NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2013, 4 (4), P. 550–554

INVESTIGATION OF QUANTUM RANDOM NUMBER GENERATION BASED ON SPACE-TIME DIVISION OF PHOTONS

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

St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia

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

PACS 03.67.-a

In this paper we investigate a quantum random number generator based on the splitting of a beam of laser emitted light. Statistics of random numbers that depend on a parameter characterizing the symmetry of the beam splitter is theoretically analyzed and simulated. Degree of deviation of the obtained distribution from the uniform random distribution is investigated on a basis of series of statistical tests.

Keywords: quantum random number generation, beam splitter, random number distribution.

1. Introduction

Random numbers are used in many areas of human activity. Historically, two approaches for their generation have been developed. Pseudorandom number generators are based on algorithms implemented on a computing device. Physical generators extract randomness out of a complex physical systems fundamental chaotic behavior, making them suitable for generating truly random sequences. In particular, quantum random number generators (QRNG) belong to the second group. There are different ways to implement QRNG using beam separation [1, 2], entangled photon states [3, 4], processes of photon emission and detection [5, 6, 7], and quantum noise of lasers [8, 9]. Truly random numbers obtained by using a QRNG find many applications requiring higher quality random sequences than pseudorandom, including both classical and quantum cryptography. For example, in quantum cryptography protocols [10], the initial choice of the basis must be truly random.

Initially, simple QRNG was based on photon passage through a beam splitter, where the photon randomly follows one of two possible paths after emission [1, 2]. Similar implementations use several photons and a beam splitter, polarized photons with a polarizing beam splitter, or photons reflected from a diffraction grating (angular measurements are performed). Another type of scheme is based on time delay in one of the arms that photons pass [2]. Detecting the photon's arrival time, we can thus determine which path it has passed, and denote the short way as "0", and the long as "1" to get a sequence of random bits. This approach allows the use of a single detector, but leads to a loss in bitrate.

Such QRNGs are of great interest in the area of optical computation. Indeed, their relatively simple structure and the fact that they consist of only the basic optical elements (light source, detector, waveguide, beamsplitter) make them suitable for implementation as a fully-functional device or 'on-chip' element of a larger setup. However, it is known that imperfectness of actual optical parts may have a large impact on device functionality. In particular, every manufacturing technique is characterized by its own technological limits. Therefore, defining the tolerance of optical element parameters and investigating how they affect random number statistics remain an important task. In this work, we study angular parameters of the beamsplitter.

2. Investigation of random distribution statistics obtained directly from a laser

We consider a system consisting only of a laser, which acts as a radiation source, and a detector. The scheme is shown in fig. 1(a).

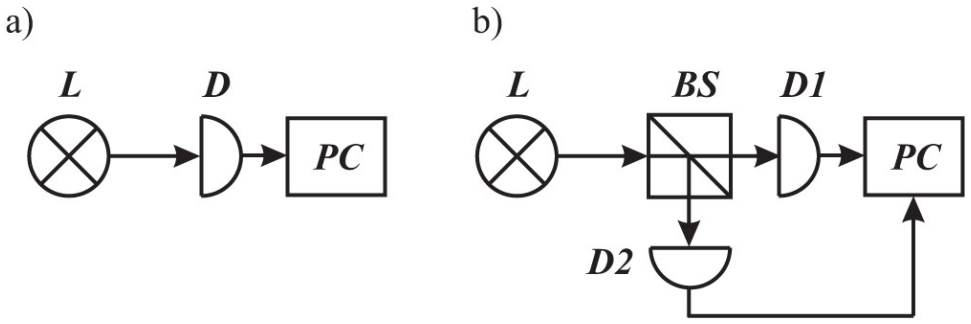

FIG. 1. a) Scheme of random distribution generation obtained directly from the laser, L - Laser, D - detector, PC - computer; b) Scheme of random distribution generation obtained by using a beam splitter, BS - beam splitter, D1, D2 - detectors

To obtain a random sequence, data received from the detector must be processed. A random variable that determines the binary sequence depends on laser radiation, which can be represented as a Poisson process:

$$P(k) = \frac{\lambda^k e^{-\lambda}}{k!},$$

where λ is the parameter of Poisson distribution.

