Reviews on Advanced Materials and Technologies, 2025, vol. 7, no. 3, pp. 148–154
DOI: 10.17586/2687-0568-2025-7-3-148-154

High-Speed QRNG Based on Phase Noise of VCSEL and DFB Laser

Karina Razzhivina [1,*], Yakov Kovach [1,2], Anton Kovalev [1], Evgenii Kolodeznyi [1]

[1] Institute of Advanced Data Transfer Systems, ITMO University, Kronverkskiy pr., 49, lit. A, St. Petersburg, 197101, Russia
[2] Ioffe Institute, Politekhnicheskaya ul., 26, St. Petersburg, 194021, Russia

Article history

Received May 30, 2025
Received in revised form, July 28, 2025
Accepted August 13, 2025
Available online August 15, 2025

Abstract

Quantum random number generators (QRNGs) are crucial for cryptography and secure data transfer; however, existing implementations often compromise between speed, cost, and complexity. In this paper we present QRNG based on a phase noise of a vertical-cavity surface-emitting laser (VCSEL) heterodyned with distributed feedback (DFB) laser, that combines the ultra-narrow linewidth and stability of DFB lasers with the high entropy phase noise of VCSELs at 1550 nm. We characterize optical beats of the setup and implement the XOR post-processing algorithm to suppress correlations when the signal is digitized, achieving random bit generation at 12 Gbps. The generated sequences pass NIST SP 800-22 tests while operating at low bias currents and with high stability, therefore, it can be successfully implemented into quantum key distribution systems that demand both speed and reliability.

Keywords: Quantum random number generation; VCSEL; DFB-laser; Phase noise

1. INTRODUCTION

Quantum random number generators (QRNGs) based on the phase noise of lasers are vital components for cryptographic applications, especially quantum key distribution systems due to high phase uncertainty and robustness to the detector noise [1]. QRNGs produce true random numbers because of quantum phenomena, particularly, because of quantum mechanics axiom of incompatibility and uncertainty for the phase-noise based QRNGs. Several groups demonstrated QRNGs with the random bit generation rates up to Gbps [2–4]. Most of the experimental setups demonstrated are self-heterodyned [5,6] and use only one light source, which means the QRNG is device-trusted. However, the device may be defective, or it can be compromised by the adversary, so the device-independent QRNGs are more secure than the device-trusted [7]. Another possible solution is a semi-device-trusted QRNG. Avesani et al. developed the semi-device-trusted QRNG setup based on the continuous-wave laser as a light source and achieved the sequence generation rate of 113 Mbps [8]. Nevertheless, such devices have lower speed despite the higher attack resistance.

In Ref. [9] one of the first delay-free device-trusted setup was demonstrated, which was based on two DFB-lasers and achieved random bit generation rate up to 600 Mbps. DFB laser diodes have been implemented into several QRNG schemes operating as continuous-wave lasers [10–13]; however, in Ref. [14] it was shown that pulsed processes can reach higher random bit rates. In contrast to VCSEL-based, QRNG based on DFB-lasers demonstrated better stability and lower autocorrelations along with high coherence. Moreover, QRNG based on DFB-lasers reached high sequence generation rates up to hundreds of Gbps [13]. Meanwhile VCSELs have numerous advantages for QRNG applications such as construction simplicity, small size, low threshold current, high energy efficiency, and high modulation speeds in comparison with edge-emitting lasers [10,15]. Moreover, broad phase noise bandwidth, up to hundreds of MHz, can be reached with VCSEL. The phase noise of VCSEL also can be increased with the gain switching mode, allowing the laser to build up from spontaneous emission with each pulse [15].

