Quantum random number generator based on quantum nature of vacuum fluctuations

A E Ivanova, S A Chivilikhin and A V Gleim
ITMO University, Kronverkskiy pr. 49, St.Petersburg 197101, Russia

Abstract. Quantum random number generator (QRNG) allows obtaining true random bit sequences. In QRNG based on quantum nature of vacuum, optical beam splitter with two inputs and two outputs is normally used. We compare mathematical descriptions of spatial beam splitter and fiber Y-splitter in the quantum model for QRNG, based on homodyne detection. These descriptions were identical, that allows to use fiber Y-splitters in practical QRNG schemes, simplifying the setup. Also we receive relations between the input radiation and the resulting differential current in homodyne detector. We experimentally demonstrate possibility of true random bits generation by using QRNG based on homodyne detection with Y-splitter.

1. Introduction
Quantum random number generators are based on the physically random processes, therefore, the random numbers generated by these systems are unpredictable, truly random and can be used in applications, requiring high degree of randomness, such as cryptography [1]. There are many different ways to implement quantum random number generation: using beam separation [2], entangled photon states [3], processes of photon emission and detection [4] and quantum noise of lasers [5]. Another method of generating is using of electromagnetic field vacuum fluctuations [6].

This work is focused on investigation of applying fiber Y-splitters in QRNG, based on the on quantum nature of vacuum fluctuations (figure 1). 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.

Figure 1. Scheme of random number generation based on homodyne detection principles: L – laser, BS – beam splitter, D1, D2 – detectors, SA – spectrum analyzer, PC – computer.
2. Quantum random number generation based on the principles of homodyne detection. Beam splitter

Optical beam splitter (figure 2(a)) is essential for quantum random number generation systems based on the fluctuations of the vacuum [6]. In these schemes to one of beam splitter's input ports strong laser radiation is sent, and second port receive only vacuum fluctuations. Vacuum and high-intensity laser signals are mixed on the beam splitter and splitted into two signals arriving at the detector. After detecting one of these signals is subtracted from other and thus only vacuum noise remains in final signal. It is completely random and can be used to random numbers generation.

We obtain in operator form mathematical description of beam splitter’s work in QRNG using fluctuations of vacuum, when a strong laser signal, which can be described by Poisson distribution, is sent to one of its inputs, and vacuum state is sent to other input.

If input radiation $a_1$ can be characterized by Poisson distribution with parameter $\alpha$ and radiation passes through a beam splitter with angle $\theta$ (figure 2(a)), then signal at first of beam splitter outputs $b_1$ can be characterized by Poisson distribution with parameter $\alpha \cos \theta$, and signal at the second output $b_2$ can be characterized by Poisson distribution with parameter $\alpha \sin \theta$.

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

$$b_1 = b_2 = \frac{1}{\sqrt{2}} a_1$$

(1)

For the case of an asymmetric beam splitter and different quantum efficiencies of detectors we calculate mean differential current, dispersion and amplitude of difference current deviation.

Differential current after detecting can be defined as follows

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

(2)

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

For detectors with equal quantum efficiencies and symmetric beam splitter, mean value of differential current is determined to be zero and amplitude of differential current deviation is directly proportional to intensity of input radiation. In case of using detectors with different quantum efficiencies and asymmetric beam splitter, mean value of differential current is characterized by following equation

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

(3)

and in this case amplitude of differential current deviation can be estimated by formula (4)

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

(4)

3. Y-splitter. Experimental results.

The fiber splitter with one input and two output ports (figure 2(b)) has been presented as a system with three inputs and three outputs, because signal in each of the ports may be distributed in two opposite
directions. Relations between input and output signals of the optical fiber splitter were derived by using a matrix description allowing show the interaction between each pair of signals:

\[
\begin{pmatrix}
    b_1 \\
    b_2 \\
    b_3
\end{pmatrix} = 
\begin{pmatrix}
    -\sqrt{1-2\lambda^2} & \beta & \beta \\
    \lambda & -\gamma & \sqrt{1-\beta^2-\gamma^2} \\
    \lambda & \sqrt{1-\beta^2-\gamma^2} & -\gamma
\end{pmatrix}
\begin{pmatrix}
    a_1 \\
    a_2 \\
    a_3
\end{pmatrix},
\] (5)