This distribution includes multiphoton states, therefore, additional processing is required to provide binary generation results. We consider empty samples in a given time interval as "0", and samples with any number of photons in it as a "1". The parameter λ in the Poisson distribution should be set to $\lambda = \ln 2$ in order to achieve equal probabilities of zeros and ones in the final sequence. We simulated random sequence vector corresponding to Poisson distribution in Mathcad, using the previously calculated λ optimum value. Simulation results are shown in fig. 2.

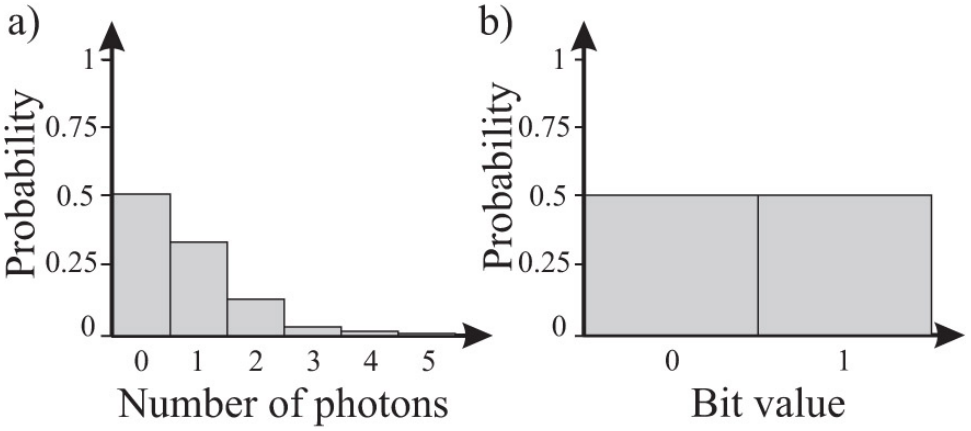

FIG. 2. Probability of occurrence of a) several photons (0-5) in the sequence before processing; b) zeros and ones in the sequence after processing

3. Investigation of distribution statistics obtained by using a beam splitter

We perform the simulation of a probabilistic process by dividing laser radiation with a beam splitter and alternating the obtained data from the detectors. The scheme is shown in fig. 1 b). Taking samples from the two outputs of the beam splitter, we obtain two Poisson distributions, from which, the final (output) binary distribution is generated.

Encoding of random bits from two sequences obtained after separation of the initial laser radiation with the beam splitter is performed as follows: if a non-zero number of photons comes to one of the detectors, and the other detector does not read any photons, such a condition is considered as a binary value 1. The opposite case is considered to be a binary value 0. Situations when both sensors detect or do not detect photons are ignored.

Generation of random numbers was modeled in Mathcad using a symmetric beam splitter. Angle θ of beam splitter in this case was 45°. Thus, the beam splitter output generates two Poisson sequences with the same value λ, which are processed. After modeling and processing, the final binary sequence was obtained. Its probabilities of zero and one bit values are shown in fig. 3(b).