In this paper, we present the hybrid approach to basic QRNG setup based on the phase noise using VCSEL and DFB-laser. Using the advantages of both types of lasers:

* Corresponding author: Karina Razzhivina, e-mail: krrazzhivina@itmo.ru

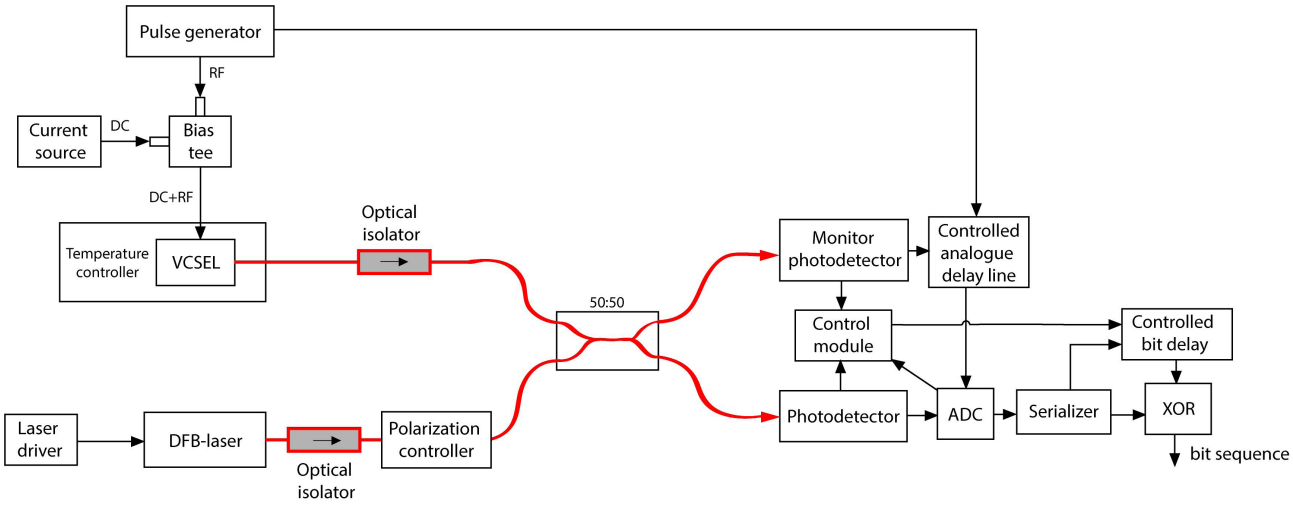

Fig. 1. The scheme of the proposed QRNG.

high entropy extraction and stability for quantum key distribution links, we applied the post-processing algorithm which included the XOR operation as one of the fastest and simplest algorithms for random bits generation to mitigate correlations that are possible when the heterodyne beat signal of the lasers is digitized. The post-processing algorithm includes determining the optical beat signal registration time which corresponds to the highest differential entropy value.

2. METHODS

We developed the setup using the 1550 nm VCSEL with strained quantum wells InGaAs/InAlGaAs [16] and the InGaAsP/InP laser module Nolatech DFB-1550-14BF. The proposed quantum random number generator setup is presented in Fig. 1. The VCSEL is pumped by a constant current source and a pulse generator Keysight M8195A connected through a bias tee provides gain-switching mode, while DFB-laser operates in continuous wave mode and is controlled by a laser driver. The laser module DFB-1550-14BF is butterfly-packaged with a built-in thermo-electric cooler and a temperature sensor, and the DFB laser temperature is stabilized by the driver. The temperature of the VCSEL is stabilized using a temperature controller. To protect the lasers from the reflected signals, two optical isolators are placed after the laser outputs.

Optical splitter combines the output signals of the VCSEL and the DFB-laser resulting in their heterodyning and divides the signal into two equally-power signals. The lasers have polarized output and the setup uses standard single mode fibers for interconnects, that are fixed to the optical table. To maximize heterodyne signal amplitude, the polarization controller is used. The heterodyned signal shows optical beating signals when the VCSEL is gain-switched, with the phase of the VCSEL being random as the laser is switched-off between pulses.

