I. J. Computer Network and Information Security, 2021, 3, 28-38
Published Online June 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.03.03

Novel Certification Method for Quantum Random Number Generators

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

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

Andriy Fesenko
Taras Shevchenko Kyiv National University, Kyiv, Ukraine, 01033
E-mail: a.fesenko@meta.ua

Received: 20 January 2021; Accepted: 11 April 2021; Published: 08 June 2021

Abstract: Random numbers have many uses, but finding true randomness is incredibly difficult. Therefore, quantum mechanics is used, using the essentially unpredictable behavior of a photon, to generate truly random numbers that form 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 performance of our device and the quality of the random bits generated. Self-testing as well as device independent quantum random number generation methods are analyzed in the paper. The advantages and disadvantages of both methods are identified. The model of a novel semi self-testing certification method for quantum random number generators is offered in the paper. This method combines different types of certification approaches and is rather secure and efficient. The method is very important for computer science, because it combines the best features from self-testing and device independent methods. It can be used, when the random numbers' entropy depends on the device and when it does not. In the related researches, these approaches are offered to be used separately, depending on the random number generator. The offered novel certification technology can be properly used, when the device is compromised or spoiled. The technology can successfully detect unintended irregularities, operational problems, abnormalities and problems in the randomization process. The offered mythology assists to eliminate problems related to physical devices. The offered system has the higher certification randomness security and is faster than self-testing approaches. The method is rather efficient because it implements the different certification approaches in the parallel threads. The offered techniques make the offered research must more efficient than the other existing approaches. The corresponding programming simulation is implemented by means of the simulation techniques.

Index Terms: Information security, cryptography, quantum random number generator, randomness.

1. Introduction

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. Everything can be recreated and a random number generator can be built, but this is not suggested. There are many reliable algorithms and devices that have withstood years of cryptanalysis and attack attempts, proven to be robust.

This means that the user must trust the device or algorithm. A problem that seems theoretical or simple may not be easily remedied. Recent events have shown that random number generators are especially attractive for secret attacks. For example, the pseudo-random number generation algorithm DUAL_EC_DBRG, proposed as the NIST standard, allows an attacker to retrieve an entire random sequence with minimal information, with practical consequences during Juniper network attack (CVE7755, 2015) [1-4].

There are the 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.

For physical random number generators occur the problems such as possible spontaneous interruption. The quality of the output bits can change if a device's components stop working or deteriorates. If the device generates values, the hidden flaws of the device are particularly difficult to detect. For this reason, safety recommendations require some kind of self-testing in true quantum number generators. At all times, the device's condition should be supervised by the subsystem (Bucci and Luzzi, 2005; Fischer, 2012).

Quantum ways to work with unreliable devices are reviewed. The first approach examines the quality of the bits generated by analyzing the properties of a quantum event. Second, it collects what are known as device independent quantum random number generators, which are built on the premise that quantum correlations provide analytical independence unless reliable physical concepts are wrong. The third approach refers to quantum certification methods that are based on device independent generators but employ less demanding experimental tests of different aspects of quantum theory, resulting in more limited certification with more relaxed safety assumptions [5].

The aim of this study is to establish a certification method for generating safe and efficient random numbers that integrate self-testing and device-independent quantum random number generators.

Even if the devices are unreliable and it is not possible to rely on physical integration, the randomness in the case of self-testing can be established. Self-testing methods can be used for both classical and quantum models of entropy. The entropy of the source of random numbers can be monitored. Randomness can be verified by detecting a bell inequality violation, even if classical noise interferes with quantum processes. Self-testing methods can detect random anomalies, operational problems, irregularities in the randomization process, and problems.

Device independent random number generators are designed with completely reliable devices and, if properly modeled, provide high-speed random number generation. Device independent models are characterized by high productivity and efficiency. These types of random number generators help to eliminate problems related to physical devices. For example, the device is compromised or damaged. It is possible for an attacker to gain access to our device, thus generating real random numbers and being able to hide in a manipulated device. Solving problems of this style is especially difficult because the sequence of random bits obtained passes through randomized self-testing random tests.

To eliminate problems with device reliability, it is necessary to use device independent quantum random number generators that use Bell's violation and rely on an uncertainty process.

