NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2016, 7 (2), P. 378–383

The use of beam and fiber splitters in quantum random number generators based on vacuum fluctuations

A. E. Ivanova, S. A. Chivilikhin, A. V. Gleim

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

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

PACS 03.67.-a **DOI 10.17586/2220-8054-2016-7-2-378-383**

Quantum random number generators based on vacuum fluctuations produce truly random numbers that can be used for applications are requiring a high degree of randomness. A beam splitter with two inputs and two outputs is normally used in these systems. In this paper, mathematical descriptions were obtained for the use of such beam splitter and fiber Y-splitter in quantum random number generation systems with homodyne detection. We derived equations which allowed us to estimate the impact of the scheme parameters' imperfection upon measurement results. We also obtained mathematical expressions, demonstrating the equivalence of quantum descriptions for a Y-splitter and a beam splitter with two inputs.

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

Received: 22 January 2016

1. Introduction

Random numbers can be generated algorithmically, but resulting sequences are pseudorandom and not suitable for applications in which a high degree of randomness is needed, such as quantum cryptography [1]. These applications necessitate true random number generation obtained by indeterminate physical processes, including quantum processes. Existing approaches to quantum random number generation include the use of radiation separation [2], entangled photon states [3], quantum noise of a laser [4], processes of photon emission and detection [5]. An alternative approach is quantum random number generators based on quantum vacuum fluctuations (Fig. 1) [6, 7].

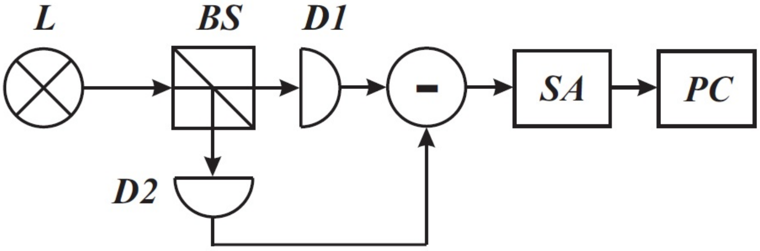

FIG. 1. Quantum random number generation scheme based on vacuum fluctuations: L – laser, BS – beam splitter, D1, D2 – detectors, SA – spectrum analyzer, PC – computer

This type of quantum random number generator extracts randomness from quantum noise obtained when balanced detector subtracts signals received from beam splitter outputs. In these schemes, beam splitters with two inputs and two outputs (Fig. 2a) are normally used. To the first splitter input, a coherent state is sent from a laser, and to the other input – a vacuum state. These two signals are mixed via a beam splitter, then, signals are sent from the beam splitter outputs to the balanced detector. The subtracted signal is quantum noise, which can be processed on a PC. Random numbers are obtained as a result of received differential signal processing. The purpose of this research was the comparison of quantum descriptions of optical beam splitter and a fiber splitter with one input and two outputs (Fig. 2b). If these quantum descriptions are equal, it will allow us to use a Y-splitter to implement a quantum random number generation system based on quantum vacuum fluctuations.

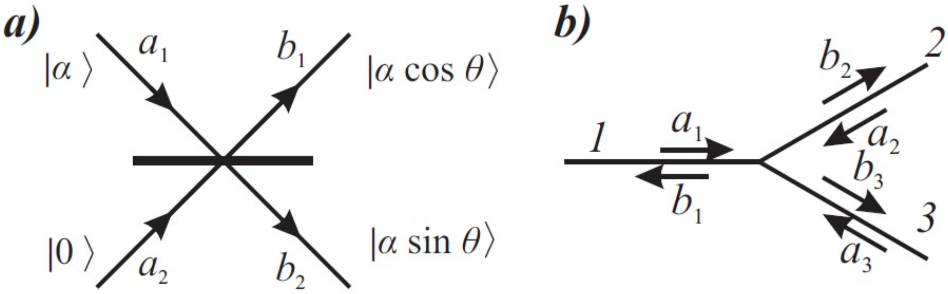

FIG. 2. *a*) Scheme of a beam splitter with angle θ, where a coherent state is sent to the 1st spitter input, and to the other input – a vacuum state. *b*) Optical Y-splitter. a_1, a_2, a_3 – input signals of the 1st, 2nd and 3rd ports, respectively, b_1, b_2, b_3 – output signals from the splitter

2. Beam splitter

Beam splitter is a key element for quantum random number generation schemes based on vacuum fluctuations [6,7]. We consider its impact upon the signal. Mathematical description of a beam splitter, when a strong laser signal, described by the Poisson distribution, arrives at one of its inputs and vacuum state arrives at the other, has been derived in the operator form. In this description, the mean photon number of laser signal α, the angle of beam splitter θ and quantum efficiencies of detectors γ_1 and γ_2 were taken into account.
If signals a_1 and a_2 come to beam splitter inputs, as shown on Fig. 2a, then signals at outputs, b_1 and b_2 can be described by formula (1):

