discussion of the test context in the quantum randomness verification model

This statistical test is very similar in its assumptions to the test of finding non-patterns. This test also examines the occurrence of specific bit patterns (substrings), using the m-bit frame to search for deterministic patterns in the tested string. The difference in the definition of the test as per the name is the admission of the occurrence of overlapping patterns. This is achieved by shifting the frame by one bit also when a pattern is found (in the case of qualifying only non-overlapping patterns, after finding the pattern, the frame is shifted by the length of the found pattern, i.e. to the bit position immediately after it). If the overlapping patterns are allowed, the frame is shifted one bit also when the pattern is found and the search is repeated on the rest of the found pattern.

Test parameters and configuration for verification of quantum randomness:

Similarly to the test for finding non-overlapping patterns, the main test parameters include: n (minimum length of the tested random sequence), m (bit length of the searched patterns), B specific bit pattern with the length of m bits (specified binary string), M (predefined value of the length of the initial substring of the entire string ε generated in the process of randomness generation, to which the search for patterns is limited, adopted at a level less than the length n, e.g. 500,000, only for additional control - limiting - requirements test computing resources) and N (the number of independent blocks used in the definition of the test procedure). Significance level adopted at $\alpha = 0.1$ (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. As mentioned above, pattern search tests, including non-overlapping patterns, are the most important area of statistical verification of quantum randomness - the discussion of test parameterization in this area is analogous to the test of non-overlapping patterns. Searching for longer patterns paid for by the exponential increase in computational complexity is crucial, as the key part of the developed quantum randomization verification model regarding the use of quantum entanglement to enable the previously unattainable public randomness verification in the absence of computational resource limitations (their scalability in the external center) but maintaining the secrecy generated randomly thrust for applications. Parametric values of the K, M and N tests are selected in such a way that the requirements of the minimum length of 1 million bits of the generated random string, adequate for verification of quantum randomness (small deviations), are met. According to the above notes for verification of quantum randomness are important longer patterns with lengths from m = 15. This configuration of the test was subjected to model qualification on truly random sequences obtained in the laboratory in quantum processes and showed no entry into the critical test area of the calculated P-values for 15-bit standards at the limit of computational practicality.

Mathematical test procedure:

1. Divide the string into N independent blocks (substrings) of length M, discarding the remaining bits which are not enough to create the last complete block.
2. Calculate the number of occurrences of pattern B in each of the N blocks. The pattern search should be carried out by a frame with the length of m bits shifted by the tested string always by one bit position. After each shift, compare the contents of the frame with the searched patterns and if a pattern is found, increase the value of the corresponding counter, where $i = 0, ..., 5$: the counter is increased if there is no pattern B, it is increased for one occurrence of pattern B, etc. until it is increased for 5 or more instances of pattern B.
3. Calculate the values of λ and η that will be used to calculate the theoretical probabilities corresponding to the classes:
4. Calculate the distribution, where

5. Calculate where the chi-distribution returns the one-tail probability of the chi-square distribution a specifies the number of degrees of freedom.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. In the event that 2-bit reference would be sought and the whole tested string would contain too many 2-bit e.g. sequence of ones, then the counter would be too high, therefore the test statistic was too high and P-value low, below the significance level , which would indicate a string's non-randomness.

2.9. Universal Maurer test (Universal Maurer test) - a broader discussion of the test context in the quantum randomness verification model

The essence of the test is to examine the number of bits between compatible bit patterns, which is a measure related to the length of the compressed string. The purpose of the test is to detect whether the random sequence under test can be significantly compressed in a lossless way. An adequately significantly compressible lossless string cannot be considered random.

Parameters and test configuration for quantum randomness verification:

The basic parameters for the universal test are L (length of each block), n (length of the bit string whose randomness is to be tested) and ε (actually tested random string of length greater than n). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. The configuration for quantum randomization verification also includes L values from 6 to 16, due to increasing computational complexity. The expected value for block length L equal to 6 (minimum value of the test run in the established model) is μ (6) = 5.2177052 and variance σ (6) = 2.954. Combinations of parameters n, Q for this configuration (L = 6) are: and $n \geq 387840$, which can be taken as meeting the string length requirements for quantum randomization verification (order of several hundred thousand to one million bits, as expected to detect possible long-range correlations showing classic deviations).

