NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2021, 12 (2), P. 156–160

Quantum random number generator using vacuum fluctuations

B. E. Pervushin[1], M. A. Fadeev[1,2], A. V. Zinovev[1], R. K. Goncharov[1], A. A. Santev[1], A. E. Ivanova[1,2], E. O. Samsonov[1,2]

[1]ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia
[2]Quanttelecom LLC, 6 liniya, Vasilievsky island d.59, korp. 1, lit. B, St. Petersburg, 199178, Russia

borispervushin@itmo.ru, wertsam@itmo.ru, avzinovev15@yandex.ru, rkgoncharov@itmo.ru, aasantev@itmo.ru, aeivanova@itmo.ru, eosamsonov@itmo.ru

PACS 03.67.-a **DOI 10.17586/2220-8054-2021-12-2-156-160**

Experimental implementation of a quantum random number generator based on vacuum fluctuation is presented in this paper. A Y-splitter is used in optical setup of the quantum random number generator. The generation of random numbers in real time with a speed of 300 Mb/s is demonstrated. The conditional minimum entropy is used to estimate the randomness. A cryptographic hashing function is used for post-processing. The resulting sequence has passed DieHard and NIST statistical tests successfully.

Keywords: quantum random number generation, homodyne detection, vacuum fluctuation.

Received: 1 March 2021

Revised: 4 March 2021

1. Introduction

There is a demand for random numbers in many fields of science and technology [1–4]. Existing random number generators (RNG) can be divided into two groups: pseudo-random [5] and physical [6]. Pseudo-random RNGs are based on the use of mathematical algorithms, the output bit sequences of such generators can be predictable. Physical generators using classical physical processes as a source of entropy can also be potentially predictable due to the determinism inherent in classical processes. Such generators can be used in fields that do not require true randomness. However, for certain tasks, more reliable random number generation devices should be used. In particular, the generation of encryption keys in cryptographic systems requires truly random numbers, which can be obtained only by using a quantum random number generator (QRNG). QRNGs are based on quantum processes, which are nondeterministic. Randomness in such generators can be extracted based on the principle of detecting single photons in different optical modes [7], using entangled photons [8], laser phase noise [9], or measuring fluctuations of vacuum [10, 13]. The last type of QRNGs is of the interest due to the simplicity of implementation, relatively compact size, and high speed of random sequence generation. On-chip implementations of the QRNG have been actively developed, due to small dimensions and stability of work [11, 12]. This paper demonstrates the implementation of a quantum random number generator based on vacuum fluctuations using a Y beam splitter. The presented device provides generation of random numbers in real time at a speed of 300 Mb/s. To determine the unpredictability of the output sequence, an estimate of the conditional minimum entropy was employed using the approach described in [15, 16]. The resulting random sequence was tested using the well-known battery of statistical tests DieHard [17] and NIST [18].

2. Quantum randomness generation system

The result of the interference of the reference field, described by Poisson statistics, and the vacuum field on an optical beam splitter with two input and two output ports is described in operator form in [19], these beam splitters were used in the QRNG based on vacuum fluctuations in a number of works [10, 13, 14]. In this work, for the experimental implementation of QRNG based on vacuum fluctuations, the Y-beam splitter is used, the mathematical substantiation of the possibility of using it is presented in [20, 21]. The QRNG scheme based on vacuum fluctuations is shown in Fig. 1.

In the presented QRNG, laser beam (reference field) is mixed with the vacuum field at a polarizing Y beam splitter [22]. A polarization controller is used to fine-tune the division ratio. Thus, two inputs of the balanced detector receive signals containing an amplified vacuum signal as one of its components, which appears as shot noise as a result of detection.

After detection, the differential photocurrent is amplified using a transimpedance amplifier. The resulting voltage, randomly varying in time, is converted into a numerical sequence by an ADC. An extractor is used to extract a truly

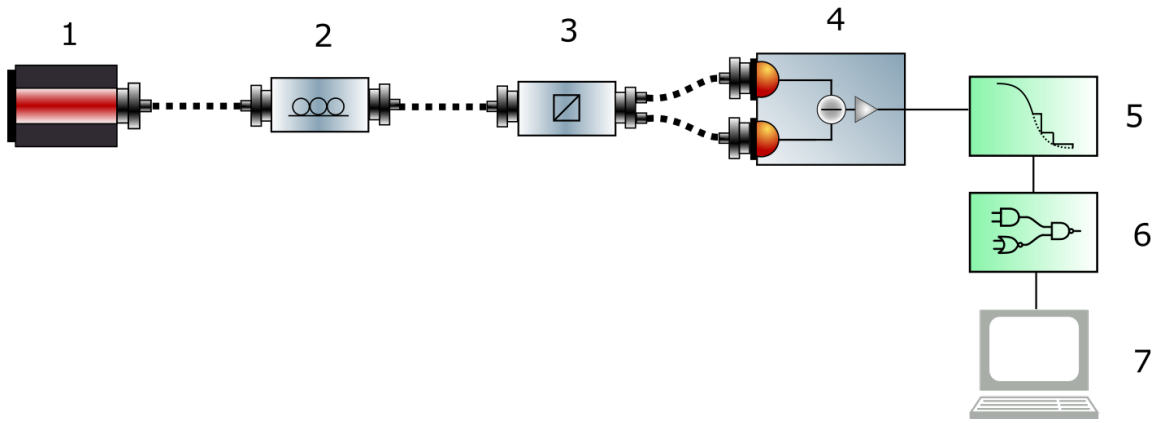

FIG. 1. Scheme of the quantum random number generator based on vacuum fluctuation. 1 – laser; 2 – polarization controller; 3 – Y beam splitter; 4 – balanced detector; 5 – ADC; 6 – FPGA; 7 – computer.

