Final report

Quantum Random Numbers Generation Standardization (QRNGS) project implementation

To help monitor impact please indicate how your contribution is impacting EU or International ICT Standardisation Landscape.

The project implementation supported Quantum Technology standardization in the field of Quantum Random Numbers Generation.

Before the project has begun there have been only Quantum Key Distribution standardization workgroups, despite the fact that the QRNG technology is similarly mature in TRL terms.

Upon the project implementation there were drafted 3 Request for Comments documents with technical specifications on:

1) QRNG definition, key theoretical concepts of true randomness and use cases,

2) QRNG testing and verification schemes (including sustaining secrecy),

3) QRNG processes, devices and operative parameters,

with special focus set on entanglement based QRNG (EQRNG) schemes.

In its subsequent stage the project impacted ICT standardization community by establishing of a workgroup dedicated to EQRNG technical reference standards development as a part of the Quantum Standards Group hosted under the EITCI Institute,

cf. https://eitci.org/technology-certification/qsg .

The members of the Entanglement Quantum Random Numbers Generation workgroup were invited among experts from industry, academy and standardization bodies to contribute to the EQRNG technical specification drafting on the basis of the RFC documents.

The major impact of the project was in final acceptance of the iterated RFC specifications as Reference Standards by 154 EQRNG-QSG Workgroup members,

cf. https://eitci.org/technology-certification/qsg/eqrng .

Indicate which gaps you have addressed?

Cybersecurity / Information security

Cybersecurity / Use, retention, and disclosure limitation

IoT / Deployment / Safety

Other (Please indicates belonging group (e.g IoT, Biga Data, etc.)

Cybersecurity / Randomness generation

Please indicate the overall measurable KPIs & what has been the principal achievement (s) now this been completed

First preparation of the QRNG technical RFC drafts documents took place:

1. QRNG definition, key theoretical concepts of true randomness and use cases

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-theoretical-concepts

2. QRNG testing and verification schemes (including sustaining secrecy)

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-protocols

3. QRNG processes, devices and operative parameters

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-testing

Then the RFCs were distributed to relevant WGs of European and international SDOs which already dealt with quantum communication standards, including ETSI QKD-ISG, ITU-T SG13 (Future Networks) and SG17 (Security), IEEE and IEEE ISTO, IETF, IEC TC 57, IEC TC 292, IEC TC 65/WG10, ISO/IEC JTC 1/SC 27, CEN, CENELEC, ANSI/ASC and NIST.

Furthermore cooperation invitations were directed to relevant SDOs as well as to QIPC researchers and relevant cybersecurity and quantum engineering experts. Upon issued invitations the EQRNG-QSG workgroup membered by 155 experts has been established under EITCI Institute.

The last phase of the project was in reiteration of the comments, remarks and contributions within the 3 RFC drafts and the final acceptance and publication of the RS documents along with their dissemination aimed at stimulating further QRNG standards development with the international SDOs (as documented in the links above).

Which Standards Group(s) have you contributed to?

CEN, CENELEC, ETSI, IEEE, IEC, IETF, ISO, ITU, NIST

Other Standard Group?

ANSI, ASC, X12 and EITCI -QRNG / -QIP / -QKD WGs

In which way within the context of your application?

The RFCs as well as developed RS specifications in randomness generation were disseminated to leading European and international SDOs that are working in fields such as cybersecurity,

cryptography, secure networking, etc. that might benefit from QRNG standards in randomness. These RFC and RS specifications were shared with the above listed SDOs with aim to lead to stimulation of international SDOs' own WGs towards increasing collaboration and reaching of the consensus on technical specifications for true randomness generation. The QRNG standardization drafting process was open and the RFC documents, as well as accepted RS also remain of open access. These specifications will support further standardization work in relevant WGs of international SDOs, as true randomness has vast applications, especially in the domain of cybersecurity. The particular RS documents distributed to relevant SDOs are attached to this report. The considered EQRNG protocol was accepted for publishing in Nature Scientific Reports. Any members of the related technical standards committees or workgroups of any SDO that might be interested with Entanglement Quantum Random Numbers Generation or other areas of QT (including e.g. QKD) were invited to join the EQRNG-QSG by submitting the form at https://eitci.org/technology-certification/qsg or by requesting admission to the LinkedIn Group at https://www.linkedin.com/groups/8850635 and participate in further standards development.

What is the progress towards completion of that specific standards to become a specification?

Very Mature

Other state of maturity

These standards has been accepted by the EQRNG-QSG

Indicate here what final recommendations you propose?

Action Successfully finalised

Other recommendations

Further EU support for development of Quantum Information technical standards is strongly advised.

What is the final status of your contribution and what is the target release or publication expected date?

The final status of the contribution is completed with 3 Reference Standards accepted by EQRNG-QSG membering experts and disseminated to leading international SDOs to stimulate further technical development and cooperation.

After two corrective iterations the RFCs has been accepted by the EQRNG-QSG as the Reference Standards, upon an acceptance vote procedure.

The vote took place between 27th December 2019 and 31st December 2019. 155 EQRNG-QSG Members were entitled to voting on acceptance of the three RS documents:

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

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-theoretical-concepts

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

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-protocols

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

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-testing

The vote has concluded on 31st December 2019 with almost unequivocal support for the three above listed Reference Standards. Of the 155 EQRNG-QSG Members entitled for voting, 154 Members supported the acceptance of RS and 1 Member has expressly abstained from voting).

The final accepted RS publication date was 31st December 2019.

Please provide any public links available to demonstrate your work

The Quantum Standards Group of EITCI Institute (QSG):

https://eitci.org/technology-certification/qsg

The Quantum Standards Group membership application form:

https://eitci.org/technology-certifcation/qsg/membership

The Entanglement Quantum Random Numbers Generation Workgroup (EQRNG-QSG):

https://eitci.org/technology-certification/qsg/eqrng

The LinkedIn Group of the EQRNG-QSG:

https://www.linkedin.com/groups/8850635

Accepted Reference Standards:

RS-EITCI-QSG-EQRNG-THEORY-STD-VER-1.0:

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-theoretical-concepts

RS-EITCI-QSG-EQRNG-PROTOCOLS-STD-VER-1.0:

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-protocols

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

https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-testing

Public directory of the EITCI EQRNG-QSG Members:

https://eitci.org/quantum-standards-group.pdf - with 105 members as updated on 22nd Nov 2019, the full list of 155 members is available at https://www.linkedin.com/groups/8850635

Please use this free text space to include any additional items you'd like to share that are not covered above

All further corrections to the EQRNG technical reference specifications as published in the RS documents will be continuously accepted at qsg@eitci.org and added to the list of improvements for further reiterations of the Reference Standards accepted by the EQRNG-QSG.

If any member of a related committee or workgroup hosted under any SDO would like to provide any comments or corrections without joining the EITCI QSG, it is also possible to do so by sending an email directly to qsg@eitci.org .

More details on proceeding with the EQRNG Reference Standards can be found at https://eitci.org/technology-certification/qsg/eqrng .

The EITCI QSG aim is to pursue technical quantum standards reference specifications in areas such as QKD, QRNG, QC and supporting undertaking of such efforts by international Standards Developing Organizations.

We are looking forward for the future cooperation in this regard.

Milestone ID

Final report

Attachment

eitci-eqrng-qsg-accepted-rs.pdf

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-THEORY-STD-VER-1.0

Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Theoretical Concepts (Definitions, True Randomness, Use Cases)

EITCI INSTITUTE QUANTUM STANDARDS GROUP

EITCI-EQRNG-QSG

Brussels, 22nd December 2019
Version: 1.0

Table of contents

1. Theoretical context of the reference standard

1.1. Definition of the Random Number Generator

A Random Number Generator (RNG) is a device that produces random numbers, usually encoded as binary sequences of bits 0 and 1 as a common convention in information processing architectures.

1.1.1. Classification of RNGs due to physical process – PRNG vs TRNG

Random Number Generators in principle can be divided into two classes: the Pseudo RNGs (PRNGs) and True RNGs (TRNGs) depending on the physical process of random number generation. Most of the currently used RNG devices are based upon deterministic processes and classical (deterministic) chaos, that is the generation of randomness is based upon classical physics laws. In this case, in PRNGs randomness is not true, but is fully dependent on the complexity of the system involved in physical process of randomness generations and in principle can be predicted with sufficient knowledge of initial conditions regarding the physical system and computational power to simulate its behavior. As the macroscopic systems constituting such PRNGs devices undergo classical physics behavior which is deterministic, even if very complex and seemingly unpredictable, a sufficiently complex technology can in principle measure the physical evolution of RNGs and its interaction with the environment and thus predict the produced random sequence. An example of PRNGs are classical computer processors which can generate pseudo random sequences in relation to their deterministic operation within complex algorithms (the algorithm is fed with a seed number which is then processed in a complex manner providing new pseudo-random number).

The other class of Random Number Generators are True RNGs in which the randomness is absolute. The notion of absolute randomness is strictly equivalent to nondeterministic evolution of physical systems that constitute TRNGs. However truly nondeterministic evolution is characterizing only quantum physical systems and in more precise terms it is present only in the measurement of those quantum system states. Therefore True RNGs are indeed equivalent with so called Quantum RNGs, which describe class of RNGs in which generation of absolute, i.e. unbiased and unpredictable randomness is based upon the fundamental laws of quantum mechanics, rather than of classical physics.

1.1.2. Classification of RNGs due to implementation model – SRNG vs HRNG

Sometimes another division of RNG classes is used: differentiating Software against Hardware RNGs. The classically understood Software RNGs (SRNGs) operate on deterministic information processing devices (for example classical computers or other electronic appliance chips) and thus are always PRGNs, however one can also think about SRNGs based on algorithms for quantum computer and such SRNGs will therefore be able to provide truly randomness, becoming TRNGs (or in fact QRNGs). On the other hand Hardware RNGs (HRNGs) are devices based solely on physically implemented processes, instead of algorithmic information processing, and as such can be either PRNGs (if they are based on deterministic classical systems) or TRNGs/QRNGs (if based on nondeterministic, truly random processes, i.e. on quantum processes). Therefore the proper and meaningful distinction between RNGs is either they are classical (pseudo-random: PRNGs) or quantum (truly-random: TRNGs/QRNGs).

1.2. Definition of the Random Bit Sequence

The basic model of a random bit sequence is a repeatable event of a measurement which gives only two possible results (labeled as 0 and 1), where each result is absolutely independent form previous results -- such situation is commonly modelled as coin flipping with use of an unbiased coin (50% of heads and 50% of tails). In a random bit sequence each bit is generated independently of previous

bits, which means that regardless of how many elements of such sequence are already know, the resultant of the next bit cannot be predicted. Such a model is an idealization of a random bit sequence generator which cannot be implemented with use of classical information science due to the deterministic nature of classical physics – each generator based solely on classical physics mechanisms will always work according to some deterministic process (even highly complex but still predictable). Thus it is a common fact that classical random number generators cannot produce a real random bit sequence.

But in the case of a quantum methods of information processing or generally quantum physics such ideal model is achievable. Quantum mechanics provides fundamental rules which allows to construct a simple system which according to the von Neumann measurement scheme will allow to generate independently 2 possible values with probability equal to 50%. Thus the quantum random number generators are of such interest for modern applications in the information security area.

1.3. Randomness testing of a bit sequence

One of the most important aspect of generating a random sequence of bits is testing whether it is random or not. It is stated that randomness is a probabilistic property, which allows to characterize a random bit sequence in terms of probability.

Each sequence can be analyzed in comparison to truly random sequence expressed in probabilistic values. But there is a fundamental problem – there exists an infinite number of possible statistical tests, each corresponding to some unique pattern. Each test assesses whether such pattern is present in tested sequence or not (if the patter is present then such sequence is considered as nonrandom). Thus it is impossible to find a complete set of test which verify if a sequence is truly random.

The randomness testing of a bit sequence is thus a pattern finding procedure which scales exponentially with the increasing of the possible correlations range or the bits pattern size.