Mathematical test procedure:

1. Test random sequence of length n bits divided into two substrings (segments). The so-called. the initialization segment contains Q non-overlapping blocks with a length of L bits and a test segment containing K non-overlapping blocks with a length of L bits. The bits remaining at the end of the string that are not sufficient to form the full L-bit block are discarded. Use the first Q blocks to initiate the test. The remaining K blocks are test blocks.
2. Using the initialization segment, create an array for each possible L-bit value (the L-bit value is used as the array index). The block number of the last occurrence of each L-bit block is written to the table (e.g. for *i* from 1 to *q* , where j is the decimal representation of the content of the i-th L-bit block).
3. Examine each of the K blocks within the test segment and determine the number of blocks since the last occurrence of the same L-bit block (ie). Add the calculated distance between repetitions of the same L-bit block to the accumulative sum of all differences detected in K blocks (ie)
4. Calculate the test statistics: where is the content of the array cell corresponding to the decimal representation of the content of the ith L-bit block.
5. Calculate the P-value =, where *kfb:,* is the complementary error function, μ (*L*) is the average value and σ the variance determined on the basis of additional calculations where

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. In case it deviates significantly from μ (*L*) then the string is significantly compressible, i.e. non-random.

2.10. Linear complexity test - a broader discussion of the test context in the quantum randomness verification model The

Specificity of the definition of the linear complexity test is the use of the concept of a linear feedback shift register (LFSR). It is a data structure of the register type whose input bit is a linear function of its previous state. In Boolean algebra, only two operations (logic gates) are linear functions in the field of single bits. These are the negative alternative (XOR) and negative negative (XNOR) operations. One of the possible definitions of LSFR is the shift register, from which the input is given by the XOR operation of selected register states. The task of the test using the LSFR concept is to determine whether the random sequence under test is complex enough to be considered random. Random strings should be complex to cause larger sizes of the corresponding LSFR registers. The LSFR register, which is too short in relation to the parameters of the test string, indicates that the string is not random.

Test parameters and configuration for quantum random verification:

Basic parameters for the linear complexity test are n (minimum length of the bit string whose randomness is to be tested), M (bit length of blocks - substrings), K (number of degrees of freedom), N (number of blocks) and ε (actually tested random sequence of length N, greater than n). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. The configuration for quantum randomization verification also includes, according to the arguments presented earlier, determining the minimum length of a string verified in randomness per million bits. In this situation, empirically confirmed (as part of model qualification) configuration optimization requires the determination of M (block length) in the range of $500 \leq M \leq 5000$ and N (number of blocks) in the range of $200 \leq N \leq 2000$, respectively. This parameterization is optimized in terms of compliance with the distribution for the requirements of verification sensitivity for potential small classic deviations in the quantum random generation that can be seen in strings of at least 1 million bits. In the presented samples of the qualification results of the model, the upper limit of the block size M = 5000 was adopted (i.e. the tests worked on the border of practicality with respect to computational complexity, but they qualified the model without detecting in the laboratory random quantum sequences of classical deviations, also with such parameters).

Mathematical test procedure:

1. Divide the tested random string with a length of n bits into N blocks with a length of M bits (so that n = MN). Discard the remaining bits with too few to form a full M-bit block.
2. Using the Berlekamp-Massey algorithm to determine the linear complexity τ of each of the N blocks (i= 1, ...,N). τ is the length of the shortest shift register (LSFR) of the string that generates all bits in block i. By adding modulo 2 within the string of τ bits, the specified bit combinations get the next bit in the string (bit τ + 1).
3. Assuming randomness, calculate the theoretical mean value of μ:
4. Calculate the value for each substring
5. Save the values in the counter categorization.
6. Calculate where are the separately calculated probabilities of the linear complexity test.
7. Calculate the P-value.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. When the P-value is less than 0.1 it indicates that the empirically found frequencies stored in the meters have deviations from those expected for a random string.