random normally distributed sequence. In particular, to extract a random sequence, an AES-based cryptographic hashing algorithm is used.

3. Experiment

In the proposed experimental implementation, the laser power is set to 40 mW. The reference field is divided on the beam splitter after polarization controller, the total loss of which is 1.06 dB. Two outputs of the Y-splitter are connected to two inputs of a balanced detector, the bandwidth of which is 100 MHz. The electrical signals from the two photodiodes are subtracted and the resulting current is converted to voltage using a transimpedance amplifier. The resulting voltage signal is digitized using a high-speed 8-bit ADC with 100 MHz bandwidth and 150 MHz sampling rate.

The rate of generating a raw sequence of random numbers is:

$$v = \min\left(\tau^{-1}, 2BW\right) \cdot n, \tag{1}$$

where τ^{-1} is the ADC measurement frequency, BW is the smallest bandwidth of the analog signal, n is a number of bits per measurement.

From the formula (1) it can be seen that the generation rate is limited by the measurement frequency and the smallest bandwidth in the circuit. Thus, the raw sequence speed is 1200 Mb/s.

Since, in addition to quantum noise, the system contains untrusted electronic noises, it is necessary to estimate the conditional entropy of the source, taking into account that the intruder can control classical noise. For this purpose, the minimum entropy is used, which, in comparison with the Shannon entropy, is a more rigorous estimate and is generally determined by:

$$H_{\min}\left(M_{dis}\right) = -\log_2\left(\max_i p_i\right), \tag{2}$$

where M_{dis} is a measured discrete signal, p_i are probabilities of different measurement outcomes.

When taking into account the eavesdropper, the conditional minimum entropy in our case is [15]:

$$H_{\min}\left(M_{\text{dis}} \mid E\right) = -\log_2\left(\max\left\{\frac{1}{2}\left[\operatorname{erf}\left(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}\sigma_q}\right) + 1\right], \operatorname{erf}\left(\frac{\delta}{2\sqrt{2}\sigma_q}\right)\right\}\right), \tag{3}$$

where R is a half the dynamic range of the ADC, $\delta = R/2^{n-1}$, $e_{\max}$ is a maximum value of the electronic signal, and σ_q is a standard deviation of a quantum signal.

Due to the independence of the quantum and electronic signals, the standard deviation of the quantum signal is defined as:

$$\sigma_m^2 = \sigma_e^2 + \sigma_q^2, \tag{4}$$

where σ_m is a standard deviation of the measured signal (sums of quantum and electronic signals), σ_e is a standard deviation of the electronic signal. In the experimental QRNG system, the minimum entropy of the source was 4.78.

The unpredictability of the resulting bit sequence can be guaranteed by the Leftover Hash Lemma [23]. If the hash function converts k bits to

$$l < k \cdot H_{\min}/n - 2\log_2(1/\varepsilon), \tag{5}$$

then the output sequence will be ε-close to the uniform distribution. In this case $k = 1024$, $l = 256$, then the security parameter is less than 2^{-177}. A rather strict security parameter was chosen here, since the hashing algorithm used in this work is not universal [15]. The final sequence generation rate is:

$$V = v \text{ Mb/s} \cdot \frac{256}{1024} = 300 \text{ Mb/s}. \tag{6}$$

DieHard and NIST statistical tests were used to check the resulting output sequence. The results are shown in Tables 1 and 2.

TABLE 1. DieHard statistical test results. The obtained p-value for successful passing of the test must lie in the interval $0.025 <$ p-value < 0.975

No.	Test	p-value
1	BIRTHDAY SPACINGS TEST	0.165456
2	THE OVERLAPPING 5-PERMUTATION TEST	0.654752
3	the BINARY RANK TEST for 31x31 matrices BINARY RANK TEST for 32x32 matrices	0.792586
4	BINARY RANK TEST for 6x8 matrices	0.431478
5	THE BITSTREAM TEST	0.437767
6	OPSO	0.427352
	OQSO	0.481557
	DNA	0.482048
7	the COUNT-THE-1's TEST on a stream of bytes	0.095081
8	the COUNT-THE-1's TEST for specific bytes	0.563297
9	THIS IS A PARKING LOT TEST	0.896585
10	THE MINIMUM DISTANCE TEST	0.815571
11	THE 3DSPHERES TEST	0.039996
12	the SQEEZE test	0.134697
13	The OVERLAPPING SUMS test	0.470491
14	the RUNS test	0.290913
15	CRAPS TEST	0.466673

4. Conclusion

The paper describes an experimental implementation of a system for the generation of random numbers in real time, based on vacuum fluctuations. The quantification of unpredictability is determined by the conditional minimum entropy, taking into account the presence of the eavesdropper. The minimum entropy was 4.78. The resulting sequence has successfully passed the NIST and DieHard statistical test batteries. The parameters of the experimental model of the system made it possible to achieve a generation rate of 300 Mb/s.