One of the signals is transmitted to a monitor photodetector, and another signal goes to a photodetector and an analog-to-digital converter (ADC). The control module registers the output signal of the monitor photodetector to check the QRNG system operation and determines the time delay made with the controlled analogue delay line; therefore, the post-processing algorithm is realized according to the maximum entropy value calculated. The serializer changes the parallel output interface of ADC to sequential in compliance with the number of least significant digits M, which is equal to 4. The serializer output signal is divided into two sequences. One of these streams is transmitted through the controlled bit delay and shifted by K bits backwards in time. Then the exclusive OR (XOR) operation is applied to resulting sequences. Therefore, the output signal is the bit sequence with generation rate of M / T, i.e. multiplication of number of least significant digits M and generator pulse frequency $1 / T$, which corresponds to frequency of the appearing pulses. In the experimental approbation of the proposed scheme, the optoelectronic converter Keysight N7004A having the bandwidth of 33 GHz was used as the photodetector, and the oscilloscope Keysight UXR0204A was used as the ADC. The post-processing was done offline using Julia language software based on the recorded time traces.

The post-processing algorithm determines the time when the highest value of registered optical beats differential entropy is achieved. To evaluate it, the histograms of optical beat magnitudes were recorded according to the delay time change from 0 to pulse period T with step dt, which corresponds to the following number of values:

$$B = T / dt + 1. \tag{1}$$

The differential entropy was estimated according to the formula:

$$H = \sum_{j=1}^{J} p_j dj \log(p_j dj), \tag{2}$$

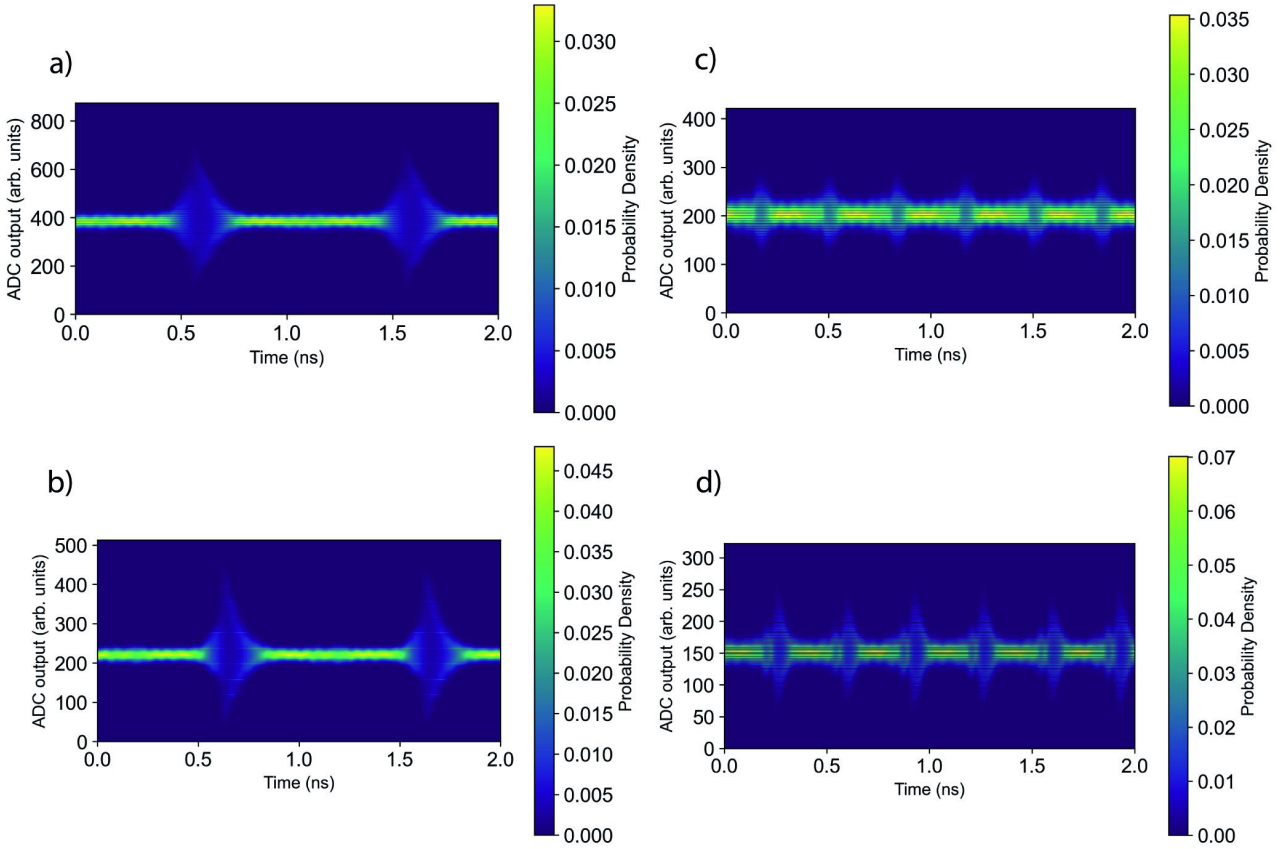

Fig. 2. Magnitude of optical beats and probability density distribution: a) pump current is 1.45 mA, pulse frequency is 1 GHz, duty cycle is 20%, pulse magnitude is 280 mV; b) pump current is 1.55 mA, pulse frequency is 1 GHz, duty cycle is 20%, pulse magnitude is 230 mV; c) pump current is 1.45 mA, pulse frequency is 3 GHz, duty cycle is 65%, pulse magnitude is 1000 mV; d) pump current is 1.55 mA, pulse frequency is 3 GHz, duty cycle is 65%, pulse magnitude is 600 mV.

where p_j is probability density of optical beat magnitude in the computed histograms, J is the number of intervals (histogram bins). The interval step dj is defined with the following equation:

$$dj = (A_{\max} - A_{\min}) / J, \tag{3}$$

where $A_{\max}$ is the maximum magnitude of optical beats, $A_{\min}$ is the minimum magnitude of optical beats. Thus, the matrix of $J \times B$ values is determined, where each value corresponds to the probability density of optical beat magnitude over the pulse delay.

3. RESULTS AND DISCUSSION

The optical beats are presented as the interference result of VCSEL and DFB laser radiation. Histograms of optical beats obtained for several cases are presented in Fig. 2 with the parameters given in the caption. We adjusted the pulse magnitude to maintain stable gain-switching mode for VCSEL and, consequently, to get distinct optical beats. Oscilloscope saved the time-domain diagrams with the sampling frequency of 128 Gbps (time step dt = 7.81 ps). For each of the 4 cases 805306368 values were recorded, and the number of amplitude intervals for the histogram was $J = 200$.

The differential entropy was calculated according to the formula (2). The time-domain distributions of the entropy are presented in Fig. 3. According to the described post-processing algorithm, the values of the signal recorded by the ADC were extracted at the time moments where the maximum entropy values of optical beats were observed. To verify the randomness of the digits, the probability distribution function (PDF), and the autocorrelation function (ACF) of the random value arrays were calculated (Fig. 4). According to the presented diagrams of PDF and ACF, all the digital sequences may be considered as random, since there is no correlation or periodicity. However, the pulse generation frequency impacts the shape of the PDF. The pulse frequency of 1 GHz corresponds to the complex distributions with bumps at the edges, but for the pulse frequency of 3 GHz the exponential decay of PDF is observed. The increase of pumping current leads to the plateau broadening.

The obtained ADC digits were then converted to bits, and the obtained binary sequences were validated with

