NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2017, 8 (4), P. 441–446

Fiber quantum random number generator, based on vacuum fluctuations

A. E. Ivanova, S. A. Chivilikhin, G. P. Miroshnichenko, A. V. Gleim

ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia

newiva@mail.ru, sergey.chivilikhin@gmail.com, gpmirosh@gmail.com, aglejm@yandex.ru

PACS 03.67.-a **DOI 10.17586/2220-8054-2017-8-4-441-446**

Quantum random number generation allows one to obtain the absolutely random sequences by using nondeterministic physical processes. Fluctuations of the vacuum, recorded by homodyne detection, can be one of the entropy sources in those generators. In this paper, a system of quantum random numbers generation, based on vacuum fluctuations and using a fiber Y-splitter is presented.

Keywords: quantum random number generation, beam splitter, Y-splitter, vacuum fluctuations.

Received: 2 July 2017

Revised: 28 July 2017

1. Introduction

Random number generators based on various sources of entropy are used in many branches of science and technology. The use of nondeterministic physical processes enables one to obtain true random sequences that can be utilized in applications where a high degree of randomness is necessary, such as cryptography both classical and quantum [1]. Quantum processes, in which randomness is determined by fundamental physical principles, can be used as a source of entropy for physical generators of random numbers.

Single photon detectors are required for most parts of quantum random number generators (QRNG), which use the spatial [2, 3] or the time [4, 5] mode as a source of entropy. This leads to the fact that the speed characteristics of these systems are limited. The same problem arises in schemes based on measuring the number of photons in radiation [6, 7]. QRNG based on vacuum fluctuations [8–11] allow one to obtain true random sequences without using single photon detection and, accordingly, with lower limitations of speed characteristics.

A QRNG scheme based on vacuum fluctuations was patented in 2007 [8]. The operation principle of this generator type is the extraction of randomness from quantum noise obtained after subtracting signals from the beam splitter outputs on the balanced detector. A coherent state is sent by a laser to first of beam splitter inputs vacuum state – to second, then these two signals are mixed at a beam splitter and output signals goes to balanced detector, where they are subtracted from each other. The obtained resulting signal is quantum noise which can be transformed into a random sequence by postprocessing. The main advantage of this scheme is the measurement of quantum states by classical detectors which is utilized in homodyne detection.

A similar QRNG with a speed of 6.5 Mbit/s [9] was demonstrated in 2010; the sequences were processed by using a cryptographic hash function. In the same year, another group of researchers achieved a generation rate of 12 Mbit/s, data was cleared from electrical noise by postprocessing [10]. A system that allows one to achieve the generation rate of 2 Gbit/s was created in 2011 [11]. In that work, two methods of postprocessing (one of them with protection against extraneous interference) were used. In all works listed above, beam splitters with two input ports and two output ports were used.

The purpose of our research was development of the fiber device for high-speed random number generation based on vacuum fluctuations that can be used in a subcarrier quantum communication system [12].

2. Theoretical modeling

In works [9–11], using beam splitters with four ports (Fig. 1a) a separate port is used to enter vacuum states. For the scheme that we use the Y-splitter acts as the splitter of radiation (Fig. 1b).

The advantages of using the Y-splitter are following: compactness of the final device, possibility of integration with solutions based on fiber optics, implementation of high-speed devices created from integrated elements and, in the future, integrated circuits.

We compared the mathematical description of the beam splitter with two input ports and two output ports with a mathematical description of the Y-splitter to analyze the possibility of applying Y-splitter in the experimental QRNG based on vacuum fluctuations.

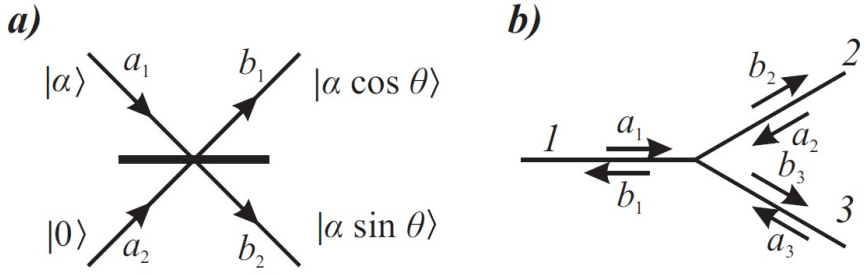

FIG. 1. a) Scheme of a beam splitter with angle θ, where to the first splitter input a coherent state is sent, and to other input - a vacuum state. b) Optical Y-splitter. a_1, a_2, a_3 – operators arriving at the 1st, 2nd and 3rd ports, respectively, b_1, b_2, b_3 – operators at the outputs of the splitter

