UDC 004.421.5 **doi: 10.32620/reks.2021.4.09**

M. IAVICH[1], T. KUCHUKHIDZE[2], G. IASHVILI[1], S. GNATYUK[3]

[1] ***Caucasus University, Georgia***
[2] ***Georgian Technical University, Georgia***
[3] ***National Aviation University, Ukraine***

HYBRID QUANTUM RANDOM NUMBER GENERATOR FOR CRYPTOGRAPHIC ALGORITHMS

*The **subject matter** of the article is pseudo-random number generators. Random numbers play the important role in cryptography. Using not secure pseudo-random number generators is a very common weakness. It is also a fundamental resource in science and engineering. There are algorithmically generated numbers that are similar to random distributions but are not 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. The **goal** is to develop a mathematical model of the generator, which generates 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. The **goal** of the research is also to develop the model of a hybrid semi self-testing certification method for quantum random number generators (QRNG). The **tasks** to be solved are to create the mathematical model of a random number generator, which generates the fast random numbers at a lower cost. To create the mathematical model of a hybrid semi self-testing certification method for quantum random number generators. To integrate a hybrid semi self-testing certification method to the hybrid random number generator. the **methods** used are mathematical optimization and simulation. The following **results** were obtained: we present the improved hybrid quantum random number generator, which is based on QRNG, which uses the time of arrival of photons. The model of a hybrid 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 hybrid certification method is integrated into the model of the new quantum random number generator. **Conclusions**. The scientific novelty of the results obtained is as follows: 1. The hybrid quantum random number generator is offered, which is based on QRNG, which uses the time of the arrival of photons. It uses the simple version of the detectors with few requirements. The hybrid QRNG produces more than one random bit per the detection of each photon. It is rather efficient and has a high level of randomness. 2. The hybrid semi self-testing certification method for quantum random number generators (QRNG) is offered. The Self-testing, as well as device-independent quantum random number generation methods, are analyzed. The advantages and disadvantages of both methods are identified. Based on the result the hybrid method is offered. 3. The hybrid semi self-testing certification method for quantum random number generators is integrated into the offered model of the quantum random number generator. The paper analyzes its security and efficiency. The paper offers to use the new random number generator in the crypto-schemes.*

Keywords: *cryptography; quantum; quantum cryptography; random number generator; quantum random number generator; hybrid quantum random number generator; certification; hybrid certification method.*

Introduction

Random numbers are widely used in various fields, for example, simulation, encryption, cryptography, and 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 num-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ber 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 Quantum Random Number Generator (QRNG) of the True Random Number Generator (TRNG) that uses innate randomness in quantum processes as a random source.

Nowadays most of the existing QRNGs are based on quantum optics. Light from lasers, luminous diodes, or various photon sources, is more affordable and more common than radioactive material. Many light quantum state parameters have inherent randomness, which allows us to implement many variants. Light particles are used as a source of quantum randomness and are available to many detectors. 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 many reliable algorithms and devices 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. For example, RNGs are a tempting target for covert attacks. Pseudorandom number generation algorithm DUAL_EC_DBRG, proposed as the NIST standard, allows an attacker to retrieve an entirely 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. Therefore, safety recommendations are essential for some sort of self-testing in real quantum number generators. The subsystem should monitor the condition of the device at all times so as not to miss any faults.

The goal is to generate fast random numbers at a lower cost. A high level of randomness is obligatory. We offer the model of the improved hybrid 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 Optical Quantum Random Number Generator (OQRNG) produces more than one random bit per detection of each photon.

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. This certification method is known as a self-testing method, in which the device is checked after it produces the random number. Second, it collects propositions collectively known as device-independent quantum random number generators based on the assumption that there are quantum correlations that provide some statistical independence unless reliable physical principles are incorrect.

The third method describes quantum certification methods that are inspired by device-independent generators but use less rigorous experimental tests of various aspects of quantum theory, resulting in more limited certification with 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.

The third category of generators is the hybrid of the self-testing certification method and the device-independent quantum random number generator certification method. It is partly based on the properties of our first, self-testing method, therefore it is called a semi self-testing certification method. The papers offer the security and efficiency proof of the offered scheme.

State of the Art

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 can crack the crypto RSA system. In [3-5], several pseudo-random number generators are considered which use different methods to ensure the randomness of the sequences and a higher level of security. Based on the digitized time interval between random photon arrivals, paper [6] suggests more efficient and secure optical quantum random generators. Random numbers are widely used in different applications; the paper [7] presents the different technologies in quantum random number generation and the multiple ways to use this to gather entropy from a quantum origin.

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 au-

thors analyze their security and efficiency. Paper [11] describes the measurement of quantum randomness.

The authors of the 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], a new simple and fast algorithm for entropy extraction and pseudo-random numbers generation from a robust chaotic map is offered. The authors offer to use this method as an entropy source in some cryptographic applications. 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 the paper [17] are working on the improvement of self-testing optical quantum random number generators 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, and the authors offer the protocol which 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, the 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]. Additionally, paper [23] introduces Kochen-Specker theorem, which can be used in other experimental tests of the basic characteristics of quantum theory.

Different protocols are introduced in [24-26] to secure quantum channels to ensure confidentiality and security. The authors of [27] demonstrate that different quantum algorithms feasible on concrete devices can address a challenge central to the field of quantum metrology. They introduce a general framework that allows for sequential updates of variational parameters to improve the measurements and probe states. They also demonstrate the practical functioning of this approach using numerical simulations. In [28] and [29] are described different software implementations which can use random number generators.

Optical Quantum Random Number Generators

Randomness is the basis for cryptography. Most PRNGs cannot generate cryptographically secure random numbers [12-14]. For example, the internal state of Mersenne Twister can be guessed if we have sufficient output values. However, there are established ways to use pseudo-random number generators in cryptography. Algorithmic generators that meet additional criteria are called cryptographically secure pseudo-random generators, CSPRNGs.

The design of secure random number generators is a complicated task. 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 a source is a quantum random number generator.

