Using of optical splitters in quantum random number generators, based on fluctuations of vacuum

A E Ivanova¹, S A Chivilikhin¹ and A V Gleim¹,²
¹ITMO University, Kronverkskiy pr. 49, St. Petersburg 197101, Russian Federation,
²Kazan National Research Technical University, K.Marl st. 10, Kazan 420111, Russian Federation
E-mail: newiva@mail.ru

Abstract. In this paper mathematical description of using of fiber Y-splitter and optical splitter with two input and two output ports in quantum random number generation systems were obtained.

1. Introduction
Quantum random number generators are based on non-deterministic physical processes. They allows to obtain sequences of random numbers, that can be used in applications requiring high degree of randomness, for example, in cryptography [1].

Existing approaches to quantum random number generation include the use of separation of radiation [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 fluctuations of vacuum [6, 7].

In quantum random number generation schemes based on quantum fluctuations (Fig. 1) beam splitters with two inputs and two outputs are normally used. The purpose of this research was a comparison of quantum descriptions of such beam splitter and a fiber splitter with one input and two outputs. If these quantum descriptions will be equal, it will allow us to use the Y-splitter for the implementation of a quantum random number generation system based on quantum fluctuations of vacuum.

2. Beam splitter
Beam splitter is a key element for quantum random number generation schemes based on vacuum fluctuations [6, 7]. In these schemes a strong coherent emission from the laser comes to the one input of beam splitter and quantum fluctuations of vacuum come to another input. The beam splitter prepares the mixture of these signals, and then separates it to two signals, arriving at balanced detector. One of output signals after detection is subtracted from the other, and thus, the final signal is only quantum vacuum noise, which is completely random and can be used to random number generation.

Mathematical description of a beam splitter (Fig. 2), when strong laser signal, described by the Poisson distribution, arrives to one of its inputs and vacuum state arrives to other, has been received in the operator form. In this description mean photon number of laser signal $\alpha$, the
angle of beam splitter $\theta$ and quantum efficiencies of detectors $\gamma_1$ and $\gamma_2$ were taken into account. If signals $a_1$ and $a_2$ comes to beam splitter inputs, as shown on fig. 2, then signals at outputs, $b_1$ and $b_2$ can be described by this formula

$$
\begin{align*}
    b_1 &= a_1 \cos \theta - a_2 \sin \theta, \\
    b_2 &= a_1 \sin \theta + a_2 \cos \theta.
\end{align*}
$$

(1)

Laser radiation at first input is characterized by Poisson distribution with parameter $\alpha$ (describing mean photon number), which in operator form is described as follows

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

(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 to first splitter input a coherent state is send, and to second splitter input a vacuum state is send, then beam splitter input signal is expressed as a tensor product

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

(3)

In this case, if angle of beam splitter is $\theta$, then one of beam splitter outputs is characterized by Poisson distribution with parameter $|a \cos \theta\rangle$, and second is characterized by Poisson distribution with parameter $|a \sin \theta\rangle$. 

---

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

**Figure 2.** Scheme of a beam splitter with angle $\theta$, where to the 1st splitter input a coherent state is send, and to other input - a vacuum state.

**Figure 3.** Optical Y-splitter. $a_1$, $a_2$, $a_3$ - input signals of 1st, 2nd and 3rd ports, respectively, $b_1$, $b_2$, $b_3$ - output signals from the splitter.
In case of symmetric beam splitter we obtain expression, describing signals at both outputs

\[ b_1^+ = b_2^+ = \frac{1}{\sqrt{2}} a_1^+. \]  

(4)

Differential current after detecting can be defined as follows

\[ \Delta i = i_2 - i_1 = \gamma_2 b_2^+ b_2 - \gamma_1 b_1^+ b_1, \]  

(5)

where \( i_1, i_2 \) are photocurrents at first and second detectors, \( \gamma_1, \gamma_2 \) are quantum efficiencies of detectors.

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

In case of using an asymmetric beam splitter and detectors with different quantum efficiencies, mean value of differential current \( \langle \Delta i \rangle \) and amplitude of differential current deviation \( \delta i \) are characterized by the following equations

\[ \langle \Delta i \rangle = a^2 (\gamma_2 \sin^2 \theta - \gamma_1 \cos^2 \theta), \delta i = a \sqrt{\gamma_2^2 \sin^2 \theta + \gamma_1^2 \cos^2 \theta}, \]  

(6)

where \( \gamma_1, \gamma_2 \) are quantum efficiencies of the detectors, \( \theta \) is beam splitter angle.