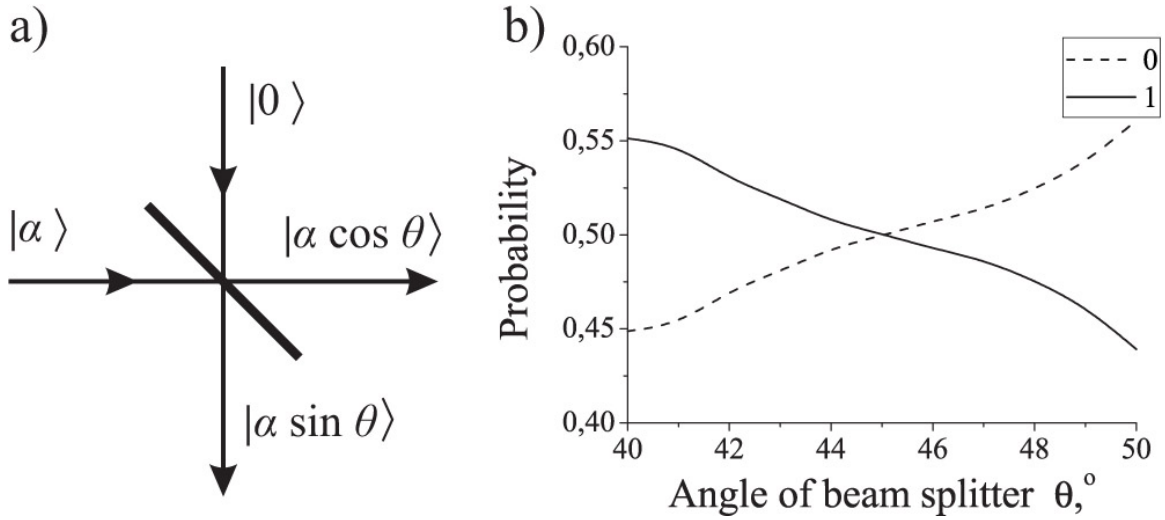

FIG. 3. a) Scheme of a beam splitter b) Probability of occurrence of "0" and "1" in the resulting sequence, depending on the beam splitter angle

4. Investigation of the beam splitter asymmetry influence on the quality of generated sequences

In case of an asymmetrical beam splitter (in practice it's very difficult to achieve perfect symmetry), asymmetry affects the probability of occurrence of ones and zeros in the final sequence of bits. We considered the effect of beam splitter angle on the quality of the generated sequence. The beam splitter scheme is shown in fig. 3(a).

Taking samples from two outputs of the beam splitter, we get two Poisson distributions with parameter values $\lambda_1 = \lambda\cos\theta$, $\lambda_2 = \lambda\sin\theta$. Using these distributions, output binary distribution is generated. Processing of two sequences is the same as in the previous case.

Beam splitter asymmetry affects the quality of the generated sequence. Statistical parameters of the binary distribution obtained with an asymmetric beam splitter are shown in fig. 3(b)). By increasing deviation of the beam splitter angle value from $\theta = 45°$, we increase the difference in zeros and ones generation probability in the final sequence. It is necessary

to calculate tolerance of beam splitter angular deviation from 45°, at which the final binary sequence can still pass tests of randomness.

5. Investigation of detector influence on the quality of generated sequences

Detector parameters affect the quality of generated sequences of random numbers. Let's consider a situation when the percentage of failure of both detectors is equal and detectors do not operate at some random times. Technically, it means that some random samples in two sequences produced by the beam splitter will be forced to zero. In this case, if the beam splitter asymmetry is initially low, the quality of the resulting sequence is not decreased, because the changes are random and the failure percentage is equal for both detectors. If the asymmetry is significant, the difference between the probabilities of zeros and ones remains at the same level, as with perfect detectors.

We also considered a situation when the percentages of failure of the two detectors are different. In this case, one of the sequences produced by the beam splitter will contain more zero samples than the other. Thus, the final sequence quality falls, because changes made by the detectors cause asymmetry in the processing sequences. Fig. 4 illustrates the probability of "0" or "1" bits occurrence depending on the ratio of detection probability on the first detector P_1 to probability of detection on second detector P_2.