A quick and efficient quantum random number generator must be created. It must be tested on the various types of attacks, and its effectiveness must be evaluated using the certification process. Only certain types of problems are tested with self-testing and an independent generator on the device, and one of them must be chosen: device reliability or system malfunctions. The second problem is that the processing speed of the self-test is very slow. When selecting a method independent of the device it is necessary to have completely reliable devices, otherwise, the results obtained will not be accidental.

Self-testing and device independent random number generators are typically used separately. And in case of unification still the certain types of restrictions are set. For example, consider a source of randomness less trustworthy and devices trustworthy. Also, in contrast, the input values are well drawn, but do not trust physical devices.

Our goal is to get a certification method with as few restrictions as possible, which will cover many types of problems, the generation speed will not be slow and the absolute reliability of the physical device will not be necessary.

By combining self-testing and device independent random number generators, it will be possible to incorporate the positive attributes: the ability to test various types of problems, the certification method will be efficient and productive, with high random generation speeds. Respectfully to the caution of the possible efficiency problems of the received results, they must be assessed. As there is not the opportunity to check the offered approach using the necessary quantum equipment, the implementation of it is done using the simulation techniques.

2. Literature Review

The scientists are working on the creating different quantum random number generators and the certification methods from them. In [1] self-test and device-independent certification methods approaches are described. The pros and cons of different types of certification are discussed. The paper also describes different quantum random generators. The authors analyze their security and efficiency. The results of the analysis of the security and efficiency are taken into the consideration in our research. In paper [2] theoretical and informational stability is achieved through the use of unique quantum particles and the inviolability of quantum physics postulates, in addition, it does not depend on the intruder computational capabilities. Although these quantum cryptography methods have some drawbacks, the authors have developed a reliable trit generation method and software tool to obtain a fast and safe PRNG. The drawbacks are taken into the account during the research. Authors in an article [3, 4] provide the improved hash based digital signature scheme, which uses the truly random number received using the quantum random number generator. The good idea is to integrate the certification methods in such approaches. The authors show that the algorithm is fast; offered scheme is secure and can be used as post-quantum security tool. Paper [5] describes the measurement of quantum randomness.

The authors divide QRNG-s into different groups and secured and efficient certification methods are described. The authors of paper [6] are working on general design of the implementation of a self-testing optical quantum random number generator (OQRNG) as a portable incorporated photonic circuit. The paper [7] describes a self-testing quantum random number generation protocol that allows the user to control the entropy in real-time and provides the continuous generation of high-quality randomness but without comprehensive system characterization. Paper [8] offers a simple method for certifying the use of qubits in the vicinity of artificial noise and objectively low detection reliability, in which witnesses are highly resistant to technical flaws. A lower bound of the possible true randomness can be determined by running quantum system experiments and switching between two mutually impartial bases. The authors presented an efficient method for testing the dimension of classical and quantum systems of arbitrary dimension. The paper [9] proposes a quick method for obtaining true randomness.

Randomness generation in quantum systems is only feasible if it is certified by a Bell inequality violation typically used on device independent QRNG, which is proposed in [10]. In the article [11], the semi-device-independent approach is offered, where the protection is based on comparisons between one-way QKD, dimension witnesses, and random-access codes. Different protocol for device independent QRNG is introduced in [12]. Additionally, paper [13] introduces Kochen-Specker theorem, which can be used in other experimental studies of quantum theory's fundamental properties. It is interesting to combine the results of the papers [6-13] in order to get better security and efficiency in the certification stage. The authors of the paper [14] discuss quantum secure direct communication. They have a new quick privacy acceleration method for quantum cryptography protocols. According to the results, the proposed method outperforms analogs while maintaining the same degree of protection against non-coherent attacks. The protection methodology must be used when creating the new certification approaches. The authors of the papers [15] offer how to improve the pseudo-random number generators. The new certification method can be implemented into these improvements in order to check the seed of PRNGs. The authors of [16, 17] offer how to use correctly quantum properties for creating the new approaches in computer science. They explain how to make quantum calculations in the optimal way. The offered approaches are used in order to create the novel certification method for QRNGs.

3. Self-testing Quantum Random Number Generators

The majority of quantum random number generators do not provide a complete description of their random source. When a photon passes through a beam splitter, for example, problems like detector inefficiency, imperfections in the dividing phase, 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 is only true in principle, since there are still issues with detectors, lasers, and beam splitters, and their characteristics are often affected by environmental conditions. There are device-specific approaches to research, but most of the time, random use of the software is followed by processing to correct the unequal distribution of probability [6].