1.3.1. Non-deterministic and non-local quantum physical processes at the basis of randomness generation in Entangled Quantum Random Numbers Generator

Physical evolution of quantum systems can be either unitary or non-unitary if the system leaves its pure (normalized) state configuration and becomes a mixed subsystem of a larger entangled complex system. As opposed to the unitary evolution (or conversingly the process of changing of bases, which might be considered a subjective property of the classical observer) the entanglement between subsystems of a larger complex quantum system (e.g. of 2 qubits) possesses a qualitative advantage as a new informational resource and indeed possesses non-classical properties (violating the local realism assumptions). Entanglement between the components of the complex systems (e.g. between the two qubits) is due to their superposition becoming inseparable in terms of the tensor product of states belonging to Hilbert spaces of both subsystems (qubits), which resolves to a non-unitary evolution of each qubit (altogether they evolve unitarily in joint Hilbert space and a complex system remains pure in this space which is just a matter of alternative formulation in changing of the bases - i.e. a subjective process dependent on the observer making measurement upon the joint Hilbert space, but what is most important is that the subsystems become entangled and mixed upon leaving normalized pure states and their own respective normalized Hilbert spaces). Within this situation vector states formalism is thus not sufficient anymore to describe each qubit (as they are not normalized) and the density matrix formalism is required as a resort to describe the mixed state (the mixed states being the reduced density matrices of the complex system, i.e. a density matrices traced over degrees of freedom of the remainisgs of the complex system). For the pure state the density matrix is a projection operator to this pure state, while for the mixed state it becomes after this reduction a probability mixture of the pure states (i.e. an entangled mixed state resides with given

probabilities in the relevant pure states - hence the name of the mixed state). To prove that the reduced density matrix describing the mixed states is a probabilistic mixture, one needs to refer to the density matrix properties (that are easily proven themselves) stating that density matrices are hermitian, not negatively-valued and have their traces equal to 1. From this it follows upon the spectral decomposition theorem that each density matrix can be diagonalized and decomposed into linear combination of projection operators towards the eigenvectors (or subspaces spanned by them in case of degeneration) and with corresponding eigenvalues which are real numbers (hermitian property), such however that are limited from 0 to 1, and all sum to 1 (respectively from the properties of density matrices being non-negatively valued operators with traces, i.e. sums of diagonal elements equal to 1). This however implies i.e. the eigenvalues in question form indeed probabilities of a random variable (also real numbers, limited from 0 to 1, and altogether summing to 1). Therefore the density matrix of a pure state is a projection operator to this state (i.e. a pure state in probability equal to 1) and of a mixed state density matrix becomes a probability mixture of pure states (represented by projection operators to those states each with a certain corresponding probability). This probability mixture can be therefore treated as a random variable and thus enable definition of the von Neumann entropy, exactly as the Shannon entropy but based on the probabilities present in the mixed state. In this manner the von Neumann entropy measures the extent of how much the state can be mixed, but on the other hand as well the level of entanglement - if the 2 qubits system is in the Bell state e.g. (|00> + |11>), it resolves to both qubits being in maximally mixed states (maximally entangled state of the whole system), with the probabilities equal to exactly 1/2 for the mixed states qubits to reside in pure states |0> and |1>. Now if the measurement of e.g. first qubit is made in the assumed as the reference basis { |0>, |1> } then assuming the complex state of 2 qubits was really in a perfect Bell state, the result will be truly random with a classical bit unveiled from the first qubit to be either 0 or 1 with exactly 1/2 probability and then the second qubit being instantly (non-locally, i.e. clearly violating limitation of interaction propagation at most with velocity of light despite possible spatial separation of those 2 entangled qubits, while preserving the realism supposition, meaning that the measurement only unveils the physical states properties) determined in a correlated state in this configuration (i.e. projected to a classical information). The statistics of these correlations can be measured and are already proven experimentally (after highly important theoretical debate starting from Einstein's Podolsky's and Rosen's objections in the 1935 formulated as the famous EPR paradox) to violate classical limits imposed on such correlations (Bell inequalities).

Therefore discussing of entanglement as a fundamental aspect of truly non-deterministic QRNGs is important and in this context the Entangled QRNG protocol on correlated and anticorrelated Bell states is justified, because the entanglement by itself seems to be a basis for proper definition of quantum information, which in that view consists rather of non-classical, non-local correlations (violating the classical Bell inequalities in statistics and also possesing the negative conditional entropy , alternatively formulated as the concept of partial information only present for quantum information, measuring the ammount of classical information to be communicated in extent in the super-dense coding protocol , with the maximum limit for the Bell state entanglement equal to 1 additional bit of extent information on 1 bit communicated on each 1 qubit (encoding of 2 bits on 1 qubit by local operations under assumption that it is entangled with another qubit, later measured with upon in Bell basis).

The entanglement main characteristic is that it is a fundamentally non-local physical phenomenon. Therefore it is qualitatively different resource against problem of decoherence than local pure state of e.g. a qubit, because decoherence due to physical interaction is of a fundamentally local character . Within the problematics of how to combat the decoherence, beyond the standard Shor's concept based quantum error correction codes , the advanced multi-particle entangled states are one of the possible options for decoherence resilience, and it is evident if one considers e.g. a generalization of the 3-qubits W entanglement state: 1/sqrt(n) |10..0> + |01..0> + .. + |00..1> (only one state |1> in

the non-seperable n-qubits tensor product). In such a case local decoherence of any one of entangled n qubits will not cause any significant deviation for state of the whole system, and in particular to the degree of mixedness of any other individual qubit (the decohered qubit in the worst case of the complete decoherence will simply disentangle from the whole W state entangled ensamble, leaving the n-1 qubits state in the following not much deviated from the original configuration, especially when n is large: 1/sqrt(n-1) |10..0> + |01..0> + .. + |00..1> (again symmretic configuration of only one state |1> in the non-seperable now n-1 qubits tensor product). Due to the general concept of non- locality versus local decoherence , recently there has been a lot of interest towards considering quantum information within the topological degrees of freedom , what is naturally concerning consideration of the topological character of quantum entanglement and thus emphasize the role of present reference standard for entangled quantum randomness.

1.3.2. Not entanglement based quantum randomness

The further discussion contextualizing the present reference standard concerns generation of true randomness from the perspective of quantum mechanics not necessarily based on entanglement phenomena with an important conclusion that no classical statistical tests can prove true quantum randomness of either entanglement or no-entanglement origin for the fundamental reasons (this can be proved only by a physical experiment in area of system dynamics taking place in accordance with the laws of quantum mechanics, leading to empirical phenomena such as quantum interference caused by superposition or non-local violation of classical statistic limits upon Bell or CHSH inequalities with the quantum entanglement).

The basic aspect of random number generators is the physical or mathematical algorithm for selecting random bits in a string. There is no truly nondeterministic mathematical algorithm, which excludes the true randomness of all numerical implementations (they are useful but are not truly random, hence are uncertain for cryptographic applications or exact Monte-Carlo integrals). That is why hardware implementations of a generator using physical processes are being sought. These can be processes of classical nature and therefore be pseudo-random, using complexity and deterministic chaos. From a practical point of view, such randomness seems safe, although deterministic in theory like all classical behaviors. An example would be measuring the fluctuation of sunlight passing through the Earth's atmosphere - although deterministic it is difficult to repeat. Someone would say that it is possible to break a similar measurement at the same time. No - that's not true. the individual path of photons consists of a series of unique quantum dispersions - they are completely non-deterministic. And here the advantage of quantum measurement is marked - it is simply not possible to simultaneously measure similarly. This advantage of the quantum generator is decisive and guarantees the indisputable uniqueness of quantum generated random sequences. Another thing is how to ensure the quantum nature of the draw. The standard approach here is to generate randomness by measuring von Neumann (as described in the Appendix XXX). However, this is impractical - slow and difficult to implement because von Neumann projection is difficult to implement in the macroscopic world.

The main premise of the present reference standard and the research behind it is to test and organize proper quantum structure of the random generator. It is about applying the Fermi Golden Rule (described below and in the appendix XXX). It is Fermi's golden rule that is the aspect of quantum that manifests itself macroscopically and contains a quantum element of randomness.

From the theoretical point of view, this view is new - it has not been clearly identified so far, although some previously proposed physical generators used this randomness but rather in a less-known 'engineering' way in the field of electronics, where randomness was seen in various noises well known especially from microcircuits semiconductor diodes, transistors etc.

Due to the fact that the source of entropy in the quantum generator is subject to the heuristic 'a priori' assumption, it is clear that identifying quantum nature in electronic noise is essential here and should not be replaced by the intuitive concept of 'irregularity - noise'. While the source of entropy for perfect von Neumann projection does not raise any objections, in the case of electronic noise, easier to record, it is not. Usually we deal with a system at finite temperature - and therefore thermodynamic.

The question arises whether thermodynamic chaos is quantum? The answer is not easy, because most often there is a statistical mixing of the thermal and the quantum chaos - it is well seen in the description of quantum thermodynamics (correct, contrary to classical thermodynamics, intuitively understandable but not true). If one bases the random number generator on thermodynamic fluctuations, one can be sure that the quantum component of these fluctuations is absolutely random. The difficulty here is in recording quantum-thermodynamic fluctuations in the appropriate regime.

It seems that on the fundamental level helpful can be the fluctuation-dissipation theorem, which links quantum-thermodynamic fluctuations with transport effects (conductivity). It is an extremely deep phenomenon that the same quantum-thermodynamic features of fluctuations are manifested in the linear response of the systems responsible for the transport. To see this theoretically, it is necessary to shift the linear response of quantum thermodynamic systems in the form of appropriate correlation functions defined by quantum Hamiltonian interactions in the system - this is the language of Green's functions well developed in the second half of the 20th century. Without going into its advanced nature, however, it can be stated for the use of quantum generators that the transport characteristics of complex quantum thermodynamic systems should also have the required entropy of randomness. If you could accurately measure conduction fluctuations in any system, it would be a source of truly random numbers. It must be remembered, however, that the source of quantum randomness lies in the microscopic processes of quantum scattering in the conductor, and not in e.g. voltage fluctuations or other external - non-quantum factors. The task is therefore to identify in electronic noise this quantum component not blurred by external non-quantum randomities.

Why are the distractions random in the guide, for example? Here the golden Fermi rule gives the answer. It's about quantum transitions - by calculations of disturbances for time-dependent disorders, we find the *likelihood of* transition between quantum steady states, before and after the disorder. The disorder is not important - it is important that this probability is *quantum, and therefore perfectly random! same as von Neumann's projection*. This probability, however, behaves very strangely - it increases like a square of the time the disorder is turned on. It's completely unclassical - simply put, the likelihood of moving on to a unit of time is proportional to time. This is not observed in the macroscopic world - here quantum transitions (e.g. optical transitions in atoms) are all per unit of time fixed! So where is the quantum unpredictability? It didn't disappear, just hid in the Fermi's golden rule. If the true quantum transition was proportional to (*T* time of disruption) then one *T* can be divided and then we have the probability of transition per time unit but one more remains *T*. According to the Fermi's idea, called 'golden', the second *T*, if it is long enough, can be replaced by the Dirac delta (as noted in the appendix), and the Dirac delta can be plotted to one, as long as it is then integrated. Thus, the Fermi's golden rule boils down to the integration of one *T,* e.g. on a continuous spectrum of end states or on a continuous dispersion of a disturbance - no matter what, it is important to have a continuous variable after which it can be integrated. This variable continuous brings the whole closer to the classic and the prudence per unit of time are already constant, as we see with the classical senses. *But these probabilities remained absolutely non-deterministic*. So these are processes based on the Fermi's golden rule - they are quantum. All transport phenomena modeled by the Boltzmann equation with collision integrals describing quantum scattering meet the required criterion. The integral of collisions has the golden Fermi rule.

Also processes take place massively in electronic systems and a relatively slow transport channel should be selected to record subsequent bits of the generated string with sufficient resolution. Low currents through reverse-polarized diode or transistor connectors are good here - easy for practical implementation.

2. Quantum random numbers generation use cases

The turn of the 20th and 21st centuries can be regarded as the beginning of the currently observed rapid development and spread of the information technologies in almost all areas of the economy, science and in the field of many different applications. Information technologies in many key aspects require consideration of random variable generation algorithms. Therefore, the problem of random number generators plays a fundamental role in the field of IT techniques and in particular IT security.