True randomness can be generated from any quantum process that breaks the 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. From many variants of quantum state, Fock and coherent states give us the most appropriate description of light quantum states in random number generators. Fock condition, or numerical condition, is |n> in which n photons share a mode (have the same frequency, polarization, transition profile, and common path). Coherent condition, shared by many properties of classical light, can be written in a superposition of numerical state

$$|\alpha>=e^{\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n>, \qquad (1)$$

where α is a complex number, n is the photon number. The amplitude |α|2 corresponds to the average number of photons in the state. The light of the weak laser is close to the coherent state. We can use a coherent state from a laser to get the state of one photon if we choose a sufficiently low intensity.

In many cases, we are only interested in generating uncorrelated photons. Many different technologies can generate and detect single photons, such as photomultiplier tubes (PMTs), single-photon avalanche photodi-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

odes (SPADs), and 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 detecting photons. The next limitation for single-photon detectors is the time required to recover after the detection of photons, which is called dead time.

Time of Arrival Quantum Random Number Generators

Many methods can be used to generate random bits from photon detection times. In most cases, QRNG that uses time has a weak source of photons, also a detector and time schemes that record either the exact 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, the average number of photons per second. The time of the detection of two photons is the difference between two exponential random variables, which is also exponential. We can compare the time difference between t_0 and t_1. 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. The probability $t_0=t_1$, with a negligible probability of measuring an ideal continuous time, must be taken into account. We have two consecutive sequences 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.

One of the first quantum random number generators which use time detection takes the photons from a LED arriving at a PMT after it compares the arrival times in the chart, which is similar to comparing the arrival times of two particles in a Geiger counter. The random time of arrival can be used as a signal that selects the time bins from the clock. We can use a variation of the even-odd generation method. If a photon is detected in the even clock cycle, assign 1 and 0 if it is discovered in an odd 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 equivalent to using the time bins where we found the photon, throwing away some consistent counts.

There are many ways we can generate random numbers using time measurements. The time difference t_i is a real number and, we can withhold an infinite number of entropies from only two impulses. However, all of the extracted bits are not usable. If our timing information has a precision p bit, the time bin where we can find the photon is a random variable, $N=2^p$ possible values. After this, we can calculate the probability of a photon coming into each time bin. Some OQRNGs use digital time differences for n bits and divide available entropy into random bits string with a mathematical function. 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. For an irregular flow laser diode, we have an inhomogeneous Poisson process, we can adjust the standby time. For a variable photon flow, $\psi(t)$ is the distribution of the arrival time

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

Ideal is uniform distribution, which can be approached using a laser current, which periodically repeats the final approach of the function

$$\frac{1}{R-t}, \quad (3)$$

where R is the reset parameter that determines when the pulse cycle in the source will be loaded.

The current returns to the initial value when R is completed or when the pulse is detected.

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. For a random time, exponential variable, the amount of photons that go in a fixed T time follows the Poisson distribution. With this formula, we can find the probability of finding n photons at this interval.

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

For example, the generator H. Fürst et al. [30] 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 the first measurement has n_1 photons, and the second one n_2, 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 may have a higher entropy. There are ways to make the most of the information available. When a photon is detected, some generators assign more than one bit, depending on the number of photons. Possible outcomes are divided into groups that have equal probability. 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. S. Tisa et al. [32], generator, which has an integrated CMOS SPAD array of detectors, receives light from an LED and generates random numbers in a 32 × 32 detector matrix in parallel. This is the principle of the design of a micro photon device generator. In this approach it is important to properly characterize the dead time, because the dead time affects the speed of the detector ψ_{dc} counter. Improved rate

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

help us make choices about how many bits to use from the counted number of photons.

Attenuated Pulse Quantum Random Number Generators

In some cases, the generator doesn't need 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 current single-photon detectors have a limited number of photon number counting capabilities and have a binary response to clicking or no clicking. Methods for counting photons are usually based on many clicks over a long period, which is divided by the detector into smaller 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. Superposition of an empty and one photon state in the same spatio-temporal model, so that the state of one photon is

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

We can assign 0 if detection does not happen and 1, if a click is made. 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 the equation $\sum_{c-1}^{\infty} |\alpha_c|^2 = \frac{1}{2}$ 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. For a coherent state with α amplitude, the probability of finding a photon 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 simplest idea is to find α for which pr(n = 0) = = pr(n ≥ 1), which in this formula is $\alpha = \sqrt{\ln 2}$. The probability of the desired discovery is given by the Poissonian source, where $\psi T = \ln 2 \approx 0.693$.

In practice, the generator operates on a detector with an effective average photon number $\eta\psi T$, 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, von Neumann extraction can be used. For two detections, the output value is 1, if $n_0 > 0$ and $n_1 = 0$ and 0 if $n_0 = 0$ and $n_1 > 1$, where n0 and n1 are the photon numbers.

The results are ignored if two consecutive blank periods or two clicks are generated. For the Poissonian source, this values are equal with probably

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

$pr(n > 0)pr(n = 0) = e^{-n\psi T}(1-e^{-n\psi T})$. The resulting bit rate is at least four times slower but free of all bias.

Self-testing in Quantum Random Number Generators

Most quantum random number generators do not fully describe their random source. For example, 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. 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. Therefore the different methods were offered to check the quality of the random numbers produced in physical random number generators. The self-testing approaches are directly related to the quantum properties of the random number generator. There are device-specific approaches to testing, but typically random use of the program afterward and processing is done to correct the uneven distribution of probability [17].

