I. J. Mathematical Sciences and Computing, **2021, 3, 41-53**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2021.03.05

Novel Quantum Random Number Generator with the Improved Certification Method

Maksim Iavich
Caucasus University/CST/Tbilisi, Georgia, 0102
E-mail: miavich@cu.edu.ge

Tamari Kuchukhidze
Georgian Technical University, Georgia, Tbilisi, 0160
E-mail: tamari.kuchukhidze@gmail.com

Giorgi Iashvili
Caucasus University/CST/Tbilisi, Georgia, 0102
giiashvili@cu.edu.ge,

Sergiy Gnatyuk
National aviation univercity, Kyiv, Ukraine, 03058
E-mail: s.gnatyuk@nau.edu.ua

Razvan Bocu
Transilvania University of Brasov, Romania, Brasov, 500036
Email: razvan.bocu@unitbv.ro

Received: 16 April 2021; Accepted: 30 May 2021; Published: 08 August 2021

Abstract: Random numbers play an important role in many areas, for example, encryption, cryptography, static analysis, simulations. It is also a fundamental resource in science and engineering. There are algorithmically generated numbers that are similar to random distributions, but are not actually random, called pseudo random number generators. In many cases the tasks to be solved are based on the unpredictability of random numbers, which cannot be guaranteed in the case of pseudo random number generators, true randomness is required. In such situations, we use real random number generators whose source of randomness is unpredictable random events.

Quantum Random Number Generators (QRNGs) generate real random numbers based on the inherent randomness of quantum measurements. Our goal is to generate fast random numbers at a lower cost. At the same time, a high level of randomness is essential.

Through quantum mechanics, we can obtain true numbers using the unpredictable behavior of a photon, which is the basis of many modern cryptographic protocols. It is essential to trust cryptographic random number generators to generate only true random numbers. This is why certification methods are needed which will check both the operation of the device and the quality of the random bits generated.

We present the improved novel quantum random number generator, which is based the on time of arrival QRNG. It uses the simple version of the detectors with few requirements. The novel QRNG produces more than one random bit per each photon detection. It is rather efficient and has a high level of randomness.

Self-testing as well as device independent quantum random number generation methods are analyzed. The advantages and disadvantages of both methods are identified. The model of a novel semi self-testing certification method for quantum random number generators (QRNG) is offered in the paper. This method combines different types of certification approaches and is rather secure and efficient. Finally, the novel certification method is integrated into the model of the new quantum random number generator. The paper analyzes its security and efficiency.

Index Terms: Quantum, quantum cryptography, random number generator, quantum random number generator, novel quantum random number generator, certification, novel certification method.

1. Introduction

Random numbers are widely used in various fields, for example, simulation, encryption, cryptography cryptography, fundamental science [1,2]. Algorithmically generated numbers look like random numbers but are not truly random; they are called pseudo random numbers. These numbers are generated by computer algorithms, which use mathematical formulas to generate random number sequences, which are called pseudo random number generators [3-5]. Because, we cannot use pseudo random generators in situations, where true randomness is necessary, we use true random number generators. In this case, we use unpredictable random events as a random source. In situations where it is possible to use pseudo randomness a pseudo random number generator, a deterministic method which mimics the expected behavior of a truly random source, is often used due to the large speed advantage. [6].

In some applications, such as quantum cryptography, not all true random number generators are cryptographically secured, the unpredictability of random numbers generally cannot be guaranteed in classical processes. We single out a specific QRNG of the TRNG that uses innate randomness in quantum processes as a random source.

Nowadays, quantum optics is used in the majority of quantum random numbers generators. Photon sources such as laser light, light-emitting diode, and other resources are less expensive and more common than radioactive material. Many light quantum state parameters have inherent randomness, which allows us to implement many variants. Many detectors have access to light particles, which are exploited as a resource of quantum randomness. As a result, optical quantum random generators are faster and more efficient [7].

Cryptographic random number generators have a trust problem. Users must fully trust the algorithms of pseudo random number generators or the device that implements the method of generating truly random numbers. Creating new random number generators from scratch is undesirable when there are many reliable algorithms and devices that have endured years of cryptanalysis and attack attempts, proven to be sturdy. This means that the user must trust at some point the device or algorithm. A problem that may seem simple may not be so easy to fix. Random number generators, for example, are an appealing prospect for covert attacks. PRNG algorithm DUAL_EC_DBRG, suggested as a NIST standard, allows an attacker to retrieve an entire random sequence with minimal information, with practical consequences during a Juniper network attack [8-10]. We have examples in the event of a device-level attack on how a dishonest manufacturer or any attacker was able to cause errors when accessing the device. In such a technically advanced attack, an attacker could make mistakes that are difficult to detect in real world RNGs.

There are also problems with physical random number generators such as possible spontaneous termination. If a device component stops working or degrades, it may cause the output bits to change in quality. Also, if the device creates values, it is especially difficult to detect hidden flaws in the device. As a result, for any type of self-testing in real QRNGs, safety guidelines are required. To avoid missing any faults, the sub-system should continuously check the device's condition.

The goal is to generate fast random numbers at rather lower cost. A high level of randomness is obligatory. We offer the model of the improved novel quantum random number generator, which is based on the time of arrival QRNG. This QRNG is very efficient, because it uses the simple version of the detectors with rather few requirements. The offered OQRNG produces more than one random bit per each photon detection.

We review quantum ways to work with unreliable devices. The first method uses the properties of some quantum event to observe the quality of the bits produced. Second, it gathers propositions known as device independent quantum random number generators, which are founded on the idea that quantum correlations give statistical independence unless trustworthy physical laws are flawed. The third technique refers to quantum certification approaches that are based on device independent generators but employ less rigorous experimental evaluations of different parts of quantum theory, resulting in more restricted certification and more relaxed safety assumptions [11]. We combine different types of certification methods, practical, device independent quantum random number generators and self-testing QRNG. We get a semi self-testing generator. It is rather secure and efficient. The paper analyzes its security and efficiency.