The current applications of random number generators (RNG) extend in the area of information technology in the field of:

- applications in the area of cryptography
- for applications for individual users
- generation of random initialization strings (so-called *seeds*) for encryption, authentication or signature algorithms digital;
- key generation (for asymmetric and symmetrical cryptography, e.g. forcipher *One-Time-Pad* to ensure unconditional security), nonces / initiating vectors (IV), challenges (*challenges*) for authentication, selection of exhibitors in the Diffie-Hellman protocol
- other IT applications: eg tags / tokens for communication protocols, for indexing in databases, etc .;
- statistical applications (e.g. selection of a representative sample for statistical analysis;)
- numerical simulations of the Monte Carlo type)
- non-deterministic behavior of artificial intelligence (SI) - SI in computer games, in self-sufficient devices (e.g. drones), etc.
- algorithms of artificial intelligence: neural networks (e.g. random weight allocation for networks) and genetic algorithms (e.g. random introduction of mutations, random mixing of representatives)
- structure and support services of currently popular cryptocurrencies (e.g. bitcoin wallets, bitcoin exchanges, etc.)
- games of chance (e.g. online casinos, including for cryptocurrencies)
- randomness in control processes (important issue of sample selection for quality control processes)
- randomness in administration (e.g. randomization of order on electoral lists, randomization in courts).

The above list briefly shows the scale in which randomness and random number generators application areas currently span. In this context, the quality of randomness and its veracity are becoming a fundamental problem.

2.1. Threats to classical random number generators

The consequences of the predictability of the generated predictable pseudo-random sequence are obvious - the lack of randomness in any of the previously indicated applications is an obstacle to the intended functioning. For cryptographic applications, the consequences can be particularly significant. The problem with classic random number generators, i.e. pseudo-random number generators, is the possible knowledge of the deterministic process of pseudo-random string

generation by unwanted persons. This can result in security compromise for cryptographic applications. It is suspected (based on Snowden reports) that the NSA several years ago made extensive use of the knowledge of the deterministic operation introduced as a standard and a random number generator built into the motherboard for surveillance (breaking ciphers whose keys were made on based on compromised pseudo-random strings).

Another problem may be incorrect handling of the generated string - in most cryptographic applications the generated random string is used once. Its repeated use may lead to a security breach (e.g. in the case of an OTP cipher, by definition a sufficiently long key should be truly random and used once in this protocol, otherwise the cipher may be broken).

It is worth noting that classic random number generators, due to the deterministic generation process (dictated by the deterministic laws of classical physics or deteministic mathematical information algorithms), generate strings that, despite the ideal balance between the numbers 0 and 1 (balance), inevitably always they will be characterized by the occurrence of certain deterministic long-range patterns - correlations that may pose a potential risk to IT security, unexpected errors in scientific simulations or gaps in physical process tests .

It should also be emphasized that regardless of the reduction of the above threats (e.g. the use of randomness tests to avoid repetitive patterns, adequate security of the generation process, one-time use of the generated strings) there is a certain threat that classic computer science will not be able to handle - it is a quantum computer . The emergence of a functional quantum computer (currently pseudo-quantum computers are commercialized, e.g. D-Wave , significantly exceeding the computational power of classic devices, e.g. with acceleration of the order with Monte Carlo optimizations) will cause any classic random number generator will be potentially endangered - theoretically, a quantum computer will find in real time the deterministic nature of the generation process, provided that this process is based on the phenomenon of classical physics. The answer to this threat seems to be quantum random number generators, which are becoming more and more popular, despite the fact that the prospect of the appearance of an efficient scalable quantum computer is still shifted in time due to technological limitations, or perhaps due to still unspecified physical conditions preventing its construction.

2.2. Attacks on random number generators

In the light of the threats of random number generators, it is worth presenting the scale of attacks that have been successfully carried out in the last several years, precisely using the gaps in random number generators. The selected attacks and threat information are summarized below:

- 2006-2012 - over the years, there have been many reports of attacks on cryptographic keys generated by weak PRNG (which makes it possible to carry out e.g. a *brute-force* attack on SSH protected by RSA keys) .
- 2010 - a spectacular attack was carried out on Sony PlayStation 3 (PS3) game users (data theft was as much as 77 million users). The attack was carried out using a vulnerability in the implementation of the ECDSA algorithm by Sony (the disclosed materials informed about the incorrect multiple use of the same random number as the so-called *nonce* for authentication)
- Year 2012 - two groups of researchers revealed a large number of RSA keys for encryption, which were then actively used on the Internet as safe, and were at risk of fracture due to insufficient randomness of the generator that was used to produce them
- 2013 - after Snowden disclosed these deficiencies to the US National Security Agency (NSA), Reuters together with NewYorkTimes conducted investigations revealing that the NSA deliberately secretly lowered the security of hardware and software solutions

popular around the world to perform crypto attacks on encrypted content (including RNG attacks):

- Dual_EC_DRBG (*Dual Ellipti c Curve Deterministic Random Bit Generator*), PRNG created and strongly forced as a standard by NSA. It wasn't until 2013 that the NSA was the only one to have a *backdoor* for this generator and thanks to this the NSA could break the cryptographic keys that were generated using these generators. After disclosing this fact, RSA Security and the National Institute of Standards and Technology in the USA (NIST) ordered not to use the Dual EC DRBG generator.
- • The NSA was carrying out a secret project codenamed *Bullrun*, focusing on exploiting the gaps of PRNG, which was randomly accessed, in various devices (e.g.network devices *Juniper*).
- It also turned out that random number generators mounted on Intel and Via on-chip HRNG motherboards probably also had *backdoors* . It was pointed out that the RdRand and Padlock instructions most likely have *backdoors* in Linux kernels up to v 3.13.
- It is suspected that the NSA scandal of eavesdropping on leaders of 35 European countries was just related to the use of attacks on the RNG.
- 2013 - Google confirmed that the IBM Java SecureRandom class in Java Cryptography Architecture (JCA) generated repetitive (therefore predictable) strings, which resulted in the compromise of the security of the application created for Android for the electronic currency Bitcion - the equivalent of USD 5,700 was stolen Bitcoin .
- 2014 - It is suspected that the attack on the Tokyo MtGox cryptocurrency exchange in which more than 800,000 Bitcoins were stolen (which resulted in the bankruptcy of MtGox) was related to the attack on RNG
- Year 2015 - Difficult to detect remote attack using externally connected hardware Trojan horse on TRNG based on FPGA
- 2015 - theft of 18866 bitcoins from the Bitstamp exchange (12% of the currency being traded on this exchange) - RNG attack signature number
- Year 2017 - ANSI x9.31 PRNG up to 2016 compliant with FIPS USA (Federal Information Processing Standards) - compromised if used with *rigidseed* encoded(DUHK attack - Don't Use Hard-coded Keys)

The presented attacks clearly indicate that classic random number generators may be exposed on various attacks, or they may have so-called *backdoors*. This justifies the need to develop alternative technologies that could replace classic generators on a large scale. The most promising, because they have a fundamental justification for randomness in the quantum mechanics formalism, are quantum random number generators.

2.3. Further classification of random number generators in applications perspective

As already indicated there are many types of random number generators. Their basic division can take place in relation to the physical implementation of generators - programming generators or hardware generators - and to the physical nature of the generation process - classic generators and quantum generators. These two main divisions perspectives partly overlap - programming generators are purely classic, while hardware generators are divided into classical, quantum, and generators in which the nature of the physical process cannot be clearly distinguished.

Further subdivisions are possible, e.g. different types of pseudo-*random number generators* (PRNGs), among which are *cryptographically secure pseudorandom number generators* (CSPRNGs). Classic hardware generators can be divided due to the specific physical process underlying the generation, just like quantum generators. Each type of generator can also additionally carry out on-going testing of generated strings based on implemented tests, assessing the deviation from assumed randomness

parameters of the generated string. There are also hybrid generators that combine the features of many categories.

The basic subgroup of PRNG pseudo-random generators are programming generators - these generators are based on the algorithmic process of generating a random sequence based on an initial random key (initial portion of entropy). The initialization key represents some entropy that remains unchanged regardless of how long the string will be generated. Therefore, programming generators are obviously pseudo-random. Knowledge of the initial key compromises the randomness of the entire generated string (based on the knowledge of the key and algorithm parameters, the entire generated string can be reproduced). The string generated by PRNG has repetitions or the generation process ceases to be effective in terms of resource use.

Classic hardware random number generators do not require initial entropy - the source of entropy is in this case the classic physical process. If the entropy used is consumed, the generator must wait until the generation process provides enough of it. Generators in this class are also pseudo-random generators due to the determinism of classical physics and, therefore, can be a potential target of attack. In particular, an effective attack on such a generator could be made using a quantum computer.

Quantum hardware random number generators, or quantum random number generators QRNG can be divided into three categories :

- Practical quantum random number generators - fully trusted and calibrated devices. Randomness depends on the correct modeling and implementation of the physical quantum process. Usually, the generation speed is medium high and the device costs relatively low. In practice, in these devices, quantum randomness is often mixed with classical noise (which can, however, be removed if the basic quantum process is properly modeled). For these devices, security is conditioned by trust in the device and its components, which can be a problem for external suppliers.
- (Self-) Testing quantum random number generators - the generated string is tested for randomness due to a lack of confidence in the implementation of the physical process. Testing can be done on the basis of classic tests, but also, e.g. verification of the existence of quantum entanglement, by checking the statistical fracture of the so-called Bell inequalities . These devices are also referred to as quantum random number generators independent of implementation (device independent QRNG) . Due to the complexity of the testing process, such generators are usually very slow.
- Semi-test quantum random number generators - this category includes devices in which compromising testing and implementation trust have been compromised, which allows you to modify the parameters of the randomization speed and confidence in the generated randomness. Some components in such a device are considered safe / trusted due to their exact characterization, others cannot be recognized as such and therefore randomization tests need to be performed.

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-PROTOCOLS-STD-VER-1.0

Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Protocols, Processes, Devices and Operative Principles

EITCI INSTITUTE QUANTUM STANDARDS GROUP

EITCI-EQRNG-QSG

Brussels, 22nd December 2019
Version: 1.0

Table of contents

1. Introduction to protocols of Entangled Quantum Random Numbers Generation

As mentioned above the essential character of quantum entanglement, a purely quantum concept, can be described as a non-local or thus global phenomenon. Discussion of non-locality of quantum entanglement has been very active since formulation of the EPR programme in 1935 . Since then it became clear in the sixties, that quantum entanglement correlations in measurements violate classical limits imposed by statistical consideration . There have long been discussed so called hidden-variables theories to complement for the seemingly missing elements of reality lacking in quantum mechanics description. But the Bell inequalities violation as well as the empirical confirmation by Aspect experiment , have ruled out the possibilities to address hypothetical variables as local. This resolves now to common understanding that quantum entanglement is essentially non-local if one is to sustain the realism assumption in science. As the property of non-locality lies in the center of interest of topology, it can be justified to search for some mathematical objects which can model the entanglement from the topological point of view. Such ideas were developed within last years, as well as in recent conjectures based on the concept of entanglement being equivalent to curved space-time features of Einstein-Rosen Bridge. The present reference standard aims to address some special aspects of quantum entanglement in a topological notions as well as to concretize its applications in entangled quantum random number generator (EQRNG).

1.1. Topological aspect of entanglement

On a very abstract level the most intuitive model of the entanglement between two quantum states (for simplicity we limit our consideration to most simple two-dimensional quantum states, which are referred to as qubits) might be considered topologically in terms of the entanglement between two geometrical rings. Topological character of such rings resembles entanglement between two qubits— despite the space separation the quantum entanglement remains intact same as the entanglement of two rings regardless of their sizes. It should be noted, that links of fundamental aspects of quantum mechanics with topological description and in particular braid groups, are all well-known concepts, leading from the most obvious example to geometrical explanation of quantum statistics (distinction of fermions and bosons in 3D) by topological differences in trajectories for elementary particles quantum states replacements, as well as concept of anyons in 2D physical systems and discussion of QHE (Quantum Hall Effect).

In terms of the braid group for 2D plane the elementary entanglement would be represented by a 2-braid of form σ_i^2, cf. Fig. *1.* b) — two hooked rings. On the other hand, two unentangled qubits state would be represented by a trivial 2-braid, ε — two unentangled rings, cf. Fig. *1.* a). However, such analogy is only able to describe the sole existence of the entanglement (hooked/entangled or unhooked/unentangled rings), while not the peculiarities of the modelled entanglement (e.g. differences between maximally entangled states in the Bell basis or the differences in a degree of entanglement between two qubits, such as $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$).