This is why various methods have emerged to test the quality of random numbers generated in physical random number generators. This is not just for quantum random number generators. 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 characterizing the realization 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 uncharacterized 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 property of the randomness self-testing. 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. 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, there is still a risk that the attacker will change the outcome and create a predictable sequence that will pass the test, but these self-testing systems can detect spontaneous disturbances and less sophisticated 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 QRNG of Fiorentino, designed to work in a single-photon polarization superposition

$$\psi = \frac{|H> + |V>}{\sqrt{2}}. \qquad (10)$$

Or in an entangled state

$$\psi = \frac{|H>_1|V>_2 + |V>_1|H>_2}{\sqrt{2}}. \qquad (11)$$

The quantum random number generator uses the principles of path branching.

|H> and |V> indicate the state of a single vertically or horizontally polarized photon. Polarizers let photon pass through with 50 % probability. In theory, the 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. The device has a testing phase where a complete tomography of the input state is performed from a set of measurements to determine a 2 × 2 matrix. For a single photon, we get a two-level photon system, while for a photon pair the two-dimensional Hilbert space is efficient. Based on the measurement results, the generator determines $H_\infty(pr)$ which is the minimum possible entropy for the overall condition of the user and listener, and 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 method protects us from attacks where the opponent can control the quantum state from which we get the entropy. We are protected from cases where we make repeat-

ed measurements on one state. To perform conditional tomography correctly, we must assume that the measured condition is maintained throughout the process. Such self-testing offers limited protection, however, it is an effective way to detect accidental errors in devices. Tomography provides a reasonable estimate of the entropy of such 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. One such model is presented in the self-testing QRNG of Lunghi, where a quantum source of randomness is separated from the technical noise using dimension witness.

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

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 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.

An alternative approach is to apply the principle of uncertainty. This principle allows any opponent to access a limited amount of information. Our goal is not just to generate random bits, but to make sure these bits are confidential. For example, if we use formula (11) we get 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. We can use the certification method in quantum random number generators to protect confidentiality without complete tomography by switching two mutually unbiased bases. Instead of a complete tomographic measurement, two bases are sufficient [20].

Device Independent Quantum Random Number Generators

We can also ignore the details inside the quantum random number generator and evaluate the results based solely on the output. Especially, if we want to prove that outputs must be accidental or some physical law will be violated. This is the second approach of the random number certification. The basic model for processing device-independent quantum information was started by Mayers and Yao in 1998 and Barrett in 2005.

During random number generation, we imagine the worst-case scenario when an opponent can generate real random numbers using a quantum random number generator, and then hide them inside a manipulated device. If the devices are manipulated by opponents, the output may not be random. The manufacturer can predict the output of the QRNG device. During the check of the output values of this device, the sequence will pass all randomness tests and we will trust the results because the opponent can generate the real random numbers. This problem is difficult to avoid, but there is a quantum solution. That's why it is important to use the device-independent certification method.

Device-independent quantum random number generators solve the problem of device reliability by trusting the device with schemes based on Bell tests. The ideas of Bell's violation stem from a discussion of quantum theory and the apparent inconsistency of relativity known as the Einstein-Podolsky-Rosen paradox. In the entangled state, the measurement of one particle immediately determines the state of the other particle as well. This seems to go against the no-signal principle, then prohibits faster communication than light. John Bell showed that resistance can be solved experimentally.

The Clauser-Horne-Shimony-Holt (CHSH) configuration of Bell inequalities was chosen for the functional quantum random number generator. Using the measurements of two devices we will look at the 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

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

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:

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

where $\Pr(a = b \mid sm)$ and $\Pr(a \neq b \mid sm)$ are the probabilities of $a = b$ or $a \neq b$ when s and m are parameters. For a realistic local theory we must always find $I \leq 2$, because any value greater than 2 indicates non-locality. To evaluate the 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

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

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 ($a \neq B$, sm) is defined similarly [21].

This correlation function can be calculated by estimating the probabilities after a series of measurements. As long as the systems are separated and do not interact with each other, the laws of quantum mechanics apply. 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

If the system has a classical description, $\tilde{I} \leq 2$, the restriction is zero and the system can be deterministic. If we take measurements on states that show any entanglement, the random bits generated are guaranteed to have some kind of randomness. The resulting sequence of bits is not necessarily uniformly random but is bounded by its minimal entropy, which means that using the appropriate randomness extractor, the sequence can be converted to a randomly uniform string.

Consider quantum devices that have spacelike separate parts. If they have access to independent random sources, there are no additional restrictions on devices or input states until $\tilde{I} > 2$. The only additional requirement is that the selected measurement parameters s_i and m_i have any randomness at each stage of the protocol and should not be completely predictable.

In this respect, the generator described in the random expansion scheme is similar to the quantum key distribution. Starting from a random seed, the protocol gives us a larger string of random output values whose randomness is certified by quantum mechanics.

In 2010 QRNG was implemented with trapped ion qubits to eliminate detection gaps. Ionic systems generate more slowly than optical implementations but offer almost perfect performances. Each atom first emits a photon that is entangled, and then ions are trapped 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, over about a month of continuous running.

In later implementations, some of the requirements were lessened, allowing optical implementations and faster generation rates. Most optical detectors have low efficiencies, transition-edge-sensor detectors offer sufficiently high efficiencies to eliminate gaps in some versions of bell's inequality. Also, use it to generate certified quantum random numbers at a speed of about half a bit per second.

Device-independent quantum random number generators can be developed as a more general model where the principles of quantum mechanics may not be true. 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, 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.

The limit in device-independent quantum random number generators is also a no-signaling constraint. The exact limit varies on conditional minimum entropy, but general results remain. In the new model, the protocols still work as random amplification schemes that require uniform random seeding [22].

All of the described device-independent random number generators, both quantum and non-signal, are in fact implementations of protocols that use the results of physical experiments to extend randomness. They start from small random seeds and form a larger number of bits that will surely be random.

Other Forms of Quantum Certification

Instead of using the Bell equation, we can try to create certified quantum random number generators based on other experimental tests of the basic features

of quantum theory. The Kochen-Specker theorem shows that there are states for which no non-contextual hidden variable model fulfills the predictions of quantum mechanics. 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].

Quantum random number generators based on the contextuality test give us access to quantum randomness rather than classical noise. In this model, we still work with unreliable devices, but in less aggressive environments. We believe that the manufacturer of the random number generator is not actively trying to fool us, but we admit the device can be faulty or poorly designed. The contextuality test shows whether the bits are really from a quantum source.