2. Literature Review

The authors of paper [2] are working on the creation of quantum computers, which can easily solve the problem of factoring large numbers and they are able to crack the crypto RSA system. In [3-5], several pseudo random number generators are considered, that use a different methods to ensure the randomness of the sequences and higher level of security. Based on the digitized time interval between random photon arrivals, paper [6] suggests, fast, more efficient, secure optical quantum random generators. Random numbers are widely used in different applications, the paper [7] presents the various quantum random number generating technologies and the multiple ways to use them to collect entropy from a quantum basis.

In [8-10] several self-test and device independent QRNG are described. The pros and cons of different types of certification are discussed. The papers also describe different quantum random generators. The authors analyze their security and efficiency. Paper [11] describes the measurement of quantum randomness.

The authors of paper [12] describe a fundamentally different approach using the trit generation method and software tool TriGen v.2.0 PRNG, which has significant advantages over traditional cryptography methods. In [13-14], the authors present a study of high-speed and secure pseudo random number (PRN) generation techniques. In the article [15], it is offered to use hash based pseudo random number generator and Merkle signature scheme are proposed. Additionally, paper [16] introduces the first provable-security analysis of the Intel Secure Key hardware RNG.

The authors divide QRNG-s into different groups. The authors of paper [17] are working on general design of self-testing optical quantum random number generator and the ways to implement it as a compact integrated photonic circuit. The paper [18] presents self-testing quantum random number generation, in which the user can monitor the entropy in real-time, protocol that guarantees the continuous generation of high quality randomness, without the need for a detailed characterization of the devices. Based on generating nonlinear dimension witnesses for systems of arbitrary dimension paper [19] presents a simple method, where witnesses are highly robust to technical imperfections and can certify the use of qubits in the presence of arbitrary noise and arbitrarily low detection efficiency. By repeating the measurements of a quantum system and by swapping between two mutually unbiased bases, a lower bound of the achievable true randomness can be evaluated. This efficient method is proposed in [20] to extract true randomness.

Randomness generation is possible in quantum systems only if certified by a Bell inequality violation typically used on device independent QRNG, which is proposed in [21].

Different protocol for device independent QRNG is introduced in [22]. In addition, paper [23] introduces Kochen-Specker theorem, which can be used in additional experimental testing of quantum theory's fundamental properties.

Different protocols are introduced in [24-26] to secure quantum channels to ensure confidentiality and security.

3. Optical Quantum Random Number Generators

Randomness is the basis for cryptography. The vast majority of PRNGs are incapable of generating cryptographically secure random numbers [12-14]. If we have sufficient output values, we can infer the internal state of Mersenne Twister, for example. Pseudorandom number generators may, however, be used in cryptography in well-established methods. CSPRNGs are cryptographically secure pseudo random generators (algorithmic generators that fulfil extra conditions).

Creating cryptographically secured random number generators is not easy. Physical RNGs, including QRNGs, can be used as seeds for CSPRNGs [15-16]. But we must take precautions. Some attacks are specifically targeted at TRNGs and are sensitive to variables derived from environmental conditions. True randomness can only be obtained through processes that have innate randomness. Such source is a quantum random number generator.

True randomness can be generated from any quantum process that breaks coherent superposition of states. Nowadays, high-quality optical components are available, so most practical QRNGs are implemented in photosystems.

At the quantum level, the optical field can be described by photons. Fock and coherent states are the most suitable descriptions of light quantum states in random number generators, out of many other quantum state variations. The Fock condition, often known as the numerical condition, is an |n> in which n photons have the same mode (have the same frequency, polarization, transition profile, and common path). Many aspects of classical light have a coherence condition, which may be expressed as a superposition of numerical states

$$|\alpha >= \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n> \tag{1}$$

Where α is a complex number and n is the number of photons. The average number of photons in the state is represented by the amplitude $|\alpha|^2$. The weak laser's light is very near to being coherent. If we pick a sufficiently low intensity, we may utilize a coherent state from a laser to obtain the state of one photon.

In numerous cases, all we care about is producing unconnected photons. Many different technologies can generate and detect single photons, such as photomultiplier tubes (PMTs), single photon avalanche photodiodes (SPADs), superconducting nanowire detectors. These are examples of popular detectors.

Traditionally, single photon detectors have limited ability to count photons. We can also generate randomness from quantum states containing multiple photons. There are improved detectors, but they have a high cost. Most apps take a binary approach to detect photons. The time needed to retrieve after photon detection, which is known as dead time, is the next limitation for single-photon detectors.

4. Time of Arrival Quantum Random Number Generators

Many methods can be used to generate random bits from photon detection times. In most cases, QRNGs that use time have a photon source that isn't very powerful, and a detector and timed schemes that record either the precise time of each discovery or the amount of time it takes to click. Within a short period of time, for an average we have one or few photons. The detector receives photons from LED incoherent. The consistent state from the laser goes to the detector at an exponentially distributed time, photons per second on average. The difference between two exponential random variables, which is likewise exponential, is the time between two photodetections. We can examine t_0 and t_1 in terms of time. Assign 1 if $t_1> t_0$ and 0 if $t_0> t_1$. This gives us a uniform random bit.

In time of arrival generators, the accurate time is the most important. Measurements will always be limited and these differences are noticeable when digitizing time intervals. Instead of real-time t_0 and t_1, we can use integers n_1 and n_2, which are counted clock periods. It is necessary to consider the likelihood $t_0=t_1$, which has a minimal chance of measuring an ideal continuous time. We have two sequences that follow each other, where the same time is read, $n_0 = n_1$. In a basic scheme that generates 0 or 1. The value depends on whether the second interval is shorter than the first, if not, the output value is not defined and we must exclude these results. If we consider an equation as a valid result, it requires analysis of each output value and assigning a binary bit.

Among the first time-detection generators, QRNGs utilize photons from an LED entering at a PMT and compares the arrival times on the chart, which is similar to comparing the arrival times of two particles in a Geiger counter. The clock's random arrival time can be applied as a signal to choose time bins. We can use a variation of the even-odd generation method. If a photon is discovered in an even clock cycle, assign 1 and 0 if it is discovered in an odd clock cycle. An interesting alternative is where time bins are grouped into pairs. We can assign the output value 0 to the empty bin when no discovery is made and 1 if the empty bin is followed by the discovery. It is essentially the same as utilizing the time bins where we discovered the photon and discarding some consistent counts.

