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

Request for Comments

RFC-EITCI-QSG-EQRNG-THEORY-STD-VER-0.1

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

Authored by prof. dr. habil. Witold A. Jacak
Brussels, 25th October 2019
Version: 0.1

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 sequences of bits 0 and 1 constituting a logical framework of binary encoded information processing, e.g. in computation and communication 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 [1, 2] (after highly important theoretical debate starting from Einstein's Podolsky's and Rosen's objections in the 1935 [3] formulated as the famous EPR paradox) to violate classical limits imposed on such correlations (Bell inequalities [4, 5]).

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 [6], alternatively formulated as the concept of partial information [7] only present for quantum information, measuring the ammount of classical information to be communicated in extent in the super-dense coding protocol [8], 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 [9, 10]. Within the problematics of how to combat the decoherence, beyond the standard Shor's concept based quantum error correction codes [11], the advanced multi-particle entangled states are one of the possible options [12] 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 [13], recently there has been a lot of interest towards considering quantum information within the topological degrees of freedom [14-16], 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* [OTP] 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 [nsaR, nsaN] 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 [rngat1, rngat2, rngat3].

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 [twove], significantly exceeding the computational power of classic devices, e.g. with acceleration of the order with Monte Carlo optimizations [googledwave]) 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. aattack *bruteforce* on SSH protected by RSA keys) [at1, t2].
- 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) [ps3]
- 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 [rsakeyat1]
- 2013 - after Snowden disclosed these deficiencies to the US National Security Agency (NSA), Reuters [nsaR] together with NewYorkTimes [nsaN] 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* [intelHRNG]. 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 [euNSA] 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 [android1, android2].
- 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 [mtgox]
- Year 2015 - Difficult to detect remote attack using externally connected hardware Trojan horse on TRNG based on FPGA [johnson2015]
- 2015 - theft of 18866 bitcoins from the Bitstamp exchange (12% of the currency being traded on this exchange) - RNG attack signature number [Bitstamp]
- 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) [DUHK]

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 from application perspectives

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 [qrngdiv]:

- 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 [bellineq]. These devices are also referred to as quantum random number generators independent of implementation (device independent QRNG) [diqrng]. 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.