Therefore, various methods have emerged to test the the randomness of numbers provided by physical random number generators. It can be used with a wide range of random number generators. When it comes to classics, there are various ways to verify the data obtained, such as the NIST and Diehard random tests. Only self-testing methods closely related to the quantum properties of random numbers are covered in this section.

A quantum random number generator's production randomness can be constructed in such a way that it is not dependent on any physical integration. True randomness can be generated in a self-testing fashion even if the realization devices are not perfectly characterized. By detecting a violation of Bell's inequality, a self-testing generator will experience quantum entanglement or nonlocality without the use of a computer. Even if the output randomness is mixed with uncharacterized classical noise, a lower bound on the amount of genuine randomness can be found, which is based on the amount of nonlocality found. This type of quantum random number generator benefits from the self-testing property of randomness. Since it must show nonlocality, the self-testing generator's generation speed is usually very slow.

Self-testing quantum random number generators have the number of technical highlights and advancing features prior to the other approaches. The main fetare is that the self-testing approaches can be used to test both standard noise and quantum models of entropy. For instance, (Saito et al., 2010) describe a self-testing scheme that compares random pulses on time of arrival. The pulses can be from thermal noise or from radioactive decay. The obtained distribution is then examined to determine if a poisson distribution of arrival time is anticipated. Only the random numbers that meet those standards are transferred to output values, removing apparent anomalies.

While an intruder may still alter the outcome to establish a predictable sequence that passes the test, these self-testing systems will detect accidental disruptions and less complex attacks. These systems provide good additional protection. Tests can also detect operation errors.

Testing is important to obtain good quality random numbers, so it must be done carefully. Accurate assessment of entropy is difficult. 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 was created to work for quantum random number

generator that uses the path branching principle.

For the position of the single-photon polarization superposition

$$\psi = \frac{|H>+|V>}{\sqrt{2}} \tag{1}$$

Or in an entangled state

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

|H> and |V> indicate a configuration of a single photon vertically or horizontally. 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. Quantum correlations disappear if relative angle has been chosen to be 45 degrees.

There is a testing phase in the device where a complete tomography of the input state is performed using a collection of measurements to create a 2 × 2 matrix that defines a two-level photon structure for one photon or an efficient two-dimensional Hilbert space for a photon pair. Based on the measurement results, the generator determines $H_\infty(\widehat{pr})$, which is the smallest possible entropy for the user's and listener's overall state, and $\widehat{pr}$ represents the worst-case scenario. The bits are then transferred to a random extractor (Barak et al., 2003), which generates a smaller, objective random string for appropriate entropy.

This method protects the users from attacks in which the opponent may affect the quantum system from which the entropy is drawn while the experiments within the same state are repeated. It must be ensured that the determined condition is sustained during the process in order to perform conditional tomography correctly. Such a case is fascinating when an intruder may alter the photon's source or the generator is physically damaged. While such self-testing provides lax security, it is a helpful in detecting incidental system errors.

In models where errors are expected during implementation or irregularities can occur during execution, tomography provides a good entropy estimation. It is implied that errors do not occur due to an unreliable manufacturer. Using dimension witness, a quantum source of randomness can be isolated from technical noise.

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

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, the distribution pr(o | s, m) from the input can be calculated and estimated the value of the witness WT, from which the entropy of the raw data can be measured. In order to obtain the final random bit string, sufficient post processing of the raw data is performed based on the entropy bound [7, 8].

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. In the generator under consideration, the four states correspond to the circular right and left polarization or the diagonal and anti diagonal polarization of the second photon from the tangled pair, measured on the basis of diagonal or circular polarization. The first photon acts as a messenger.

WT refers to the extent to which preparation and calculations are integrated. Any WT greater than zero indicates that some of the measurements are incompatible and there is some quantum randomness that allows a predictable probability to be assigned. In a random extractor, the result can be used to calculate the compression rate. For small quantities of WT, the input bits produce a small number of pure random bits. An experimental test of this method shows 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.

Using the principle of uncertainty as an alternative is a viable option. Allowing only a small amount of knowledge to be held by any competitor. Our objective, as with the prior methods, is not just to produce random bits, but also to ensure that these bits are safe. For instance, if the formula (2) is used to calculate photon polarization in an entangled state, the completely random numbers are got, but an opponent with access to the second half of the bits knows the exact sequence the can be got from the identical measurements. For certain implementations, such as modeling, this may be acceptable, but any information leakage in cryptography should be avoided. By swapping two separate trustworthy sources, the certification approach protects confidentiality without requiring full tomography [9].