There are many ways we can generate random numbers using time measurements. The time difference t_i is a real number andand, we can withhold an infinite number of entropies from only two impulses. However, all of the extracted bits are not usable. If our time data does have an accuracy *b* bit, a random variable $N = 2^b$ is the time bin, when we can find the photon. Then we may compute the likelihood of a photon going into every bin. Some optical quantum random number generators divide available entropy into random bits strings using a mathematical formula and digital time differences for n bits. All of these processed algorithms attempt to transform the exponential distribution into equal bit sequences, requiring additional equipment and effort to process.

There are ways to generate photons that will give us a more uniform arrival time. We can use counting statistics. We have a non - homogeneous Poisson distribution for an irregular flow laser diode, and we can alter the standby period. $\psi(t)$ is the distribution of arrival time for a continuous photon flow

$$\psi(t)e^{-\int_x^y \lambda(t')dt\prime} \tag{2}$$

The ideal is rectangular distribution, which can be achieved by utilizing a laser beam that periodically repeats the function's final approach.

$$\frac{1}{R-t} \tag{3}$$

Where R is the source's restart variable, which controls when the pulse cycle is received. When R is finished or a pulse is recorded, the current returns to its original value (which will occur firstly).

5. Photon Counting Quantum Random Number Generators

There is one group of generators that use time measurements. In this case, we need the number of fixed time detections T to generate random numbers. The amount of photons that go in a constant T time follows the Poisson distribution for a random time exponential element. With this formula, we can find the probability of finding *n* photons at this interval

$$Pr(n) = \frac{(\psi T)^n}{n!}\mathrm{e}^{-\psi\mathrm{T}} \tag{4}$$

For example, the generator F ̈urst et al produces bits equal to the total amount of counts, registered in the fixed period. LED is a light source, used for the rapid detection of PMTs. In this case, the generator uses the dead time of the detector. The random variable of the parity method, estimates the number of photocounts, has a small bias if we compare it to a pure Poisson process.

Some generators use a similar approach, discussed in the previous section, to compare time differences. If as a result of the first observation we get n_0 number of photons, and as a result of the second measurement n_1, we can generate 1 when $n_0> n_1$ and 0 if $n_0 <n_1$. Using the methods, we generate one bit for one measurement. But, given ψT, measurements could have a larger entropy. There are methods to get the most out of the data supplied. Depending on the quantity of photons observed, some generators give a few bits. The possible outcomes are separated into groups with an equal chance of occurring. For this, it is necessary to manage all sources.

The frequency of ψT photons in the T period depends on whether the second, third, or other counted least significant bits of photon will be equal. A generator with an integrated CMOS SPAD array of detectors takes light from an LED and creates random numbers in parallel in a 32x32 detection matrix. This is how the MPD generator works. It is critical to appropriately quantify the dead time in this strategy since it impacts the speed of the detector ψ_{dc} counter. Improved rate

$$\psi_{dc} = \frac{\psi}{1+\psi\frac{\psi_{dt}}{T}} \tag{5}$$

allows us to choose how many bits to utilize from the total amount of photons measured.

6. Attenuated Pulse Quantum Random Number Generators

In some cases, it is not necessary for the generator to meet all requirements and it is possible to get the desired result with fewer requirements for detectors. It is sufficient to use simplified versions of the methods already discussed. In such cases, we use Attenuated Pulse Quantum Random Number Generators. Most existing single photon detectors can only count a certain amount of photons. The following reaction is given to clicking (photon detection) or not clicking: one is allocated 1 and the other is assigned 0. Methods for counting photons are usually based on many clicks over a long period of time, which is divided by the detector into smaller time periods.

OQRNG is called an attenuated pulse generator if it has a weak source of light and the probability of photon generation and not generation is the same. Positioning of an empty and one photon state in the same spatio-temporal model, so that the single photon's state is preserved

$$\frac{|0>_1+|1>_1}{\sqrt{2}} \tag{6}$$

If no detection occurs, we can apply a value of 0; if a click occurs, we can assign a value of 1. We do not care how many photons are used. Any superposition can be written as following:

$$\frac{1}{\sqrt{2}}|0>_1+\sum_{c=1}^{\infty}\alpha_c\,|c>_1 \tag{7}$$

where $\sum_{c-1}^{\infty}|\alpha_c|^2 = \frac{1}{2}$ is valid. We can only take it from the first click and it doesn't matter if it is caused by one photon or many.

Given the coherent state, it is easy to form such superpowers. The chance of discovering a photon in a coherent mode with amplitude is 0

$$pr(n=0) = e^{-|\alpha|^2} \tag{8}$$

probability of finding one or more photons

$$pr(n \geq 1) = (1 - e^{-|\alpha|^2}) \tag{9}$$

The most basic concept is to determine α whatever for pr(n = 0) = pr (n ≥ 1), that is equal in this formula $\alpha = \sqrt{ln2}$. The probability of the desired discovery is given by the Poissonian source, where ψT = ln2 ≈ 0.693.

In practice, the generator operates on a detector with an effective average photon number ηψT, where the efficiency is η. OQRNG can be managed by adjusting variables. The generator can also operate as a light source. OQRNG can manage the LED flow to achieve the desired balance, which will give us a 50% chance of detection.

However, even after the adjustment, the bias may remain. To solve this problem, Wei and Guo generator uses von Neumann extraction. For two detections, where photon number is n_0 and n_1, the output value is 1, if n_0> 0 and n_1 = 0 and 0 if n_0 = 0 and n_1> 1. If two consecutive blank periods or clicks are generated, the findings are ignored. These values are basically comparable for the Poisson source, with $pr(n>0)pr(n=0) = e^{-\eta\psi T}(1-e^{-\eta\psi T})$. The bit rate is at least 4 times slower as a result, yet it is completely bias-free.