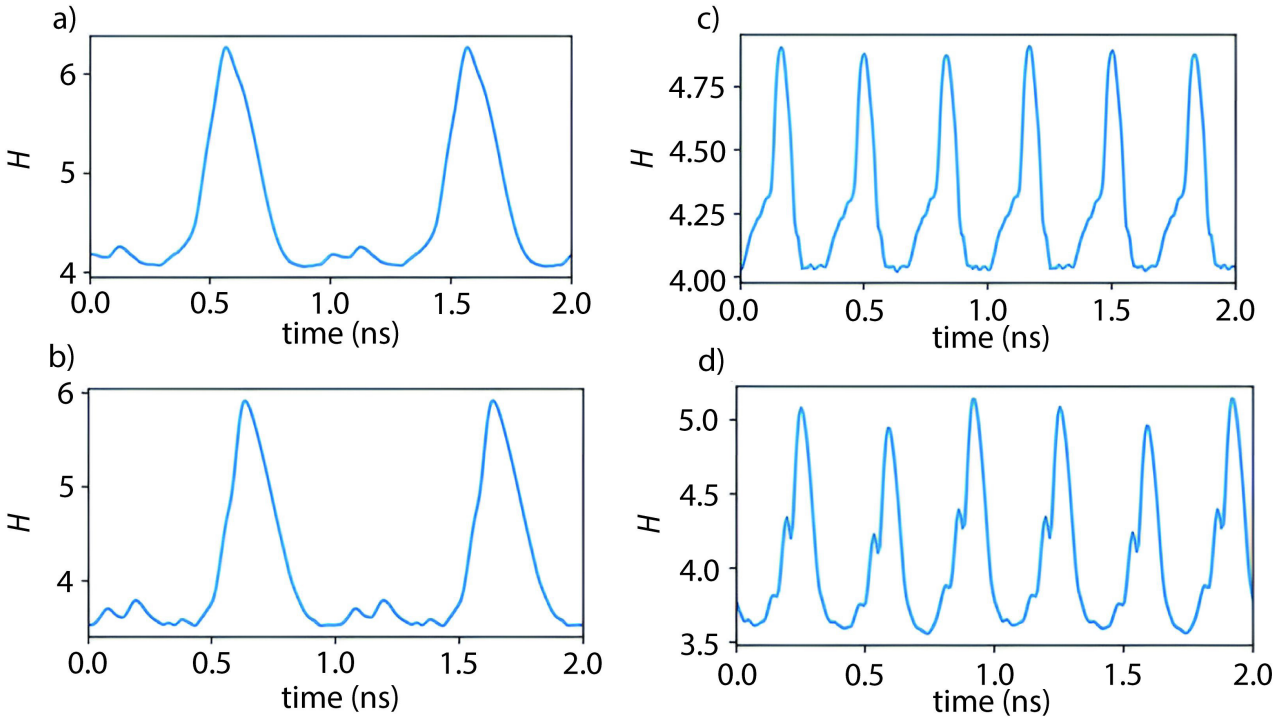

Fig. 3. Time-domain distributions of the differential entropy. Parameters for (a–d) corresponds to those of Fig. 2.

