Spatially Multiplexed Quantum Entropy Source With Single LD for 100-Gbps Random Numbers and Beyond

Ken Tanizawa, *Member, IEEE*, Kentaro Kato, *Member, IEEE*, and Fumio Futami, *Member, IEEE*

***Abstract*— Fast quantum random number (RN) generation is an essential technology for cryptographic applications requiring unpredictable RNs. This letter reports a spatially multiplexed quantum entropy source (QES) with a single laser diode (LD), utilizing parallel homodyne measurement of vacuum fluctuation, for an aggregated RN generation rate of 100 Gbit/s and beyond. The QES uses a high-power distributed feedback LD and a low-loss 1 × 16 silica planar lightwave circuit splitter and achieves eight-channel parallel operation with a broad bandwidth of 4 GHz each. A four-channel aggregated RN generation rate of 4 × 25 Gbit/s and further scalability up to 8 × 25 Gbit/s with eight channels are demonstrated via offline post-processing.**

***Index Terms*— Photonics, quantum random number generator, random number generation.**

I. Introduction

TRUE random numbers (RNs) play an essential role in cryptographic applications and stochastic simulations. Various hardware RN generators utilizing classical noise, chaotic behavior, or quantum mechanics have been demonstrated. Among these, quantum RN generators (QRNGs) display potential in terms of true randomness because intrinsically unpredictable quantum phenomena are utilized as a source of randomness for extracting RNs or a quantum entropy source (QES). The QES has been realized based on the path difference or arrival time of a photon, phase fluctuation of a laser, and vacuum fluctuation [1], [2]. Recently, a quantum RN cloud platform that consumes a substantial amount of RNs for various applications was proposed and demonstrated [3]. Unpredictable RN streams are particularly essential for some cryptographic applications, such as the seed of a quantum key distribution system [4] and signal randomization for physical layer encryption [5]. Thus, fast and reliable QRNGs are required to satisfy the growing demand of RNs. Here, we focus on fast device-dependent or trusted QRNGs, rather than device-independent but relatively slow ones assuming the existence of adversaries.

A QRNG based on vacuum fluctuation is suitable for reliable, low-cost, and fast RN generation [6]. It consists of a homodyne measurement setup and a conventional continuous-wave laser for a local oscillator (LO). The highest rate of 18.8 Gbit/s for QRNGs was demonstrated using a compact Si-photonic homodyne chip integrated with a balance photo detector (BPD) and a high-speed field-programmable gate array (FPGA) [7]. A feature of the QRNG is that the QES is able to employ spatial multiplexing for parallel operation. Coherent LO lights divided from a laser are uncorrelated in principle. Therefore, a parallel homodyne measurement setup with a single laser and an optical 1 × N splitter realizes spatial multiplexing. This technique was originally proposed in [8] for facilitating the hardware implementation of digital post-processing, and real-time parallel operation with 7 channels × 0.44 Gbit/s = 3.08 Gbit/s was demonstrated using a lithium niobate waveguide splitter and a common FPGA.

The implementation of post-processing at a throughput of over 10 Gbit/s has ceased to be a fundamental issue because of the continuous progress in the performance of digital circuits, as demonstrated in [7]. Therefore, we recently utilized the multiplexing technique for achieving a high aggregated rate. A high-power laser for LO and a low-loss optical splitter are key enabler to increase the aggregate rate related to the product of the number of parallel channels and photodetection bandwidth. A four-channel parallel QES for an aggregated RN generation rate of 100 Gbit/s was demonstrated using a low-loss 1 × 8 silica planar lightwave circuit (PLC) splitter [9]. The silica PLC exhibits low insertion loss and high reliability [10] and is suitable for the QES.

This letter reports scaling of the number of parallel channels in the spatially multiplexed QES based on vacuum fluctuation for further increasing an aggregated RN generation rate. We demonstrated an eight-channel parallel QES with a high-power distributed feedback (DFB) laser diode (LD) at a fiber-coupled output power of >180 mW and a low-loss 1 × 16 silica PLC splitter. Eight parallel quantum randomness sources with a bandwidth of 4 GHz each were digitized, and RNs were extracted via offline post-processing. The aggregated rate attained 4 channels × 25 Gbit/s = 100 Gbit/s, and scalability up to 8 channels × 25 Gbit/s = 200 Gbit/s was demonstrated. Although the RN extraction process is offline here, the spatial multiplexing in the QES exhibits

Manuscript received 21 December 2022; accepted 1 January 2023. Date of publication 11 January 2023; date of current version 16 January 2023. This work was supported in part by the Innovative Science and Technology Initiative for Security, Grant Number JPJ004596, ATLA, Japan. *(Corresponding author: Ken Tanizawa.)*

The authors are with the Quantum ICT Research Institute, Tamagawa University, Tokyo 194-8610, Japan (e-mail: tanizawa@lab.tamagawa.ac.jp).