7. Self-testing Quantum Random Number Generators

The random source of the majority of quantum random number generators is not fully described. When a photon passes through a beam splitter, for example, complications can arise: detector inefficiency, imbalance in the splitting process, source imperfection, and multiple unknown sources of correlation. Theoretically, detectors can generate an ideal random bit because a photon has a 50% probability that the beam will split and a 50% probability that the beam will reflect. This happens only in theory, because in practice, there are always problems with detectors, lasers, beam splitters, and their characteristics depend to some extent on environmental conditions as well. As a result, many approaches for determining the quality of random numbers generated by physical random number generators have emerged. The ways of self-testing that are directly tied to the random number generator's quantum features. Testing can be done in a variety of ways depending on the device, but typically random use of the program afterwards and processing is done to correct the uneven distribution of probability [17].

As a result, numerous approaches for evaluating the quality of random numbers generated by physical random number generators have arisen. Quantum random number generators aren't the only ones who can benefit from this. In the case of classics, there are various ways to verify the data obtained, such as the NIST and Diehard random tests.

A QRNG can be created so that its output randomness does not rely on any physical implementations. True randomness can be generated through self-testing even without perfectly characterising the realisation instruments. The structure of a self-testing QRNG is based on device-independently witnessing quantum entanglement or non-locality by observing a violation of the Bell inequality. Even if the output randomness is mixed with uncharacterised classical noise, we can still get a lower bound on the amount of genuine randomness based on the amount of non-locality observed. The advantage of this type of QRNG is the self-testing property of the randomness. However, its production rate is usually very low, as the self-testing QRNG must demonstrate non-locality.

We can distinguish self-testing methods that can work with both classical noise and quantum sources of entropy. For instance, (Saito et al., 2010) describe a self-testing scheme that compares random pulses on time of arrival. The pulse can be obtained from both thermal noise and radioactive decay received by the Geiger counter. We then check the obtained distribution to see if Poisson's arrival time is expected. We convert such random numbers into output values that successfully pass the tests. Through this process, we filter out obvious irregularities.

Of course, the attacker might still change the outcome and construct a predictable sequence that passes the test, but these self-testing systems may detect spontaneous disturbances as well as less complex attacks. These systems provide good additional protection. Tests can also detect operation errors.

Testing is an important component to get good quality random numbers, so it must be done carefully. To obtain random numbers, it is necessary to accurately estimate the entropy, which is a complicated procedure. If the system that evaluates the existing entropy is poorly implemented, it may be vulnerable to attacks.

The first example of a self-testing in a quantum environment is an optical quantum random number generator, designed to work for quantum random number generator that uses the path branching principle. For the position of the single-photon polarization superposition

$$\psi = \frac{|H>+|V>}{\sqrt{2}} \tag{10}$$

Or in an entangled state

$$\psi = \frac{|H>_1|V>_2+|V>_1|H>_2}{\sqrt{2}} \tag{11}$$

|H> and |V> indicate the state of a single vertically or horizontally polarized photon. Polarizers let photon pass through with 50% probability. In theory, coincidence counter in this case registers perfect anti-correlation. Perpendicular orientation of polarizing axes gives 100% correlated photon detections. This happens only in theory, because in practice, there are always problems with detectors, lasers, beam splitters, and their characteristics depend to some extent on environmental conditions as well. Quantum correlations disappear if relative angle has been chosen to be 45 degrees.

A complete tomography of the input state is performed from a set of data to determine a 2x2 matrix in the device's testing phase. A two-level photon system is efficient for a single photon, but a two-dimensional Hilbert space is efficient for a photon pair. Based on the measurement results, the generator determines $H_\infty(\widehat{pr})$, which is the minimum possible entropy for the overall condition of the user and listener, and $\widehat{pr}$ is the worst of all possible cases. The bits are then transferred to a random extractor, which generates a shorter, unbiased random string for available entropy.

This strategy defends us against attacks in which the opponent has influence over the quantum state from which we derive entropy. We are protected from cases where we make repeated measurements on one state. To perform conditional tomography correctly, we must assume that the measured condition is maintained throughout the process. Although such self-testing provides minimal protection, it is an excellent approach to detect inadvertent device faults.

When faults are foreseen during implementation or abnormalities may arise during operation, tomography gives a realistic estimate of the entropy of such models. We imply that errors do not occur due to an unreliable manufacturer. Using dimension witness, a quantum source of randomness can be isolated from technical noise.

$$WT = \begin{vmatrix} pr(1|0,0) - pr(1|1,0) & pr(1|2,0) - pr(1|3,0) \\ pr(1|0,1) - pr(1|1,1) & pr(1|2,1) - pr(1|3,1) \end{vmatrix} \tag{12}$$

The self-testing quantum random number generator protocol consists of these steps. First, an experiment is carried out in which the user selects a prepared state s and a measurement m, after which an outcome o is collected. Following that, we can calculate the distribution pr(o | s, m) from the input and estimate the value of the witness WT, from which we can measure the entropy of the raw data. In order to obtain the final random bit string, sufficient post processing of the raw data is performed based on the entropy bound [18, 19].

pr (o | s, m) gives the conditional probability of finding the result of o (from ± 1) for a condition that is one of the defined probabilities s = 0, 1, 2, 3. The measurement parameter m might be either 0 or 1. The four states in the generator under examination correspond to the circular right and left polarization, as well as the diagonal and anti-diagonal polarization, of the second photon from the entangled pair, as measured by diagonal or circular polarization. The initial photon serves as a message for the rest of the photons.

WT refers to the extent to which preparation and calculations are integrated. Any WT larger than zero implies that some of the measurements are incompatible and that quantum randomness exists, allowing a predictable probability to be attributed. The result may be used to compute the compression rate in a random extractor. The input bits yield a modest amount of pure random bits for modest quantities of WT. A practical test of this technology revealed a final bit rate of tens of bits per second and also responded correctly to changes in the environment, such as turning off the air cooling in the laboratory.

An alternative approach is to apply the principle of uncertainty. This principle allows any opponent to access a limited amount of information. Not only do we want to produce random bits, but we also want to make sure they're secure. For example, if we use formula (11) we get absolutely random numbers, but the opponent can learn the exact sequence because he has access to the second half of the bits. Our sequence can be obtained from the same measurements because the bits are just uniform and are not confidential.This may be acceptable for applications such as simulation, but any information leakage in cryptography should be avoided. By switching two mutually unbiased bases, we may utilize the certification technique to maintain secrecy without using full tomography. Two bases are adequate instead of a complete tomographic measurement [20].