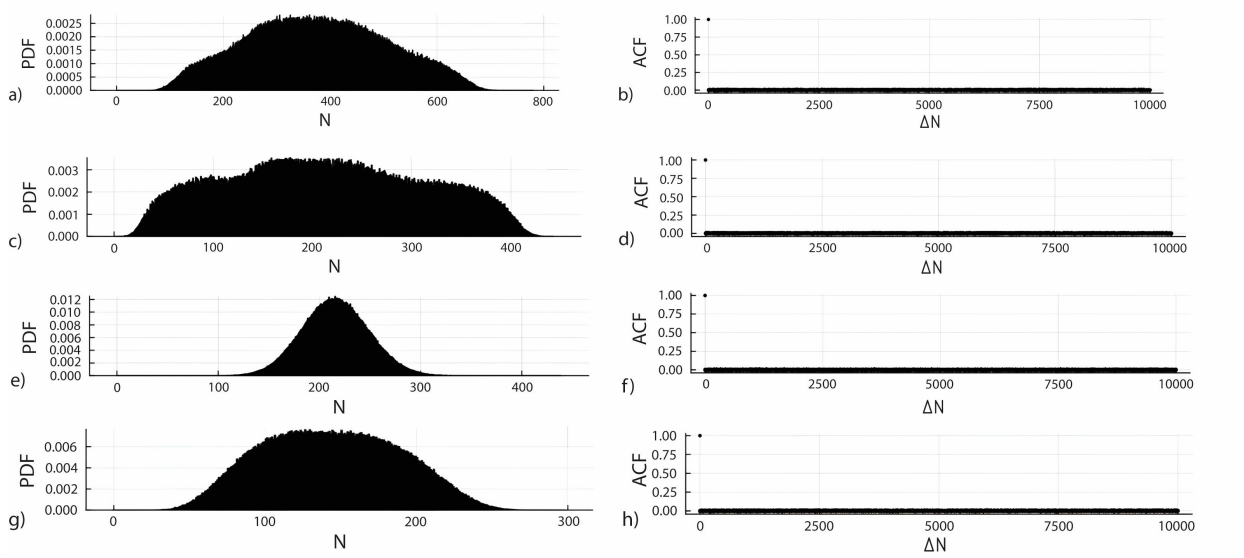

Fig. 4. Probability distribution fuction (a, c, e, g) and autocorrelation function (b, d, f, h): when pumping current is 1.45 mA, pulse repetition frequency is 1 GHz (a, b); pumping current is 1.55 mA, pulse repetition frequency is 1 GHz (c, d); when pumping current is 1.45 mA, pulse repetition frequency is 3 GHz (e, f); pumping current is 1.55 mA, pulse repetition frequency is 3 GHz (g, h).

NIST SP 800-22 tests [17] using *p*-value of 0.01. Therefore, the fraction of sequences which passed the tests at significance level α of 0.01 should be equal to:

$$p_f = 0.99 \pm 3\sqrt{(1-\alpha)\alpha / m}, \quad (4)$$

where m is the number of random beats subarrays consisting of 10^6 number of bits.

The fractions of sequences which were verified with the tests without post-processing are presented in Table 1. The fractions of sequences marked with gray color correspond to the failed test.

Then, the binary sequences were post-processed with XOR operation with 1-bit shift where two neighboring bits undergo XOR, to eliminate possible correlations related to the digitizing. The fractions of sequences passed the test with post-processing are presented in Table 2.

The tables show that all the tests were passed for the combination of the following parameters: 1) without the

Table 1. The fraction of sequences passed the corresponding NIST SP 800-22 test without post-processing.

Test	Fraction of sequences passed the test			
	1 GHz		3 GHz	
	1.45 mA	1.55 mA	1.45 mA	1.55 mA
Frequency (Monobit) Test	1	1	1	0.973
Frequency Test within a Block	1	1	0.987	1
Runs Test	1	1	1	1
Test for the Longest Run of Ones in a Block	1	0.96	1	0.987
Binary Matrix Rank Test	1	1	1	0.973
Discrete Fourier Transform (Spectral) Test	1	1	1	1
Non-overlapping Template Matching Test	1	1	1	1
Overlapping Template Matching Test	1	1	1	0.973
Maurer's "Universal Statistical" Test	0.96	1	0.96	0.987
Linear Complexity Test	1	1	1	1
Serial Test	0.96	1	1	1
Approximate Entropy Test	1	1	0.987	0.987
Cumulative Sums (Cusum) Test	1	1	1	0.947
Random Excursions Test	0.96	0.96	0.947	0.867
Random Excursions Variant Test	0.92	0.96	0.96	0.96

Table 2. The fraction of sequences passed the corresponding NIST SP 800-22 test with post-processing.

Test	Fraction of sequences passed the test			
	1 GHz		3 GHz	
	1.45 mA	1.55 mA	1.45 mA	1.55 mA
Frequency (Monobit) Test	1	1	1	1
Frequency Test within a Block	1	1	1	1
Runs Test	1	1	1	0.933
Test for the Longest Run of Ones in a Block	0.92	1	1	1
Binary Matrix Rank Test	0.96	1	0.987	1
Discrete Fourier Transform (Spectral) Test	1	1	1	0.96
Non-overlapping Template Matching Test	1	1	1	0.987
Overlapping Template Matching Test	1	1	1	1
Maurer's "Universal Statistical" Test	1	0.96	1	1
Linear Complexity Test	1	1	1	1
Serial Test	1	1	0.987	0.973
Approximate Entropy Test	1	1	1	1
Cumulative Sums (Cusum) Test	1	1	1	1
Random Excursions Test	0.96	0.72	0.96	0.907
Random Excursions Variant Test	0.88	0.88	0.96	0.933

post-processing, pulse frequency of 1 GHz and current of 1.55 mA; 2) with the post-processing, pulse frequency of 3 GHz and current of 1.45 mA. According to Table 2, the applied postprocessing improved the performance of QRNG at the pulse frequency of 3 GHz and current of 1.45 mA, but for the other sequences the performance was deteriorating. Particularly, there is a strong decrease in the fraction of sequences that passed the random excursions variant test.

