NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2015, 6 (1), P. 95–99

ON THE POSSIBILITY OF USING OPTICAL Y-SPLITTER IN QUANTUM RANDOM NUMBER GENERATION SYSTEMS BASED ON FLUCTUATIONS OF VACUUM

A. E. Ivanova, S. A. Chivilikhin, I. Yu. Popov, A. V. Gleim
ITMO University, St. Petersburg, Russia
newiva@mail.ru, sergey.chivilikhin@gmail.com, popov1955@gmail.com, aglejm@yandex.ru

PACS 03.67.-a **DOI 10.17586/2220-8054-2015-6-1-95-99**

Quantum random number generation allows the obtaining of true random numbers that can be used for applications (e.g.,a cryptography) requiring a high degree of randomness. In this paper, we give a mathematical description of a quantum random number generation system using homodyne detection. As a result of the theoretical research, we obtained the description of the relationship between beam splitter input radiation and differential current on detectors after beam splitting. We derived equations allowing one to estimate the scheme parameters imperfection impact on measurement results. We also obtained mathematical expressions, demonstrating the equivalence of quantum description of Y-splitter and beam splitter with two inputs, which allows the use Y-splitter for the implementation of quantum random number generation systems based on vacuum quantum fluctuations.

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

Received: 27 November 2014 Revised: 20 December 2014

1. Introduction

Random numbers are widely used in classical and quantum cryptography. Perfect randomness is very important for quantum cryptography protocols (see, e.g., [1]), but it is rather difficult to obtain ideally random numbers in real devices. In principle, there are two means to achieve this. The first, one uses special computer algorithms, however, this way leads only to pseudo-random numbers. The second way is to use physical systems with inherent random behavior. It is preferable to have fundamental character of this randomness. The quantum random number generator (QRNG) is one such type of device. Accordingly, QRNG can be divided into several groups, depending upon the physical phenomenon serving as the background for the device: beam separation [2–4], entangled photon states [5, 6], processes of photon emission and detection [7, 8], quantum noise of lasers [9, 10], vacuum fluctuations of the electromagnetic field [11].

2. Quantum random number generation based on the principles of homodyne detection

This type of QRNG is based on the randomness of the quantum noise where the balanced detector subtracts signals received from beam splitter outputs (fig.1).

A coherent state from the laser comes to the first splitter input and in a vacuum state – to another input. The beam splitter prepares the mixture of these signals, then the signals from the beam splitter outputs arrive at the balanced detector. The subtracted signal is

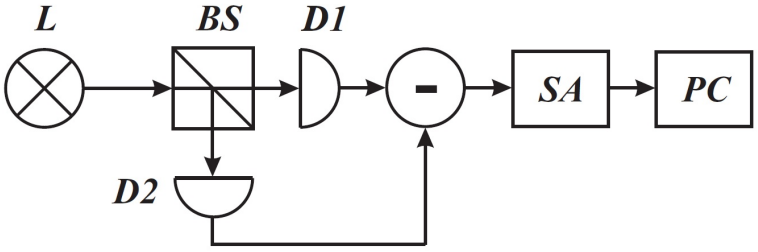

FIG. 1. QRNG scheme, based on vacuum fluctuations: L - laser, BS - beam splitter, D1, D2 - detectors, SA - spectrum analyzer, PC - computer

quantum noise, which can be processed by the PC. Random numbers are thus obtained as a result of the received differential signal processing.

3. Beam splitter

The main element of such schemes is the beam splitter. We consider how it transforms a signal. If incoming signals are a_1 and a_2, then the signals at outputs, b_1 and b_2, can be described by formula (1), where θ - is the angle of the beam splitter.

$$\begin{cases} b_1 = a_1 \cos\theta - a_2 \sin\theta, \\ b_2 = a_1 \sin\theta + a_2 \cos\theta. \end{cases} \tag{1}$$

The radiation is characterized by the Poisson distribution with parameter α (describing mean photon number), which is described as follows (in the operator form)

$$|\alpha\rangle = e^{\alpha a_1^+ - \alpha^* a_1}|0\rangle, \tag{2}$$

where a_1^+ and a_1 are photon creation and annihilation operators at the first input of the beam splitter, $|\alpha\rangle$ is the coherent state, $|0\rangle$ is the vacuum state.

If a coherent state is sent to the first splitter input, and a vacuum state - to another, then the beam splitter input signal is expressed as a tensor product:

$$|\alpha\rangle|0\rangle = e^{\alpha a_1^+ - \alpha^* a_1}|0\rangle_1|0\rangle_2. \tag{3}$$

Let the radiation be characterized by the Poisson distribution with parameter $|\alpha\rangle$. If it passes through the beam splitter with an angle θ (fig.2.*a*), then one of the beam splitter outputs is characterized by the Poisson distribution with parameter $|a\cos\theta\rangle$, and the second is characterized by the Poisson distribution with parameter $|a\sin\theta\rangle$.