8. Device Independent Quantum Random Number Generators

We may also disregard the complexities behind the quantum random number generator and just look at the output. Especially if we wish to show that the outputs are unintentional or that some physical law is being broken. This is the random number certification's second method. This is especially true when the researchers try to show that outputs must be accidental or regulations will be breached. In the context of quantum key distribution, this is a basic device independent quantum information processing model.

During random number creation, we assume the worst-case situation, in which an adversary can use a quantum random number generator to generate genuine random numbers, which are then hidden inside a controlled device. The output may not be truly random if the devices are tampered with by opponents. The output of the QRNG device can be predicted by the maker. Because the opponent can generate true random numbers, we can trust the outcomes if we check the device's output values. Although avoiding this issue is tough, there is a quantum solution. As a result, using a device-independent certification mechanism is critical.

Device-independent quantum random number generators tackle the problem of device trustworthiness by relying on systems based on Bell tests to trust the device. The principles behind Bell's violation come from a study of quantum theory and the Einstein-Podolsky-Rosen paradox, which is an apparent conflict in relativity. The measurement of one particle in the entangled state indicates the condition of the other particle as well. This appears to be in violation of the no-signal principle, preventing quicker transmission than light. Resistance can be addressed experimentally, as John Bell demonstrated.

The Clauser-Horne-Shimony-Holt (CHSH) configuration of Bell inequalities was chosen for the functional quantum random number generator. Measurements of two devices we will look at estimation of correlations and create two variables for each module, s and m. These variables may have two values: 0 and 1, which correspond to binary measurement values. Both measurement instruments are the same. In the s configuration, the measurements give a binary value of a and the measurement defined by m gives the result b. We are particularly interested in the correlation function, which is defined as follows:

$$I = \sum_{s,m} (-1)^{s,m} [\Pr(a = b \mid sm) - \Pr(a \neq b \mid sm)] \tag{13}$$

When s and m are parameters, Pr (a = b | sm) and Pr (a ≠ b | sm) are the probabilities of a = b or a ≠ b. I ⩽ 2 must be found, since any value greater than 2 implies nonlocality. To evaluate bell's inequality, this experiment must be performed n times. The choice of each (s, m) measurement is defined by a probability distribution that is identical and independent of Pr(sm). The final output string of n is r = (a_1, b_1;...; a_n, b_n), and the input s = (s_1, m_1;...; s_n, m_n). $\tilde{I}$ is the estimator of CHSH formula (13), which is defined as follows

$$\tilde{I} = \frac{1}{n} \sum_{s,m} (-1)^{s,m} [N(a = b \mid sm) - N(a \neq b \mid sm)/\Pr(sm)] \tag{14}$$

Where N (a = b, sm) is a number, how many times (s, m) have been measured. Results a and b were found to be equal to n after realization. N (a≠B, sm) is defined similarly [21].

After a sequence of observations, this correlation function may be determined by estimating probabilities. The principles of quantum physics apply as long as the systems remain distinct and do not interact. We can generate s_i and m_i through independent random processes at any stage of operation. The evaluation of I, $\tilde{I}$, after some work gives us the lower limit of the minimum entropy of the results

The limitation is zero and the system can be deterministic if the system has a classical description, $\tilde{I} \leq 2$. When we perform measurements on states that have any interaction, the random bits that are created are guaranteed to be random. The resultant bit sequence is not definitely equally random, but it is constrained by its minimal entropy, which implies it can be transformed to a randomly uniform string using the right randomness extractor.

Consider quantum devices that have spacelike separate parts. There are no extra limits on devices or input states until $\tilde{I}$> 2 if they have access to independent random sources. The only other condition is that the chosen measurement parameters s_i and m_i contain some unpredictability at each stage of the technique and are not totally predictable.

In this regard, the random expansion scheme's generator is analogous to the quantum key distribution (QKD). Starting with a random seed, the protocol creates a bigger string of random output values whose unpredictability is validated using quantum mechanics. It's a quadratic procedure, to be precise. Generating certified random n bits requires an already existing $\sqrt{n}$ bit random sequence. To defend against quantum adversaries, the protocol generates strings of n random bits, starting with the $\log_2 3$ n bit-length seed, which allows exponential extension.

To minimize detection differences, QRNG was implemented with trapped ion qubits to eliminate detection gaps (Olmschenk et al., 2007). Ionic systems are slower to create than optical implementations, but they provide almost flawless results. Each atom generates an entangled photon, which is eventually used to capture ions by interfering with the photons. This is a heralded process. Experimental violation of Bell's inequality is a precarious task, and the generation process is very slow, giving us only 42 certified random bits, but with a good, 99% confidence level, throughout the course of nearly a month of nonstop running.

Some of the rules have lately been loosening, allowing for optical frameworks and faster generation times. Despite the poor profitability of most optical detectors, transition-edge-sensor detectors provide adequate efficiency advantages to close gaps in some types of Bell's inequality. It can also generate verified quantum random numbers at a rate of roughly 1/2 bit per second.

DIQRNG can be developed as a more general model where the principles of quantum mechanics may not be true. An example of this is the device independent quantum key distribution protocols (Barrett et al., 2012, 2005), which only require maintenance of the no-signaling principle. This principle prohibits the transmission of information faster than the speed of light. A communication device faster than the speed of light will allow it to send messages to the past and create a conflict with causality (Tolman, 1917), reflecting the grandfather paradox. The no-signaling principle is definite. In entangled states, as long as there is non-localization and there are correlations that appear to move faster than the speed of light, it is virtually impossible to use them to send information (Bussey, 1982; Dieks, 1982; Jordan, 1983).

The limit in device independent quantum random number generators (Pironio et al., 2010) and (Vazirani and Vidick, 2011) is also a no-signalling constraint. The precise limit depends on the conditional minimum entropy, but the fundamental principles remain the same. The techniques still operate as random amplification techniques in the new model, which need uniform random seeding [22].