With regard to an agent, conditional minimum entropy gives us a random number that can be safely deduced from measurements. The uncertainty principle ensures that every potential input state has a low relation (from the results of our assessment, the minimum entropy can be confirmed). To choose bases in this framework, small random samples must be used. The seed's initial randomness will be enlarged to a confidential string after measurements. These seeds must be equal and cannot be separated from the same weak random source as the other remaining bits. Tangled photon

pairs produced by parametric down-conversion and measured at diagonal / anti-diagonal and horizontal / vertical polarization bases were used to demonstrate the process.

The accuracy estimation methods can be used in order to build a complex generator model that accounts for all sources of uncertainty and all experimental flaws in the most conservative way possible. The conceptual criteria that associated the estimation of precision were challenged in atomic clocks and yielded promising results. They can also be used to generate quantum random numbers. A metrology-based characterization was followed (Mitchell et al., 2015) to obtain randomness in the QRNG based on the to vouch phase noise. The prototype will provide us with a clear mean minimum entropy margin, which is also used to choose a random extractor. This method not only deals for hypothetical circumstances, but it also allows for the incorporation of restrictions based on additional observations or data collected.

4. Device Independent Quantum Random Number Generators

The second method of random number certification would be to overlook the quantum random number generator's inner workings and test the results solely on their accuracy. Particularly when the researchers try to demonstrate that outputs must be unintentional or rules will be broken. This is a simple device independent quantum information processing model that was developed in the sense of quantum key distribution.

If it is needed to generate random numbers, the worst case scenario must be taken into account when an opponent generated real random numbers, for example, with the help of generator, after which they were placed inside a tampered machine. QRNG can produce randomness with theoretical security only when system concepts are followed. The performance cannot be completely random if opponents manipulate the machines. The producer will be able to predict the output of the quantum random number generator device. If the device's output values are examined, it can be noticed that the series passes all randomness checks and researchers can trust the results. This is a difficult problem to prevent, although there are quantum ways to avoid such a situation.

Quantum random number generators that are not dependent on the device are used to solve device reliability problems using bell-based circuit diagrams. The theories behind Bell's violation come from an analysis of quantum theory and the Einstein-Podolsky-Rosen paradox. The analysis of first particle in the entangled state influences the state of the other particle as well. If the impulse of the first particle is determined, the outcome of calculating the impulse of the second particle can be predicted. This seems to violate the no-signal principle, which forbids quicker communication than light. This problem can be solved experimentally. The local realistic universe, in which no interaction happens faster than light and the laws of quantum mechanics are different from spatial-like measurements of entangled particles. Laws of quantum mechanics operate in this world. Both options are mutually exclusive. Several experiments back up the quantum theory. However, the theory has experimental shortcomings that prevent it from being specific or functional. A series of more detailed experiments confirm quantum theory's assumptions, which demonstrates Bell inequality rather than locality in greater detail.

The Clauser-Horne-Shimony-Holt (CHSH) configuration of Bell inequalities was chosen for the functional quantum random number generator. During measurements of two devices, two variables for each module will be created, 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. The correlation function must be analyzed, which is defined as follows:

$$I = \sum_{s,m} (-1)^{s,m} [\Pr(a = b \mid sm) - \Pr(a \neq b \mid sm)] \tag{4}$$

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 the bell 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 CHSH formula (4) evaluator, which is defined as follows

$$\tilde{I} = \frac{1}{n} \sum_{s,m} (-1)^{s,m} [N(a = b \mid sm) - N(a \neq b \mid sm) / \Pr(sm)] \tag{5}$$

Where N (a = b, sm) represents the number of times (s, m) have been calculated. After realization, results a and b were found to be identical to n. Similarly N (a≠B, sm) can be defined[10].

This correlation function can be determined after a series of measurements by estimating the probabilities. The laws of quantum mechanics apply as long as the systems are isolated and do not interact, then s_i and m_i at any level of operation are generated by separate random processes. The evaluation of I, $\tilde{I}$, after some work gives us the lower limit of the minimum entropy of the results. The initial minimum entropy source had some technological flaws, but they were fixed, and new features were introduced to the protocol, such as its composition and usefulness in cryptography to

create random bits.

