An Integrated Silicon Photonic Chip for Continuous-Variable Quantum Random Numbers Generator Based on Vacuum Fluctuation

Menglin Zhu\textsuperscript{1,2}, Xiangyu Wang\textsuperscript{1,*}, Bingjie Xu\textsuperscript{3}, Song Yu\textsuperscript{1}, Ziyang Chen\textsuperscript{2} and Hong Guo\textsuperscript{2}

\textsuperscript{1}State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
\textsuperscript{2}State Key Laboratory of Advanced Optical Communication, Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China
\textsuperscript{3}Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, No. 6, Chuangye Road, Chengdu 610041, China

\*Corresponding author: xywang@bupt.edu.cn

Abstract. The deployment of quantum random number generator in fiber optics is strongly limited in real world applications due to the size of the components and their cost. Here we present a quantum random number generator based on vacuum fluctuation using an optical homodyne detection in silicon photonic chip achieving minimum entropy/bit of 8.5 for 10 bits sample. The produced random numbers have passed all NIST randomness tests.

Keywords: Fiber optics, optical homodyne detection, silicon photonic chip, minimum entropy.

1. Introduction
Random number is an essential resource for many applications, such as in simulation [1] and lotteries, especially classical and quantum cryptography [2, 3]. However, with the development of computer science and technology, random numbers generated by mathematical algorithms and classical physical processes will cause safety issues in cryptography applications due to their intrinsic determinacy [4]. In contrast, random numbers generator based on quantum mechanics [5] can offer the ultimate in randomness. In the past few decades, quantum random number generators (QRNG) have made significant achievement using different quantum entropy sources including photon path [6], photon arrival time [7], photon number distribution [8], vacuum fluctuation [9, 11], phase noise [12, 13], amplified spontaneous emission noise of quantum states [14], etc. QRNG can be divided into discrete type and continuous type according to different entropy sources. Compared with the discrete-variable QRNG, the continuous-variable QRNG (CV-QRNG) is easy to prepare entropy sources, has low requirements for detection devices, and has a high generation rate, so it can save a lot of cost and has a very broad application prospect.
Typically, one of the most prominent optical CV-QRNG schemes is based on vacuum fluctuation for the simplicity and compactness of the experimental device and high random numbers generation rate. So far, the development of vacuum states QRNG has been very mature and the generation speed has met the current needs. Now the QRNG is gradually facing the application market. However, most of vacuum fluctuation QRNGs are usually realized using either with bulk or fiber components, which leads to strong limitations in real application because of the large size, high cost, instability and the difficulty of integrating into other complex systems. To dispose of this, silicon optoelectronic technology compatible with complementary metal oxide semiconductor (CMOS) craft has entered people's field of vision.

In recent years, the vacuum fluctuation QRNG [10] by using the homodyne detector integrated in silicon-on-insulator (SOI) has been experimentally realized. However, after equal interval quantization, the calculating minimum entropy/bit of 5.9 for 8 bits sample is relatively small in the experiment by Raffaelli et al [10]. In this paper, we use the homodyne detector integrated in SOI and the off-chip laser, the off-chip transimpedance amplifier (TIA) to independently build a vacuum states QRNG system. The scheme is simple, highly integrated and small in size. The minimum entropy achieved through equal probability quantization is 8.5 for 10 bits sample. The final produced random numbers pass all NIST [15] randomness tests.

2. Experiment realization
The experimental setup of QRNG based on vacuum fluctuation is depicted in Figure 1. The scheme consists of three sections, including the off-chip laser, the off-chip transimpedance amplifier (TIA) and the on-chip homodyne detector. The laser light emitted by an off-chip NKT laser with 1550 nm is used as the local oscillator (LO). The on-chip homodyne detector contains two grating couplers, three multi-mode interferences (MMIs), a thermo-optical phase shifter and two germanium p-i-n photodiodes (PD). The LO is coupled into the single mode waveguides through the pigtail and the vertical grating coupler. While the port of other grating coupler input the vacuum states as signal. The MMI as a beam splitter makes the signal interfere with the LO to amplify the weak vacuum signal. One of the output waveguide of the MMI which passes through Mach-Zehnder interferometer with a thermo-optic phase shifter in one arm is detected by PD. However, due to limited time, the experiment did not use a thermo-optic phase shifter. The other output port of the MMI is directly connected to the PD through waveguide. The photocurrents generated by the two photodiodes are input into the printed circuit board (PCB) through wire bonding and a TIA is used in the PCB to amplify the difference of the two photocurrents. The whole system including PCB and silicon chip is only a few centimeters square in size. The chip-based QRNG can reduce costs, achieve mass production, and is easier to integrate into other complex systems.