Color versions of one or more figures in this letter are available at https://doi.org/10.1109/LPT.2023.3234260.

Digital Object Identifier 10.1109/LPT.2023.3234260

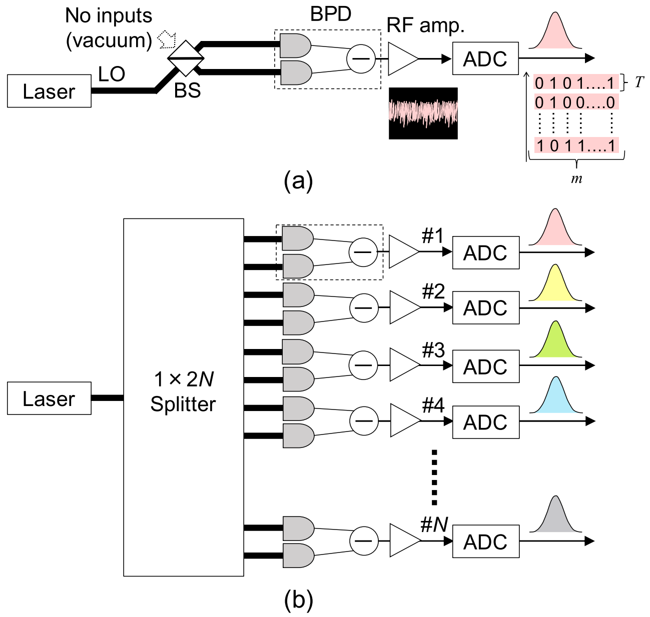

Fig. 1. Configurations of QES: (a) conventional setup with a BS, and (b) N-channel parallel setup with a 1 × $2N$ splitter.

high potential to achieve the highest RN generation rate for QRNGs. The generated RN sequences passed the randomness test according to NIST SP800-90B [11].

II. Operating Principles

Fig. 1(a) shows the basic configuration of a QES based on vacuum fluctuation. It is a homodyne setup without signal input. The LO light from a laser is injected into the input port of a beam splitter (BS). There are no inputs to the other ports. The LO light is divided by half and detected using a BPD. The two LO beams or two coherent states are uncorrelated. This can be explained as follows: a BS is a two-input two-output passive device and is expressed by a unitary operator. When the two-mode coherent state $|\alpha\rangle|0\rangle$ is incident on a half BS U, the output state is $U|\alpha\rangle|0\rangle = U|\alpha/\sqrt{2}\rangle|\alpha/\sqrt{2}\rangle$, where α is the complex amplitude of coherent light and $|0\rangle$ is the vacuum state [12]. In this case, the output state is separable; hence, quantum noise in each output mode is uncorrelated. The BS can be replaced with waveguide devices without a vacuum input such as a multimode interference coupler or a Y-branch splitter [7], [8], because quantum noise is introduced by linear attenuation. Furthermore, additive (classical) noises of the LO beams are cancelled at the subtraction process in the BPD. Thus, the vacuum fluctuation, i.e. quantum noise, is obtained with zero mean. Then, Gaussian distribution of quantum noise is digitized by an analog-to-digital converter (ADC), and raw random bits are stored. The generation rate of the raw bits is m / T bit/s. Here, m and T are the bit resolution and sampling period of the ADC, respectively. The sampling ratio 1 / T is typically set equivalent to the bandwidth of the detected quantum noise, and undesirable correlation between adjacent samples are suppressed. Hence, broadband noise detection increases the generation rate while a high LO power is required. Finally, post-processing is performed to extract true RNs from the raw random bits. Typically, hashing with a Toeplitz matrix is utilized [13].

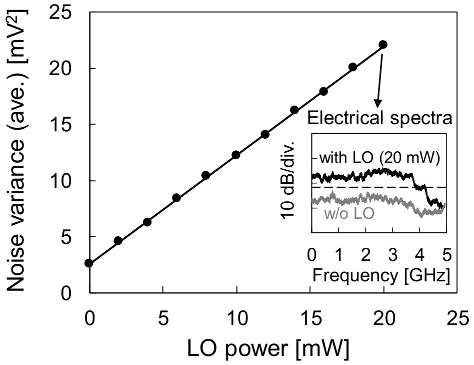

Fig. 2. Noise variances for different LO powers in a single QES with a bandwidth of 4 GHz. The inset shows electrical spectra with and without LO.