If the system seems to have a classical definition, $\tilde{I} \leq 2$, the limitation is 0, and the system is deterministic. When the entanglement states are calculated, the random bits generated are supposed to be random. The ensuing bit string is not inherently uniformly random, but it is bounded by its minimum entropy, which means that it can be transformed to a randomly uniform string using the necessary randomness extractor.

Consider quantum devices that have spacelike separate parts. There are no further limitations on machines or entry states if they have access to unbiased random sources until $\tilde{I} > 2$. The chosen estimation parameters s_i and m_i must also have some randomness. Each level of the protocol should not be completely predictable.

In this respect, the generator described in the random expansion scheme is similar to the quantum key distribution (QKD). The protocol generates a larger string of random output values whose randomness is checked by quantum mechanics, starting with a random seed. It is a quadratic protocol.

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 offers exponential expansion.

To minimize detection differences, QRNG was implemented using trapped ion qubits (Olmschenk et al., 2007). Ionic systems produce at a slower rate than optical technologies but provide nearly perfect efficiency. Each atom first produces an entangled photon, after which ions are trapped by interfering with the photons. This is a well-publicized procedure. The experimental violation of Bell's inequality is a perilous challenge, and the generation process is very slow, yielding only 42 certified random bits with a good, 99% confidence level after a month of nonstop activity.

Some of the standards have recently been relaxed, allowing for optical frameworks and higher generation speed. Although most optical detectors have low profitability, transition-edge-sensor detectors have high enough efficiency gains to close gaps in some variants of Bell's inequality. It can also be used to produce certified quantum random numbers at about 1/2 bit each second.

There are QRNGs that employ an alternative model, allowing the users to use a lower detection efficiency, semi-device independent approach, in which they don't trust the device but believe we're dealing with a bounded-dimensional quantum system [11]. Using SML, this experiment encoded quantum information in linear transverse momentum within a single photon. Although only two paths are available in this demonstration, existing space light modulators allow us to monitor the spectral properties of single photons in order to encode high dimension quantum levels. The bit rate of this optical device is 0.28-bit per second.

Some optical applications concentrate on improving device-independent quantum random number generators in entangled photon combination research. This approach has been used in many QRN generators, such as NIST's randomness beacon.

Device-independent QRNG has been built as a more general model where quantum mechanics concepts can or may not apply. The device independent QKD protocols, for sure, only require the no-signaling principle to be followed. Data cannot be transferred faster than light speed under this principle. A communication system that can transmit messages faster than the speed of light would generate a conflict with causality, representing the grandfather paradox. The concept of no signaling is definite. It is absolutely futile to use tangled states to send information as long as there is non-localization and relations that tend to travel faster than the speed of light.

The limits in many device-independent QRNG are a no-signaling constraint. The exact limit depends on the conditional minimum entropy, but the general conclusions remain the same. The protocols also function as random enhancement systems in the new version, requiring randomly generated seeding [12].

All of the mentioned device-independent RNGs are actually applications of protocols that increase randomness by using the results of physical experiments. They start with a basic number of small seeds and build up to a larger number of bits that are all guaranteed to be random.

5. Other Quantum Certification Methods

Rather than using the Bells equation, qualified quantum random number generators using other experimental studies of quantum theory's fundamental properties can be constructed. The Kochen-Specker hypothesis establishes that there are certain conditions for which no noncontextual concealed variable model can explain quantum mechanics' predictions. In quantum mechanics, contextuality refers to the presence of noncommutative observations in which the measurement sequence is significant and no predefined model can give us the results of two truly conflicting quantities. Contextuality implies nonlocality [13, 14].

QRNG assumed from the contextuality test allows users to discover quantum randomness rather than classical noise. Through this prototype, the operation with untrustworthy systems in less hostile environments is conducted. It is assumed that the RNG's producer is not attempting to mislead us, butit is recognized that the product may be defective or poorly built. The contextuality test evaluates whether or not the bits came from a quantum process[15]. Quantum random number generators have the advantage of allowing us to determine the origin of random bits in a given quantum process [16, 17]. These qualified generators can identify traditional noise, imperfections, and flaws in the device, and only receive quantum entropy. Contextuality assessments may be performed even if the systems are not divided

spectrally. This approach has both a strength and a drawback in this regard. While complex nonlocal entangled states aren't needed for these tests, we can't depend solely on the assumption that the bits would be random. Unlike device-independent protocols, a fraudulent manufacturer may provide pregenerated bits that it is impossible to comprehend.