In case of symmetric beam splitter we obtain the following expressions for the signals at the both outputs:

$$b_1^+ = b_2^+ = \frac{1}{\sqrt{2}} a_1^+. \tag{4}$$

The differential current can be determined as follows:

$$\Delta i = i_2 - i_1 = \gamma_2 b_2^+ b_2 - \gamma_1 b_1^+ b_1, \tag{5}$$

where i_1 and i_2 are the photocurrents at the first and the second detectors, γ_1 and γ_2 are the quantum efficiencies of the detectors. Correspondingly, the general expression for the differential current is as follows:

$$\langle \Delta i \rangle = \alpha^2(\gamma_2 \sin^2\theta - \gamma_1 \cos^2\theta). \tag{6}$$

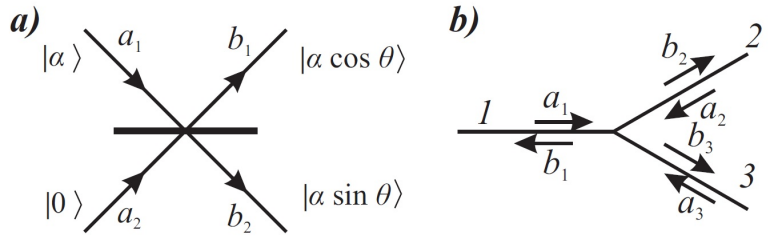

FIG. 2. *a*)Scheme of a beam splitter with angle θ, where to the first splitter input a coherent state is send, and to other input - a vacuum state.*b*)Optical Y-splitter. a_1, a_2, a_3 - input signals of the 1st, 2nd and 3rd ports, respectively, b_1, b_2, b_3 - output signals from the splitter

One can see that in the case of using of a symmetric beam splitter and detectors with identical quantum efficiencies, the mean value of the differential current is zero, and the amplitude of the differential current deviation is proportional to the intensity of the incident radiation:

$$\Delta i = \alpha\gamma. \tag{7}$$

In the case of using an asymmetric beam splitter and detectors with different quantum efficiencies, the amplitude of the differential current deviation is characterized by the following expression:

$$\Delta i = \alpha\sqrt{\gamma_2^2 \sin^2\theta + \gamma_1^2 \cos^2\theta}. \tag{8}$$

4. Y-splitter

In quantum random number generators based on the quantum fluctuations of vacuum, a beam splitter with two inputs and two outputs is normally used. We will consider the possibility of applying a fiber optical Y-splitter for these constructions. For this purpose, it is necessary to compare the quantum descriptions of the beam splitter (Fig. 2.*a*) and Y-splitter (Fig. 2.*b*). We consider the Y-splitter as a system with three inputs and three outputs, because input and output signals can pass through the same channel.

The relationship between the signals at inputs and outputs of the Y-splitter can be described by the following expression:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} -\sqrt{1-2\lambda^2} & \beta & \beta \\ \lambda & -\gamma & \sqrt{1-\beta^2-\gamma^2} \\ \lambda & \sqrt{1-\beta^2-\gamma^2} & -\gamma \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}. \tag{9}$$

where λ is the real proportionality factor, relating the output signals at the second and the third ports and the input signal applied to the first port; β is the real proportionality factor, relating the output signal at the first port and the input signal applied to the second or the third port; γ is the real proportionality factor, relating the input and the output signals of the second or the third port. Other coefficients are selected in accordance with requirements of the unitary property of the matrix. The following expressions are also caused by the unitarity conditions:

$$\begin{cases} -\sqrt{1-2\lambda^2}\beta - \lambda\gamma + \lambda\sqrt{1-\beta^2-\gamma^2} = 0, \\ -\sqrt{1-2\lambda^2}\beta + \lambda\sqrt{1-\beta^2-\gamma^2} - \lambda\gamma = 0, \\ \beta^2 - 2\gamma\sqrt{1-\beta^2-\gamma^2} = 0. \end{cases} \tag{10}$$

Parameters λ and β can be expressed in terms of γ from this system:

$$\alpha = \beta = \sqrt{2\gamma(1-\gamma)}. \tag{11}$$

Then original matrix takes the form:

$$\begin{pmatrix} 1-2\gamma & \sqrt{2\gamma(1-\gamma)} & \sqrt{2\gamma(1-\gamma)} \\ \sqrt{2\gamma(1-\gamma)} & -\gamma & 1-\gamma \\ \sqrt{2\gamma(1-\gamma)} & 1-\gamma & -\gamma \end{pmatrix}. \tag{12}$$

We consider the special case when the signal from input port 1 is distributed only between ports 2 and 3. In this case, $\sqrt{1-2\lambda^2} = 0$, and $\lambda = \dfrac{1}{\sqrt{2}}$ and by using expressions obtained above, we can obtain the following values: $\beta = \dfrac{1}{\sqrt{2}}$ and $\gamma = \dfrac{1}{2}$.