![Figure 1. Experimental setup of vacuum fluctuation QRNG.](image)

In the measurement of vacuum states, some classical noise will be introduced due to various practical conditions. In order to remove the classic noise, the raw data needs to be post-processed. Following previous work [16], the quantum noise and classical noise all follow independent Gaussian distribution and the measured signal M is the superposition of classical noise E and quantum noise Q.
The relation of their variances is $\sigma_{M}^{2} = \sigma_{Q}^{2} + \sigma_{E}^{2}$. The classical noise can be measured in the absence of the LO. The range of the measurement signal is divided into $2^{10}$ bins. Each bin has equal area and is assigned a fixed binary string of length 10, similarly to Figure 1(b) in the ref [9]. Compared with equal interval quantization, this quantization method is more accurate and achieves better results. However, the 10 bits number corresponding to each sample contains classical noise. In order to extract random bits generated by quantum signals, we need to use the min-entropy. For variable $X$ with probability distribution $P_{X}(x)$, the minimum entropy is defined in unit as [17].

$$H_{\text{min}}(x) = -\log_{2}\left[\max_{x \in X} P_{x}(x)\right]$$ (1)

After obtaining the minimum entropy, the Toeplitz hashing method is used to extract random numbers that do not contain classical noise.

3. Results and analysis

To ensure that the random numbers can be extracted and the appropriate sampling rate can be obtained, the spectral power density of QRNG is measured when the power of LO is 0 and the maximum. The power spectral density is shown in Figure 2. Since the output optical power of the laser is directly coupled to the chip through the pigtail, the coupling efficiency is low and the laser optical power is relatively large. In addition, the low frequency spike on the black line may be related to the PD on the chip, but it does not affect uplift of the spectrum. The ratio of shot noise to electronic noise is near 11 dB. The fact approximately indicates that there are certain random numbers that can be extracted in the process of random extraction. The bandwidth range is near 20MHz and the corresponding sampling rate is 40MHz.

![Figure 2. The power spectrum density of the vacuum fluctuation. The black line represents the electronic noise. The red line represents the total noise when the LO is 10mW.](image-url)
In this experiment, we collect $9 \times 10^7$ samples by an oscilloscope. The probability distribution of the collected data is shown in Figure 3 which obeys the Gaussian distribution. However, some data are not in the Gaussian distribution, which may be related to the stability of laser coupling in the system. The stability of laser coupling and the repeatability of the experiment can be increased by optical package. Then value of each sample is quantized to 10 bits using the equal probability quantization method. According to the formula 1, the calculated minimum entropy which describes the amount of extractable randomness is $8.5 \text{bits/sample}$. Then we build a Toeplitz hashing matrix using a pseudorandom seed to extract pure random numbers. The autocorrelation of the extracted random numbers is much lower than the raw data and very close to 0.

An important feature of the random number is randomness. In the field of random numbers, the two most commonly used standard randomness test suite are the DIEHARD and the NIST-STS statistical test suite. Standard NIST test are applied to verify the quality of $7.6 \times 10^6$ random bit sequence. The test is provided by National Institute of Standard and Technology (NIST SP 800-22) and contains a total of 15 statistical tests. Each test corresponds to a P-value. If the P value is in the range of 0.01 and 0.99, the test is considered to be passed. The extracted random numbers passed all NIST randomness tests and the results are shown in Figure 4. The red solid line represents P-value=0.01.