Some quantum random number generators produce certified random bits without entangled states using contextuality checks, KCBS inequality, and inequality violation. Simulation is the underlying theory of certain generators. With KCBS inequality, the output value guarantees a lower entropy limit, and then the values can be entered with a random extractor. The findings can be used as a quantum certificate that can be confidently said to be of quantum origin with a limited amount of unpredictable.

Vigorous training may 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 stop the issues associated with identifying a single photon. In ionic systems random bits come to be recorded during a period of reflection (fluorescence) observations that needs approximately ten milliseconds. When using unequal measurement parameters, the devices only give us a net benefit of randomness in both cases under the tested experimental conditions, for example, they produce more random bits than they consume.

There are also conceptual formulations for random number generators that illustrate the relationship between unpredictability and inconsistency, based on contextchecking tests in a similar setting to previous Abbott's experiments for a single or entangled state.

6. Methodology

There are different ways to validate the data obtained by classic random number generators, such as the NIST and Diehard random tests. These techniques work with a wide variety of random number generators. As the true randomness is difficult to achieve using only classical mechanics procedures, the cryptographic procedures are used. As a result, quantum random number certification methods that are closely related to the quantum properties of random numbers are used.

The first example of self-testing in a quantum environment was developed for a quantum random number generator that employs the path branching principle. It works for both single-photon polarization superposition and an entangled state. One photon may be oriented vertically or horizontally. Polarizers allow photons to pass through with a 50% probability, but quantum correlations vanish when the relative angle is set to 45 degrees.

The input state's complete tomography and generated a 2×2 matrix are examined. The matrix describes a two-level photon structure for one photon or an effective two-dimensional Hilbert space for a photon pair. For the overall state of the user and listener, are obtained the smallest possible entropy. This approach defends the users against attacks in which the adversary tries to control the quantum system from which the entropy is obtained while the experiments in the same state are replicated.

The models in which a quantum source of randomness could be separated from technological noise by using dimension witness are analyzed.

The alternative solutions based on the principle of uncertainty were analyzed, only a small amount of knowledge to be held by any competitor. For certain implementations, such as modeling, this may be acceptable, but any information leakage in cryptography should be avoided. By swapping two separate trustworthy sources, the certification approach protects confidentiality without requiring full tomography.

The accuracy of estimation methods was examined in order to build a complex generator model that accounts for all sources of uncertainty and all experimental flaws in the most conservative way possible. The conceptual criteria that associated the estimation of precision were challenged in atomic clocks and yielded promising results. They can also be used to generate quantum random numbers. The prototype provided us with a clear mean minimum entropy margin, which is also used to choose a random extractor. This method not only deals for hypothetical circumstances, but it also allows for the incorporation of restrictions based on additional observations or data collected.

A variant of Bell inequalities, Clauser-Horne-Shimony-Holt (CHSH) formulation was investigated. During the measurements of two devices 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.

Other than these methods, the other quantum certification methods were examined. Rather than using the bells equation. There was the effort to construct qualified quantum random number generators using other experimental studies of quantum theory's fundamental properties. Some quantum random number generators produced certified random bits without entangled states using contextuality checks, KCBS inequality, and inequality violation.

7. Novel Semi Self-testing Method

True randomness is impossible only with classical mechanics procedures, when the classical cryptographic protocols are used. Quantum random generators are classified into several groups based on the device's reliability. The methods of certification discussed above are the most used methods in practice, because of their security and efficiency advantages. However, these methods have also some disadvantages. The advantages of the methods are used in order to create a new certification method. First self-testing QRNG was discussed, which is not device dependent. The self-testing randomness capability of this form of quantum random number generator is an advantage. However, since self-testing QRNGs should always demonstrate quantum nonlocality, their production rates are typically poor. As a result, a second type of certification methods is received: 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, a semi-self-testing generator can be received. In this case the will not be complete dependence on the devices. Device-independent QRNG is characterized by high productivity and efficiency, while the self-testing QRNG has greater security of certification randomness.

A semi self-testing QRNG that combines the acceptable features of self-testing and device-independent QRNG is offered.

Self-testing in a quantum environment that is optimized for singular-photon polarization superposition

$$\psi = \frac{|H>+|V>}{\sqrt{2}} \tag{6}$$

For an tangled state

$$\psi = \frac{|H>_1|V>_2+|V>_1|H>_2}{\sqrt{2}} \tag{7}$$

Path branching concepts are used by the quantum random number generator. Polarizers cause photons to pass through with a 50% success rate. In this case, the coincidence counter registers full anticorrelation.