In case if input signal a_1 that can be characterized by coherent state $|\alpha\rangle$ with parameter α is sent to one of the beamsplitter inputs and vacuum state $|0\rangle$ is sent to other input port, then output signals can be characterized by Poisson distribution: with parameter $|a\cos\theta\rangle$ at first output of beam splitter and with parameter $|a\sin\theta\rangle$ at the second output.

If beam splitter is symmetrical ($\theta = \pi/4$), then we obtain expression, describing signals B_1 and B_2 at both outputs:

$$B_1 = B_2 = \frac{1}{\sqrt{2}} A_1. \tag{1}$$

The fiber splitter (Fig. 1b) has been presented as a system with three inputs and three outputs as signal in each of the ports can be distributed in two opposite directions. Relations between input and output operators of Y-splitter were derived by using a matrix description, allowing us to show the interaction between each pair of signals:

$$\begin{pmatrix} b_1^+ \\ b_2^+ \\ b_3^+ \end{pmatrix} = \begin{pmatrix} -\sqrt{1-2\lambda^2} & \beta & \beta \\ \lambda & -\gamma & \sqrt{1-\beta^2-\gamma^2} \\ \lambda & \sqrt{1-\beta^2-\gamma^2} & -\gamma \end{pmatrix} \begin{pmatrix} a_1^+ \\ a_2^+ \\ a_3^+ \end{pmatrix}. \tag{2}$$

where λ is proportionality factor, connecting input signal at 1st port with output signals at 2nd and 3rd ports; β connects input signals at 2nd or 3rd ports with output signal at 1st port; γ connects input and output signals of 2nd or 3rd port. According to the unitarity conditions for the parameters of the matrix described above the following relations must be satisfied:

$$\begin{cases} -\sqrt{1-2\lambda^2}\beta - \lambda\gamma + \lambda\sqrt{1-\beta^2-\gamma^2} = 0, \\ \beta^2 - 2\gamma\sqrt{1-\beta^2-\gamma^2} = 0. \end{cases} \tag{3}$$

Solving the system, we get the following parameter values: $\lambda = \sqrt{2\gamma(1-\gamma)}$, $\beta = -\sqrt{2\gamma(1-\gamma)}$, so equation (2) takes the following form:

$$\begin{pmatrix} b_1^+ \\ b_2^+ \\ b_3^+ \end{pmatrix} = \begin{pmatrix} 1-2\gamma & -\sqrt{2\gamma(1-\gamma)} & -\sqrt{2\gamma(1-\gamma)} \\ \sqrt{2\gamma(1-\gamma)} & -\gamma & 1-\gamma \\ \sqrt{2\gamma(1-\gamma)} & 1-\gamma & -\gamma \end{pmatrix} \begin{pmatrix} a_1^+ \\ a_2^+ \\ a_3^+ \end{pmatrix}. \tag{4}$$

We also calculated some statistical parameters of signal at the outputs of the scheme, using a Y-splitter. Photon birth operators at outputs of ports 1, 2 and 3 can be described as follows:

$$b_1^+ = (1-2\gamma)a_1^+ - \sqrt{2\gamma(1-\gamma)}(a_2^+ + a_3^+), \tag{5}$$

$$b_2^+ = \sqrt{2\gamma(1-\gamma)}a_1^+ - \gamma\alpha_2^+ + (1-\gamma)a_3^+, \tag{6}$$

$$b_3^+ = \sqrt{2\gamma(1-\gamma)}a_1^+ + (1-\gamma)\alpha_2^+ - \gamma a_3^+. \tag{7}$$