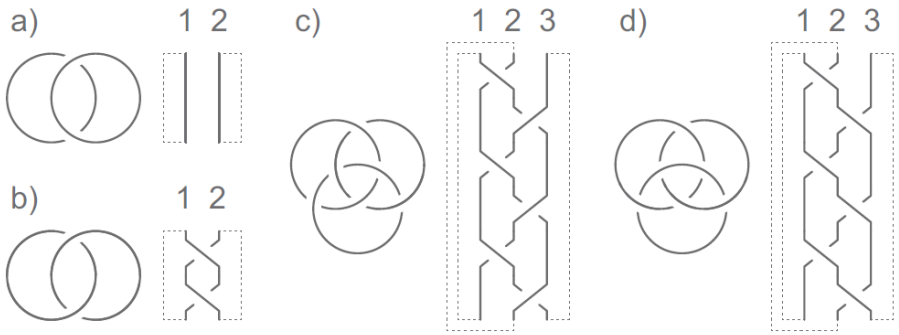

Fig.1. A simple topological model corresponding to inequivalence in terms of topology of the basic quantum entanglement types for two-dimensional quantum systems (qubits). As elements of the braid group are in fact closed loops, the gapped lines were added for clarity.

Nevertheless, the topological braid group model allows to notice some fundamental distinguishment of entanglement types by their topological inequivalence when considering the entanglement of systems with 3 or more qubits. In a case of a 3-qubit system one can distinguish two topologically inequivalent entanglement types—the one corresponding to an entangled state, in which when any of 3 (or generally n) qubits is measured then 2 (or n-1) other qubits instantly become unentangled due to von Neumann projection and the algebraic structure of the quantum states tensor product linear combination (the Greenberger-Horne-Zeilinger GHZ state), as well as the other type (a more W like state) corresponding to such an entangled state of 3 (n) qubits configuration, in which after measuring of any of the 3 (n) qubits, the 2 (or n-1) others remain still entangled (in some Bell state selected arbitrarily, but correspondingly to the first qubit measurement outcome).

In case of the GHZ state, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, or similar states, one can describe their topology (using the entangled rings model) in the form of the so called Borromean rings . It is such rings arrangement that when cut open any of the rings the two remaining would always be unentangled.

In the braid group language such topology would correspond to 3-braid in form of $\sigma_1 \cdot \sigma_2^{-1} \cdot \sigma_1 \cdot \sigma_2^{-1} \cdot \sigma_1 \cdot \sigma_2^{-1}$, cf. Fig. *1.* c).

A second (topologically inequivalent) type of entangled state of 3 qubits, is for e.g. $\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$, which in terms of entangled rings corresponds to a topology of closed 3-linked chain—after cutting open any of the chain loops the two remaining will still be entangled.

In the braid group language such a topology would correspond to 3-braid in form of $\sigma_1 \cdot \sigma_2 \cdot \sigma_1 \cdot \sigma_2 \cdot \sigma_1 \cdot \sigma_2$, cf. Fig. *1.* d).

1.2. Simple quantum circuits implementing topological inequivalence of entanglement

This topological inequivalence of above entanglement types, very evident in geometrical representation, is on the other hand not easily visible in the entanglement tensor product representation algebraic structure or within the entanglement generation process, which can be described formally for instance in the language of single and two qubits quantum gates (linear unitary operators in corresponding Hilbert spaces), as presented below.

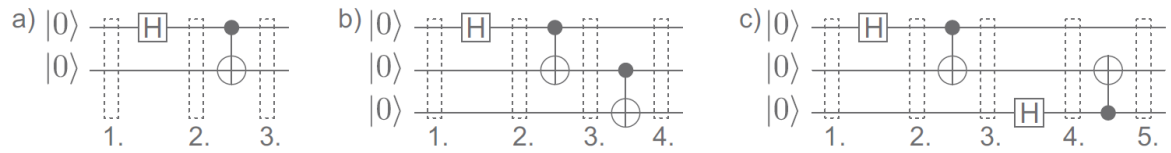

Fig. 2. *Exemplary basic quantum circuits schemas depicting topologically inequivalent entanglement types generation. Gapped regions depicts consecutive steps of quantum circuit evaluation.*

Basic quantum circuits generating different entanglement types described above are depicted in Fig. *2.*. Basic evaluations of those quantum circuits are presented below for clarity:

- Fig. *2.* a)—the Bell states generator—gapped regions evaluation:
    a. Initial state: $|0\rangle \otimes |0\rangle$
    b. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
    c. After the CNOT gate acting on qubits 1 and 2: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Fig. *2.* b)—the Borromean rings topology state generator (GHZ 3-qubit entanglement)—gapped regions evaluation:
    a. Initial state: $|0\rangle \otimes |0\rangle \otimes |0\rangle$
    b. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \otimes |0\rangle$
    c. After the CNOT gate acting on qubits 1 and 2: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle)$
    d. After the CNOT gate acting on qubits 2 and 3: $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
- Fig. *2.* c)—the closed 3-linked chain topology state generator—gapped regions evaluation:
    a. Initial state: $|0\rangle \otimes |0\rangle \otimes |0\rangle$
    b. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \otimes |0\rangle$
    c. After the CNOT gate on qubits 1 and 2: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle$
    d. After the Hadamard gate acting on qubit 3: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}|0\rangle + |1\rangle = \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle + |111\rangle)$
    e. After the CNOT gate acting on qubits 3 and 2: $\frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)$

2. Entangled Quantum Random Number Generator with public certification preserving secrecy

The present reference standard specified Entanglement Quantum Random Number Generator (Entanglement QRNG) uses a special topological configuration of multi-qubits entanglement of quantum states to produce quantum randomness with the public certification without disclosing of the generated random sequence secrecy.

The reference standard describes both the protocol and its generic implementing device, involving the specific 3-qubits quantum entanglement of generalized Bell state type (topologically inequivalent to different types of entanglements and easily generalized to multiple-qubits as shown in the present reference standard description), characterized also in the topological terms, that enables private quantum random number generation with a publicly accessible proof of randomness, thus allowing an external party to freely and publicly verify the randomness of the generated sequence without disclosing of its secrecy or distorting it in any way (this feature of QRNG is proposed for the first time and has an important role for applications in both quantum and classical cryptography).

The Entanglement Quantum Random Number Generator with public verification of randomness is based upon the originally proposed entanglement based random correlation generator, assuring that generated random sequences are randomly correlated and anti-correlated on corresponding positions: in the most basic configuration of the device its main feature is publicly verified absolute randomness not sacrificing it's secrecy, possible due to a secret correlation - anticorrelation relation on subsequent bits positions of both random bit sequences (one kept secret, and the other one revealed). Thus the described reference standard offers for the first time a technical solution to provide a publicly accessible proof of privately and secretly generated randomness without compromising its privacy and secrecy, thus allowing an external party to freely and publicly verify the randomness of the generated sequence without disclosing of its secrecy or distorting it in any way. The new important properties of the proposed reference standard find applications in many areas of technology and science where randomness is needed. These unique properties are strongly linked with multiple qubits entangled states and their topological features, which thus finds important applicability in the industry of information and communication security. The reference standard uses non-trivial quantum entanglement configuration in industrial applications harnessing its non-classical and non-local power, which leads to identification of not achieved previously practical features. The main advantage in contrast to previous discussed QRNG protocols is that all previously considered schemes did not offer any mean of public verification of true randomness keeping secrecy of the generated random number. This is very critical issue in terms of applications as potential users of QRNGs must rely on trust assumption, not being able to offer verification of the very randomness used without revealing it.

The reference standard and its generic implementing device (shown in the Fig. *3.* with workflow diagram depicted in the Fig. *4.*) solve this issue by enabling objective verification of the true randomness of the bit sequence, without compromising its secrecy. Generalized extension of the reference standard device of Entanglement QRNG (as presented in Fig. *5.* and Fig. *6.*, with four or more entangled qubits) uses shorter sequences of random bits verified statistically to be truly random in order to information theoretically certify same randomness of longer sequences of bits remaining secret (this result has not been achieved before in the field of randomness generation and is of a fundamental significance for the described present reference standard).

The technical problem which is considered upon the presented reference standard consists of:

- Provision of the truly random (upon quantum non-determinism) process as a basis for generation of random numbers (random bit sequences).

- Provision of means to certify this true randomness, that is not compromising its secrecy.

Differences mentioned above between two mentioned types of three qubit entanglement states, characterized in topological terms with 3-link chain or Borromean rings topology, can be used to discuss distinct basic protocols in area of the quantum random number generators (QRNG) based on quantum entanglement.

Let us remind the form of the Bell basis:

$$\Psi_{AB}^{+} = |00\rangle_{AB} + |11\rangle_{AB}/\sqrt{2}, \Psi_{AB}^{-} = |00\rangle_{AB} - |11\rangle_{AB}/\sqrt{2}$$

$$\Phi_{AB}^{+} = |01\rangle_{AB} + |10\rangle_{AB}/\sqrt{2}, \Phi_{AB}^{-} = |01\rangle_{AB} - |10\rangle_{AB}/\sqrt{2}$$

In a sense of quantum measurement, interpreted accordingly to probabilities represented by modulus squared of quantum superposition coefficient standing with the quantum state corresponding to measurement result and von Neumann projection postulate, those state can be grouped in two classes: the correlated and anti-correlated ones. States Ψ_{AB}^{+} and Ψ_{AB}^{-} are correlated in a specific way in sense of results of measurements of both qubits—if the first qubit is found in state $|0\rangle_A$ then the second qubit must be also in state $|0\rangle_B$, and similarly for state $|1\rangle$—this can be called type 1 of the entanglement (correlation of the measured states results). States Φ_{AB}^{+} and Φ_{AB}^{-} are in contrast correlated in a different manner—the result of the second measurement is always opposite to the result of the first measurement—type 2 of the entanglement (anti-correlation of the measured states results).

As to determine which type of correlation one deals with at the entangles state of 2 qubits, one must measure both qubits to get the classical information (measurement outcome) to identify the type of the correlation.

Let's consider those two distinct types of correlation within the Bell basis (correlation and anti-correlation) as a random results of the measurement of entangled 3-qubit state, characterized by a specific topological nature of its entanglement. This fundamental difference (correlation or anti-correlation) will be used to encode classical random bit in the sequence generated within such an entanglement based Quantum Random Number Generator protocol.

An example of such a 3-qubit state has the form $\frac{1}{2}(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB})$. In terms of topological description of entanglement as a topology of rings, this state is represented by a closed 3-linked chain (each chain is linked with both others). In such a chain entanglement configuration it is possible to cut one of the rings of chain and remove it without cutting two remaining chain rings—those two rings will remain entangled. In the notion of above quantum state the cutting procedure can be identified with the measurement of one of 3 qubits in the computational basis (i.e. von Neumann projection of quantum information of this one qubit to classical bit information of either 0 or 1). But the process of cutting one of the chain rings can be carried out in two distinct ways, which correspond to two distinct results of measurement of one of the qubits rendering the measurement outcome to be 0 or 1. Different measurement results corresponds to qualitatively different joint entangled state of the two left qubits.

According to the above 3-qubits entangled state one can write

$$1/2\,(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB})$$
$$= 1/\sqrt{2}\,|0\rangle_X\,|00\rangle_{AB} + |11\rangle_{AB}/\sqrt{2} + 1/\sqrt{2}\,|1\rangle_X\,\frac{|01\rangle_{AB} + |10\rangle_{AB}}{\sqrt{2}},$$

where the LHS of the equation is represented upon the Hilbert space in form $H_X \otimes H_A \otimes H_B$ and the RHS in form $H_X \otimes (H_A \otimes H_B)$.

The measurement of X qubit will lead to one of the two possible results with the same probability $\frac{1}{2}$. The resultant state $|0\rangle_X$ corresponds to the state $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ and the resultant state $|1\rangle_X$ corresponds to the state $\frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB})$.

The above scheme can be represented in form of a quantum circuit, cf. Fig. *3.*

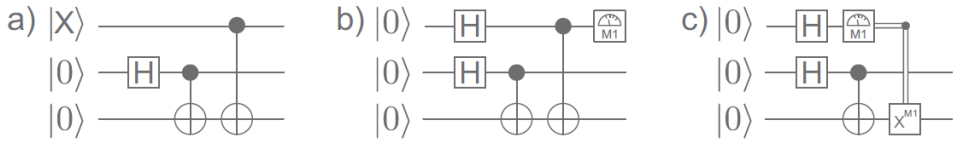

Fig. 3. *Quantum gate scheme of a random correlation entanglement generator with 2-qubit entanglement state and one auxiliary qubits X. Without (a) or with (b,c) a random selection of 2-qubit entangled state type. Double line represents classical information about the measurement result.*

Such a setup can be called an entanglement based random correlation generator. By continuously initiating the setup with state $|000\rangle_{XAB}$ and performing the measurement on auxiliary qubit X (or in fact on any other qubit) the setup will generate as an outcome, in a truly (non-deterministically quantum) random manner, the 2-qubit entanglement state in a specific correlation type, either fully correlated or fully anti-correlated (entanglement of qubit A and B if qubit X was measured).

