NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2017, 8 (2), P. 239–242

Quantum random number generator based on homodyne detection

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 10.17586/2220-8054-2017-8-2-239-242**

A quantum random number generator (QRNG) based on the quantum nature of vacuum fluctuations allows one to obtain random bit sequences that can be used in applications that require a high degree of randomness. In that type of quantum random generation system, optical beam splitters with two inputs and two outputs are normally used. A comparison of Y-splitter and spatial beam splitters shows that for two types of optical splitters, the quantum mathematical description of output signals is identical. This allows the use of fiber Y-splitters in practical QRNG schemes. The possibility of generating true random bits was demonstrated experimentally by using quantum random number generator based on homodyne detection.

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

Received: 14 January 2017

Revised: 1 February 2017

1. Introduction

The need to generate random numbers arises in many scientific and engineering disciplines. There are many types of random number generators with different entropy sources. Historically, two approaches for random number generation have been developed. According to the first method, random numbers can be generated algorithmically, but the resulting sequences in that case are pseudorandom and not suitable for applications in which a high degree of randomness is needed, such as classical or quantum cryptography [1]. These applications require true random numbers obtained by the second method, used indeterminate physical processes. For example, physical random number generators can use quantum processes. All QRNGs provide the necessary physical randomness for generated sequences that can be used in applications requiring high quality random numbers.

Existing approaches to quantum random number generation include different implementations: using separation of radiation [2], entangled photon states [3], quantum noise of lasers [4, 5] and photon emission and detection processes [6]. In alternative QRNG systems, quantum vacuum fluctuations are used as the entropy source. In this work, we investigate QRNG is based on quantum vacuum fluctuations [7–9] in which classical detectors are used, however, they can also measure quantum values. The principle of this type of QRNG is based on extracting randomness from quantum noise that appears upon subtracting the balanced detector signals received from beam splitter outputs. To first splitter input (Fig. 1a) a vacuum state is sent, and to other input – a coherent state from laser. On beam splitter these two signals are mixed, then signals from outputs of beam splitter come to balanced detector. One signal from the output of beam the splitter is subtracted from the other and the obtained signal is quantum noise, which can be processed using a PC.

A beam splitter is a key element for quantum random number generation schemes based on vacuum fluctuations [7–9]. Mathematical description of a beam splitter, when a strong laser signal, described by the Poisson distribution, arrives at one of its inputs and a vacuum state arrives to other, has been obtained in our previous research [10, 11] in the operator form. Also, we obtained mathematical description for fiber Y-splitter (Fig. 1b) and this, with the exception of phase shift, coincided with the previously-obtained expression for the beam splitter [10, 11]. Thus, as description for beam splitter and Y-splitter are equal, we can use Y-splitter for quantum random number generation system, based on homodyne detection.

2. Scheme and postprocessing methods

The scheme for our experimental setup is shown in Fig. 2a. During the research, a linear relationship between the laser power and the noise level was observed, which confirms that noise has quantum nature.

Quantum noise (Fig. 2b) obtained from our system had the following characteristics: mean value of fluctuations $\mu = 7 \cdot 10^{-6}$, standard deviation $\sigma = 0.03$, asymmetry coefficient $S = \frac{\mu_3}{\sigma^3} = -4.38 \cdot 10^{-3}$ (where μ_3 – third central moment of the noise distribution), kurtosis (a measure of sharpness of the random variable maximum) $K = \frac{\mu_4}{\sigma^4} = -3.87 \cdot 10^{-3}$ (where μ_4 – fourth central moment of the noise distribution), probability of the most

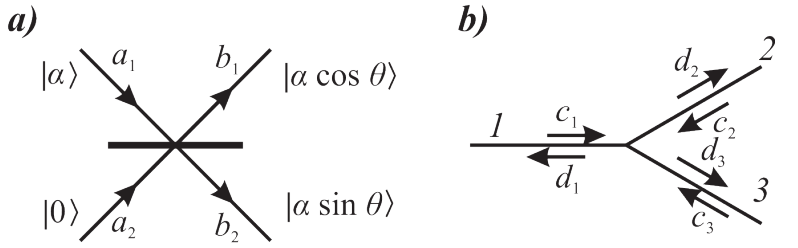

FIG. 1. a) Scheme of a beamsplitter with angle θ, where to the 1^{st} splitter input a_1 a coherent state is sent, and to other input a_2 – a vacuum state. b) Scheme of optical Y-splitter, where c_1, c_2, c_3 – input signals of 1^{st}, 2^{nd} and 3^{rd} ports, respectively, d_1, d_2, d_3 – output signals from the splitter