One of the advantages of quantum random number generators is that we can trace the origin of our random bits to a defined quantum phenomenon. These certified generators can help to detect the randomness due to classical noise, imperfections, or failures in the device and take only the randomness from quantum origin. Contextual tests can work without spacelike separation of the devices. This is both the advantage and the disadvantage of this method. These tests do not require complex nonlocal entangled states, but we cannot rely solely on the premise that the bits will be random. Unlike device-independent protocols, a fraudulent manufacturer can supply pre-generated bits so that we cannot even understand them.

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. 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 measurements that takes about 10 milliseconds. In both cases, under the tested experimental conditions, the devices give us only a net gain of randomness, i.e., generate more random bits than are consumed when using unequal measurement parameters.

Hybrid 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].

We offer an improved quantum random number generator based on the time of arrival QRNG. 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 offer to use OQRNG with a weak source of light and the probability of photon generation or not generation is the same. So that the state of one photon can be calculated using (6).

The superposition of the photon can be written using the formula (7).

We take it from the first click and 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 can be calculated by (8).

The probability of finding one or more photons can be calculated by (9).

After that we find α for which $pr(n = 0) = pr(n \geq 1)$.

The detector must have an effective average photon number $\eta \psi T$, where the efficiency is η. Von Neumann extraction must be used not to have bias during the operation. It must be mentioned, that the received bit rate does not have a bias, but it is rather slow.

To improve efficiency, we suggest using a generator that generates more than one random bit after detecting a photon. These types of generators are called 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, it 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 coun-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ter [26, 27]. The improved rate helps us to choose how many bits to use from the counted number of photons and get a high level of randomness.

The offered generator uses the aspects of Time of arrival generators, as the authors of [30] mention its speed is 128-Mb/s, which is rather low. In the paper, we offer to use the properties of Photon Counting Quantum Random Number Generators, which perform the number of bits in parallel. The authors of [31] illustrate that in this case the speed can be improved up to 5 Gb/s. Which is already a good result. Attenuated pulse Quantum Random Number Generators give us the possibility to use more affordable devices. We offer to use the XOR operation between the received values, which almost does not affect the speed. Finally, the speed of our generator will be up to 5 Gb/s.

We claim that we have created the QRNG, which generates fast random numbers at a rather lower cost. For the proof, we begin from the contrary.

Our claim is based on three assumptions:

1. Time of arrival generators are secure quantum random number generators, which offer the random seed.

2. Photon Counting Quantum Random Number Generators can assign more than one bit during each measurement.

3. Attenuated pulse Quantum Random Number Generators are based on a simplified version of the previous methods that have fewer requirements for detectors.

Let us say that the offered QRNG's seed can be predicted, but it can not be because it is based on time of arrival generators, and based on the first assumption the output is random. Let us say that our random number generator can assign only one bit per measurement so it can not work in parallel mode. Therefore it will work with a low speed. It can not be true, because it is based on Photon Counting Quantum Random Number Generators, and based on our assumption it can work in parallel mode. Let us say that the offered QRNG needs expensive hardware, but as it is based on the approaches of Attenuated pulse Quantum Random Number Generators it has much fewer requirements for detectors. So it contradicts the third assumption. All these proved that the offered QRNG generates fast random numbers at a rather lower cost.

Hybrid 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 a 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, which is designed to work in a single-photon polarization superposition, which can be calculated by (10). It also can be calculated by (11), if it is in an entangled state.

The quantum random number generator uses the principles of path branching. 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 afterward and processing is done to correct the uneven distribution of probability.

Polarizers let photons pass through with 50 % probability. There is a testing phase in the device where a complete tomography of the input state is performed from a set of measurements to determine a 2×2 matrix that describes a two-level photon system for one photon or if we have a photon pair, an effective two-dimensional Hilbert space. Based on the measurement results, the generator determines $H_{\infty}(\mathrm{pr})$, which is the minimum possible entropy for the overall condition of the user and listener, and 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 method protects us from at-

tacks where the opponent can control 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. Where WT can be calculated by (12).

We can use an alternative approach, where we apply the principle of uncertainty. This allows any opponent to access a limited amount of information. Our goal is not just to generate random bits, but to make sure these bits are confidential. 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 in order to get the 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 Bell inequalities, Clauser-Horne-Shimony-Holt (CHSH) formulation.

We will study the correlation, by means of (13). In order to evaluate the bell inequality, we will run the process n times. After this, the final output string of n must be defined. The estimator of CHSH is defined by (14).

Conclusion and Future Plans

The offered hybrid quantum random number generator can be securely used in crypto algorithms. By means of the generator it is possible to generate megabit or gigabit rates rather efficiently. The offered generator is based on the time of arrival of QRNG.

It is efficient, as it uses the simple version of the detectors with rather few requirements. The hybrid QRNG produces more than one random bits per 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 device independent quantum random number generators are discussed, they are based on the assumption that there are quantum correlations that provide some statistical independence unless reliable physical principles are incorrect. Based on the described approaches the new quantum certification method is offered.

This method is inspired by device independent generators but uses less rigorous experimental tests of various aspects of quantum theory, resulting in more limited certification with more relaxed safety assumptions.

Combining practical, device independent quantum random number generators and self-testing QRNG, we got a semi self-testing generator. The generator can be used both in classical and post-quantum crypto schemes.

The plans of the research are to check the results on the real quantum random number generators. We plan to use XOR operation, in order to combine the different approaches. Are plans are to integrate the hybrid random number generator into the post-quantum digital signature schemes.

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

References (GOST 7.1:2006)

1. Parallelisation strategies for agent based simulation of immune systems [Text] / M. Kabiri Chimeh, P. Heywood, M. Pennisi et al. // BMC Bioinformatics. – 2019. – Vol. 20. – P. 225-235. Article Id: 579. DOI: 10.1186/s12859-019-3181-y.

2. Gagnidze, A. Novel Version of Merkle Cryptosystem [Text] / A. Gagnidze, M. Iavich, G. Iashvili // Bulletin of the Georgian National Academy of Sciences. – 2017. – Vol. 11, No. 4. – P. 28-33.

3. Lewis, P. A. W. A pseudo-random number generator for the System/360 [Text] / P. A. W. Lewis, A. S. Goodman and J. M Miller // IBM Systems Journal. – 1969. – Vol. 8, No. 2. – P. 136-146. DOI: 10.1147/sj.82.0136.