Every one of the mentioned device independent random number generators, both quantum and non-signal, are really implementations of protocols that enhance randomness using the findings of physical investigations. They start with a small number of random seeds and build up to a bigger number of bits that are all guaranteed to be random.

9. Other Quantum Certification Methods

Instead of employing the Bell equation, we might strive to develop verified quantum random number generators based on various experimental evaluations of quantum theory's core properties. The Kochen-Specker theorem argues that there exist situations for which no non-contextual hidden variable model can meet quantum mechanics predictions. Contextuality in quantum mechanics is related to the existence of non-commutative observations where the measurement sequence is important and there is no pre-defined model that can give us the results of two truly incompatible measurements. Contextuality implies non-locality [23].

We can access quantum randomness rather than classical noise using quantum random number generators based on the contextuality test. We still operate with faulty equipment in this framework, albeit in a less hostile setting. Although we believe the maker of the random number generator is not attempting to deceive us, we acknowledge that the device might be defective or poorly built. The contextuality test determines whether or not the bits came from a quantum source.

One benefit of quantum random number generators is that we can easily trace the origin of our random bits to a specific quantum phenomenon. These verified generators can assist in detecting randomness caused by classical noise, flaws, or faults in the device and extracting only randomness from quantum origin. Contextuality testing can be performed without the devices being separated by a physical space. This is both a benefit and a drawback of this strategy. Although complicated nonlocal tangled states are not required for these tests, we cannot depend merely on the assumption that the bits will be random. Unlike device-independent protocols, a dishonest manufacturer can provide pre-generated bits that we are unable to comprehend.

Physical exercise can also be optical, with a photon-encoded qutrit whose superposition is in three possible ways, or three-level trapped ions are used (Um et al., 2013). This allows us to detect efficiency gaps and avoid the problems of detecting a single photon. In ionic systems random bits come to be recorded during a period of reflection (fluorescent) measurement time of around ten milliseconds. Under the studied experimental settings, the devices only provide a net gain in randomness, they create more random bits than are spent when measuring using uneven measurement settings.

10. Novel Quantum Random Number Generator

Our goal is to generate fast random numbers at a lower cost. At the same time, a high level of randomness is essential. The breaking of any quantum process leads to true randomness, but the frequency of generation depends on the detector output [24].

Based on the time of arrival QRNG, we propose an enhanced quantum random number generator. At best, we get only one random bit from each detected photon, this probability is reduced by detector inefficiency or dead time. In most cases, the frequency of random number generators is measured in Mbps, which is not enough for fast applications such as QKD. If we use multiple detectors to generate more random bits, we will have a bias that results from the different efficiencies of the detectors. By using one detector and comparing the three successful events of detection time, we can rule out this bias. It is quite convenient to use the simple version of the detectors, which has relatively small requirements. We propose to use the technology used in attenuated pulse quantum random number generators.

We propose using an optical quantum random number generator with a low light source, with the same chance of photon generation or non-production. As a result, one photon's state must be:

$$\frac{|0>_1+|1>_1}{\sqrt{2}} \tag{15}$$

If no detection occurs, we can assign a value of 0; if a click occurs, we can assign a value of 1. We do not care how many photons are used. Any superposition can be written as following:

$$\frac{1}{\sqrt{2}}|0>_1+\sum_{c=1}^{\infty}\alpha_c\,|c>_1 \tag{16}$$

where $\sum_{c-1}^{\infty}|\alpha_c|^2 = \frac{1}{2}$ is valid. We take it from the first click and it we do not care if it is caused by one photon or many. For a coherent state with α amplitude, the probability of finding a photon is 0

$$pr(n=0) = e^{-|\alpha|^2} \tag{17}$$

probability of finding one or more photons

$$pr(n \geq 1) = (1 - e^{-|\alpha|^2}) \tag{18}$$

The simplest idea is to find α for which pr(n = 0) = pr (n ≥ 1), which in this formula is $\alpha = \sqrt{ln2}$. The probability of the desired discovery is given by the Poissonian source, where ψT = ln2 ≈ 0.693.

The detector must have an effective average photon number ηψT, where the efficiency is η. Not to have the bias during the operation, von Neumann extraction must be used to solve this problem. For two detections, where photon number is n_0 and n_1, the output value is 1, if n_0> 0 and n_1 = 0 and 0 if n_0 = 0 and n_1> 1. If two consecutive blank periods or clicks are generated, the findings are ignored. These values are basically comparable for the Poisson source, with $pr(n > 0)pr(n = 0) = e^{-\eta\psi T}(1 - e^{-\eta\psi T})$. The bit rate is at least 4 times slower as a result, yet it is completely bias-free.

To improve efficiency we suggest using a generator that generates more than one random bit after detecting a photon. These type of generators are photon counting quantum random number generators. The results obtained will be divided into groups that have equal probability. In this case, we can use a single detector for data generation. We can take the time of arrival of photons as a quantum random variable. Successful photon time can be divided into time flats, created by a meter that works in parallel with the detector. The given discovery time interval gives us a few bits per discovery. In this process the events develop independently, is a Poissonian process [25].

To increase the frequency of random number generation, we suggest taking measurements in high-dimensional quantum space, such as photon temporal and spatial mode. By measuring the time of arrival of a photon, we obtain random bits by detecting two events in the time interval Δt. In the case of temporal mode, we can get more than one random bit by detecting one photon. Using the spatial mode of the photon, we can assign random numbers to the detector matrix in parallel. When using this method, it is best to pay attention to dead time, as this affects the speed of the detector counter [26]. Improved rate allows us to select the amount of bits to use from the counted number of photons while maintaining a high level of unpredictability.

11. Novel Semi Self-testing Method

True randomness is impossible only with classical mechanics procedures, so we use cryptographic protocols. Quantum random generators can be divided into several categories according to the reliability of the device. We first discussed self-testing QRNG, which is not device dependent. The advantage of this type of QRNG is the self-testing randomness feature. But, because the QRNG of the self-test must show non-locality, its generation rate is usually very low. The second category is device independent quantum random number generators. It is designed with completely reliable devices and can achieve high generation speeds if the device is modeled correctly. Otherwise, when the device is controlled by opponents, the result will not be accidental.