3. Y-splitter

Using Y-splitter as a basic element for the homodyne detection allows getting lower level of determined nature noise and reducing the size of device without compromising the degree of randomness of generated sequences or the rate of generation. We consider Y-splitter as a system with three inputs and three outputs (fig. 3), because input and output signals can pass through one channel.

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

\[ \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} -\sqrt{1 - 2\lambda^2} & \beta & 0 \\ \lambda & -\gamma & \sqrt{1 - \beta^2 - \gamma^2} \\ \lambda & \sqrt{1 - \beta^2 - \gamma^2} & -\gamma \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}. \]  

(7)

where \( \lambda \) is proportionality factor, connecting input signal at 1st port and output signals at 2nd and 3rd ports; \( \beta \) is proportionality factor, connecting output signal at 1st port and input signals at 2nd or 3rd ports; \( \gamma \) is proportionality factor, connecting input and output signals of 2nd or 3rd ports.

These coefficients are selected in accordance with requirements of unitary property of matrix. Next expressions are also followed from unitarity conditions

\[ \begin{cases} -\sqrt{1 - 2\lambda^2} - \lambda \gamma + \lambda \sqrt{1 - \beta^2 - \gamma^2} = 0, \\ -\sqrt{1 - 2\lambda^2} \beta + \lambda \sqrt{1 - \beta^2 - \gamma^2} - \lambda \gamma = 0, \\ \beta^2 - 2\gamma \sqrt{1 - \beta^2 - \gamma^2} = 0. \end{cases} \]  

(8)

After selection of matrix proportionality coefficients it is possible to simplify matrix form, using fact, that parameters \( \lambda \) and \( \beta \) can be expressed from this system through the \( \gamma \):

\[ \alpha = \beta = \sqrt{2\gamma(1 - \gamma)}. \]  

(9)
We consider special case when signal from 1st input port is distributed only between ports 2 and 3. In this case, $\sqrt{1 - 2\lambda^2} = 0$, and $\lambda = \frac{1}{\sqrt{2}}$ and by using expressions was obtained above, we can receive values $\beta = \frac{1}{\sqrt{2}}$ and $\gamma = \frac{1}{2}$.

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

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -2 & 2 \\ \frac{1}{\sqrt{2}} & 1 & -1 \end{pmatrix} \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}}a_1 \\ \frac{1}{\sqrt{2}}a_1 \end{pmatrix}.$$ (10)

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

$$b_2^+ = b_3^+ = \frac{1}{\sqrt{2}}a_1^+.$$ (11)

This expression coincides with result, that we can obtain at output ports of symmetric beam splitter, when coherent state $a_1$ is send to the first splitter input, and a vacuum state - to the other. Thus, as description for 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. Conclusions

In this research quantum mathematic descriptions of using Y-splitter and beam splitter in quantum random generation schemes based on fluctuation of vacuum were obtained. For beam splitter we described relationship between input radiation and differential current for quantum random number generation scheme using homodyne detection. We also derived expressions allowing estimation of scheme parameters imperfection impact on measurement results.

A comparison of results showed that for two types of optical splitters mathematical quantum description of resulting output signals is identical. That allows using fiber splitter with one input and two output ports at quantum random number generator based on fluctuations of the vacuum, instead of optical beam splitter.

Acknowledgments

This work was financially supported by Government of Russian Federation, Grant 074-U01.

References

[1] Scarani V, Bechmann-Pasquinucci H et al 2009 Rev. Mod. Phys. 81 1301
[2] Jennewein T, Achleitner U et al 2000 Rev. Sci. Instrum 71 1675
[3] Kwon O, Cho Y-W and Kim Y-H 2009 Appl. Opt. B 48 1774
[4] Qi B, Chi Y-M, Lo H-K and Qian L 2010 Optics Letters 35 312
[5] Dynes J F, Yuan L et al 2008 Appl. Phys. Lett. 93 031109
[6] Shen Y, Tian L and Zou H 2010 Phys. Rev. 81 063814
[7] Gabriel C, Wittmann C et al 2010 Nature Phot 4 711