4. Lambić, D. Pseudo-random number generator based on discrete-space chaotic map [Text] / D. Lambić, M. Nikolić // Nonlinear Dyn. – 2017. – Vol. 90. – P. 223-232. DOI: 10.1007/s11071-017-3656-1.

5. Mcginthy, M. J. Further Analysis of PRNG-Based Key Derivation Functions [Text] / M. J. Mcginthy and A. J. Michaels // IEEE Access. – 2019. – Vol. 7. – P. 95978-95986. DOI: 10.1109/ACCESS.2019.2928768.

6. Wayne, Michael A. Low-bias high-speed quantum random number generator via shaped optical pulses [Text] / Michael A. Wayne, G. Paul Kwiat // Opt. Express. – 2010. – Vol. 18, Iss. 9. – P. 9351-9357. DOI: 10.1364/OE.18.009351.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

7. Herrero-Collantes, M. Quantum Random Number Generators [Text] / Miguel Herrero-Collantes, Carlos Garcia-Escartin // Reviews of Modern Physics. – 2017. – Vol. 87, Iss. 1. – Article Id: 015004. DOI: 10.1103/RevModPhys.89.015004.

8. Vacuum-based quantum random number generator using multi-mode coherent states [Text] / E. O. Samsonov, B. E. Pervushin, A. E. Ivanova et al. // Quantum Inf Process. – 2020. – Vol. 19. – P. 356-365. DOI: 10.1007/s11128-020-02813-3.

9. A simple low-latency real-time certifiable quantum random number generator [Text] / Y. Zhang, H. P. Lo, A. Mink et al. // Nature Communications. – 2021. – Vol. 12. – Article Id: 1056. DOI: 10.1038/s41467-021-21069-8.

10. Structures and Methods for Fully-Integrated Quantum Random Number Generators [Text] / F. Acerbi et al. // IEEE Journal of Selected Topics in Quantum Electronics. – 2020. – Vol. 26, Iss. 3. – P. 1-8. DOI: 10.1109/JSTQE.2020.2990216.

11. Quantum random number generation [Text] / X. Ma, X. Yuan, Z. Cao, et al. // npj Quantum Inf. – 2016. – Vol. 2. – Article Id: 16021. DOI: 10.1038/npjqi.2016.21.

12. High-speed and secure PRNG for cryptographic applications [Text] / Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev S., M. Iavich // International Journal of Computer Network and Information Security. – 2020. – Vol. 11, Iss. 3. – P. 1-10. DOI: 10.5815/ijcnis.2020.03.01.

13. Cang, S. Pseudo-random number generator based on a generalized conservative Sprott-A system [Text] / S. Cang, Z. Kang, & Z. Wang // Nonlinear Dyn. – 2021. – Vol. 104. – P. 827-844. DOI: 10.1007/s11071-021-06310-9.

14. Tuna, M. A. Novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation [Text] / M. A. Tuna // Analog Integr Circ Sig Process. – 2020. – Vol. 105. – P. 167-181. DOI: 10.1007/s10470-020-01703-z.

15. A Lightweight Pseudo-Random Number Generator Based on a Robust Chaotic Map [Text] / I. E. Hanouti, H. E. Fadili, W. Souhail and F. Masood // 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS). – 2020. – P. 1-6. DOI: 10.1109/ICDS50568.2020.9268715.

16. Shrimpton, T. A Provable-Security Analysis of Intel's Secure Key RNG [Text] / T. Shrimpton, R. S. Terashima // Advances in Cryptology - EUROCRYPT 2015. Lecture Notes in Computer Science. – 2015. – Vol. 9056. – P. 77-100. DOI: 10.1007/978-3-662-46800-5_4.

17. Chernov, P. S. Towards Self-testing Quantum Random Number Generators in Integrated Design [Text] / P. S. Chernov, V. S. Volkov, & D. A. Surovtsev // IOP Conference Series: Materials Science and Engineering. – 2018. – Vol. 454. – Article Id: 012087. DOI: 10.1088/1757-899X/454/1/012087.

18. Self-testing quantum random number generator [Text] / L. Tommaso, et al. // Physical review letters. – 2015. – Vol. 114, Iss. 15. – Article Id: 150501. DOI: 10.1103/PhysRevLett.114.150501.

19. Bowles, J. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices [Text]/ J. Bowles, M. T. Quintino, N. Brunner // Physical review letters. – 2014. – Vol. 112. – Article Id: 140407. DOI: 10.1103/PhysRevLett.112.140407.

20. Quantum randomness certified by the uncertainty principle [Text] / G. Vallone, D. G. Marangon, M. Tomasin, & P. Villoresi // Physical Review. – 2014. – Vol. A 90. – Article Id: 052327. DOI: 10.1103/PhysRevA.90.052327.

21. Random numbers certified by Bell's theorem [Text] / S. Pironio, A. Acín, S. Massar, et al. // Nature. – 2010. – Vol. 464. – P. 1021-1024. DOI: 10.1038/nature09008.

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

23. Realization of a quantum random generator certified with the Kochen-Specker theorem [Text] / A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, & A. Fedorov // Physical Review Letters. – 2017. – Vol. 119. – Article Id: 240501. DOI: 10.1103/PhysRevLett.119.240501.

24. Sutradhar, K. Hybrid Quantum Protocols for Secure Multiparty Summation and Multiplication [Text] / K. Sutradhar, H. Om // Scientific Reports. – 2020. – Vol. 10. – Article Id: 9097. DOI: 10.1038/s41598-020-65871-8.

25. Zhi-Gang, G. Improvement of Quantum Protocols for Secure Multi-Party Summation [Text] / G. Zhi-Gang // International Journal of Theoretical Physics. – 2020. – Vol. 59, Iss. 11. – P. 3086-3092. DOI: 10.1007/s10773-020-04555-5.

26. Ananth, P. Secure Quantum Extraction Protocols [Text] / P. Ananth, R. L. La Placa // Theory of Cryptography. TCC 2020. Lecture Notes in Computer Science. – 2020. - Vol. 12552. – P. 123-152. DOI: 10.1007/978-3-030-64381-2_5.