2.11. Serial test - a broader discussion of the test context in the quantum randomness verification model

The subject of the test is to test the frequency of occurrences of all possible overlapping m-bit patterns throughout the entire random sequence. The test has the entire determination whether the number of occurrences of patterns with length m bits in the whole string is consistent with the expectations for the random string. An important feature of random strings is their homogeneity, meaning that the occurrence of each pattern with a length of m bits is equally likely (i.e. any of the possible m-bit patterns should occur with the same probability as the other ones). The serial test for parameterization of the 1-bit standard length (m = 1) is reduced to the basic frequency test.

Parameters and test configuration for quantum random verification:

The basic parameters for the serial test are n (the minimum length of the bit string whose randomness is to be tested), m (the number of bits of each block that generates m-bit patterns) and ε (the actual random string of length N, greater than n). The configuration for quantum randomization verification includes the number n at least with a value of 1 million bits while requiring the length of the pattern. An important element of the test optimization for the search for deviations in quantum-generated strings is the use of large m (standards) approaching the upper limit with n equal to one million bits. This is due to the increasing logarithmic computational complexity and is an important aspect of the quantum randomness verification model developed during the project through external public command while maintaining the secrecy of the generated random sequence by using quantum entanglement.

Mathematical test procedure:

1. Extend the string by adding the first m-1 bits to the end of the string for different values of n.
2. Determine the frequency of all possible overlapping patterns with m-bit lengths (as well as all possible overlapping patterns with m-lengths) 1 bits (m-1 bit blocks) as well as all possible overlapping patterns with m-2 bits length (m-2 bit blocks). Take a frequency counter table storing the number of occurrences of m-bit patterns. Take the definition of frequency (m-1) bit pattern and definition of frequency (m-2) bit pattern.
3. Calculate: P-value 1 and P-value 2.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. If they have a large value, then this indicates the heterogeneity of m-bit blocks (substrings) in the tested string and thus its non-randomness.

2.12. Approximate entropy test - a broader discussion of the test context in the quantum randomness verification model

As in the case of the serial test, the subject of the entropy estimation test is the frequency of occurrences of all possible overlapping bit patterns with lengths of bits in the entire random sequence tested. The purpose of the test is to compare the frequency of occurrence of overlapping blocks of two consecutive lengths (m and m + 1) with the expected frequencies of such occurrences for random sequences.

Test parameters and configuration for quantum random verification:

Basic parameters for the entropy estimation test are n (minimum length of the bit string whose randomness is to be tested), m (number of bits of the block generating m-bit patterns, i.e. length of the first block - length of the second block is m + 1) and ε (actually tested random sequence). Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods. The configuration for quantum random verification verifies the minimum length of the tested string n at least of 1 million bits while requiring the length of the pattern. As in the case of the serial test, the test configuration for quantum randomness includes a number n at least of 1 million bits, requiring that the length of the pattern, which results from the mathematical definition of the test algorithm. An important element of model optimization for the search for deviations in quantum-generated strings is the most accurate estimated entropy possible also at small m values (short pattern lengths), moving away from the upper border in the direction of 1 bit. The accuracy of estimation of entropy value is paid for by increasing computational complexity, in which context an important aspect is the model of quantum randomness verification developed by the project through an external public computing center (with scalable resources) while maintaining the secrecy of the generated random sequence, which is possible thanks to the use of quantum entanglement. As part of the model qualification in the parameterization for quantum random verification, it has been shown to check the properties of low entropy deviation from maximum values at individual bit positions to the value assumed in the project i.e. This value determining the optimal boundary with respect to computational resources for the distinction (in a contractual manner, based on a classical statistical with all of its limitations, i.e. without the possibility of taking into account arbitrarily long deterministic patterns) of pseudo-random sequences from truly random (quantum) is verified in the calculation model using a configured in the discussed manner of entropy estimation test (test sentrop_EntropyDiscOver of set U01) for the parameter length standard m = 1. This means that entropy is estimated on a substring of 1 bit with increasing length of the tested one-time block. The results of the model qualification in relation to that assumed in the design application, the entropy limit value (adopted for theoretical quantum-generated random sequences) conducted on physically (i.e. empirically in the field of quantum mechanics experiment) confirmed true random sequences as presented in the test analyzes are met - the model is able detect deviations from entropy of (), and qualification tests conducted on laboratory randomized sequences exceed this limit of entropy approach to 1 (i.e. they do not fall into the critical area of the test and do not demonstrate classical deviations).