Conflict of interest

The authors declare no conflicts of interest.

TABLE 2. Results of passing NIST statistical tests. The p-values must be p-value > 0.025 to pass successfully

No.	Test	p-value
1	BIRTHDAY SPACINGS TEST	0.165456
2	THE OVERLAPPING 5-PERMUTATION TEST	0.654752
3	the BINARY RANK TEST for 31x31 matrices BINARY RANK TEST for 32x32 matrices	0.792586
4	BINARY RANK TEST for 6x8 matrices	0.431478
5	THE BITSTREAM TEST	0.437767
6	OPSO	0.427352
	OQSO	0.481557
	DNA	0.482048
7	the COUNT-THE-1's TEST on a stream of bytes	0.095081
8	the COUNT-THE-1's TEST for specific bytes	0.563297
9	THIS IS A PARKING LOT TEST	0.896585
10	THE MINIMUM DISTANCE TEST	0.815571
11	THE 3DSPHERES TEST	0.039996
12	the SQEEZE test	0.134697
13	The OVERLAPPING SUMS test	0.470491
14	the RUNS test.	0.290913
15	CRAPS TEST	0.466673

Acknowledgements

This work was funded by Government of Russian Federation (grant MK-777.2020.8).

References

[1] Ferrenberg A.M., Landau D.P., et. al. Monte Carlo simulations: Hidden errors from "good" random number generators. *Physical Review Letters*, 1992, **69** (23), 3382.
[2] Gennaro R. Randomness in cryptography. *IEEE security & privacy*, 2006, **4** (2), P. 64–67.
[3] Gisin N., Ribordy G., et. al. Quantum cryptography. *Reviews of modern physics*, 2002, **74** (1), 145.
[4] Metropolis N., Ulam S. The monte carlo method. *Journal of the American statistical association*, 1949, **44** (247), P. 335–341.
[5] Nisan N., Wigderson A. Hardness vs randomness. *Journal of computer and System Sciences*, 1994, **49** (2), P. 149–167.
[6] Johnston D. *Random Number Generators – Principles and Practices: A Guide for Engineers and Programmers*. Walter de Gruyter GmbH & Co KG: 2018, 439 p.
[7] Jennewein T., Achleitner U., et. al. A fast and compact quantum random number generator. *Review of Scientific Instruments*. 2000, **71** (4), P. 1675–1680.
[8] Pironio S., Acin A., Massar S., et. al. Random numbers certified by Bell's theorem. *Nature*, 2010, **464** (7291), P. 1021–1024.
[9] Guo H., Tang W., et. al. Truly random number generation based on measurement of phase noise of a laser. *Physical Review E*, 2010, **81** (5), 051137.
[10] Shi Y., Chng B., et. al. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 2016, **109** (4), 041101.
[11] Kiselev F.D., Samsonov E.O., Gleim A.V. Modeling of linear optical controlled-Z quantum gate with dimensional errors of passive components. *Nanosyst.: Phys. Chem. Math.*, 2019, **10** (6), P. 627–631.
[12] Raffaelli F., et al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Science and Technology*, 2018, **3** (2), 025003.
[13] Gabriel C., Wittmann C., et al. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 2010, **4** (10), P. 711–715.
[14] Ivanova A.E., Chivilikhin S.A., et al. How scatter of the experimental parameters affects the statistical characteristics of a quantum random-number generator. *J. Opt. Technol.*, 2014, **81** (8), P. 427–430.

[15] Haw J.Y., Assad S.M., et. al. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Applied*, 2015, **3** (5), 054004.

[16] Guo X., Liu R., et. al. Enhancing extractable quantum entropy in vacuum-based quantum random number generator. *Entropy*, 2018, **20** (11), 819.

[17] Marsaglia G. DIEHARD Test suite, 1998. `URL: http://www. stat. fsu. edu/pub/diehard`.

[18] Rukhin A., et. al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2010.

[19] Grynberg G., et. al. *Introduction to quantum optics: from the semi-classical approach to quantized light*. Cambridge university press, 2010.

[20] Ivanova A.E., Chivilikhin S.A., Miroshnichenko G.P., Gleim A.V. Fiber quantum random number generator, based on vacuum fluctuations. *Nanosyst.: Phys. Chem. Math.*, 2017, **8** (4), P. 441–446.

[21] 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. *Nanosyst.: Phys. Chem. Math.*, 2016, **7** (2), P. 378–383.

[22] Ivanova A.E. Quantum generation of random bit sequences based on vacuum fluctuations in a fiber-optic circuit. PhD Thesis, St. Petersburg, 2017, 121 p.

[23] Tomamichel M., et. al. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 2011, **57** (8), P. 5524–5535.