If the signal a_1 comes to the 1st port of the Y-splitter, then the signals from outputs 2 and 3 can be obtained by using the matrix described above:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}}a_1 \\ \frac{1}{\sqrt{2}}a_1 \end{pmatrix}. \tag{13}$$

Thus,

$$b_2^+ = b_3^+ = \frac{1}{\sqrt{2}}a_1^+. \tag{14}$$

This result coincides with the signals obtained at the output ports of the symmetric beam splitter (4), when the coherent state a_1 comes to the first splitter input, and a vacuum state - to the other. Thus, as description for the beam splitter and the Y-splitter are the same, to evaluate work of QRNG systems based on the vacuum fluctuations using the Y-splitter we can use results for the beam splitter, obtained earlier. For example, we can estimate the probability of the detecting of N different photons in the substractor [12] (Fig. 3):

$$P_N = exp(-|\alpha|^2) I_{|N|}(|\alpha|^2), \tag{15}$$

where α is the Poisson parameter of the initial radiation, corresponding to the mean number of photons, $I_{|N|}(|\alpha|^2)$ is the modified Bessel function of order $|N|$.

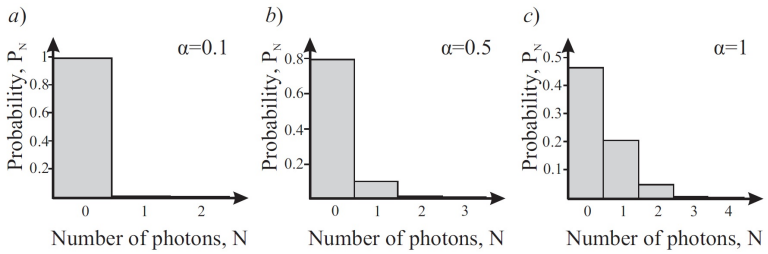

FIG. 3. Probability of detecting of N difference photons at substractor for input radiation with mean number of photons a) α =0.1, b) α=0.5, c) α =1

5. Conclusion

Expressions describing the relationship between the beam splitter input radiation and the differential current were obtained for quantum random number generation scheme using homodyne detection. For this scheme, expressions for estimations of the scheme's parameters imperfection impacts on the measurement results, were also derived. We obtained mathematical expressions demonstrating the formal equivalence for the quantum description of the beam splitter with two inputs and the quantum description of the Y-splitter. This allows us to use the Y-splitter for the implementation of a quantum random number generation system based on the quantum fluctuations of vacuum, and to use the previously obtained formulas for the beam splitter with two inputs and two outputs for the calculation of that system's characteristics.

Acknowledgements

This work was partially financially supported by the Government of the Russian Federation (grant 074-U01), by the Ministry of Science and Education of the Russian Federation (GOSZADANIE 2014/190, Project 14.Z50.31.0031).

References

[1] Scarani V., Bechmann-Pasquinucci H., Cerf N. J. et al., The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, P. 1301–1350 (2009).

[2] Jennewein T., Achleitner U., Weihs G., Weinfurter H., A. Zeilinger A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, **71**(4), P. 1675–1680 (2000).

[3] Stefanov A., Gisin N., Guinnard O., Guinnard L. Zbinden H. Optical quantum random number generator. *J. Modern Optics*, **47**(4), P. 595–598 (2000).

[4] Ivanova A.E., Egorov V.I., Chivilikhin S.A., Gleim A.V. Investigation of quantum random number generation based on space-time division of photons. *Nanosystems: Physics, Chemistry, Mathematics*, **4**(4), P. 549–553 (2013).

[5] Fiorentino M., Santori C., Spillane S. M., Beausoleil R. G., Munro W. J. Secure self-calibrating quantum random bit generator. *Phys. Rev. A.*, **75**, P. 032334 (2007).

[6] Kwon O.,Cho Y.-W. , Kim Y.-H. Quantum random number generator using photon-number path entanglement. *Appl. Opt.*, **48**, P. 1774–1778 (2009).

[7] Dynes J. F., Yuan Z. L, Sharpe A. W.,Shields A. J. A high speed, post-processing free, quantum random number generator. *Appl. Phys. Lett.*, **93**, P. 031109 (2008).

[8] Furst M., Weier H.,Nauerth S., Marangon D. G.,Kurtsiefer C., Weinfurter H. High speed optical quantum random number generation. *Optics Express*, **18**, P. 13029 (2010).

[9] Qi B., Chi Y.-M.,Lo H.-K., Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, **35**, P. 312–314 (2010).

[10] Reidler I., Aviad Y.,Rosenbluh M., Kanter I. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. *Phys. Rev. Lett.*, **103**, P. 024102 (2009).

[11] Shen Y., Tian L.,Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A.*, **81**, P. 063814 (2010).

[12] Braunstein S. L. Homodyne statistics. *Phys. Rev. A.*, **42**(1), P. 474–481 (1990).