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

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

\[
\begin{cases}
    -\sqrt{1-2\lambda^2}\beta - \lambda\gamma + \lambda\sqrt{1-\beta^2-\gamma^2} = 0, \\
    -\sqrt{1-2\lambda^2}\beta + \lambda\sqrt{1-\beta^2-\gamma^2} - \lambda\gamma = 0, \\
    \beta^2 - 2\gamma\sqrt{1-\beta^2-\gamma^2} = 0.
\end{cases}
\] (6)

After selection of matrix proportionality factors we can simplify matrix form, using fact, that parameters \( \lambda \) and \( \beta \) can be expressed from system (6) through the \( \gamma \):

\[
\lambda = \beta = \sqrt{2\gamma(1-\gamma)}
\] (7)

We consider special case when 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 receive values \( \beta = \frac{1}{\sqrt{2}} \) and \( \lambda = 0.5 \).

We reviewed elements of the matrix describing the relationship between signal is sent to first port of splitter and signals are emanating from second and third output ports.

\[
b_1 = b_2 = \frac{1}{\sqrt{2}} a_1
\] (8)

The resulting mathematical expressions were equivalent to expressions obtained earlier for the case of using a beam splitter, when strong laser signal is sent to first input, and vacuum – to second input.

Also in [7] we research case with complex parameters of expression (5). Obtained result, with the exception of phase shift, coincides with results that were obtained for symmetric beam splitter.

![Figure 3. Block diagram of the experimental setup. L – laser, OI – optical isolator, HD – homodyne detector, EP – electronic processing system, ADC – analog-to-digital converter, PP – postprocessing system.](image)

Thus, as descriptions 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. Scheme of our experimental setup is represented in figure 3. We used a Teraxion-NLL laser (L) with wavelength 1550 nm on power 10 mW. After passing optical isolator (OI) radiation goes to fiber Y-splitter with dividing coefficient 50/50. The power of signal on the homodyne detector (HD) is 6 mW. To detection we used p-i-n photodiodes (fid13z81pz) with a quantum efficiency of 60% at 1550 nm, sensitivity \( S = 0.75 \) A/W, and a 1 GHz bandwidth. The currents from two photodiodes are subtracted and then resulting signal goes to electronic processing
system (EP), where signal is amplified. This circuit contains amplifier in a transimpedance configuration with a gain of 4 kΩ. 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 digitizing the received noise is 6 GHz. After digitizing we can choose and use most optimal post processing system (PP).

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

In our research we used four different ways to convert samples to sequences of bits: 1) if noise level in count is above 0, then we write "1", else – "0"; 2) we apply XOR to sequence, received by first method; 3) we generate three bits from one sample [6] (convert initial Gaussian distribution to uniform distribution, applying Gaussian error function); 4) we discard most significant bits after analog-to-digital conversion.

If we know probability properties of true random sequence, then we can check how much the generated sequence is similar to random. To do this, we select the appropriate statistics for each of the five tests [8] (monobit test, twobit test, “poker” test, runs test and autocorrelation test) and then compare its value for the ideal sequence and the generated sequence. These tests show [9] that optimal postprocessing technique for our scheme is discarding two or three most significant bits.

4. Conclusions
In this research we derived quantum mathematical description of Y-splitter and beam splitter, which are used in quantum random number generation, based on vacuum fluctuations. Also we obtain statistical parameters of differential current on outputs. In experimental implementation of QRNG systems based on quantum fluctuations of vacuum we use Y-splitter. In our research we consider four postprocessing methods to convert experimental samples to bits and after testing we conclude that optimal postprocessing technique for our system is discarding two or three most significant bits after analog-to-digital conversion.

Acknowledgments
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 № 14.578.21.0112 № 02.G25.31.0229).

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. 48, 1774
[4] Stipcevic M and Rogina M B 2007 Rev. Sci. Instrum. 78 045104
[5] Qi B, Chi Y-M, Lo H-K and Qian L 2010 Optics Letters 35 312
[6] Symul T, Assad S M and Lam P K 2011 Appl. Phys. Lett. 98 231103
[7] Ivanova A E, Chivilikhin S A, Gleim A V 2016 Nanosyst.: Phys. Chem. Math., 7(2), 378
[8] Menezes A, van Oorschot P, Vanstone S 1996 Handbook of Applied Cryptography (Boca Raton: CRC Press) p 816
[9] Ivanova A E, Chivilikhin S A, Gleim A V 2017 Nanosyst.: Phys. Chem. Math., 8 (2), 239