4. CONCLUSIONS

In this paper, we demonstrated the QRNG setup based on phase noise of VCSEL and DFB-laser. The combination of two different sources provides stable operation in pulsed gain-switched mode. The developed QRNG produces random sequences with the generation rate up to 12 Gbps, which is significantly higher than the generation rate of QRNG based on DFB lasers, requiring only simple XOR post-processing. The autocorrelation function showed lower values than the typical autocorrelation function of VCSEL-based QRNGs, which is due to the time stamps, at which the random numbers are extracted, corresponding to the maximized differential entropy, and hence the randomness quality and the communication security may be increased. No delay line is required for the presented setup; therefore, the presented setup may be further modified

as an on-chip device. As the 1550 nm DFB-laser is usually constructed with InP or InGaAsP material platform, while the VCSEL material is InGaAs/InGaAlAs, the on-chip integration may be conducted heterogeneously using silicon or silicon nitride substrate [18]. Moreover, the additional challenge for the on-chip design is to provide optical isolation for both sources. In perspective, it may be solved with magneto-optical isolators [19] or other modifications of current scheme.

REFERENCES

[1] R. Shakhovoy, M. Puplauskis, V. Sharoglazova, A. Duplinskiy, D. Sych, E. Maksimova, S. Hydyrova, A. Tumachek, Y. Mironov, V. Kovalyuk, A. Prokhodtsov, G. Goltsman, Y. Kurochkin, Phase randomness in a semiconductor laser: Issue of quantum random-number generation, *Phys. Rev. A*, 2023, vol. 107, no. 1, art. no. 012616.

[2] M.-Y. Zhu, Y. Liu, Q.-F. Yu, H. Guo, Random number generation based on polarization mode noise of vertical-cavity surface-emitting lasers, *Laser Phys. Lett.*, 2012, vol. 9, no. 11, pp. 775–780.

[3] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, J.-W. Pan, The generation of 68 Gbps quantum random number by measuring laser phase fluctuations, *Rev. Sci. Instrum.*, 2015, vol. 86, no. 6, art. no. 063105.

[4] B. Bai, J. Huang, G.-R. Qiao, Y.-Q. Nie, W. Tang, T. Chu, J. Zhang, J.-W. Pan, 18.8 Gbps real-time quantum random number generator with a photonic integrated chip, *Appl. Phys. Lett.*, 2021, vol. 118, no. 26, art. no. 264001.

[5] V. Lovic, D.G. Marangon, M. Lucamarini, Z. Yuan, A.J. Shields, Characterizing phase noise in a gain-switched laser diode for quantum random-number generation, *Phys. Rev. Appl.*, 2021, vol. 16, no. 5, art. no. 054012.

[6] R.A. Shakhovoy, E.I. Maksimova, Gain-switched VCSEL as a quantum entropy source: the problem of quantum and classical noise, *St. Petersburg State Polytech. Univ. J. Phys. Math.*, 2022, vol 15, no. 3.2, pp. 201–205.

[7] V. Mannalatha, S. Mishra, A. Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness, *Quantum Inf. Process.*, 2023, vol. 22, no. 12, art. no. 439.

[8] M. Avesani, H. Tebyanian, P. Villoresi, G. Vallone, Semi-device-independent heterodyne-based quantum random-number generator, *Phys. Rev. Appl.*, 2021, vol. 15, no. 3, art. no. 034034.

[9] M. Huang, Z. Chen, Y. Zhang, H. Guo, A phase fluctuation based practical quantum random number generator scheme with delay-free structure, *Appl. Sci.*, 2020, vol. 10, no. 7, art. no. 2431.

[10] S.-H. Sun, F. Xu, Experimental study of a quantum random-number generator based on two independent lasers, *Phys. Rev. A*, 2017, vol. 96, no. 6, art. no. 062314.

[11] 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, *Opt. Lett.*, 2010, vol. 35, no. 3, pp. 312–314.