These two approaches have their pros and cons. In realistic implementation, it is more acceptable to take certain features and use some intermediate certification method. Combining practical, device independent quantum random number generators and self-testing QRNG, we get a semi self-testing generator. In this case we will not be completely dependent on the devices. Device independent QRNG is characterized by high productivity and efficiency, while the self-testing QRNG has greater security of certification randomness.

We offer a semi self-testing QRNG that combines the acceptable features of self-testing and device-independent QRNG.

We can use self-testing in the QRNG, designed to work for quantum random number generator that uses the path branching principle. For the position of the single-photon polarization superposition

$$\psi = \frac{|H> + |V>}{\sqrt{2}} \tag{19}$$

Or in an entangled state

$$\psi = \frac{|H>_1 |V>_2 + |V>_1 |H>_2}{\sqrt{2}} \tag{20}$$

Theoretically, detectors can generate an ideal random bit because a photon has a 50% probability that the beam will split and a 50% probability that the beam will reflect. This happens only in theory, because in practice, there are always problems with detectors, lasers, beam splitters, and their characteristics depend to some extent on environmental conditions as well. When a photon is on a beam splitter, problems can occur: detector inefficiency, imbalance in the splitting process, source imperfection, and multiple unknown sources of correlation. There are device-specific approaches to testing, but typically random use of the program afterwards and processing is done to correct the uneven distribution of probability.

Polarizers let photon pass through with 50% probability. In theory, coincidence counter in this case registers perfect anti-correlation.

In the device's testing phase, a complete tomography of the input state is conducted using a collection of data to determine a 2x2 matrix. For a single photon, a two-level photon system is efficient, but for a photon pair, a two-dimensional Hilbert space is productive. Based on the measurement results, the generator determines $H_\infty(\widehat{pr})$, which is the minimum possible entropy for the overall condition of the user and listener, and $\widehat{pr}$ is the worst of all possible cases. The bits are then transferred to a random extractor, which generates a shorter, unbiased random string for available entropy. This strategy defends us against attacks in which the opponent can manipulate the quantum state from which we get the entropy.

Tomography offers entropy estimation in models where errors are expected during implementation or irregularities may occur during operation. We imply that errors do not occur due to an unreliable manufacturer. This model is presented in the self-testing QRNG, where a quantum source of randomness is separated from the technical noise using dimension witness.

$$WT = \begin{vmatrix} pr(1|0,0) - p(1|1,0) & pr(1|2,0) - p(1|3,0) \\ pr(1|0,1) - p(1|1,1) & pr(1|2,1) - p(1|3,1) \end{vmatrix} \tag{21}$$

pr (o | s, m) gives the conditional probability of finding the result of o (from ± 1) for a condition that is one of the defined probabilities s = 0, 1, 2, 3. The measurement parameter m can be 0 or 1.

We can use an alternative approach, where we apply the principle of uncertainty. This allows any opponent to access a limited amount of information. Not only do we want to produce random bits, but we also want to make sure they're secure. For example, if we measure the photon polarization in an entangled state on a horizontal vertical base, we get absolutely random numbers, but the opponent can learn the exact sequence because he has access to the second half of the bits. Our sequence can be obtained from the same measurements because the bits are just uniform and are not confidential.

For a good result we combine self-testing QRNG with device independent quantum random number generators to get self-testing generator. A device independent quantum random number generator is designed with completely reliable devices and can achieve high generation speeds if the device is modeled correctly. Otherwise, when the device is controlled by opponents, the result will not be accidental.

That’s why we use variant of Bell inequalities, Clauser-Horne-Shimony-Holt (CHSH) formulation. Measurements of two devices we will study the measurement correlations create two variables for each module, s and m. These variables may have two values: 0 and 1, which correspond to binary measurement values. Both measurement instruments are the same. In the s configuration, the measurements give a binary value of a and the measurement defined by m gives the result b. We are particularly interested in the correlation function, which is defined as follows:

$$I = \sum_{s,m}(-1)^{s,m} [\mathrm{Pr}\ (\mathrm{a} = \mathrm{b} \mid \mathrm{sm}) - \mathrm{Pr}\ (\mathrm{a} \neq \mathrm{b} \mid \mathrm{sm})\ ] \tag{22}$$

When s and m are parameters, Pr (a = b | sm) and Pr (a $\neq$ b | sm) are the probabilities of a = b or a $\neq$ b. I $\leqslant$ 2 must be found, since any value greater than 2 implies nonlocality.

To evaluate the bell inequality, this experiment must be performed n times. The choice of each (s, m) measurement is generated by an identical and independent probability distribution Pr (sm). The final output string of n is r = (a_1, b_1;...; a_n, b_n), and the input s = (s_1, m_1;...; s_n, m_n). $\tilde{I}$ is the estimator of CHSH formula (22), which is defined:

$$\tilde{I} = \frac{1}{n}\sum_{s,m}(-1)^{s,m} [\mathrm{N}\ (\mathrm{a} = \mathrm{b} \mid \mathrm{sm}) - \mathrm{N}(\mathrm{a} \neq \mathrm{b} \mid \mathrm{sm})/\mathrm{Pr}(\mathrm{sm})\ ] \tag{23}$$

Where N (a = b, sm) is a number, how many times (s, m) have been measured. Results a and b were found to be equal to n after realization. N (a≠B, sm) is defined similarly.

12. Conclusion

Using our novel quantum random number generator it is possible to generate megabit or gigabit rates rather efficiently. Our generator is based on time of arrival QRNG. It is efficient, as it uses the simple version of the detectors with rather few requirements. The novel OQRNG produces more than one random bit per each photon detection.

In this paper quantum ways of working with unreliable devices are explored. First self-testing method for QRNG-s is analyzed, which is not device dependent, it uses the properties of some quantum event to observe the quality of the bits produced. Then, unless trustworthy physical principles are flawed, device independent quantum random number generators are considered. They are predicated on the notion that there are quantum correlations that offer statistical independence. New quantum certification techniques are proposed based on these approaches.

This method relies on device independent generators, but it employs less stringent experimental testing of many parts of quantum theory, resulting in a more restricted certification with more flexible safety standards. We combined practical, device independent quantum random number generators and self-testing QRNG, we got a semi self-testing generator.