27. Meyer, J. J. A variational toolbox for quantum multi-parameter estimation [Text] / J. J. Meyer, J. Borregaard & J. A. Eisert // npj Quantum Information. – 2021. – Vol. 7. – Article Id: 89. DOI: 10.1038/s41534-021-00425-y.

28. Доценко, С. І. Інтелектуальні системи: пост-декартове представлення метазнань [Text] /

С. І. Доценко // Радіоелектронні і комп'ютерні системи. - 2020. – № 3(95). – С. 4-19. DOI: 10.32620/reks.2020.3.01.

29. Гордєєв О. О. Моделі та оцінювання якості зручності використання інтерфейсу програмного забезпечення для людино-комп'ютерної взаємодії [Text] / О. О. Гордєєв // Радіоелектронні і комп'ютерні системи. - 2020. – № 3(95). – С. 84-96. DOI: 10.32620/reks.2020.3.09.

30. High speed optical quantum random number generation [Text] / H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, H. Weinfurter // Opt. Express. - 2010. - Vol. 18, Iss. 12. - P. 13029-13037. DOI: 10.1364/OE.18.013029.

31. Massari, N. et al. 16.3 A 16×16 pixels SPAD-based 128-Mb/s quantum random number generator with −74dB light rejection ratio and −6.7ppm/°C bias sensitivity on temperature, 2016 IEEE International Solid-State Circuits Conference (ISSCC). – 2016. – P. 292-293, DOI: 10.1109/ISSCC.2016.7418022.

32. High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors [Text] / S. Tisa, F. Villa, A. Giudice, G. Simmerle and F. Zappa // IEEE Journal of Selected Topics in Quantum Electronics. – 2015. – Vol. 21, no. 3. – P. 23-29. Article Id: 6300107. DOI: 10.1109/JSTQE.2014.2375132.

References (BSI)

1. Kabiri Chimeh, M., Heywood, P., Pennisi, M. et al. Parallelisation strategies for agent based simulation of immune systems. *BMC Bioinformatics*, 2019, vol. 20, pp. 225-235, article id: 579. DOI: 10.1186/s12859-019-3181-y.

2. Gagnidze, A., Iavich, M., Iashvili, G. Novel Version of Merkle Cryptosystem. *Bulletin of the Georgian National Academy of Sciences*, 2017, vol. 11, no. 4, pp. 28-33.

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

4. Lambić, D., Nikolić, M. Pseudo-random number generator based on discrete-space chaotic map. *Nonlinear Dyn*, 2017, vol. 90, pp. 223-232. DOI: 10.1007/s11071-017-3656-1.

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

6. Wayne, Michael A., Kwiat, Paul G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express*, 2010, vol. 18, iss. 9, pp. 9351-9357. DOI: 10.1364/OE.18.009351.

7. Herrero-Collantes, Miguel., Garcia-Escartin, Carlos. Quantum Random Number Generators. *Reviews of Modern Physics*, 2017, vol. 87, iss. 1, article id: 015004. DOI: 10.1103/RevModPhys.89.015004.

8. Samsonov, E. O., Pervushin, B. E., Ivanova, A. E. et al. Vacuum-based quantum random number generator using multi-mode coherent states, *Quantum Inf Process*, 2020, vol. 19, pp. 356-365. DOI: 10.1007/s11128-020-02813-3.

9. Zhang, Y., Lo, H. P., Mink, A. et al. A simple low-latency real-time certifiable quantum random number generator. *Nature Communications*, 2021, vol. 12, article id: 1056. DOI: 10.1038/s41467-021-21069-8.

10. Acerbi, F. et al. Structures and Methods for Fully-Integrated Quantum Random Number Generators. *IEEE Journal of Selected Topics in Quantum Electronics*, 2020, vol. 26, iss. 3, pp. 1-8. DOI: 10.1109/JSTQE.2020.2990216.

11. Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. Quantum random number generation. *npj Quantum Inf*, 2016, vol. 2, article id: 16021, DOI: 10.1038/npjqi.2016.21.

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*, 2020, vol. 11, iss. 3, pp. 1-10. DOI: 10.5815/ijcnis.2020.03.01.

13. Cang, S., Kang, Z., Wang, Z. Pseudo-random number generator based on a generalized conservative Sprott-A system. *Nonlinear Dyn*, 2021, vol. 104, pp. 827-844. DOI: 10.1007/s11071-021-06310-9.

14. Tuna, M. A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation. *Analog Integr Circ Sig Process*, 2020, vol. 105, pp. 167-181. DOI: 10.1007/s10470-020-01703-z.

15. Hanouti, I. E., Fadili, H. E., Souhail, W., Masood, F. A Lightweight Pseudo-Random Number Generator Based on a Robust Chaotic Map, *Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, 2020, pp. 1-6, DOI: 10.1109/ICDS50568.2020.9268715.

16. Shrimpton, T., Terashima, R. S. A Provable-Security Analysis of Intel's Secure Key RNG. In: *Advances in Cryptology – EUROCRYPT*, 2015, vol. 9056, pp. 77-100. DOI: 10.1007/978-3-662-46800-5_4.

17. Chernov, P. S., Volkov, V. S., Surovtsev, D. A. Towards Self-testing Quantum Random Number Generators in Integrated Design. *IOP Conference Series: Materials Science and Engineering,* 2018, vol. 454, article id: 012087. DOI: 10.1088/1757-899X/454/1/012087.

18.Tommaso, L. et al. Self-testing quantum random number generator. *Physical review letters*, 2015,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

vol. 114, iss. 15, article id: 150501. DOI: 10.1103/PhysRevLett.114.150501.

19. Bowles, J., Quintino, M. T., Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Physical review letters*, 2014, vol. 112, article id: 140407. DOI: 10.1103/PhysRevLett.112.140407.

20. Vallone, G., Marangon, D. G., Tomasin, M., Villoresi, P. Quantum randomness certified by the uncertainty principle. *Physical Review*, 2014, vol. A 90, article id: 052327. DOI: 10.1103/PhysRevA.90.052327.