There is a testing phase in the device where a complete tomography of the input state is performed using a collection of measurements to create a 2×2 matrix that defines a two-level photon structure for one photon or an efficient two-dimensional Hilbert space for a photon pair. Based on the measurement results, the generator determines $H_\infty(\widehat{pr})$, which is the smallest possible entropy for the user's and listener's overall state, and $\widehat{pr}$ represents the worst-case scenario. The bits are then transferred to a random extractor, which generates a smaller, objective random string for appropriate entropy.

This method protects us from attacks in which the opponent may affect the quantum system from which the entropy can be drawn while the experiments within the same state are repeated. It must be ensured that the determined condition is sustained during the process in order to perform conditional tomography correctly. Such a case is fascinating when an intruder may alter the photon's source or the generator is physically damaged. While such self-testing provides lax security, it is a helpful in detecting incidental system errors.

In models where errors are expected during implementation or irregularities can occur during execution, tomography provides a good entropy estimation. It is implied that errors do not occur due to an unreliable manufacturer. This model is presented in the self-testing QRNG, using dimension witness; a quantum source of randomness can be isolated from technical noise.

$$WT = \begin{vmatrix} pr(1|0,0) - p(1|1,0) & pr(1|2,0) - p(1|3,0) \\ pr(1|0,1) - p(1|1,1) & pr(1|2,1) - p(1|3,1) \end{vmatrix} \tag{8}$$

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, the distribution pr(o | s, m) can be calculated from the input and estimate the value of the witness WT, from which the entropy of the raw data can be measured. In order to obtain the final random bit string, sufficient post processing of the raw data is performed based on the entropy bound.

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. WT refers to the extent to which preparation and calculations are integrated. For small quantities of WT, the input bits produce a small number of pure random bits.

Using the principle of uncertainty as an alternative is a viable option. Allowing only a small amount of knowledge

to be held by any competitor. Our objective, as with the prior methods, is not just to produce random bits, but also to ensure that these bits are safe. For instance, if the photon polarization is used in an entangled state, the completely random numbers are got, but an opponent with access to the second half of the bits knows the exact sequence can be got from the identical measurements. This may be acceptable for applications such as simulation, but any information leakage in cryptography should be avoided. By swapping two separate trustworthy sources, the certification approach protects confidentiality without requiring full tomography.

The variant of Bell inequalities, Clauser-Horne-Shimony-Holt (CHSH) formulation can be used. 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. It is obligatory to study the correlation function, which is defined as follows:

$$I = \sum_{s,m} (-1)^{s,m} [\Pr(a = b \mid sm) - \Pr(a \neq b \mid sm)] \tag{9}$$

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 always 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 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 CHSH formula (9) evaluator, which is defined as follows

$$\tilde{I} = \frac{1}{n} \sum_{s,m} (-1)^{s,m} [N(a = b \mid sm) - N(a \neq b \mid sm) / \Pr(sm)] \tag{10}$$

Where N (a = b, sm) represents the number of times (s, m) have been calculated. After realization, results a and b were found to be identical to n. Similarly N (a≠B, sm) can be defined. In order to check the validity of the offer propose, the novel certification method using Python language was implemented. The simulations techniques were used, when the quantum devices were needed.

As for the novel certification method self-testing and device-independent approaches are used its efficiency must be improved. For this, the parallel programming was used. The implementation of self-testing mechanisms and of the device-independent approaches were occurred in the different threads. This approach greatly improved the efficiency. The security of the novel approach was analyzed.

Let us assume that our approach is vulnerable and the attacker can break it. In order to break the novel certification methodology, self-testing or the device-independent mechanisms must be broken. It contradicts our initial assumption. According our initial assumption both of them are secure. It proves the security of the novel approach.

The experiments of the implemented model of the new approach show good efficiency results. As the paper offers the model of the new certification method, this method must be evaluated by means of quantum devices in the corresponding laboratory. Based on the experiments the approach could be modified.

8. Conclusion

The paper examines quantum methods for dealing with unstable devices. First self-testing method for QRNG-s is analyzed, which is not device dependent, it uses the properties of some quantum event to keep an eye on the quality of the bits that are generated. Then, based on the assumption that there are quantum correlations that include some statistical independence unless reliable physical concepts are wrong, device independent quantum random number generators are examined. A new quantum certification method is designed based on these methods.