Specified as the main present reference standard is the Entanglement Quantum Random Number Generator (Entanglement QRNG) with publicly verifiable randomness that is an extension of the above described original concept in the field of QRNG.

It is a simple protocol representing a generic device based on any physical quantum entanglement implementation, involving specific 3-qubit quantum entanglement characterized in topological terms, for quantum random number generation with publicly accessible proof of randomness, which is conceptually achieved on a fundamental (fraud-resistant) level for the first time.

As quantum random number generators are gaining in popularity, especially with regard to possibility of a break-through with the efforts in construction of a scalable quantum computer that could endanger deterministic pseudo-randomness based on computational complexity, a protocol allowing for an external party to freely and fraud-proofly verifying of the true randomness of the generated sequence without distorting it in any way and most importantly without getting to know this very sequence by a party which is only interested in checking if the random sequence is truly random, seems to be of a potential use. In other words this protocol for the first time offers the generation of the random sequence with means to publicly prove the true randomness of the generated sequence without revealing this sequence, which would render it useless in different cryptographic applications. It should be noted that the previously considered QRNG protocols do not offer such mean of public verification of true randomness, and the randomness using party must rely on trust to the QRNG device supplier. The QRNG device based on the here proposed protocol is on the other hand publicly and objectively verifiable true randomness generator. It is worth to note that the public and objective verification of true randomness concerns in this protocol the very sequence of random bits that undergo desired randomness application, and thus when verified by any external party that these bits are truly random they are guaranteed to be so within a corresponding application without the need to reveal their values. This is in contrast to possible claims for other means of random bit sequences randomness verification, when for example random positions of the sequence are unveiled and their randomness publicly tested: in that case if the verification is positive it only guarantees to external parties that these very tested bits were random, but does not give any guarantee about the randomness of the remaining bits if one is not able to prove publicly the true

randomness of the testing bits choice. In short the novelly proposed here QRNG protocol gives mean for universal randomness proof based on the fundamental correlation / anti-correlation of quantum entangled states distributed between protocol parties. In order to prevent attacks on the protocol based on the decreased measures of entanglement between the distributed qubits states (in essence with external eavesdropping qubits being co-entangled, thus taking the 3 or in general n qubit states out of their maximal and symmetrical entangled configurations) this QRNG protocol could be supplemented in the initial stage with well-known protocols of entanglement distillation and purification).

One can consider the following formalization of the protocol, which we will call a quantum random number generator with public proof of randomness:

1. Let's assume that Alice owns generator described above.

2. Alice continuously initiate quantum setup from Fig. *3.* with state $|000\rangle_{ABC}$.

3. After each initialization Alice performs a quantum measurement on qubit A, and keeps the result of each measurement in secret (this will be called a sequence A_i). Only Alice has the knowledge what type of entanglement was randomly chosen for each generated pair.

4. In result a continuous series of entangled pairs of B and C qubits are produced, with entanglement defined by elements of the sequence A_i (cf. Fig. *5.*), as follows

   – $0 \rightarrow \frac{|00\rangle_{BC}+|11\rangle_{BC}}{\sqrt{2}}$ – correlated state,

   – $1 \rightarrow \frac{|01\rangle_{BC}+|10\rangle_{BC}}{\sqrt{2}}$ – anticorrelated state.

5. Next Alice performs a measurement on qubits in each pair, which results in two bit sequences:

   – B_i – sequence of random bits resulting from measurements of qubit B from each pair,

   – C_i – sequence of random bits resulting from measurements of qubit C from each pair (in fact there is no need to perform qubit C measurements as the sequence B_i and the sequence A_i define their states unequivocally).

6. Alice ends with 3 equal length sequences:

   – sequence of entanglement type selected for each pair, A_i,

   – B_i and C_i – mutually correlated, by the sequence A_i, random sequences.

For someone who does not have any knowledge about the types of entanglement selected for each pair, sequences B_i and C_i are completely random and a prediction of the bits from one sequence (e.g. C_i) basing only on the second (B_i) sequence is in such case impossible. On the other hand, for Alice, from all those three sequences (B_i, C_i, and entanglement type selections sequence A_i) only two (and any arbitrary two) presents a random information.

But the most important thing is that any two sequences, e.g. B_i and C_i must have identical statistical properties (due to entanglement correlation or anticorrelation), and this feature is crucial in the proposed present reference standard allowing Alice for the enhanced randomness verification.

2.1. Advantages of the reference standard EQRNG protocol

As there is always a doubt whether the generated sequence is truly random or not, both in classical and quantum case (in the classical case this doubt can be addressed to the problem of the definition of the randomness itself, and in the quantum case it corresponds to the quantum mechanics interpretation differences between the von Neumann measurement concept based on an objective frequential probability and Fuchs Quantum Bayesianism theory, so called QBism, based on a rather subjective conditional probability , for example discussed in Ref.), statistical randomness testing offers some kind of verification. But the randomness testing suffers from a fundamental problem – lack of universal set of tests. In fact, there is an infinite number of different pattern matching tests, as there is an infinite number of patterns.

Therefore comprehensive testing can be highly resource consuming, and in general not available to be implemented in miniaturized quantum random number generator solutions. On the other hand a good quality randomness for a personal cryptographic usage (initial secrets, initialization vectors, nonces, etc.) is highly desirable. The proposed protocol can be used to transfer the weight of randomness testing from the generator device or the user to some external public party (which can have unlimited computational resources in comparison to a single user/generator).

In view of the above further steps of proposed protocol can realize the following use case scenario:

7. Alice doubting the randomness of the B_i sequence publicly sends the C_i sequence to the Verification Center (VC).

8. VC publicly performs a series of resource consuming randomness testing, deciding whether the sequence C_i can be considered truly random or not.

9. VC publicly informs Alice about its decision.

10. In case of a positive decision Alice gains the certainty that the sequence B_i remaining secret is also truly random.

In this protocol Alice can perform own initial randomness testing and use VC to enhance testing procedure. Due to the specific way of generation of sequences B_i and C_i, a public announcement of one of them does not affect the secrecy of the other one. The public character of VC randomness testing procedure serves as a warranty against fraud – decision of VC can be verified by any other public party (in general Alice can use multiple VCs simultaneously to increase the precision of the decision).

It is worth mentioning that VC can be possibly equipped with the quantum computer, which could be used to check whether the generation process is truly random or biased (for example, by the presence of a classical and thus deterministic influence on the generation process).

Proposed protocol offers randomness certified by classical statistical tests performed publicly. Here the quantum randomness has a twin origin – quantum measurement choosing correlated or anticorrelated entangled state of a qubits pair, and measurement unentangling this pair. Alice, randomly performing verification of entanglement existence, tries to check whether the quantum source of entropy is of good quality or not. In this context it can be considered as a member of a wide class of so called Device Independent RNG , which are also verified statistically, as their generation process can be considered biased. In the proposed case, considered quantum randomness is based on a quantum measurement, but the bias can correspond here not only to implementations imperfections, as considered for the Device Independent RNG concept , but also to a non-trivial problem with introducing subjectivism to the quantum measurement due to questioning the correctness of using the frequentist probability in von Neumann measurement concept instead of

conditional probability as described within the Quantum Bayesianism theory . As the quantum measurement in its foundations is unrepeatable and destructive and No-Cloning theorem applies, the concept to describe a measurement with a frequentist probability is somehow problematic. But regardless of the nature of the bias (either fundamental or implementation-wise), the proposed protocol allows to perform inaccessible in a standard case, due to computational inefficiency, simultaneously (with use of multiple VCs) randomness tests on large blocks of data (instead of rather short blocks in standard tests, for example NIST test suite).

The problem of analyzing the entropy of the source of randomness is surely crucial for imperfect physical applications of quantum random generators (e.g.). Some approaches are limited to specific generating techniques and setups . More universal approaches are concepts of Device Independent RNG , where some of the protocols extract quantum randomness and discard deterministic behavior due to quantum processes implementation shortcommings. Self-testing QRNG protocols are also considered as part of device independent approach, for example in Ref. , where testing of the dimension of uncharacterized classical and quantum systems allows the observer to separate the quantum part of the randomness from a deterministic classical part, which results with very high confidence of 99

As mentioned previously, the Greenberger–Horne–Zeilinger (GHZ) state is a specific type of a 3-qubit entangled state. It has a following form

$$|\text{GHZ}\rangle = 1/\sqrt{2}\,(|000\rangle_{ABC} + |111\rangle_{ABC}).$$

It is worth noting that if both discussed states, $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\left|\text{3-link chain}\right\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$, were similarly used, as in discussed above protocol, the results, from point of view of the entropy, are quite different. If one of qubits in the series of GHZ states was measured in a computational base, then each time both other qubits are simultaneously unentangled in pure states and their measurements carry no entropy (the only entropy is within the first unentangling measurement). In the case of a series of 3-link chain states, to determine the classical states of each 3 entangled qubits, one needs to perform not one but two quantum unentangling measurements, what leads to twice as big entropy as in GHZ case. If one considers on the other hand the W state, defined as follows $|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$, then in case of a series of measurements made on each first qubit in series of W states will lead to two different results, either all 3 qubit states are defined – first qubit is in state 1, or only the first qubit is defined in state 0 and the two other qubits stays in anticorrelated entangled state - in this case another unentangling measurement is needed to define classical state of all three qubits. Of course due to the above situation all 3 bit sequences will have non-uniform distributions of 0's and 1's (which is a consequence of the lack of binary symmetry in entanglement configuration of the W state). In terms of entropy, the series of measurements of qubits triples entangled in W states leads to entropy smaller than in GHZ states.

Generalized multiple GHZ state can be written as

$$|\text{GHZ}\rangle^{(M)} = 1/\sqrt{2}\left(|0\rangle^{\overset{M}{\otimes}} + |1\rangle^{\overset{M}{\otimes}}\right),$$

where $M > 2$ is the number of qubits, and $|\alpha\rangle^{\overset{M}{\otimes}}$ is a M-times tensor product of states $|0\rangle$.

One can say that GHZ-type states are a multiple-qubits generalization based on the structure of one of the Bell basis states of qubits entangled pair, the $\Psi_{AB}^{+} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. In all of those states after the measurement each qubit is in the same state as all others. This property enables to consider another important feature for QRNG, namely the simultaneous generation of a random

number string in all parties holding qubits which state were described by a GHZ-type state, which is referred as quantum secret sharing . Such concept holds potentially important aspect for cryptography of secret communication, introducing extended concept of the Quantum Key Distribution (QKD) protocol (where all engaged in distribution parties trust an entanglement source), not hampered by point-to-point topology, which is often considered one of main drawbacks of quantum cryptography. The considered in detail multiparty QRNG protocol can be for example utilized to distribute securely (in terms of theoretical security guaranteed by quantum mechanics laws) a classical and fully random key (a random bit sequence) between multiple parties simultaneously, thus enabling symmetrically encoded secure broadcasting, or any other random numbers application which require the sequence to remain known only to engaged parties.

In case of the simplest scenario the GHZ entangled 3-qubit state can be considered with qubits A, B, C. After the first measurement of any of the qubits all of the 3 qubits will attain certain state depending on this measurement result due to the von Neumann projection postulate and GHZ state algebraical tensor product structure. Assuming continuous generation and distribution of the GHZ states, such procedure, if repeated consecutively, will generate 3 copies of a random sequence of classical information bits.

But in the case when one of the party will measure a single qubit which is in one of the below states, truly randomly selected:

$$1/\sqrt{2}\,(|000\rangle_{ABC} + |111\rangle_{ABC}), 1/\sqrt{2}\,(|001\rangle_{ABC} + |110\rangle_{ABC})$$

$$1/\sqrt{2}\,(|010\rangle_{ABC} + |101\rangle_{ABC}), 1/\sqrt{2}\,(|011\rangle_{ABC} + |100\rangle_{ABC})$$

the results of measurements of other two qubits (of qubit B and C) will be totally independent from each other and from result of qubit A measurement.

The above states can be selected in a random manner by using of another two additional qubits, as follows.