21. Pironio, S., Acín, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., Monroe, C. Random numbers certified by Bell's theorem. *Nature*, 2010, vol. 464, pp. 1021-1024. DOI: 10.1038/nature09008.

22. Vazirani, U. V., Vidick, T., Certifiable Quantum Dice-Or, testable exponential randomness expansion. *arXiv preprint arXiv*, 2011, arXiv: 1111.6054.

23. Kulikov, A., Jerger, M., Potočnik, A., Wallraff, A., Fedorov, A. Realization of a quantum random generator certified with the Kochen-Specker theorem. *Physical Review Letters*, 2017, vol. 119, article id: 240501. DOI: 10.1103/PhysRevLett.119.240501.

24. Sutradhar, K., Om, H. Hybrid Quantum Protocols for Secure Multiparty Summation and Multiplication. *Sci Rep*, 2020, vol, 10, article id: 9097. DOI: 10.1038/s41598-020-65871-8.

25. Zhi-Gang, G. Improvement of Quantum Protocols for Secure Multi-Party Summation. *Int J Theor Phys,* 2020, vol. 59, iss. 11, pp. 3086-3092. DOI: 10.1007/s10773-020-04555-5.

26. Ananth, P., La Placa, R. L. Secure Quantum Extraction Protocols. *Theory of Cryptography. TCC 2020. Lecture Notes in Computer Science*, 2020, vol. 12552, pp. 123-152. DOI: 10.1007/978-3-030-64381-2_5.

27. Meyer, J. J., Borregaard, J., Eisert, J. A variational toolbox for quantum multi-parameter estimation. *npj Quantum Information*, 2021, vol. 7, article id: 89, DOI: 10.1038/s41534-021-00425-y.

28. Dotsenko, S. Intelektual'ni systemy: postdekartove predstavlennya metaznan' [Intelligent systems: post-descartes representing metaknowledge]. *Radioelectronic and computer systems*, 2021, no. 3(95), pp. 4-19. DOI: 10.32620/reks.2020.3.01.

29. Gordieiev, O. Modeli ta otsinyuvannya yakosti zruchnosti vykorystannya interfeysu prohramnoho zabezpechennya dlya lyudyno-komp"yuternoyi vzayemodiyi [A models and assessment of quality of human-computer interaction software interface usability]. *Radioelectronic and computer systems*, 2020, no. 3(95), pp. 84-96. DOI: 10.32620/reks.2020.3.09.

30. Fürst, H., Weier, H., Nauerth, S., Marangon, D. G., Kurtsiefer, C, Weinfurter, H. High speed optical quantum random number generation. *Opt. Express*, 2010, vol. 18, iss. 12, pp. 13029-13037. DOI: 10.1364/OE.18.013029.

31. Massari, N. et al. 16.3 A 16×16 pixels SPAD-based 128-Mb/s quantum random number generator with −74dB light rejection ratio and −6.7ppm/°C bias sensitivity on temperature. *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, 2016, pp. 292-293, DOI: 10.1109/ISSCC.2016.7418022.

32. Tisa S., Villa F., Giudice A., Simmerle G. and Zappa F. High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, vol. 21, no. 3, pp. 23-29, article Id: 6300107. DOI: 10.1109/JSTQE.2014.2375132.

Надійшла до редакції 16.07.2021 розглянута на редколегії 26.11.2021

ГІБРИДНИЙ КВАНТОВИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ ДЛЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

М. Явіч, Т. Кучухідзе, Г. Іашвілі, С. Гнатюк

Предмет статті – генератори псевдовипадкових чисел. Випадкові числа відіграють важливу роль в криптографії. Використання небезпечних генераторів псевдовипадкових чисел дуже розповсюджена вразливість. Випадкові числа також мають фундаментальне значення для науки і техніки. Існують алгоритмічно згенеровані числа, які схожі на випадкові розподілення, але насправді не являються випадковими, та називаються генераторами псевдовипадкових чисел. У багатьох випадках вирішувані задачі базуються на непередбачуваності випадкових чисел, що не може бути гарантовано у випадку генераторів псевдовипадкових чисел, де вимагається істинна випадковість. У таких ситуаціях ми використовуємо справжні генератори випадкових чисел, джерелом випадковості яких є непередбачувані випадкові події. Квантові генератори випадкових чисел (QRNG) генерують реальні випадкові числа на основі притаманної квантовим вимірам випадковості. **Мета** дослідження - розробити математичну модель генератора, яка генерує швидкі випадкові числа з найменшими витратами. У той же час, дуже важливий високий рівень випадковості. За допомогою кванто-

вої механіки ми можемо отримати істинні числа, використовуючи непередбачувану поведінку фотона, який являється основою багатьох сучасних криптографічних протоколів. Дуже важливо довіряти криптографічним генераторам випадкових чисел для отримання тільки істинних випадкових чисел. Ось чому необхідні методи сертифікації, які будуть перевіряти як роботу пристрою, так і якість генерованих випадкових бітів. **Метою** дослідження також є розробка моделі нового методу напівавтоматичної сертифікації для генераторів квантових випадкових чисел (QRNG). **Вирішувані завдання** полягають у створенні математичної моделі генератора випадкових чисел, який генерує швидкі випадкові числа з найменшими витратами. Створити математичну модель нового методу сертифікації напівсамотестування для генераторів квантових випадкових чисел. Інтегрувати новий метод напівавтоматичної сертифікації у новий генератор випадкових чисел. **Методи** – це математична оптимізація та моделювання. Були отримані наступні **результати**: ми представляємо вдосконалений новий квантовий генератор випадкових чисел, який базується на часі прибуття QRNG. В статті пропонується модель нового напівсамотестуючого методу сертифікації для генераторів квантових випадкових чисел (QRNG). Цей метод поєднує в собі різні типи підходів до сертифікації, є достатньо безпечним та ефективним. Новий метод сертифікації був інтегрований в модель нового квантового генератора випадкових чисел. **Висновки**. Наукова новизна отриманих результатів полягає в наступному: 1. Запропонований новий квантовий генератор випадкових чисел, який базується на часі прибуття QRNG. Він використовує спрощену версію детекторів з невеликими вимогами. Новий QRNG виробляє більше одного випадкового біта при кожному виявленні фотона. Він достатньо ефективний та має високий рівень випадковості. 2. Пропонується новий метод сертифікації напівсамотестування для генераторів квантових випадкових чисел (QRNG). Аналізуються методи самотестування, а також методи генерації квантових випадкових чисел, які не залежать від пристрою. Виявлені переваги та недоліки обох методів. На основі отриманих результатів пропонується новий метод. 3. Новий метод напівсамотестування для квантових генераторів випадкових чисел інтегрований в запропоновану модель квантового генератора випадкових чисел. В статті аналізується його безпечність та ефективність. В статті пропонується використовувати новий генератор випадкових чисел в криптосхемах.

