Investigation of device imperfection influence on measurement results in beamsplitter-based quantum random number generation schemes

A E Ivanova, S A Chivilikhin, V I Egorov and A V Gleim
St.Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverkskiy pr. 49, St.Petersburg 197101, Russian Federation
E-mail: newiva@mail.ru

Abstract. Quantum random number generation allows acquiring true random numbers which can be used in applications that require a high degree of randomness. This paper assesses the influence of non-ideal scheme parameters on measurement results in two quantum random number generation schemes: based on laser radiation splitting, and using vacuum fluctuations.

1. Introduction
Random number generation can be performed using algorithms, but the resulting sequences are pseudo-random by their nature and hence are not suitable for applications requiring a high degree of randomness, such as quantum cryptography [1]. For these applications it is necessary to use "true" random numbers produced by non-deterministic physical processes [2], for example, of quantum nature [3].

Existing approaches to quantum random number generation include the use of entangled photon states [4], processes of photon emission and detection [5], quantum noise of a laser [6], and separation of radiation [7]. An alternative approach is to use vacuum fluctuations of electromagnetic field [8].

Any practical random number generator operates a bit differently compared to its idealistic description. Hence, it is important to model the effects of any possible disruptions and study their impact on the output statistical features. This work is focused on investigating the case when the beamsplitter division angle is disturbed. Calculations are performed for two different methods of generation, the first based on laser radiation splitting, and the second on using vacuum fluctuations in homodyne detection. Both considered schemes include a beam splitter, and our model can be further extended to any kind of setup based on using this element.

2. Quantum random number generation based on radiation division by a beam splitter
For investigating distribution statistics obtained using a beam splitter, a probabilistic process simulation was performed. In the model, laser radiation is separated by a beam splitter and detected in two channels simultaneously (figure 1). It is shown that when radiation characterized by Poisson distribution with parameter $\alpha$ (describing mean photon number) passes through
a beam splitter with angle $\theta$, one of the beam splitter outputs is characterized by Poisson distribution with parameter $\alpha_1 = \alpha \cos \theta$, and the other - with $\alpha_2 = \alpha \sin \theta$.

Processing the two sequences obtained after separating radiation is performed as follows: if the photons are not detected on the first beam splitter output, and any number of them is detected on the second output, then the resulting sequence bit is considered "0", in the opposite case "1", otherwise the bit is not determined.

It was shown that for an asymmetric beam splitter a degree of final distribution uniformity depends on the beam splitter angle. By increasing deviation of the beam splitter angle (from $\theta = 45^\circ$ value), we increase the difference in zeros and ones generation probability in the final sequence. It is necessary to calculate the beam splitter angular deviation, at which the final binary sequence is random. Statistical parameters of the binary distribution obtained from an asymmetric beam splitter are shown in figure 2. Generated sequences successfully pass tests of randomness, if the angular deviation from $\theta = 45^\circ$ does not exceed two degrees.

![Figure 1. Scheme of random number generation based on radiation division by a beam splitter: L - laser, BS - beam splitter, D1, D2 - detectors, PC - computer.](image1.png)

![Figure 2. "Zero" and "One" occurrence probabilities in the resulting sequence, depending on the beam splitter angle.](image2.png)

![Figure 3. Probability of "0" and "1" bits occurrence in the sequence obtained using beam splitters with angles $\theta = 45^\circ$ and $\theta = 50^\circ$, probability of detection of the first detector $P_1 = 10\%$.](image3.png)

Detector parameters affect the quality of generated sequences of random numbers. When both detectors quantum efficiencies are equal, some random samples in two sequences, obtained by
the beam splitter outputs zeroed. In this case, quality of the resulting sequence is not decreasing, because the changes are random and quantum efficiencies are equal for both detectors. We also considered a situation when quantum efficiencies of two detectors are different. In this case, one of the sequences produced by the beam splitter will contain more zero samples than the other. The difference in detectors parameters changes the ratio of ones and zeros in the final sequence, thus affecting the average of distribution for a given beam splitter angle, and the quality of the resulting sequence. Figure 3 illustrates the probability of "0" or "1" bits occurrence depending on detection probability ratio of the first and second detectors, $P_1$ and $P_2$. As one can see, asymmetric detectors can compensate the difference in probabilities of an asymmetric beam splitter, if their parameters are properly selected. For example, if after the beam division in one of the output sequences the amount of nonzero samples is greater than in the other, but it is detected by a device with a larger number of zero counts, an optimal balance between the probability of occurrence of zeros and ones in the final sequence of bits can be achieved.

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

The principle of this scheme lies in extracting randomness from quantum noise that appears upon subtracting balanced detector signals received from the beam splitter outputs (figure 4). To the first splitter input a coherent state is send, and the other - a vacuum state. In this case interaction between strong laser signal and vacuum fluctuations appears in the splitter. Random numbers are obtained as a result of the received differential signal processing.