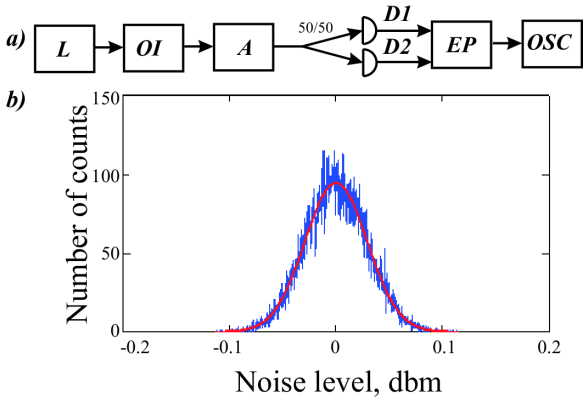

FIG. 2. a) Block diagram of the experimental setup. L – laser, OI – optical isolator, A – controllable attenuator, D1, D2 – detectors, EP – electronic processing system, OSC – oscilloscope; b) Distribution of samples on noise level

likely outcome $\max(P_i) = 3.02 \cdot 10^{-3}$ (where P_i – probability of the i-th realization of random discrete variable), min-entropy $H_{\min} = -\log_2(\max(P_i)) = 8.27$.

In our research, we used four methods to convert samples to sequences of bits:

A) If noise level in count is above 0, then we write "1", otherwise – "0" (Fig. 3a);
B) We apply XOR to sequence, obtained by the first method (Fig. 3a);
C) We generate three bits from one sample [9] (convert initial Gaussian distribution to uniform distribution, applying Gaussian error function, as shown in Fig. 3b);
D) We discard most significant bits after analog-to-digital conversion (Fig. 3c).

3. Randomness tests

Knowing the probability properties of a truly random sequence, we can verify how much of the generated sequence is genuinely random. To do this, we select the appropriate statistics for each test [12] and then compare its value for the ideal sequence and the generated sequence. If experimental sequence does not satisfy the criteria, then it is considered to be non-random. In our research we used five tests: monobit test, twobit test, "poker" test, autocorrelation test and runs test.

Monobit test is the simplest of all used tests. It is based on how equally frequent "0" and "1" appear in an ideal random number generator. If we denote the number of bits in the experimental sequence as L, quantity of "1" – n_1, quantity of "0" – n_0, then in this test, we can calculate next value:

$$X_1 = \frac{(n_0 - n_1)^2}{L}. \tag{1}$$

If the value X_1 exceeds a certain threshold (which depends on the confidence level of p, indicating the probability that test will reject a good generator, in our case $p = 0.01$), then the generator does not pass the test. Since X_1 has approximately χ^2-distribution with one degree of freedom, then the number 6.63 was taken as the threshold.

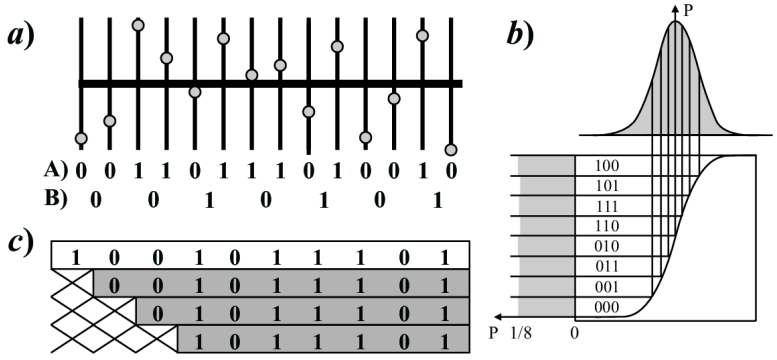

FIG. 3. Illustration of the four postprocessing methods for obtained samples: a) Illustrations of methods A and B; b) Illustration of method C, than convert one count to three bits; c) Illustration of method D, where most significant bits are discarding

In the *twobit test*, not only quantities of "0" and "1" are calculated, but also quantities of bit pairs "00", "01", "10" and "11". Numbers of this combinations we denote as n_1, n_0, n_{00}, n_{10}, n_{01}, n_{11} respectively. The function used in this test is as follows:

$$X_2 = \frac{4}{L-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{L}\left(n_0^2 + n_1^2\right) + 1, \tag{2}$$

which has χ^2 – distribution with two degrees of freedom. Therefore, the threshold for X_2 was chosen to be 9.21.