Since a coherent state is sent to the first port of the splitter, and to ports 2 and 3 – a vacuum state $|0\rangle$, then the average number of photons at outputs of the Y-splitter can be described by these expressions:

$$\overline{n_{1out}} = \langle 0|_3\langle 0|_2\langle\alpha|_1 \left((1-2\gamma)a_1^+ - \sqrt{2\gamma(1-\gamma)}(a_2^+ + a_3^+)\right) \times \\ \left((1-2\gamma)a_1 - \sqrt{2\gamma(1-\gamma)}(a_2 + a_3)\right)|\alpha\rangle_1|0\rangle_2|0\rangle_3 = (1-2\gamma)^2\alpha^2, \tag{8}$$

$$\overline{n_{2out}} = \langle 0|_3\langle 0|_2\langle \alpha|_1 \left(\sqrt{2\gamma(1-\gamma)}a_1^+ - \gamma\alpha_2^+ + (1-\gamma)a_3^+\right) \times \left(\sqrt{2\gamma(1-\gamma)}a_1 - \gamma\alpha_2^(1-\gamma)a_3\right)|\alpha\rangle_1|0\rangle_2|0\rangle_3 = 2\gamma(1-\gamma)\alpha^2, \quad (9)$$

$$\overline{n_{3out}} = \langle 0|_3\langle 0|_2\langle \alpha|_1 \left(\sqrt{2\gamma(1-\gamma)}a_1^+ + (1-\gamma)\alpha_2^+ - \gamma a_3^+\right) \times \left(\sqrt{2\gamma(1-\gamma)}a_1 + (1-\gamma)\alpha_2 - \gamma a_3\right)|\alpha\rangle_1|0\rangle_2|0\rangle_3 = 2\gamma(1-\gamma)\alpha^2. \quad (10)$$

The differential current operator Δi can be characterized as follows:

$$\Delta i = k_2 b_2^+ b_2 - k_3 b_3^+ b_3, \quad (11)$$

where k_1, k_2 – quantum efficiencies of 1st and 2nd detectors.

In the case of detectors with different quantum efficiencies, the average value of the difference current $\langle \Delta i \rangle$ is:

$$\langle \Delta i \rangle = \langle 0|_3\langle 0|_2\langle \alpha|_1 (k_2 b_2^+ b_2 - k_3 b_3^+ b_3)|\alpha\rangle_1|0\rangle_2|0\rangle_3 = 2\gamma(1-\gamma)(k_2 - k_3)\alpha^2. \quad (12)$$

The dispersion of the differential current $D(\Delta i)$ and mean square deviation of the differential current δi from the average value can be described by the following expression:

$$D(\Delta i) = 2\gamma(1-\gamma)(k_2^2 + k_3^2)\alpha^2, \quad (13)$$

$$\delta i = \alpha\sqrt{2\gamma(1-\gamma)(k_2^2 + k_3^2)}. \quad (14)$$

In the case where the signal coming from the first port is distributed only between the outputs of ports 2 and 3 of the Y-splitter, $\gamma = 1/2$. Then, the relationship between each pair of operators at the input and at the output from the system can be displayed using the following expression:

$$\begin{pmatrix} b_1^+ \\ b_2^+ \\ b_3^+ \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} a_1^+ \\ a_2^+ \\ a_3^+ \end{pmatrix}. \quad (15)$$

If we send input signal to first port only, then signals B_2 and B_3 at outputs of ports 2 and 3 can be described by the following expression:

$$B_2 = B_3 = \frac{1}{\sqrt{2}} A_1. \quad (16)$$

We can see that the signals obtained at the outputs of the beam splitter with four ports, when laser and vacuum signals were sent to inputs, coincide with signals obtained at the outputs of the Y-splitter. In this particular case, the average numbers of photons at the Y-splitter outputs are:

$$\overline{n_{1out}} = 0, \quad (17)$$

$$\overline{n_{2out}} = \overline{n_{3out}} = \frac{1}{2}\alpha^2. \quad (18)$$

In the case of detectors with different quantum efficiencies, the average value of the differential current, the dispersion, and the mean square deviation of the differential current from the mean value can be expressed as follows:

$$\langle \Delta i \rangle = \frac{1}{2}(k_2 - k_3)\alpha^2, \quad (19)$$

$$D(\Delta i) = \frac{1}{2}(k_2^2 + k_3^2)\alpha^2, \quad (20)$$

$$\delta i = \alpha\sqrt{\frac{1}{2}(k_2^2 + k_3^2)}. \quad (21)$$

The above described calculations were carried out for a symmetric Y-splitter. Since experimental devices do not have an ideal symmetry, it is necessary to consider the asymmetric case. We can describe the relationship between of the vector of the input signals A and the vector of the output signals B via the sum of the conversion matrix U

indicated in (15) and the matrix $\widetilde{U}$ describing the small perturbations on the system. We consider the case when the matrix $\widetilde{U}$ is real.