Figure 3. Distribution histogram of the measured total noise. The probability distribution follows Gaussian distribution.

Figure 4. Graphical results of the NIST statistical tests. The NIST test suites contain a total of 15 statistical tests. Each test corresponds to a P-value. If the P-value is in the range of 0.01 and 0.99, the test is considered to be passed. Moreover, the pass rate is above 0.9849 for each type of test.
4. Conclusion
A QRNG by measuring vacuum states with an integrated homodyne detector has been experimentally demonstrated. The QRNG have achieved smaller size and lower cost by using silicon photonic chip. After equal probability quantization, minimum entropy reaches 8.5 bits. The final random bits processed by Toeplitz matrix pass the all NIST tests. Future work can study the influence of the thermo-optic phase shifter integrated on the silicon photonic chip of the homodyne detector.

Acknowledgements
This work was supported by the Key Program of National Natural Science Foundation of China under Grant No. 61531003, National Natural Science Foundation of China under Grant No. 62001041, U19A2076, 61771439, Sichuan Science and Technology Program under Grant No. 2019JDJQ0060, China Postdoctoral Science Foundation under Grant No. 2020TQ0016, and the Fund of State Key Laboratory of Information Photonics and Optical Communications.

References
[1] N. Metropolis, S. Ulam, The monte carlo method, J. Am. Stat. Assoc. 44.247 (1949) 335-341.
[2] Y. Zhang, Z. Chen, S. Pirandola, et al, Long-distance continuous-variable quantum key distribution over 202.81km fiber, Phys. Rev. Lett. 125.1 (2020) 010502.
[3] Y. Zhang, Z. L, Z. Chen, et al, Continuous-variable QKD over 50km commercial fiber, Quantum Sci. Technol. 4.3 (2019) 035006.
[4] T. Stojanovski, L. Kocarev, Chaos-based random number generators-part I: analysis [cryptography], in IEEE Transactions on Circuits & Systems I Fundamental Theory & Applications, 2001, pp. 0-288.
[5] M. Herrero-Collantes, J. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. 89.1 (2017) 015004.
[6] A. Stefanov, N. Gisin, O. Guinnard, et al, Optical quantum random number generator, J. Mod. Optic. 47 (2000) 595.
[7] Y. Nie, H. Zhang, Z. Zhang, et al, Practical and fast quantum random number generation based on photon arrival time relative to external reference, Appl. Phys. Lett. 104.5 (2014) 2435.
[8] W. Guo, Bias-free true random-number generator, Opt. Lett. 34.12 (2009) 1876-8.
[9] C. Gabriel, C. Wittmann, D. Sych, et al, A generator for unique quantum random numbers based on vacuum states, Nat. Photonics. 4 (2010) 711-715.
[10] F. Raffaelli, G. Ferranti, D. Mahler, et al, A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, Quantum Sci. Technol. 3 (2018) 025003.
[11] B. Xu, B. Chen, Z. Li, et al, High speed continuous variable source-independent quantum random number generation, Quantum Sci. Technol. 4 (2019) 025013.
[12] H. Guo, W. Tang, Y. Liu, et al, Truly random number generation based on measurement of phase noise of laser, Phys. Rev.E. 81 (2010) 051137.
[13] J. Liu, J. Yang, Z. Li, et al, 117Gbits/s quantum random number generation with simple structure, IEEE Photon. Technol. Lett. 29.3 (2017) 283-286.
[14] C. Williams, J. Salevan, X. Li, et al, Fast physical random number generator using amplified spontaneous emission, Opt. Express. 18.23 (2010) 23584-23597.
[15] A. Rukhin, J. Soto, J. Nechvatal, et al, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Appl. Phys. Lett. 22.7(2010) 1645-179.
[16] T. Symul, S. Assad, and R. Lam, Real time demonstration of high bitrate quantum random number generation with coherent laser light, Appl. Phys. Lett. 98 (2011) 231103.
[17] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min-and max-entropy, in IEEE Transactions on Information Theory, 2009, pp. 4337-4347.