Acknowledgments

The work was conducted as a part of PHDF-19-519 financed by Shota Rustaveli National Science Foundation of Georgia.

References

[1] Kabiri Chimeh, M., Heywood, P., Pennisi, M. et al. Parallelisation strategies for agent based simulation of immune systems. BMC Bioinformatics 20, 579 (2019). https://doi.org/10.1186/s12859-019-3181-y

[2] Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33

[3] P. A. W. Lewis, A. S. Goodman and J. M. Miller, "A pseudo-random number generator for the System/360," in IBM Systems Journal, vol. 8, no. 2, pp. 136-146, 1969, doi: 10.1147/sj.82.0136.

[4] Lambić, D., Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn 90, 223–232 (2017). https://doi.org/10.1007/s11071-017-3656-1

[5] J. M. Mcginthy and A. J. Michaels, "Further Analysis of PRNG-Based Key Derivation Functions," in IEEE Access, vol. 7, pp. 95978-95986, 2019, doi: 10.1109/ACCESS.2019.2928768.

[6] Michael A. Wayne and Paul G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express 18, 9351-9357 (2010)

[7] Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/RevModPhys.89.015004.

[8] High-Speed and Secure PRNG for Cryptographic Applications; T. Okhrimenko, S. Tynymbayev, M. Iavich; mecs-press.org, 2020.

[9] Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; ceur-ws.org, Vol-2698, 2020.

[10] Improvement of Merkle Signature Scheme by Means of Optical Quantum Random Number Generators; M. Iavich, A. Gagnidze, G. Iashvili, T. Okhrimenko, A. Arakelian, A. Fesenko; Springer, 2020.

[11] Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation.

[12] Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S., Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020.

[13] Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. Experimental Study of Secure PRNG for Q-trits Quantum Crypto-graphy Protocols, Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.

[14] Z. Hu, S. Gnatyuk, T. Okhrimenko (Zhmurko), V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.

[15] A.Gagnidze, M.Iavich, G. Iashvili, Advantages and challenges of QRNG integration into Merkle, Scientific and Practical Cyber Security Journal (SPCSJ) 4(1):93-102, 2020

[16] Shrimpton T., Terashima R.S. (2015) A Provable-Security Analysis of Intel’s Secure Key RNG. In: Oswald E., Fischlin M. (eds) Advances in Cryptology -- EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9056. Springer, Berlin, Heidelberg.

[17] Chernov, P. S., Volkov, V. S., & Surovtsev, D. A. (2018). Towards Self-testing Quantum Random Number Generators in Integrated Design. In IOP Conference Series: Materials Science and Engineering (pp. 012087-012087).

[18] Lunghi, Tommaso, et al. "Self-testing quantum random number generator." Physical review letters 114.15 (2015): 150501.

[19] Bowles, J., Quintino, M. T., & Brunner, N. (2014). Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Physical review letters, 112(14), 140407.

[20] Vallone, G., Marangon, D. G., Tomasin, M., & Villoresi, P. (2014). Quantum randomness certified by the uncertainty principle. Physical Review A, 90(5), 052327.

[21] Pironio, S., Ac ń, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell’s theorem. Nature, 464(7291), 1021-1024.

[22] Vazirani, U. V., & Vidick, T. (2011). Certifiable Quantum Dice-Or, testable exponential randomness expansion. arXiv preprint arXiv:1111.6054.

[23] Kulikov, A., Jerger, M., Potočnik, A., Wallraff, A., & Fedorov, A. (2017). Realization of a quantum random generator certified with the Kochen-Specker theorem. Physical Review Letters, 119(24), 240501.

[24] Gnatyuk S., Okhrimenko T., Iavich M., Berdibayev R. Intruder control mode simulation of deterministic quantum cryptography protocol for depolarized quantum channel, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 825-828.

[25] S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.

[26] Qoussini A.E., Daradkeh Y.I., Al Tabib S.M., Gnatyuk S., Okhrimenko T., Kinzeryavyy V. Improved model of quantum deterministic protocol implementation in channel with noise, Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2019), 2019, pp. 572-578.

Authors’ Profiles

Dr. Maksim Iavich is an affiliated professor and Head of Cyber Security Direction at Caucasus University, Caucasus School of Technology. He leads bachelor and master IT programs at this university and is also invited professor at Georgian Technical University. Maksim is CEO & President of Scientific Cyber Security Association (SCSA). He is PhD in mathematics and professor of computer science. Maksim is cyber security consultant in Georgian and International Organizations. He is author of many scientific papers. The topics of the papers are: cyber security, cryptography, post-quantum cryptography, quantum cryptography, mathematical models and simulations.

Mrs. Tamari Kuchukhidze is Ph.D. candidate at Georgian Technical University. She is making her thesis on the creation of the quantum random number generators for cryptography. She is the developer and cryptographer at Scientific Cyber Security Association.

Dr. Sergiy Gnatyuk is Expert in Cybersecurity and CIIP, Lead Researcher in Cybersecurity R&D Lab. He is Doctor of Sciences (Cybersecurity), Professor in IT-Security Academic Dept at National Aviation University (Kyiv, Ukraine) are: cyber security, cryptography, post-quantum cryptography, quantum cryptography, mathematical models and simulations.

Mr. Giorgi Iashvili is Ph.D. candidate at Georgian Technical University. He is making his thesis on the secure design of cryptography schemes. He is the technical director of Scientific Cyber Security Association (SCSA) and the lecturer at Caucasus University.

Dr. Razvan Bocu is PhD in Computer Science (National University of Ireland, Cork, 2010), MSc in Computer Science (Transilvania University of Brasov, 2006), BSc in Computer Science (Transilvania University of Brasov, 2005), BSc in Sociology (Transilvania University of Brasov, 2007).

How to cite this paper: Maksim Iavich, Tamari KuchukhidzeGiorgi Iashvili, Sergiy Gnatyuk, Razvan Bocu," Novel Quantum Random Number Generator with the Improved Certification Method ", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.7, No.3, pp. 41-53, 2021. DOI: 10.5815/ijmsc.2021.03.05