$$B = (U + \widetilde{U})A, \tag{22}$$

$$\begin{pmatrix} b_1^+ \\ b_2^+ \\ b_3^+ \end{pmatrix} = \left(\begin{pmatrix} 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} + \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} \right) \begin{pmatrix} a_1^+ \\ a_2^+ \\ a_3^+ \end{pmatrix}. \tag{23}$$

To observe the unitarity conditions obtained by summing the matrix, it is necessary in the linear approximation for u_{ij} to satisfy the condition:

$$\begin{cases} u_{31} = -u_{21}, \\ u_{32} = \sqrt{2}u_{12} + u_{22}, \\ u_{33} = \sqrt{2}u_{12} + u_{22} - \sqrt{2}u_{21}, \\ u_{11} = -\sqrt{2}u_{21} + \sqrt{2}u_{12} + 2u_{22}, \\ u_{23} = u_{22} - \sqrt{2}u_{21}, \\ u_{13} = -u_{12}. \end{cases} \tag{24}$$

The changes of signals, receiving on the outputs of Y-splitter ports 2 and 3, are affected by the components u_{21} and u_{31} due to asymmetry. From the expressions described above it is clear that these elements of the matrix $\widetilde{U}$ are the same in absolute value, but they are different in sign.

In the asymmetric case, the average numbers of photons at the outputs of the Y-splitter are:

$$\overline{n_{1out}} = 0, \tag{25}$$

$$\overline{n_{2out}} = \left(\frac{1}{2} + \sqrt{2}u_{21}\right)\alpha^2, \tag{26}$$

$$\overline{n_{3out}} = \left(\frac{1}{2} + \sqrt{2}u_{31}\right)\alpha^2. \tag{27}$$

In the case of detectors with different quantum efficiencies, the average value of the difference current, dispersion of the differential current, and mean square deviation of the differential current from the average value can be described by the following expressions:

$$\langle \Delta i \rangle = \left(\frac{1}{2} + 2\sqrt{2}u_{21}\right)(k_2 - k_3)\alpha^2, \tag{28}$$

$$D(\Delta i) = \left(\frac{1}{2}(k_2^2 + k_3^2) + \sqrt{2}(k_2^2 - k_3^2)u_{21}\right)\alpha^2, \tag{29}$$

$$\delta i = \alpha\sqrt{\frac{1}{2}(k_2^2 + k_3^2) + \sqrt{2}(k_2^2 - k_3^2)u_{21}}. \tag{30}$$

The practical possibility of generating true random numbers by QRNG based on vacuum fluctuations and using Y-splitter was confirmed experimentally.

3. Experimental setup and postprocessing

The scheme of our experimental setup is represented in Fig. 2. We used a 10 mW 1550 nm Teraxion-NLL laser (L). After passing fiber optical isolator (OI), based on the Faraday Effect (isolation $\geq$ 28 dB at 1550 nm), to reflections neutralization, and attenuator (A) the radiation goes to fiber Y-splitter with dividing coefficient 50/50. Two p-i-n photodiodes (fid13z81pz) with quantum efficiencies of 60 % at 1550 nm, sensitivity $S = 0.75$ A/W, and a 1 GHz bandwidth were used as detectors (D1, D2). The currents from two photodiodes are subtracted in electronic processing system (EP) and then resulting signal is amplified. Amplification circuit contains amplifier OPA847 (Texas Instruments) in a transimpedance configuration with a gain of 4 $k\Omega$. All components are located on a specially designed board. The frequency band of the circuit is 100 MHz. The bandwidth of the oscilloscope Tektronix dpo70604c (ADC) used to digitize the received noise is 6 GHz. After digitization, we can use various post-processing (PP) algorithms to convert true random quantum noise into a sequence of random bits.

If the initial power of laser radiation is on the order of 10 mW, power of the difference signal amplitude is about 0.1–1 μW. If we take into account the sensitivity of photodiodes, difference current is about 0.1–1 μA.