Mathematical test procedure:

1. Extend the tested n-bit string to create n overlapping blocks of length m bits by adding m-1 bits from the beginning of the string to its end.
2. Calculate the incidence of n overlapping blocks. If the m-bit block - substring - containing bits for is considered in iteration j, then the block containing bits for is considered in the next iteration j + 1.
3. Express the number of all possible m-bit (and (m + 1) -bit) values as where and is the m-bit value.

4. Calculate the P-value.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. Small values of the function indicate a proportionally high regularity, while large values indicate a proportionally low regularity or severe fluctuations indicating deviations from randomness.

2.13. Cumulative sums test - a broader discussion of the test context in the quantum randomness verification model

The test operates in the area of defining the problem of graph transition with random path selection (problems of wandering or random walk in graph theory). The subject of the test is the maximum trip from 0 in random wandering defined by the growing sums of the transformed form of the binary random sequence (from zeros and ones, respectively, to the value of +/- 1). The purpose of the test is to determine whether the value of the growing sum of transformed bit values in the substrings occurring in the tested random sequence is too large or too small in relation to the expected value of the growing sum in the random sequence. The value of the increasing sum can be treated as random wandering in graph theory. For a random passageway defined in this way, random wandering should be close to zero. However, for deviations from the randomness of this type of transition under random wandering will be severely deviated from zero (having large positive or negative values). The test is derived from the concept of dr. Georg Marsaglia presented in the Diehard collection.

Parameters and test configuration for quantum random verification:

The main parameter of the increasing sum test is n - the minimum length of the bit string whose randomness is to be tested. ε is the random string actually tested. The growing sum test is also parameterized by the direction of its execution, which is determined by the parameter of mode A (mode A = 0: performing the test from the beginning of the random sequence to its end or mode A = 1: performing from the end to the beginning). NIST's basic recommendations for verifying the randomness of pseudo-random strings (classic generators) impose a limit on the minimum string length of only n = 100 bits. The configuration for quantum randomization verification includes a minimum length of the tested string n of at least 1 million bits. Significance level adopted at $\alpha = 0.1$ (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Create a normalized string from the tested binary string by converting zeros and ones in ε to -1 and +1, respectively, using the function.
2. Calculate the partial sums of successively increasing substrings, each starting with a bit (in mode 0 from the beginning) or (in mode 1 from the end).
   a. Mode 0 (from the beginning).
   b. Mode 1 (from the end), i.e. for mode 0 and for mode 1.
3. Calculate the test statistics, where is the largest of the absolute values of the partial sums.
4. Calculate the P-value.

where Φ is the standard, normal, increasing probability distribution.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. In the case

of mode 0 (performing the test from the beginning of the tested random sequence), large values of calculated statistics indicate that there are too many (relative to expectations of randomness) ones or zeros in the initial areas of the string. In the case of mode equal to 1, large values of the calculated statistics, in turn, indicate that there are too many ones or zeros in the final fragments of the sequence. This test is therefore an important criterion for verifying the ergodicity and stationarity of a random source. However, too small values of the calculated statistics, in turn, indicate too even distribution of zeros and ones, which must also be interpreted as a deviation from randomness.