When we use the *"poker" test* the experimental sequence is divided into blocks with length m. This test is based on fact that in an ideal random sequence, all bits have equal probability. If we denote n_i as quantity of m-bit blocks, which have a binary representation of i, then we can consider the next statistics function:

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k, \tag{3}$$

where $k = L/m$ is the total number of m-bit blocks in the investigated sequence. Since the X_3 has the distribution χ^2 with $2m-1$ degrees of freedom, for $m = 4$ we need to choose a threshold of 30.6.

Runs test measures the number of occurrences of identical bits series (runs) with different lengths. In an ideal random number sequence, the average quantity of series with length i is equal $l_i = \dfrac{L-i+3}{2i+2}$. If we denote B_i and G_i as numbers of single and zero runs in tested sequences with length i, then we can calculate statistics:

$$X_4 = \sum_{i=1}^{n} \frac{(B_i - l_i)^2}{l_i} + \sum_{i=1}^{n} \frac{(G_i - l_i)^2}{l_i}, \tag{4}$$

which has the distribution χ^2 with $2n-2$ degrees of freedom, and we choose a threshold equal to 32.

Autocorrelation test is based on the fact that repetitive subsequences should not be in an ideal random sequence. In this test, we calculate the number of matching bits in the original and shifted by N_{shift} bit sequences. The statistics function is shown in the next formula:

$$X_5 = \frac{1}{\sqrt{L - N_{\text{shift}}}}\left(2\left(\sum_{i=0}^{L-N_{\text{shift}}-1} XOR\left(b_i, b_{i+N_{\text{shift}}}\right)\right) - L + N_{\text{shift}}\right), \tag{5}$$

where b_i – i-th bit of sequence. Since X_5 has a normal distribution with zero mean and variance equal to 1, the threshold is 2.33.

The results of randomness tests applied to sequences, which were obtained by four different post processing techniques, are shown in Table 1. We can see that the optimal postprocessing technique for our scheme is to discard two or three of the most significant bits.

4. Conclusion

We use Y-splitter for experimental implementation of QRNG systems based on quantum vacuum fluctuations. In our research, we considered four postprocessing methods to convert experimental samples to bits and after testing, we concluded that the optimal postprocessing technique for our system is to discard two or three of the most significant bits after analog-to-digital conversion.

TABLE 1. Results of randomness tests applied to sequences, obtained by different post processing techniques. "+" – test passed, "–" – test failed

Generation method	Method A	Method B	Method C	Method D. Discarding N MSB			
				$N=1$	$N=2$	$N=3$	$N=4$
Monobit test	+	+	+	+	–	+	+
Twobit test	–	+	+	–	–	+	+
"Poker" test	–	–	+	–	–	+	+
Runs test	+	+	–	–	–	+	+
Autocorrelation test	–	–	–	–	–	+	+

Acknowledgements

This work was financially supported by Government of Russian Federation, Grant 074-U01 and by the Ministry of Education and Science of Russian Federation (projects No. 14.578.21.0112, No. 02.G25.31.0229).

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] Reidler I., Aviad Y., Rosenbluh M., Kanter I. Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser. *Phys. Rev. Lett.*, 2009, **103**, P. 024102.
[6] 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.
[7] 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.
[8] Gabriel C., Wittmann C., et al. A generator for unique quantum random numbers based on vacuum states. *Nature Phot.*, 2010, **4**, P. 711–715.
[9] Symul T., Assad S.M. and Lam P.K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.*, 2011, **98**, P. 231103.
[10] Ivanova A.E., Chivilikhin S.A., Gleim A.V. Using of optical splitters in quantum random number generators, based on fluctuations of vacuum. *Journal of Physics: Conference Series*, 2016, **735**, P. 012077(1–4).
[11] Ivanova A.E., Chivilikhin S.A., Gleim A.V. The use of beam and fiber splitters in quantum random number generators based on vacuum fluctuations. *Nanosystems: Physics, Chemistry, Mathematics*, 2016, **7**, P. 378–383.
[12] Menezes A., van Oorschot P., Vanstone S. H*andbook of Applied Cryptography*. CRC Press, 1996, 816 p.