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

Laser radiation at the first input is characterized by a Poisson distribution with parameter α (describing mean photon number), which in operator form is expressed as follows:

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

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

When a coherent state is sent to first splitter input and a vacuum state is sent to the second splitter input, then the input signal on the beam splitter is expressed as a tensor product:

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

If the radiation is characterized by a Poisson distribution with parameter $|\alpha\rangle$ that passes through a beam splitter with angle θ (Fig. 2a), then one of beam splitter outputs is characterized by a

Poisson distribution with parameter $|a\cos\theta\rangle$, and second is characterized by Poisson distribution with parameter $|a\sin\theta\rangle$.

In the case of the symmetric beam splitter, we obtain expression, describing signals at both outputs:

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

The differential current after detection can be defined 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, i_2 are photocurrents at first and second detectors, γ_1, γ_2 are quantum efficiencies of detectors.

For a symmetric beam splitter and detectors with equal quantum efficiencies, the mean value of the differential current is determined to be zero, and amplitude of the differential current deviation is directly proportional to the intensity of incident radiation.

In the case of using an asymmetric beam splitter and detectors with different quantum efficiencies, the mean value of the differential current is characterized by the following equation:

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

In this case, the amplitude of differential current deviation can be estimated by the following formula (7):

$$\delta i = \alpha\sqrt{\gamma_2^2\sin^2\theta + \gamma_1^2\cos^2\theta}. \tag{7}$$

3. Y-splitter

Using a Y-splitter as a basic element for homodyne detection allows one to obtain the lower level of determined ambient noise and reduce the size of the device without compromising the generation rate or degree of randomness for the generated sequences. We consider the Y-splitter (Fig. 2b) as a system with three inputs and three outputs [8], because input and output signals can pass through one channel.

The relationship between the input and output signals in a Y-splitter which allows showing the correlation between each pair of signals, can be described by the following expression:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} -\sqrt{1-2\lambda^2} & \beta & \beta \\ \lambda & -\gamma & \sqrt{1-\beta^2-\gamma^2} \\ \lambda & \sqrt{1-\beta^2-\gamma^2} & -\gamma \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \tag{8}$$

where λ is the proportionality factor connecting the input signal at the 1st port and output signals at 2nd and 3rd ports; β is the proportionality factor connecting the input signals at the 2nd or 3rd ports and the output signal at the 1st port; γ is the proportionality factor connecting the input and output signals of the 2nd port or input and output signals of the 3rd port.

These coefficients are selected in accordance with requirements of the unitary property for the matrix. The next expressions also arise from unitarity conditions:

$$\begin{cases} -\sqrt{1-2\lambda^2}\beta - \lambda\gamma + \lambda\sqrt{1-\beta^2-\gamma^2} = 0, \\ -\sqrt{1-2\lambda^2}\beta + \lambda\sqrt{1-\beta^2-\gamma^2} - \lambda\gamma = 0, \\ \beta^2 - 2\gamma\sqrt{1-\beta^2-\gamma^2} = 0. \end{cases} \tag{9}$$

After selection of matrix proportionality factors, it is possible to simplify the matrix form using the fact that the parameters λ and β can be expressed for this system through the γ:

$$\lambda = \beta = \sqrt{2\gamma(1-\gamma)}. \tag{10}$$

Then, the original matrix takes form:

$$\begin{pmatrix} 1-2\gamma & \sqrt{2\gamma(1-\gamma)} & \sqrt{2\gamma(1-\gamma)} \\ \sqrt{2\gamma(1-\gamma)} & -\gamma & 1-\gamma \\ \sqrt{2\gamma(1-\gamma)} & 1-\gamma & -\gamma \end{pmatrix}. \tag{11}$$

We consider the special case when a signal from 1st input port is distributed only between ports 2 and 3 without reflection on the 1st port. In this case $\sqrt{1-2\lambda^2} = 0$, and $\lambda = \frac{1}{\sqrt{2}}$, then by using expressions were obtained above, we can derive the values $\beta = \frac{1}{\sqrt{2}}$ and $\gamma = \frac{1}{2}$.