2.14. Random trip test - wider discussion of the test context in the quantum randomness verification model

The subject test examines the number of cycles in which there are exactly K visits in random walk (random walk) defined based on the concept of increasing sums in a normalized binary sequence. Random wandering of the increasing sum is obtained by changing the zero-one binary sequence to the corresponding sequence -1 and +1, respectively. The cycle in random walk consists of a series of steps of unit length randomly performed, which start and end at the same place (beginning). The purpose of the test is to determine whether the number of visits in a particular state within the cycle has a deviation from the number expected in the case of a random string. As part of the test, a series of eight sub-tests is carried out with a conclusion for each of them related to each of the eight states: -4, -3, -2 -1, +1, +2, +3, +4.

Parameters and test configuration for quantum randomness verification:

The main parameter of the random trip test is n - the minimum length of the bit string whose randomness is to be tested. ε is the random string actually tested. The configuration for quantum randomization verification includes a minimum length of the tested string n of at least 1 million bits. Significance level adopted at α = 0.1 (10%) by a row above the NIST recommendations requirements in the Diehard and U01 methods.

Mathematical test procedure:

1. Normalize the tested binary string by converting zeros and ones into the numbers -1 and +1, respectively, generating the string X. The conversion of 0 and 1 of the tested string ε to -1 and +1 is done by the function.
2. Calculate the partial sums of the next large substrings starting from.
   As part of the set: ...
3. Create a new string S 'by appending zeros before and after the string S:
4. Take J = the total number of zero intersections in the string S', where zero intersection is the zero value in the string S 'after the initial zero. J is also the number of cycles in S ', where the cycle in S' is a substring consisting of zero occurrence followed by non-zero values and ending with another zero. The final zero value in one cycle may be the zero initial value in another cycle. The number of cycles in S 'is the number of zero intersections J. If J <500, abort the test.
5. For each cycle and for each x value of a non-zero state in the range $-4 \le x \le -1$ and $1 \le x \le 4$, calculate the frequencies of the given x value in each cycle.
6. For each of the eight states x, calculate as the total number of cycles in which state x occurs exactly k times among all cycles for $k = 0.1, \ldots, 5$ (for k = 5, the total number of cycles in which all frequencies are greater than 5 are counted in the counter). It happens.
7. Calculate the test statistic for each of the eight states x: where is the probability that the states x occur k randomly. The values are calculated separately. The calculations will apply to eight distributions (for $x = -4, -3, -2, -1, 1, 2, 3, 4$)

8. Calculate the P-value for each state x Present eight final p-empirical values.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test. If the empirical distribution is too large, it means that the string manifests a deviation from the theoretical random distribution for a given state in cycles.

2.15. Variant random tours test - wider discussion of the test context in the quantum randomness verification model

The task of the variant random tours test is to determine the number of visits (occurrences) of a specific state in the random walk (walk) of a growing sum in a normalized binary sequence. The purpose of the test is to detect possible deviations from the expected number of visits to various states in random walks. The variant variant of the random trip test consists of a series of eighteen subtests (and corresponding statistical conclusions) for the states −9, −8, ..., −1, + 1, + 2, ..., + 9.

Parameters and test configuration for quantum random verification:

The main parameter of the variant random tour test is n - the minimum length of the bit string whose randomness is to be tested. ε is the random string actually tested. The configuration for quantum randomness verification, similarly to the basic random trip test, includes a minimum length of the tested string n of at least 1 million bits. Significance level adopted at the level α = 0.1 (10%) by a row above the NIST recommendations requirements in the scope of Diehard and U01 methods.

1. Normalize the string ε by converting 0 to -1 and 1 to +1, generating a string where
2. Calculate the partial sums of successively larger substrings, each starting from. Create a collection.
3. Create a new S 'string by appending zeros before and after the S string:
4. For each of the eighteen non-zero states x calculate ξ (*x*) equal to the total number of occurrences of state x in all J cycles.
5. For each ξ (*x*), calculate. Present eighteen final empirical p-values.

Apply corresponding decision rule and interpretation of test results.

If the calculated P-value is less than 0.1 (parameterization of quantum randomization verification), then the tested string is not random. Otherwise, the string passed the randomness test.