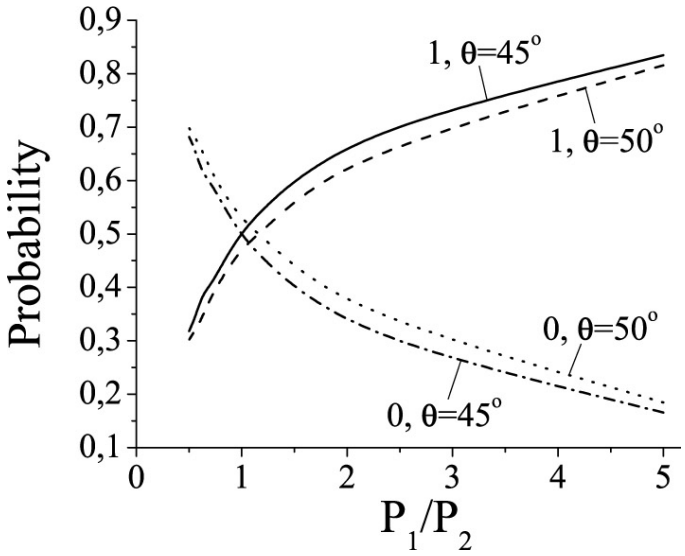

FIG. 4. Probability of zero or single bits occurrence in the sequence obtained by using beam splitters with angles $\theta = 45°$ and $\theta = 50°$, probability of detection of the first detector $P_1 = 10\%$

However, asymmetric detectors can compensate the difference in the probabilities of an asymmetric beam splitter, if their parameters are properly selected. For example, if after the beam division, in one of two resulting 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 observed.

6. Analysis of obtained results

A series of tests were used for controlling the quality of simulated sequences. These tests allowed the determination of all the continuous sequences of identical bits, and comparing

their distribution with the expected distribution of the series for a truly random sequence. In particular, we used monobit and twobit tests. During the analysis, we received the following results: both the sequence obtained directly from the laser, and the sequence obtained using a symmetric beam splitter, passed all the performed tests of randomness. For an asymmetric beam splitter, the uniformity of the distribution depended on the angle of the beam splitter. The generated sequences passed tests for randomness, if the deviation of the angle $\theta = 45^\circ$ was no more than two degrees.

The detector parameters also affected the generated sequences; with the difference in the frequency of detector responses degrading their quality.

7. Conclusion

A theoretical analysis and modeling of a random number distribution obtained directly from the laser and using the beam splitter, was performed. The influence of beam splitter parameters and parameters of detector to randomly generated sequence were investigated. The generated sequences passed tests for randomness if the deviation of the beam splitter angle $\theta =$ from 45° was less than two degrees. It was found that asymmetric detectors can compensate for the difference in the probabilities of an asymmetric beam splitter.

References

[1] T. Jennewein, U. Achleitner, et al. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, **71** (4), P. 1675–1680 (2000).

[2] A. Stefanov., N. Gisin, et al. Optical quantum random number generator. *J. Modern Optics*, **47** (4), P. 595–598 (2000).

[3] M. Fiorentino, C. Santori, et al. Secure self-calibrating quantum random bit generator. *Phys. Rev. A.* **75**, P. 032334 (2007).

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

[5] M. Stipcevic, M.B.Rogina. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum.*, **78**, P. 045104 (2007).

[6] J.F. Dynes, Z.L. Yuan, A.W. Sharpe, A.J. Shields. A high speed, post-processing free, quantum random number generator. *Appl. Phys. Lett.*, **93**, P. 031109 (2008).

[7] M. Furst, H. Weier, et al. High speed optical quantum random number generation. *Optics Express*, **18**, P. 13029 (2010).

[8] B. Qi, Y.M. Chi, H.-K. Lo, L. Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, **35**, P. 312–314 (2010).

[9] I. Reidler, Y. Aviad, M. Rosenbluh, I. Kanter. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. *Phys. Rev. Lett.*, **103**, P. 024102 (2009).

[10] V. Scarani, H. Bechmann-Pasquinucci, et al. The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, P. 1301–1350 (2009).