5-qubits system can be organized to generate a random state from above set after being initialized by state $|00000\rangle_{XYABC}$, where qubits X and Y are auxiliary qubits. The quantum circuit setup state before the measurement of any of two auxiliary qubits states should be in the state

$$\begin{aligned}\psi_{XYABC} \quad &= 1/2\,|00\rangle_{XY}\, 1/\sqrt{2}\,(|000\rangle_{ABC} + |111\rangle_{ABC}) + 1/2\,|01\rangle_{XY}\, 1/\sqrt{2}\,(|001\rangle_{ABC} + |110\rangle_{ABC}) \\ &+ 1/2\,|10\rangle_{XY}\, 1/\sqrt{2}\,(|010\rangle_{ABC} + |101\rangle_{ABC}) + 1/2\,|11\rangle_{XY}\, 1/\sqrt{2}\,(|011\rangle_{ABC} + |100\rangle_{ABC}).\end{aligned}$$

According to above state ψ_{XYABC} after the measurements of qubits X and Y, the overall state of qubits A, B and C is defined, but in an entirely random manner, same as the two mentioned measurements results.

After the measurement of any single qubit of these three qubits, the states of the other two qubits will, in a random manner attain their respective values depending on the type of the entanglement.

Public announcement of one of the random sequences will not affect the security of random sequences.

Now Alice can verify the randomness of all sequences just by public announcement of one of them to the Verification Center (VC). All other, kept in secret, random sequences share the same statistical correlation as the one published and verified. In case of a positive assessment of the VC, the protocol leads to an interesting result – Alice certified twice the long random sequence as the sequence being tested for randomness.

This is an example of a generalization of the discussed above scheme for quantum random number generator with public proof of randomness. Only one sequence is required to be publicly exposed to be checked for randomness thus verifying the randomness of the other sequences, while all other sequences (in case of 3-qubit scheme only one sequence, in 5-qubit scheme 2 sequences, etc.) have the same statistical properties but their actual values stay undisclosed.

A quantum circuit scheme is depicted in Fig. *5.* To achieve random selection of qubits A, B and C entangled state the 2 measurement gates are introduced, which control the single-qubit gates (measurement gates controlling other unitary quantum gates in quantum information circuit is a well-known approach, e.g. present in the circuit of the quantum teleportation).

Similar setup can be proposed for higher number of entangled qubits. For clarity with the 4-qubits entangled state one will have

$$\psi_{XYZABCD} =$$

$$\begin{aligned}
&= 1/2\,|000\rangle_{XYZ}\,1/\sqrt{2}\,(|0000\rangle_{ABCD} + |1111\rangle_{ABCD}) + 1/2\,|001\rangle_{XYZ}\,1/\sqrt{2}\,(|0001\rangle_{ABCD} + |1110\rangle_{ABCD})\\
&+ 1/2\,|010\rangle_{XYZ}\,1/\sqrt{2}\,(|0010\rangle_{ABCD} + |1101\rangle_{ABCD}) + 1/2\,|011\rangle_{XYZ}\,1/\sqrt{2}\,(|0011\rangle_{ABCD} + |1100\rangle_{ABCD})\\
&+ 1/2\,|100\rangle_{XYZ}\,1/\sqrt{2}\,(|0100\rangle_{ABCD} + |1011\rangle_{ABCD}) + 1/2\,|101\rangle_{XYZ}\,1/\sqrt{2}\,(|0101\rangle_{ABCD} + |1010\rangle_{ABCD})\\
&+ 1/2\,|110\rangle_{XYZ}\,1/\sqrt{2}\,(|0110\rangle_{ABCD} + |1001\rangle_{ABCD}) + 1/2\,|111\rangle_{XYZ}\,1/\sqrt{2}\,(|0111\rangle_{ABCD} + |1000\rangle_{ABCD}),
\end{aligned}$$

where qubits X, Y and Z are auxiliary qubits for setting random state of 4 qubits A, B, C and D.

The measurement of 3 auxiliary qubits results in arrangement, in a truly random manner (guaranteed by the fundamentally non-deterministic quantum measurement property), of a specific type of the 4 qubits entanglement.

One can also consider different setup, this time consisting of four qubits, A, B, C and D, initiated in the following state:

$$\begin{aligned}
\Psi_{ABCD} = \;& 1/2\sqrt{2}\,|0\rangle_A(|000\rangle_{BCD} + |011\rangle_{BCD} + |101\rangle_{BCD} + |110\rangle_{BCD})\\
+ \;& 1/2\sqrt{2}\,|1\rangle_A(|111\rangle_{BCD} + |100\rangle_{BCD} + |010\rangle_{BCD} + |001\rangle_{BCD}).
\end{aligned}$$

The measurement in this entangled four qubit state of the qubit A will lead to one of two possible 3-link chain states for qubits B, C and D. Next measurement on any of those three remaining qubits (for example qubit B) will choose appropriate entangled state for 2 remaining qubits, C and D. Final measurement of one of the C and D qubits set their states (all three measurements are considered in computational basis, similarly as all mentioned measurements in the present reference standard description). Iterating of such procedure for series of states Ψ_{ABCD} will result in 4 sequences, where 3 are independent, similarly as in the beginning of this section.

Hereinafter we would like to shortly summarize different possible approaches to entangled QRNG protocols and outline some basic differences in such possible protocols regarding topological configurations of utilized entanglement (for 2-qubits entangled protocol the situation is trivial, however in 3-qubits protocols it becomes more complex with different possible scenarios for GHZ , generalized Bell states and W entanglement types used for QRNG) - in order to highlight advantages of the proposed present reference standard. Before we proceed to the protocols summary, one should remind that 3-qubits GHZ state if measured for 1 qubit projects all remaining qubits to disentangled pure states, the 3-qubits generalized Bell state if measured for 1 qubit projects the remaining 2 to maximally entangled 2-qubits Bell states - correlated or anticorrelated based on the 1st qubit measurement outcome, and finally the 3-qubits W state after measurement of 1 qubit projects the remaining 2 to either unentangled correlated (the same) pure states or alternative to maximally entangled Bell state (depending on the outcome of the first qubit measurement). One should also remark that the 3-qubits GHZ and generalized Bell states will behave similarily if one

change the basis of the measurement to the maximally non-orthogonal basis (thus the GHZ state will behave like the generalized Bell state and conversingly).

The most simple case is the 2-qubits Bell state based QRNG. This basic protocol can be utilized towards proof of the true randomness but also generalized towards secret sharing (if Alice and Bob share entangled qubits), and be extended upon the generalized 3-qubits (or even n-qubits) Bell states, to make sure, that the choice whether the subsequent positions in coupled resulting bits strings are correlated or anticorrelated. The latter case of the extension of proposed entangled QRNG protocol towards secret sharing can be found linked to the original formulation of the GHZ based quantum secret sharing protocol, with the differences related to a problem of the basis changes necessity (while the GHZ state is measured without the basis change it then finds very convenient application towards multi-party topology in quantum key distribution). Finally there remains discussion of how would differ the entanglement based QRNG defined upon the 3-qubits W state along with the n-qubits generalization (the below analysis is to show that such an entanglement QRNG protocol based on the W state would fall substantially short of QRNG requirements and would not be suited for true randomness generation, illustrating that the symmetry of the generalized Bell states topologically different from the lack of W state symmetry plays a crucial role for QRNG). Let us then consider the following scenario: Alice, Bob and Charlie share each one a qubit from a 3-qubits W state: 1/sqrt3 (|100> + |010> + |001>). The first step would be for Alice to make a measuement of her qubit: with probability 1/3 she will get her qubit projected to state |1>, while the remaining qubits of Bob and Charlie will both collapse to states |0> - anticorrelated with Alice's result - yet with probability 2/3 Alice will measure |0>, thus projecting two remaining qubits of Bob and Charlie into fully mutually anticorrelated Bell state. The situation is thus the following, in each position of the classical bits sequences where Alice has 1's, Bob and Charlie will have 0's (note that Alice has 1's in 1/3 of the bits string positions, while the remaining 2/3 of the bits string is occupied by 1's). This immediately points to non-uniform distribution of bits in the Alice's string due to lack of binary symmetry of the W state (the departure from the symmetry will only deepen with the increasing number of qubits, while it is clear that generalized n-qubits W states will recursively reduce to n-1 qubits W states upon subsequent measurements by the protocol parties). Similarily Bob and Charlie in their respective bits strings will have 1/3 of 0's (at the positions where Alice has 1's) as well as additional 1/3 of 0's and 1/3 of 1's (in n anticorrelated coupling between their both strings, after any of them first performs measurement on Bell states carried on qubits registers' positions where Alice projected her qubits to states of |0>). Therefore Bob and Charlies bits sequences will of course effectively contain nonuniform distribution of 2/3 bits in values of 0's and 1/3 of 1's. Due to this analysis it is evident that W state based QRNG is not valid upon the lack of symmetry and thus requires to discarding certain part of generated outcome thus significantly lowering its efficiency.

3. Entangled quantum random number generating devices

Generally the QRNGs are currently considered to be in the stage of industry adoption technology level (there are commercial companies already selling production QRNG devices, which hold one key advantage over RNGs based on classical in contrast to quantum physical effects, i.e. fundamentally non-deterministic randomness, which is impossible to predict due to quantum mechanical laws, no matter what technology used).

The presented above present reference standard for entanglement based quantum random number generator is based on multi-qubit entanglement properties. In 2016, an experimental setup for generation for the ten-photon polarization entanglement with use of BBO (beta-barium borate) crystals was presented, cf. Ref. , opening new area for the quantum engineering and potential extension of the proposed device implementation.

In view of the current development in quantum technologies, the requirements of presented schemes can already be technologically met and the herewithin proposed present reference standard can be implemented technically with the use of qubits carriers and quantum circuits employing Hadamard and Quantum Controlled Negation (CNOT) logical gates along with the quantum measurement interfaces.

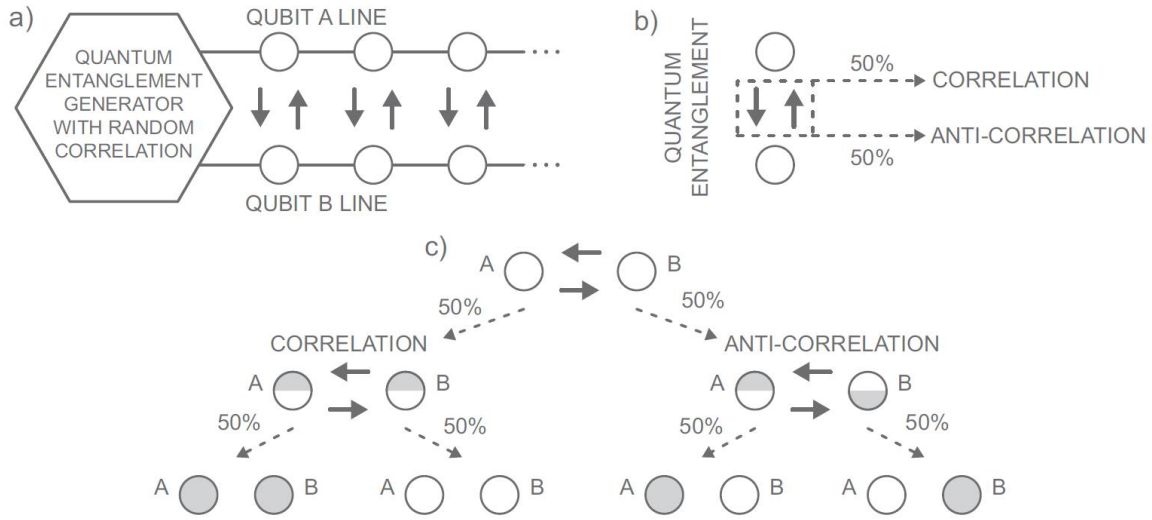

Fig. **4.** *Schematic elements of protocol for quantum random number generator with public proof of randomness: a) generation of random correlations; b) correlation types; c) possible measurement outcomes.*

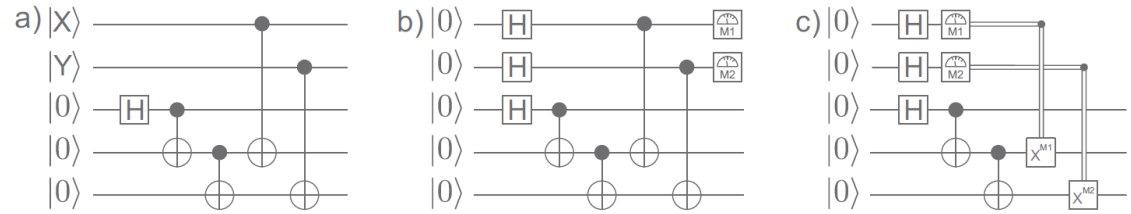

Fig. 5. Quantum circuit scheme with gates of a random correlation entanglement generator with 3-qubit entanglement state and two auxiliary qubits X and Y. The generalization of the protocol (increased security of the multiple consent) is attained with the random selection of 3-qubits entangled state type, which is omitted in case (a) and included in cases (b,c). Double line represents classical information about the measurement result.