If signal a_1 is sent to 1st port of Y-splitter, then signals from outputs 2 and 3 can be described by using matrix with these proportionality factors:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}}a_1 \\ \frac{1}{\sqrt{2}}a_1 \end{pmatrix}. \tag{12}$$

Thus,

$$b_2^+ = b_3^+ = \frac{1}{\sqrt{2}}a_1^+. \tag{13}$$

Then, we can consider the matrix elements describing the interconnection between signal at 1st input port of Y-splitter and signals, emanating from 2nd and 3rd ports, thus:

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

This expression coincides with signals that were obtained at output ports of symmetric beam splitter, when the coherent state a_1 was sent to the first splitter input, and a vacuum state – to the other. Thus, as the description for the beam splitter and Y-splitter are equal, we can use results for beam splitter, obtained earlier, to evaluate work of quantum random generation systems, based on vacuum fluctuations using the Y-splitter.

4. Y-splitter with complex parameters

When we use complex parameters to mathematically describe the Y-splitter, then original system (8) is changing. Relationship between signals at inputs and outputs of Y-splitter is shown in the following expression:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} -\sqrt{1-2|\lambda|^2} & \beta & \beta \\ \lambda & -\gamma & \sqrt{1-|\beta|^2-|\gamma|^2} \\ \lambda & \sqrt{1-|\beta|^2-|\gamma|^2} & -\gamma \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}. \tag{15}$$

In the next matrix parameters, λ and β were derived from the original matrix through the parameter $\gamma = \gamma_r + i\gamma_i$:

$$\begin{pmatrix} 2\gamma_r - 1 & \sqrt{2\gamma_r(1-\gamma_r)} + i\gamma_i\sqrt{\frac{1-\gamma_r}{2\gamma_r}} & \sqrt{2\gamma_r(1-\gamma_r)} + i\gamma_i\sqrt{\frac{1-\gamma_r}{2\gamma_r}} \\ \sqrt{2\gamma_r(1-\gamma_r)} + i\frac{\gamma_i\sqrt{1-\gamma_r}}{\sqrt{2\gamma_r(2\gamma_r-1)}} & -\gamma_r - i\gamma_i & 1-\gamma_r \\ \sqrt{2\gamma_r(1-\gamma_r)} + i\frac{\gamma_i\sqrt{1-\gamma_r}}{\sqrt{2\gamma_r(2\gamma_r-1)}} & 1-\gamma_r & -\gamma_r - i\gamma_i \end{pmatrix} \tag{16}$$

We can see, that coefficient γ shows reflection at port 2, when signal a_2 is sent to the 2st port of Y-splitter, and there are no input signals at other ports. Then, we consider when signal a_1 is sent to the 1st port of Y-splitter, and there are no input signals at other ports, then signal is distributed only between output ports 2 and 3, and we can estimate signals for the 2nd and 3rd ports:

$$b_2^+ = b_3^+ = \sqrt{2(1-\gamma_r)}\exp\left(i\frac{\gamma_i}{2\gamma_r(2\gamma_r-1)}\right)a_1^+. \tag{17}$$

These result, with the exception of phase shift, coincides with signals that were obtained at output ports of symmetric beam splitter, when coherent state a_1 was sent to the first splitter input, and a vacuum state - to the other.

5. Conclusion

In this research, we obtained expressions describing the relationship between beam splitter input radiation and differential current. For a symmetric beam splitter and detectors with equal quantum efficiencies, the mean value of differential current is determined to be zero, and the amplitude of the differential current deviation is directly proportional to the intensity of the incident radiation. We also derived equations for an asymmetric beam splitter, allowing estimation of how the scheme parameters imperfection affect the measurement results.

We obtained mathematical expressions, demonstrating the equivalence for the quantum description of beam splitter with two inputs and Y-splitter, when we didn't use complex parameters in equations. When we use complex parameters in equations, then the results, with the exception of the phase shift, coincide with the signals obtained for output ports of symmetric beam splitter with two inputs and two outputs, when coherent state is sent to the first splitter input, and a vacuum state – to the other. That allows us to use a Y-splitter for the implementation of a quantum random number generation system based on quantum vacuum fluctuations, and to apply formulas previously-obtained for the calculations of systems consisting of a beam splitter with two inputs and two outputs.

Acknowledgements

This work was partially financially supported by the Government of the Russian Federation (grant 074-U01).

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

[4] Qi B., Chi Y.-M., et. al. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, 2010, **35**, P. 312–314.

[5] 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.

[6] 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.

[7] Gabriel C., Wittmann C., et. al. A generator for unique quantum random numbers based on vacuum states. *Nature Phot.*, 2010, **4**, P. 711–715.

[8] Ivanova A. E, Chivilikhin S. A, Popov I. Yu, Gleim A. V. On the possibility of using optical Y-splitter in quantum random number generation systems based on fluctuations of vacuum. *Nanosyst.: Phys., Chem., Math.*, 2015, **6**(1), P. 95–99.