Ключові слова: криптографія; квантова; квантова криптографія; генератор випадкових чисел; квантовий генератор випадкових чисел; новий квантовий генератор випадкових чисел; сертифікація; новий метод сертифікації.

ГИБРИДНЫЙ КВАНТОВЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

М. Явич, Т. Кучухидзе, Г. Иашвили, С. Гнатюк

Предмет статьи - генераторы псевдослучайных чисел. Случайные числа играют важную роль в криптографии. Использование небезопасных генераторов псевдослучайных чисел очень распространенная уязвимость. Это также является фундаментальным ресурсом в науке и технике. Существуют алгоритмически сгенерированные числа, которые похожи на случайные распределения, но на самом деле не являются случайными, и называются генераторами псевдослучайных чисел. Во многих случаях решаемые задачи основаны на непредсказуемости случайных чисел, что не может быть гарантировано в случае генераторов псевдослучайных чисел, для этого требуется истинная случайность. В таких ситуациях мы используем настоящие генераторы случайных чисел, источником случайности которых являются непредсказуемые случайные события. Квантовые генераторы случайных чисел (QRNG) генерируют реальные случайные числа на основе присущей квантовым измерениям случайности. **Цель** состоит в том, чтобы разработать математическую модель генератора, который генерирует быстрые случайные числа с наименьшими затратами. В то же время важен высокий уровень случайности. С помощью квантовой механики мы можем получить истинные числа, используя непредсказуемое поведение фотона, которое является основой многих современных криптографических протоколов. Важно доверять криптографическим генераторам случайных чисел для генерации только истинных случайных чисел. Вот почему необходимы методы сертификации, которые будут проверять как работу устройства, так и качество генерируемых случайных битов. **Целью** исследования также является разработка модели нового метода полуавтоматической сертификации для генераторов квантовых случайных чисел (QRNG). Решаемые задачи заключаются в создании математической модели генератора случайных чисел, который генерирует быстрые случайные числа с наименьшими затратами. Создать математическую модель нового метода сертификации полусамотестирования для генераторов квантовых случайных чисел. Интегрировать новый метод полуавтоматической сертификации в новый генератор случай-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ных чисел. Используемые методы — это математическая оптимизация и моделирование. Были получены следующие результаты: мы представляем усовершенствованный новый квантовый генератор случайных чисел, который основан на QRNG по времени прибытия. В статье предлагается модель нового метода сертификации полусамотестирования для генераторов квантовых случайных чисел (QRNG). Этот метод сочетает в себе разные типы подходов к сертификации, является достаточно безопасным и эффективным. Наконец, новый метод сертификации интегрирован в модель нового квантового генератора случайных чисел. **Выводы.** Научная новизна полученных результатов заключается в следующем: 1. Предложен новый квантовый генератор случайных чисел, основанный на времени прибытия QRNG. Он использует упрощенную версию детекторов с небольшими требованиями. Новый QRNG производит более одного случайного бита при каждом обнаружении фотона. Он достаточно эффективен и имеет высокий уровень случайности. 2. Предлагается новый метод сертификации полусамотестирования для генераторов квантовых случайных чисел (QRNG). **Анализируются методы** самотестирования, а также методы генерации квантовых случайных чисел, не зависящие от устройства. Выявлены достоинства и недостатки обоих методов. На основании полученных результатов предлагается новый метод. 3. Новый метод полусамотестирования для квантовых генераторов случайных чисел интегрирован в предлагаемую модель квантового генератора случайных чисел. В статье анализируется безопасность и эффективность. В статье предлагается использовать новый генератор случайных чисел в криптосхемах.

Ключевые слова: криптография; квантовая; квантовая криптография; генератор случайных чисел; квантовый генератор случайных чисел; новый квантовый генератор случайных чисел; сертификация; новый метод сертификации.

Явич Максим – д-р наук, проф., руководитель направления кибербезопасности, Кавказский университет, Тбилиси, Грузия.

Кучухидзе Тамар – канд. техн. наук, докторант, Грузинский технический университет, Тбилиси, Грузия.

Иашвили Гиоргий – лектор, исследователь, Кавказский университет, Тбилиси, Грузия.

Гнатюк Сергей – главный исследователь R&D Lab; д-р наук, проф., проф. каф. безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Maksim Iavich – D.Sc., Professor, head of cyber security direction, Caucasus University, Tbilisi, Georgia,
e-mail: miavich@cu.edu.ge, ORCID: 0000-0002-3109-7971.

Tamari Kuchukhidze – PhD candidate, Georgian technical university, Tbilisi, Georgia,
e-mail: tamari.kuchukhidze@gmail.com, ORCID: 0000-0003-1997-465X.

Giorgi Iashvili – Lecturer, researcher, Caucasus university, Tbilisi, Georgia,
e-mail: giiashvili@cu.edu.ge, ORCID: 0000-0002-1855-2669.

Sergiy Gnatyuk – Lead Researcher in Cybersecurity R&D Lab; Doctor of Sciences (Cybersecurity), Professor in IT-Security Academic Dept at National Aviation University, Kyiv, Ukraine,
e-mail: s.gnatyuk@nau.edu.ua, ORCID: 0000-0003-4992-0564.