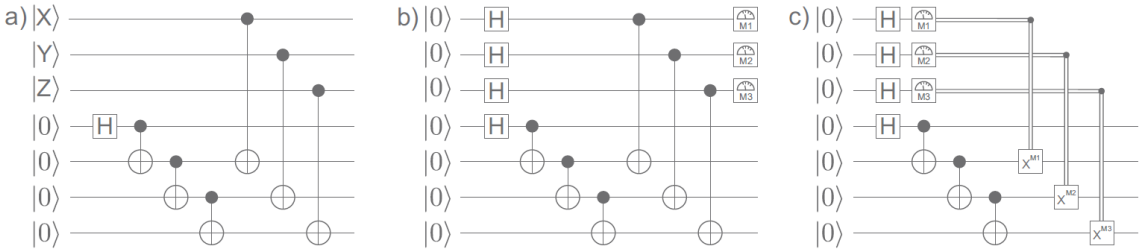

Fig. 6. Quantum gate scheme of a random correlation entanglement generator with 4-qubits entanglement state and three auxiliary qubits X, Y and Z. Without (a) and with (b,c) random

selection of 4-qubits entangled state type. Double line represents classical information about the measurement result.

The basic device component of the proposed present reference standard of Entanglement QRNG with public certification of randomness is the device implementing the originally proposed entanglement based random correlation generator. The implementation of this device (as a crucial component of the EQRNG) is presented upon its quantum circuits architecture in the Fig. *3.*

The generic device implementing the Entanglement QRNG with public randomness verification is built upon the quantum engineering components providing implementations of qubits and their control operations producing quantum entanglement. Those technologies are already matured and can be used as subcomponents of the system implementing the proposed present reference standard accordingly with the presented its schematic architecture (cf. Fig. *5.* for the extended device architecture presented in the quantum circuits specification).

The workflow of the device is presented on the diagram in the Fig. *4.*

The choice of particular implementation of given components upon realization of the quantum circuit architecture of the actual device are of less importance. The generic device can work on any regime of quantum information processing and control (with qubits implemented upon different degrees of freedom in physical systems of both light and matter). The recent progress is implemenation of qubits and their control operations including the required Hadamard and CNOT gates (for introducing multi-qubits entanglements) is summarized in publications .

The measurement setups for each single qubit in the above schemes can be implemented with use of one polarization beam-splitters and two single-photon detectors and the quantum gates for polarization encoded qubits are also widely available and rapidly developed, with currently ongoing implementations of integrated gates.

The discussed device is thus within the reach of practical implementation and its quantum circuit architecture is presented on the Fig. *3.* (entanglement based random correlation generator), Fig. *5.* (extended entanglement QRNG with public certification of randomness) and Fig. *6.* (its generalized version).

4. EQRNG device operative principles and industrial applicability

The range of applications of random numbers is vast, especially in the domain of information and communication security, to answer such needs as assisting in providing secrecy, authenticity and integrity of information processing and communication. In this special domain of randomness utilization also the privacy of generated random number plays fundamental role for security related issues of informaiton processing and communication.

On the plane of possible applications the proposed novel QRNG protocols, i.e. quantum random number generator with publicly verifiable randomness, with their discussed generalizations is thus of high significance for cryptography and secure communications (including also problems of authentication), as they introduce new important properties. The main advantage in contrast to standard QRNG protocol is that all previously considered schemes did not offer any mean of public verification of true randomness. This is very critical issue in terms of applications as potential users of QRNGs must rely on trust assumption, not being able to offer verification of the very randomness used without revealing it. The originally proposed here QRNG protocol and its generic implementing device will hence enable objective verification of the true randomness of the used bit sequence, without disposing of its secrecy.

The new important properties of the proposed Entanglement QRNG with certified proof of randomness present reference standard described above find important applications in many areas of technology and science where randomness is needed. These unique properties are strongly linked with multiple qubits entangled states and their topological features, finding important applicability in the industry of information and communication security.

It could be added that the topology related nature of quantum entanglement is currently a hot topic of consideration relating the links between quantum mechanics and relativity, being revisited in the efforts of the Grand Unification of physical theories . Understanding of how quantum entanglement manifests its non-local peculiar properties, or as Einstein called it, the spooky action over a distance, violating (empirically verified) the local realism assumptions of classical physics, is certainly not yet achieved. But in terms of recent progress topology (with links to direct topology of space-time) may be considered one of the most promising directions. In that regards employing the topological properties of non-trivial quantum entanglement configurations in industrial applications is important part of the effort to better understand complex quantum entanglement and harness its non-classical, non-local power. This as shown in the description of the present reference standard can to lead identification of important practical features, that can be then used as a basis for definition of new quantum information processing and communication applications, such as the demonstrated novel Entanglement QRNG protocol with the publicly verifiable randomness.

In view of industrial applications another important feature is also the property of the proposed generalized entanglement QRNG protocols (with four or more entangled qubits) to use shorter sequences of random bits verified statistically to be truly random in order to information theoretically certify same randomness of longer sequences of bits remaining secret, which is a result of fundamental significance.

One should also add that the proposed Entanglement QRNG protocol with its main feature towards publicly verified absolute randomness not sacrificing it's secrecy, possible due to a secret correlation - anticorrelation relation on subsequent bits positions of both random bit sequences (one kept secret, and the other one revealed) establishes a connection with the device independent security concept in field of industrially applied quantum communication, first proposed in 1998-1999 for QKD . The device independent security QRNGs (or device independent quantum randomness) concept relates to the idea of abstracting two independent issues in quantum engineering, namely the theoretical model of a quantum system and it's practical implementation, which suffers shortcomings related to the overlap of two fundamentally different physical domains, i.e. quantum and classical ones (with the latter domain required to make practical use of quantum systems, i.e. to implement deterministicly a qubit model within a needed for the absolute randomness maximally symmetrical linear combination yielding a truly random result with exactly 1/2 probability within also by definition classically implemented quantum measurement). In a simple case of non-entanglement QRNG protocol the device independent true randomness is meant to provide for a combined post-processing on the QRNG generated bit sequence aimed at abstracting it's verifiable true randomness from the particularities of the quantum mechanical system and measurement implementation. In other words the theoretical model of such a non-entanglement QRNG can be defined as a symmetrical, maximally non-orthogonal state of a qubit 1/sqrt2|0> + 1/sqrt2|1> with a result of measurement being classical bit 0 or 1 each with the probability equal to exactly 1/2 according to the von Neumann quantum measurement postulate. This situation however in practical implementation can deviate from the model, by e.g. biassing the pure quantum state (changing the qubit superposition coefficients to slightly different then 1/sqrt2, but still following the norm condition for a quantum pure state) or even departing the pure state towards a mixed state (which indeed is a realistic scenario taking into account that it is impossible to ideally isolate the system from the external interaction, and therefore this systems will entangle with the degrees of freedom of the surroundings). For such realistic scenarios the device independence comes into action, with the idea to abstract the particularities of the quantum process involved (and its shortcommings) to a black-

box. Such a black-box if deemed to be in a perfect implementation of quantum engineering would indeed generate true random bit sequence. If it is non-entangled QRNG then the black-box is a single register of qubits, upon which subsequent measurements are performed and the output of the QRNG black-box yields the sequence of the classical bits. Device independence putting to abstract the terms of how exactly the quantum mechanic system had generated these classical bits only focuses on making sure upon statistical procedures that these bits are truly random (within post-processing of the generated classical bits sequence). Therefore a QRNG system combining both the quantum black-box and the system for post-processing of the generated classical bits (in most trivial case only verifying upon strongest classical measures the level of randomness of the generated bits sequence, that it is really random, thus by measuring entropies of the subsequent bits positions and the entropy of the subsequences as well as the whole sequence which includes finding of possible patterns, and testing the deviation from the statistical model with entropies on each bit being as little deviated from 1 as possible – which is usually achieved by employing the standardized tests of randomness issued by independent mathematitians or standards and certification organizations basing their standards on mathematics advancements. There are two main important problems of the black-box approach in the device independent quantum randomness generation, i.e. 1) a necessity to reveal the secrecy of the random bits sequence of its randomness is to be proven to external observers and 2) a possibility that the black-box is leaking the quantum information, that can be achieved by adversary entangling qubits in his disposal with the qubits used in QRNG black-box to generate randomness. Both situations can be resolved with the proposed protocol of entanglement QRNG, because if the black-box is operating on the maximally entangled Bell states for qubits (i.e. it operates on two registers of qubits mutually entangled in one of either correlated or anticorrelated perfect Bell state at each corresponding registers' position, rather than on a single qubits register), than 1) the randomness verification by the external parties within the post-processing of the one of the generated bits sequence (e.g. departing the black-box and being published) can be performed without the need to reveal the other sequence.

Also in view of related problems of the device independent security of QRNG is the adverse situation that the quantum black-box constituting QRNG core device can leak quantum information in form of entanglement (this is referred to as the side-channel). In our protocol this situation is fully eliminated by the theoretical construct of the protocol itself which requires quantum Bell states exchanged between the parties - such states are by the definition maximally entangled and therefore cannot share any entanglement with external quantum states due to algebraical tensor product properties in Hilbert spaces within the quantum mechanics foundations (thus effectively excluding any additional co-entangled qubits hypothetically under control by an adversary). Of course this is only idealistic (i.e. theoretical) protocol definition and practical implementations of it are doomed to fall shortcomming of this one assumption of pure Bell states, most importantly due to unavoidable decoherence interfering with both the spatial distribution of entangled quantum states as well as their temporal storing (a less relevant problem here in direct application). For space distribution of entanglement, decoherence can be overcome with the concept of the quantum repeater in a chain-like segmented linear or hierarchical quantum channel (based on the entanglement swapping protocol or more generally on quantum teleportation), while the temporal storing is of course associated with the quantum memories (the problem of temporal storing of entangled states – despite not being the key criteria for the proper implementation of the entanglement QRNG protocol, as the entangled subsyste

ms - individual qubits, can be measured on the fly right after being spatially distributed - or in view of the fact that generally the simplest quantum memory can be thought of a closed path spatial distribution quantum channel, especially for the qubits being photons, and thus the time vs space coherence is less divided – is however important, as quantum memories do play important role in quantum repeaters themselves). Even if the distribution of purely entangled qubits would not possible to be achieved in the protocol QRNG implementation (the first quantum repeater successful

implementation has been demonstrated in 2007 but is not perfect and still under development, e.g.), yet there exists procedures such as entanglement distillation (or entanglement purification, investigated both theoretically and experimentally) schemes that can be used to achieve the desired result of effectively sharing only pure Bell states (condition by required feasibility of quantum local operations), thus eliminating any possible quantum information leakage (that would must have been in the form of entanglement). Therefore the basic assumption of our entanglement QRNG protocol of the Bell states sharing (requiring noiseless quantum channel) is theoretically obtainable by the entanglement distillation satisfying this requirement and effectively providing the noiseless quantum channel for sharing of maximally entangled qubits (the entanglement distillation effectively transforms a number of arbitrarily (not purely) entangled states into smaller number of arbitrarily pure Bell pairs by quantum local operations and classical communication (LOCC) only, thus compensating decoherence of noisy quantum channels and transforming these channels into noiseless, yet with lower time rates of qubits exchange efficiencies and by the cost of the quantum information processing necessity.