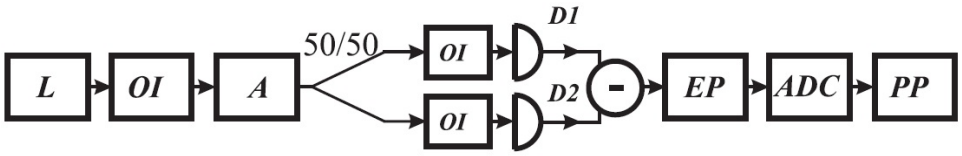

FIG. 2. Block diagram of the experimental setup. L – laser, OI – optical isolator, A – attenuator, D1, D2 – detectors, EP – electronic processing system, ADC – analog-to-digital converter, PP – postprocessing system

Since we used an amplifying scheme with one cascade gain of 4 kΩ, value of the final difference signal after amplification is on the order of mV.

During our research, a linear relationship between the intensity of laser radiation and the level of mean noise deviation was observed, that confirms that noise has a quantum nature. Quantum noise (Fig. 3a) obtained from our system had the following characteristics: mean value of fluctuations $\mu = 7 \cdot 10^{-6}$, standard deviation $\sigma = 0.2$, asymmetry coefficient $S = \mu_3/\sigma^3 = 0.01$ (where μ_3 – third central moment of the noise distribution), kurtosis (a measure of sharpness of the random variable maximum) $K = \frac{\mu_4}{\sigma^4} = -4.5 \cdot 10^{-3}$ (where μ_4 – fourth central moment of the noise distribution), probability of the most likely outcome $\max(P_i) = 3.19 \cdot 10^{-3}$ (where P_i – probability of the i-th realization of random discrete variable), min-entropy $H_{min} = -\log_2(\max(P_i)) = 8.29$.

The time dependence of obtained noise, probability distribution of noise at a mean level, autocorrelation function, and noise spectrum are shown in Fig. 3.

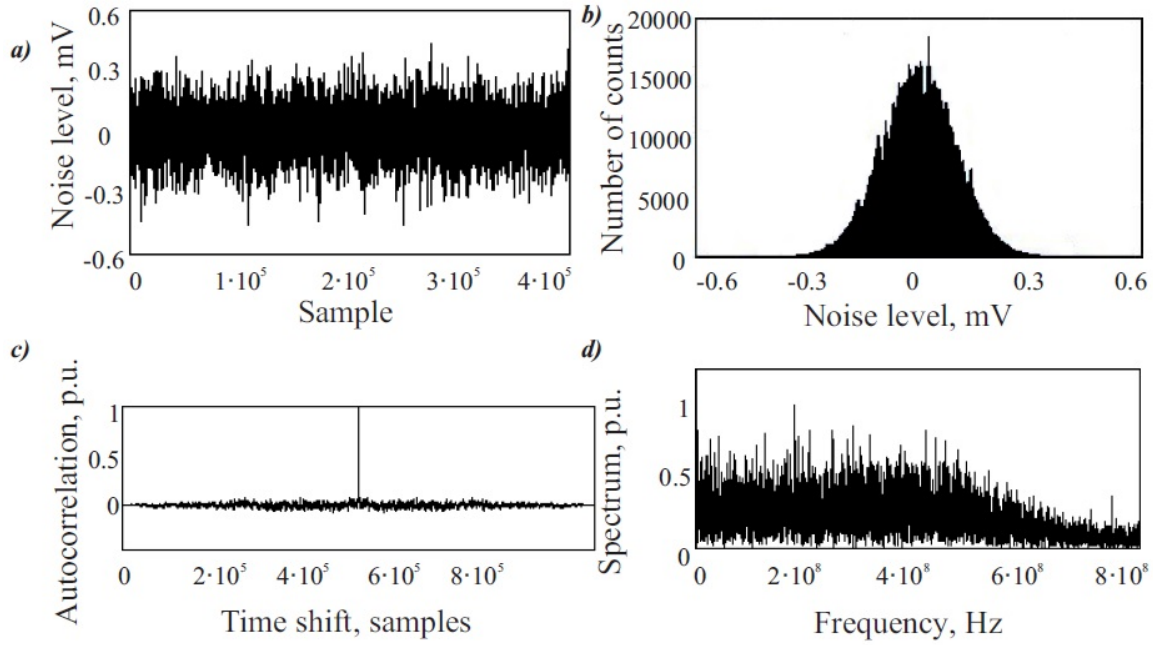

FIG. 3. a) Time dependence of obtained noise; b)Probability distribution of noise at a certain level; c) Autocorrelation function; d) Noise spectrum