The novel method is based on device independent generators, but it employs less demanding experimental testing of different aspects of quantum theory, resulting in a more specific certification with looser safety assumptions.

A new certification method is introduced. Two types of self-testing and device-independent random number generators are combined. Our certification method is powerful and effective as it can detect unintended irregularities, operational problems, abnormalities and problems in the randomization process. In addition, it helps to eliminate problems related to physical devices.

The goal of the research was to create a certification process that could be used for both device and system failures. The system that tests for a variety of issues was implemented. It is reliable and productive, and the generator has higher certification randomness security and it is faster than self-testing. By means of the parallel implementation, the efficiency of the new system is improved. The aim of this study was to establish a certification method for generating safe and efficient random numbers that integrate self-testing and device-independent quantum random number generators. The security analyses of the novel method prove the security of the novel approach. Because of the parallel implementation, the efficiency of the new system is improved.

In the future, it is planned to integrate the certification method into the model of the secure and efficient QRNG. By means of this we will get the complete secure and efficient system for the generating the true random numbers. The plans are to test the system in the laboratory with the quantum devices. The system will be updated accordingly. It is also planned to integrate the new methodology of generating the random numbers into the post-quantum crypto systems.

Acknowledgement

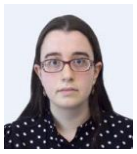
This work was financed by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) [CARYS-19-121] grant.

References

[1] Herrero-Collantes, Miguel & Garcia-Escartin, Juan Carlos. (2016). Quantum Random Number Generators. Reviews of Modern Physics. 89. 10.1103/ RevModPhys.89.015004.
[2] Zhengbing Hu, Sergiy Gnatyuk, Tetiana Okhrimenko, Sakhybay Tynymbayev, Maksim Iavich, "High-Speed and Secure PRNG for Cryptographic Applications", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.3, pp.1-10, 2020. DOI: 10.5815/ijcnis.2020.03.01
[3] Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; CEUR Workshop Proceedings, Vol. 2698, 2020.
[4] 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; Advances in Intelligent Systems and Computing, Vol. 1247, Springer, 2020.
[5] Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation.
[6] 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.
[7] Lunghi, Tommaso, et al. Self-testing quantum random number generator. Physical review letters 114.15 (2015): 150501.
[8] 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.
[9] Vallone, G., Marangon, D. G., Tomasin, M., & Villoresi, P. (2014). Quantum randomness certified by the uncertainty principle. Physical Review A, 90(5), 052327.
[10] 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), pp. 1021-1024.
[11] Pawłowski, M., & Brunner, N. (2011). Semi-device-independent security of one-way quantum key distribution. Physical Review A, 84(1), 010302.
[12] Vazirani, U. V., & Vidick, T. (2011). Certifiable Quantum Dice-Or, testable exponential randomness expansion. arXiv preprint arXiv:1111.6054.
[13] 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.
[14] Z. Hu, S. Gnatyuk, T. Okhrimenko, 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] Pushpam Kumar Sinha, Sonali Sinha," The better pseudo-random number generator derived from the library function rand() in C/C++", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.5, No.4, pp.13-23, 2019. DOI: 10.5815/ijmsc.2019.04.02
[16] K.Sundara Rao, Mrudula Singamsetti, Vuyyuru Tejaswi, " Design of Adder Using Quantum Cellular Automata", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.9, No.6, pp. 11-18, 2019.DOI: 10.5815/ijwmt.2019.06.02
[17] Vladimir K. Voronov, "Quantum-dot Controlled Electronic Block Triggering a Quantum Computation Procedure", International Journal of Information Technology and Computer Science (IJITCS), Vol.12, No.2, pp.42-48, 2020. DOI: 10.5815/ijitcs.2020.02.05

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.

Dr. Andriy Fesenko is the specialist of cyber security. Andriy is working as associate professor at Taras Shevchenko National University of Kyiv on the faculty of information technologies. His main interests are cyber security and cryptography.

How to cite this paper: Maksim Iavich, Tamari Kuchukhidze, Sergiy Gnatyuk, Andriy Fesenko, "Novel Certification Method for Quantum Random Number Generators", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.3, pp.28-38, 2021. DOI: 10.5815/ijcnis.2021.03.03