[12] S. Xiang, W. Liu, X. Zhang, J. Wang, *Quantum random number generation combining intensity fluctuations with phase fluctuations of a DFB laser*, in: J. Kang et al. (Eds.), Conference on Lasers and Electro-Optics, OSA Technical Digest, Optica Publishing Group, 2021, art. no. JTu3A.154.

[13] J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, B. Xu, H. Guo, 117 Gbits/s quantum random number generation with simple structure, *IEEE Photonics Technol. Lett.*, 2016, vol. 29, no. 3, pp. 283–286.

[14] M. Gräfe, B. Septriani, O. de Vries, New insights on quantum random number generation (QRNG) by phase diffusion (Conference Presentation), *Proc. SPIE*, 2019, vol. 11134, art. no. 111340B.

[15] A. Quirce, A. Valle, M. Valle-Miñón, J. Gutiérrez, Characterization of the polarization fluctuations in gain-switched VCSELs for quantum random number generation, *J. Opt. Soc. Am. B*, 2023, vol. 41, no. 1, pp. 240–250.

[16] S.A. Blokhin, Ya.N. Kovach, M.A. Bobrov, A.A. Blokhin, A.V. Babichev, L.Ya. Karachinsky, I.I. Novikov, A.G. Gladyshev, P.E. Kopytov, D.S. Papylev, K.O. Voropaev, A.Yu. Egorov, S.-C. Tian, D. Bimberg, Energy efficiency of optical data transmission by 1.55 μm range vertical-cavity surface-emitting laser with the active region based on InGaAs/InAlGaAs quantum wells [in Russian], *Opticheskii Zhurnal*, 2024, vol. 91, no. 12, pp. 35–45.

[17] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22 Rev. 1, 2001.

[18] D. Liang, J.E. Bowers, Recent progress in heterogeneous III-V-on-silicon photonic integration, *Light: Adv. Manuf.*, 2021, vol. 2, no. 1, pp. 59–83.

[19] Y. Zhang, Q. Du, C. Wang, T. Fakhrul, S. Liu, L. Deng, D. Huang, P. Pintus, J. Bowers, C.A. Ross, J. Hu, L. Bi, Monolithic integration of broadband optical isolators for polarization-diverse silicon photonics, *Optica*, 2019, vol. 6, no. 4, pp. 473–478.

УДК 621.3

Квантовый генератор случайных чисел на основе фазового шума ВИЛ и РОС-лазера

К.Р. Разживина [1], Я.Н. Ковач [1,2], А.В. Ковалев [1], Е.С. Колодезный [1]

[1] Институт перспективных систем передачи данных, Университет ИТМО, Кронверкский пр., 49, лит. А, Санкт-Петербург, 197101, Россия

[2] Физико-технический институт им. А.Ф. Иоффе Российской академии наук, Политехническая ул., д. 26, Санкт-Петербург, 194021, Россия

Аннотация. Квантовые генераторы случайных чисел (КГСЧ) являются важными компонентами для криптографии и безопасной передачи данных, однако в разрабатываемых устройствах часто необходимо искать компромисс между скоростью генерации случайных чисел, стоимостью и сложностью устройства. В данной статье представлен КГСЧ, основанный на фазовом шуме сигнала оптических биений РОС-лазера и ВИЛ, что позволяет сочетать узкую спектральную линию и стабильность РОС-лазера вместе с высокой энтропией, характерной для фазового шума ВИЛ, на длине волны излучения 1550 нм. В статье описан сигнал оптических биений на выходе из представленной гибридной установки, в качестве алгоритма пост-обработки применена операция исключающее ИЛИ для подавления корреляций, достигнута скорость генерации случайных бит до 12 Гбит/с. Сгенерированные последовательности успешно прошли тесты NIST SP 800-22 при поддержании низкого смещения и высокой стабильности установки, в связи с чем такая гибридная схема может быть применена для систем квантового распределения ключей, для которых необходимы скорость и надежность устройства.

Ключевые слова: квантовые генераторы случайных чисел; ВИЛ; РОС-лазеры; фазовый шум