It should be noted that apart from the above explained scenario for utilization of randomly selected either correlated or anti-correlated Bell states on subsequent qubits' register positions in the entanglement QRNG protocol for a proof of it's true randomness there exist also a simple extension of the proposed protocol, generalizing possible application to the cryptographic procedure known as secret splitting or secret sharing . The proposed entanglement QRNG protocol based upon opposite Bell states correlations is the most simple solution to the secret splitting problem, enabled if we assume, that the randomly correlated and anti-correlated Bell states are shared between Bob and Charlie, while Alice (and only her) knows exactly on which positions of the qubits' register Bob and Charlie share these either correlated or anti-correlated maximally entangled qubits. How to achieve this situation to guarantee that only Alice has this knowledge? It should be noted that in the original our proposition the selection of correlated or anti-correlated Bell states for the QRNG protocol is fully random and this information is not available to other parties. If we assume that this happens under control of Alice she can keep this knowledge a secret and then send her two registers of mutually maximally entangled qubits to Bob and Charlie without any other information. This secret of Alice is in either of the form of a random classical bit sequence (random secret) or in the form of some meaningful information (secret message) that she would want to define as a secret to be splitted between Bob and Charlie. After Alice distributes the correlated and anticorrelated qubits in known only to her positions between Bob and Charlie, both Bob and Charlie share entangled Bell pairs of qubits, but each of them has completely no information on which positions are occupied by respectively correlated or anti-correlated pairs. If either Bob and Charlie runs his QRNG procedure by measuring his corresponding qubits' register and obtains a truly random classical sequence of bits, his counter-party's entangled qubits' register is projected (upon the von Neuman quantum measurement) to states that will deterministicly unveil upon future measurement a classical bit sequence in this very special correlation and anti-correlation relation on given bits positions, known only to Alice but not to them. Let's assume that Bob had measured his qubits, and obtained a secret random bit sequence, then Charlie upon performing his measurement also obtains a truly random bit sequence, however specifically correlated to Bob's bits sequence. This very correlation / anti-correlation configuration of two truly random bit strings of Bob's and Charlie's is carrying the split (or shared) secret of Alice between Bob and Charlie. Due to a true randomness of the sequences of both Bob and Charlie, guaranteed by quantum mechanics laws and the symmetry of entangled Bell states, neither of them has any information about this correlation (Alice's secret) until they join and compare both their bits sequences, what will instantly reveal Alice's secret to them. The basic application scenario of such protocol is to secure e.g. critical control system (such as as nuclear weapons control as was a known practice on intercontinental ballistic missiles submarines with two physical keys for the captain and the first officer) or in a generalization of this scheme to n parties for more advanced cryptographic applications, such as some paradigms of virtual crypto-currencies.

Due to theoretically proofed randomness in Bob's and Charlie's QRNG generated bits sequences carrying together Alice's secret, it's impossible to gain any information on the secret from any possible and even technology independent attack performed by Bob or Charlie seperately on their sequences, which is in contrary to the original classical secret sharing protocol, conditioned computationally . The quantum secret sharing protocols discussed later do not discuss a simplest possible scenario as presented above. It should be emphasized also that the extension of the proposed correlation / anti-correlation entanglement QRNG protocol for secret sharing problem has symmetry property: it is fully symmetric between the 3 parties. Each party's sequence of bits is known only to this party and secret to all others. Each pair of the 3 parties can thus combine their 2 secrets and in instant obtain a secret of the remaining party, in contrary to other quantum secret sharing protocols. Our proposed extension of the entanglement QRNG protocol based on the generalized Bell states towards secret sharing can be also much more intuitively generalized to n parties than is a case with the previously proposed quantum secret sharing schemes.

One more interesting take on this kind of application of entanglement based QRNG defined upon correlated and anti-correlated Bell states towards secret sharing cryptographic problem is to further investigate the case in which Alice's secret is not a meaningful message, but rather a truly random bits string.

This idea can lead to another concept of application of the distributed entangled QRNG generator. In this case we can assume two QRNG devices each operating on a single quantum register, but being in entanglement with the register of qubits in it's coupled counterpart. There are 2 main cases possible. For the first case, let's assume that these two devices are operated only by Alice and Bob and that only Alice knows which positions on the qubits registers are fully correlated and which are fully anticorrelated Bell states (this means that Alice loads both QRNG devices with entanglement, and then hands Bob one of the devices). It doesn't matter which of the parties performs their measurements first, both of them will have perfectly random strings, but only Alice will know exactly how both classical bits strings are correlated and anti-correlated (thus she will essentially know the string of Bob, but Bob won't know Alice's string). If Alice is publicly trusted institution, she can publish her random bits string coupled to Bob's string but unknowingly how to all else and perform public post-processing of her revealed string, proving (in a most trivial form of the device independent security) that Bob's random string is indeed truly random (Alice won't reveal her information on the way how her bits were coupled to Bob's and thus Bob's sequence will remain secret, while proven to be truly quantumly random).

The first issue arising is how Alice can make sure that the selection of correlation vs. anticorrelation is truly random. The answer is she cannot unless she is using a perfect QRNG to this end. So the more generalized situation is in the 3-parties scenario. If there are Alice, Bob and Charlie, we can assume that all of them share generalized 3-qubits entangled Bell states (in engineering terms they share 3 QRNG devices each of them storing a register of qubits, and each qubit is in the one chosen state of the generalized 3-qubits Bell basis). This state is in the such linear superposition that upon it's measurement by Alice, she will instantly project the states of Bob's and Charlie's qubit with exactly 1/2 probability to either correlated or anti-correlated Bell state. It is important to mention that by doing this Alice will have also a truly random bits sequence on her own (not known to both Charlie and Bob and this stage, as well as to anyone else). This will now guarantee also that Bob and Charlie share truly random distribution of correlated and anticorrelated Bell states in their QRNG devices. Upon their measurement (by either party) Bob and Charlie will now both have truly random bits strings adequately correlated and anti-correlated (in a manner known by Alice but not by anyone else, including Bob and Charlie before their compare their strings). This scenario is thus the basis of the distributed randomness generation related to the simple solution of the shared secret (or split secret) cryptographic problem, because each pair (Alice-Bob, Bob-Charlie or Alice-Charlie) can now combine their bits sequence revealing the sequence of the third party. However this extension is also representing the distributed quantum randomness generation because now it is enough that Alice

(alone by herself, as a trusted institution) will publish the random string sequence and in this way she will prove that both random sequences used by Bob and Charlie are truly random (yet unknown to the public). This proof is of course conditioned by the ability to prove in the first place that all the 3 parties had their maximally entangled Bell states distributed to their respective devices, as well as in the previous paragraph to prove that the share Bell states are really Bell states, and this is the second important issue. As the most trivial solution to this second issue, it's possible that the involved parties (Alice, Bob, Charlie for the latter case or just Alice and Bob for the former) will measure and reveal e.g. 99

How Bob and Charlie will use their random sequences in the latter scenario is another question, but the best option they have in terms of security is that one of them discards their string completely and only the other one will use it (they can reiterate the whole procedure and discard their strings by turns, which will guarantee that in all sessions each of them will use a secret but publicly proven to be fully random bits sequence).

A critique of similarity to the above presented application in its extension towards secret sharing (or secret splitting) could be based upon the mentioned publication , which uses 3-qubits GHZ entangled states to solve the secret sharing cryptographic problem. In this original and non-trivially, however differently formulated approach to a secret sharing, based on a then novle theme of GHZ state (described shortly before) a measurement of one qubit of the GHZ entangled state is proposed to be carried out by both Alice and Bob in the maximally non-orthogonal basis |+>,|-> what only after measuring of the 2 qubits out of GHZ state's 3 qubits would project the remaining one qubit of Charlie into state |+> or |-> (the projection would yield |+> if Alice and Bob obtained same results, i.e. either |++> or |–> and |-> for the case of different Alice's and Bob's outcomes |+-> and |-+>). This subtle difference in the protocol is based upon changing the basis of the measurement to the |+>,|-> (along x and y axes in more detailed formulation of the protocol) in relation to the originally defined GHZ state in the standard basis |0>,|1>. This difference on the first glance can be considered non-relevant, however it should be noted that changing of the measurement basis, quietly introduces into the quantum protocol a very classical factor: i.e. a fundamental impossibility to classically implement a perfect change of the basis from originally defined |0>,|1> to the maximally non-orthogonal basis |+>,|-> – as it is a classical device rotation problem, it's resolution will be always fundamentally limited. This problem does not affect situation when the entangled state has been prepared in the standard basis |0>,|1> because this basis is not changed for the measurement.

It should be stressed that the proposed present reference standard has also a possible modification towards implementing a multi-party topology quantum key distribution (QKD), trivially evident when one considers a GHZ state shared between 3 parties (or generalized n-qubit GHZ state shared between n parties). Recent propositions discuss different related scenarios and associated protocols in detail, however it is important in the context of discussing our proposed entanglement QRNG protocol to mention the simplest construct of n-to-n topology QKD based upon GHZ 3-qubit state: i.e. to split a GHZ state between 3 parties (or a generalized GHZ state between n parties). If the 3 (n) parties share the perfect GHZ states (or generalized GHZ states in case of n parties) in the GHZ state of full corellation 1/sqrt2(|000>+|111>) (or it's n-qubit generalization) the obvious application will be generating of a shared by all parties, identical classical keys (or random bits sequences). Upon measuring by one of the parties own qubits (doesn't matter by which party) all the qubits shared by remaining parties will be projected to classical information fully correlated with the classical outcomes of the measuring party. This results in an instant sharing of the same classical and secret key between 3 (or n) parties in the protocol. This key is shared by all the parties but fully unknown to all external parties if assumption of sharing really perfect GHZ states holds.

5. EQRNG device reference standard summary

The present reference standard of the Entanglement Quantum Random Number Generator with public verification of randomness is based upon the originally proposed entanglement based random correlation generator, assuring that generated random sequences are randomly correlated and anti-correlated on corresponding positions: in the most basic configuration of the device its main feature is publicly verified absolute randomness not sacrificing it's secrecy, possible due to a secret correlation - anticorrelation relation on subsequent bits positions of both random bit sequences (one kept secret, and the other one revealed). The described present reference standard of the Entanglement Quantum Random Number Generator with public verification of randomness offers for the first time in history a technical solution to provide a publicly accessible proof of privately and secretely generated randomness without compromising its privacy and secrecy, thus allowing an external party to freely and publicly verify the randomness of the generated sequence without disclosing of its secrecy or distorting it in any way. This feature of QRNG is proposed for the first time in randomness generation technical field and has an important role for applications in both quantum and classical cryptography as specified in the description of the present reference standard.

The new important properties of the proposed Entanglement QRNG with certified proof of randomness present reference standard find applications in many areas of technology and science where randomness is needed. These unique properties are strongly linked with multiple qubits entangled states and their topological features. The have crucial applicability in the industry of information and communication security. The present reference standard uses non-trivial quantum entanglement configuration in industrial applications harnessing its non-classical and non-local power, which leads to identification of not achieved previously practical features of public verification of true randomness (certified randomness proof) without disposing of the secrecy of the very proven-random sequence. The main advantage in contrast to standard QRNG protocol is that all previously considered schemes did not offer any mean of public verification of true randomness keeping secrecy of the generated random number. This is very critical issue in terms of applications as potential users of QRNGs must rely on trust assumption, not being able to offer verification of the very randomness used without revealing it. The proposed present reference standard and its generic implementing device (shown in the Fig. *3.* with workflow diagram depicted in the Fig. *4.*) solve this issue by enabling objective verification of the true randomness of the bit sequence, without compromising its secrecy. The generalized extension of the reference standard device of Entanglement QRNG (as presented in Fig. *5.* and Fig. *6.*, with four or more entangled qubits) uses shorter sequences of random bits verified statistically to be truly random in order to information theoretically certify same randomness of longer sequences of bits remaining secret. This result has not been achieved before in the field of randomness generation and is of a fundamental significance for the described present reference standard. As the quantum random number generators are gaining in popularity, especially with regard to possibility of construction of a scalable quantum computer, a new present reference standard is proposed in this area based upon topological properties of quantum entanglement. The proposed Entanglement Quantum Random Number Generator (Entanglement QRNG) uses a certain multi-qubits entanglement of quantum states to produce randomness with public certification. The present reference standard describes both the protocol and its generic implementing device, involving the specific 3-qubits quantum entanglement of generalized Bell state type (topologically inequivalent to different types of entanglements and easily generalized to multiple-qubits as shown in the present reference standard description), characterized also in the topological terms, that enables private quantum random number generation with a publicly accessible proof of randomness, thus allowing an external party to freely and publicly verify the randomness of the generated sequence without disclosing of its secrecy or distorting it in any way (this feature of QRNG is proposed for the first time and has an important role for applications in both quantum and classical cryptography).

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.