**Figure 4.** Scheme of random number generation based on homodyne detection principles: L - laser, BS - beam splitter, D1, D2 - detectors, SA - spectrum analyzer, PC - computer.

**Figure 5.** Scheme of a beam splitter with angle $\theta$, where a coherent state is send to the first splitter input, and a vacuum state - to the other.

The input beam splitter signals are $a_1$ and $a_2$, the output signals are $b_1$ and $b_2$, respectively (figure 5). The output signals for the given input signals are expressed as follows

$$b_1 = a_1 \cos \theta - a_2 \sin \theta,$$

$$b_2 = a_1 \sin \theta - a_2 \cos \theta.$$ 

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

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

where $a_1^+$ and $a_1$ are photon creation and annihilation operators at the first input of the beam splitter, $|\alpha\rangle$ - coherent state, $|0\rangle$ - vacuum state.
When a coherent state $|\alpha\rangle$ is send to the first splitter input, and a vacuum state $|0\rangle$ is send to the other, beam splitter input signal is expressed as a tensor product

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

Radiation characterized by Poisson distribution with parameter $|\alpha\rangle$ passes through a beam splitter with angle $\theta$, one of the beam splitter outputs is characterized by Poisson distribution with parameter $|\alpha \cos \theta\rangle$, and the other with $|\alpha \sin \theta\rangle$. Photocurrents at the first and second detectors are defined as

$$i_1 = \gamma_1 b_1^+ b_1,$$

$$i_2 = \gamma_2 b_2^+ b_2,$$

where $\gamma_1$, $\gamma_2$ are quantum efficiencies of first and second detectors. Mean value of differential current can be expressed as follows

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

In case of using a symmetric beam splitter and detectors with equal quantum efficiency mean value of the differential current was determined to be zero. We also calculated the amplitude of its deviation, which appears to be directly proportional to the intensity of laser radiation at the splitter input. For an asymmetric beam splitter and detectors with different quantum efficiencies the amplitude of differential current deviation is characterized by the following equation

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

where $\gamma_1$, $\gamma_2$ are quantum efficiencies of the detectors.

Relative deviation of the differential current on the deviations of detectors and beam splitter parameters dependence takes the following form

$$\frac{\Delta \langle \delta i \rangle}{\langle \delta i \rangle_0} = \frac{1}{2} \left( \frac{\Delta \gamma_1 + \Delta \gamma_2}{\gamma} + \frac{\Delta \gamma_1^2 + \Delta \gamma_2^2}{2 \gamma^2} + \sin(2\Delta \theta) \left( \frac{\Delta \gamma_2 - \Delta \gamma_1}{\gamma} + \frac{\Delta \gamma_2^2 - \Delta \gamma_1^2}{2 \gamma^2} \right) \right),$$

where $\gamma_1 = \gamma + \Delta \gamma_1$, $\gamma_2 = \gamma + \Delta \gamma_2$ are quantum efficiencies of the detectors, $\theta = \frac{\pi}{4} + \Delta \theta$ is beam splitter angle.

4. Conclusions
We investigated influence of non-ideal scheme parameters of quantum random number generation on the measurement results. Two types of generators were considered: based on beam separation and vacuum fluctuations. We show that the sequences generated by beam splitting successfully pass randomness tests, if the deviation of the beam splitter angle $\theta$ remains no more than two degrees. It was determined that in general inequality of detector parameters degrades the quality of generated sequences, but at the same time careful selection of their parameters can compensate asymmetry of the beam splitter. For quantum random number generation scheme using homodyne detection expressions describing the relationship between beam splitter input radiation and differential current were obtained. We also derived equations allowing estimation of the scheme parameters imperfection impact on the measurement results.

Acknowledgments
This work was financially supported by Government of Russian Federation, Grant 074-U01.
References
[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Duks M, Ltkenahus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[2] Argyris A, Deligiannidis S, Pikasis E, Bogris A and Syvridis D 2010 Optics Express 18 18763
[3] Jennewein T, Achleitner U, Weihs G, Weinfurter H and Zeilinger A 2000 Rev. Sci. Instrum 71 1675
[4] Kwon O, Cho Y-W and Kim Y-H 2009 Appl. Opt. B 48 1774
[5] Stipevi M and Rogina M B 2007 Rev. Sci. Instrum. 78 045104
[6] Qi B, Chi Y-M, Lo H-K and Qian L 2010 Optics Letters 35 312
[7] Ivanova A E, Egorov V I, Chivilikhin S A and Gleim A V 2013 Nanosist.: fiz. him. mat. 4 550
[8] Shen Y, Tian L and Zou H 2010 Phys. Rev. 81 063814