During experiments, it was shown that asymmetry of fiber splitter, expressed as a change in a length of one arm of the Y-splitter, has a negative impact on the balancing of detection. For the processing of noise obtained by experimental QRNG and based on vacuum fluctuations and using a Y-splitter, we used four different conversion methods:

"A": If noise level in count is above 0, then we write resulting bit "1", else – "0". Number of counts coincides with number of bits in resulting sequence;

"B": We divide sequence of bits was obtained by method "A" into two subsequences with equal length. Then we apply XOR to all pairs of elements with same index of both subsequences and write result of this operation to resulting sequence. The generation rate is twice smaller that in method "A", but bias between "0" and "1" bits (asymmetry of the beamsplitter may be reason for its appearance) decreases;

"C": We generate three bits from one sample [11] (convert initial Gaussian distribution to uniform distribution, applying Gaussian error function). All experimental counts are dividing to eight possible noise intervals with the same probability, each interval is coding by three bits, that allows us to increase generation rate;
"D": After analog-to-digital conversion we can discard most significant bits of digitized value of noise amplitude. Initial probability of counts being in a certain noise level is Gaussian, but when we discard most significant bits, probability is approaching to uniform distribution. This method, as the previous one, allows one to increase generation rate by extracting few bits from one count.

If we know the probabilistic properties of a true random sequence, then we can check the degree of similarity between generated sequence and random sequence. For this purpose, we performed a series of tests [13] (monobit, twobit, "poker", autocorrelation test, and runs test), and then compared their results for an ideal and experimental sequence. Results of randomness tests applied to sequences, obtained by four different post processing techniques were given in detail in [14].The results of a series of tests showed that optimal post processing technique is discarding two or three most significant bits.

4. Conclusion

In this research, we developed a quantum description of the Y-splitter in the QRNG based on fluctuations in the vacuum. The statistical parameter values of the differential current at the circuit output were obtained. We consider four postprocessing methods to convert experimental samples to bits, and after testing, we conclude that the optimal post processing technique for our system is discarding two or three most significant bits after analog-to-digital conversion.

Acknowledgements

This work was financially supported by Government of Russian Federation, Grant 074-U01 and by the Ministry of Education and Science of Russian Federation (project No. 14.578.21.0112 No 02.G25.31.0229).

References

[1] Scarany V., Bechmann-Pasquinucci H. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 2009, **81**, P. 1301–1350.
[2] Jennewein T., Achleitner U. et al. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, 2000, **71**(4), P. 1675–1680.
[3] Stefanov A., Gisin N. et al. Optical quantum random number generator. *Journal of Modern Optics*, 2000, **47**, P. 595–598.
[4] Dynes J. F., Yuan Z. L, et al. A high speed, post-processing free, quantum random number generator. *Appl. Phys. Lett.*, 2008, **93**, P. 031109.
[5] Wahl M. et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 2011, **98**, P. 171105.
[6] Furst H. et al. High speed optical quantum random number generation. *Optics express*, 2010, **18**, P. 13029–13037.
[7] Applegate M. et al. Efficient and robust quantum random number generation by photon number detection. *Applied Physics Letters*, 2015, **107**, P. 071106.
[8] Trifonov A. and Vig H. Quantum noise random number generator, U.S. Patent N 7284024. 2007. B1.
[9] Gabriel C., Wittmann C. et al. A generator for unique quantum random numbers based on vacuum states. *Nature Phot.*, 2010, **4**, P. 711–715.
[10] Shen Y., Tian L.,Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A*, 2010, **81**, P. 063814.
[11] Symul T. ,Assad S. M., Lam P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.*, 2011, **98**, P. 231103.
[12] Gleim A. V., Egorov V. I. et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics Express*, 2016, **24**(3), P. 2619–2633.
[13] Menezes A., van Oorschot P. , Vanstone S. *Handbook of Applied Cryptography*. CRC Press., 1996, 816 p.
[14] Ivanova A. E, Chivilikhin S. A, Gleim A. V. Quantum random number generator based on homodyne detection. *Nanosystems: Physics, Chemistry, Mathematics*, 2017, **8**(2), P. 239–242.