Spatial multiplexing is achieved using a multistage optical splitter because the LO lights are uncorrelated even after cascaded BSs. Fig. 1(b) shows the N-channel parallel setup with a 1 × $2N$ splitter. The LO light from a single laser is split using the splitter, and $2N$ LO beams are detected with the BPDs. After the digitization, N-channel independent and identically distributed (IID) raw bit sequences based on vacuum fluctuation are obtained. The aggregated generation rate of raw random bits becomes $N \times m/T$. For a high rate, it is necessary to increase N while maintaining broadband photodetection or a large $1/T$. To achieve this, a high LO power for each BPD is essential. Thus, the use of a low-loss silica PLC splitter and high-power DFB LD is advantageous in terms of the generation rate, cost, and reliability. Furthermore, heterogeneous integration of multiple BPDs on a silica PLC for downsizing the QES displays potential, as demonstrated in a coherent receiver front-end circuit [14].

III. Experiments

An eight-channel QES ($N = 8$) with a single DFB LD was demonstrated experimentally. We used a high-power LD at 1.31 μm, a low-loss 1 × 16 silica PLC splitter, and broadband BPDs in the experiment. The DFB LD achieved a high fiber-coupled output power of > 180 mW, while maintaining a narrow linewidth of typically 200 kHz and low relative intensity noise of less than −155 dBc/Hz at above 1 MHz. The loss of the PLC splitter at 1.31 μm was 13.4 ± 0.3 dB, which includes an intrinsic splitting loss of 12 dB. The power imbalance between the two inputs of a BPD was less than 0.3 dB. The high output power of the LD and low loss of the splitter achieved an LO power of 17.4 mW on an average for each BPD. The BPDs had a bandwidth of 5 GHz and were followed by low-noise broadband RF amplifiers. The vacuum fluctuations were digitized using an oscilloscope with 12-bit resolution and a bandwidth of 4 GHz (rather than using ADCs) in this offline experiment.

First, a preliminary test involving a single-channel QES with a 3 dB coupler was performed. Fig. 2 shows the variance of noise for various LO powers. The noise variance increases linearly with the LO power ($R^2 = 0.9997$). This result indicates

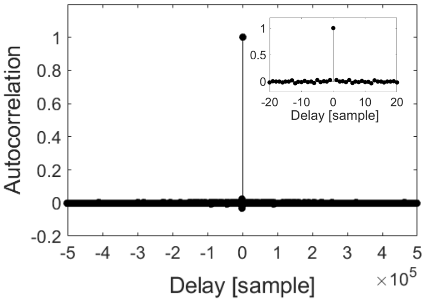

Fig. 3. Autocorrelation of the noise at an LO power of 20mW.

that the vacuum fluctuation contributes the most to the noise because the variance of classical noise increases as the square of LO power. The inset shows the electrical spectra with and without LO input of 20 mW, measured using an electrical spectrum analyzer. The dashed line indicates 6 dB reduction. The noise bandwidth (6 dB) is approximately 4 GHz. The clearance from the background classical noise without LO is approximately 10 dB in the bandwidth. Fig. 3 shows the normalized autocorrelation trace at an LO power of 20 mW. The sampling rate of the noise was set at 4 Gsample/s corresponding to the noise bandwidth of 4 GHz. The inset shows the magnified results around zero. The sampled noise has no significant correlations among adjacent samples, suitable for random number generation.

Next, the eight-channel QES with the 1 × 16 PLC splitter was demonstrated. The average LO power for each BPD was 17.4 mW. The number of inputs of the oscilloscope was four, whereby we could not obtain the eight-channel vacuum fluctuations simultaneously. However, the feasibility of the eight-channel operation can be shown without the simultaneous measurement. This is because it is established theoretically that each channel is independent. Moreover, the cross-correlations between channels of #1-4 and #5-8 were experimentally evaluated to confirm the independence among the channels. The absolute values of normalized correlations were less than 1×10^{-3}. The negligibly small values demonstrated the independence among at least four channels.

Fig. 4 shows histograms of the noise amplitude. The quantum noises with a Gaussian distribution were obtained in the eight channels. Fig. 5 shows the average and standard deviation (SD) of the noise variances for 10 measurements of 4×10^6 samples. The average noise variances were 20.4 ± 1.3 mV^2 for the eight channels. The noise variances were sufficiently uniform for parallel operation. The SDs on the right axis, corresponding to measurement errors, were less than 0.4 mV^2. The stability at a few percent variation is sufficient for random number generation. On the other hand, future investigations using real-time processors are needed to evaluate long-term stability.

Here, post-processing for RN generation was performed offline. The first two digits of the 12-bit binary data for each sampling was discarded to adjust the amplitude range of the measurements. Thereby, 10 raw bits were obtained from a sample. Subsequently, RNs were extracted. We tested two methods: 1) hashing with a Toeplitz matrix in a channel-by-channel manner and 2) XOR operation of two channels.

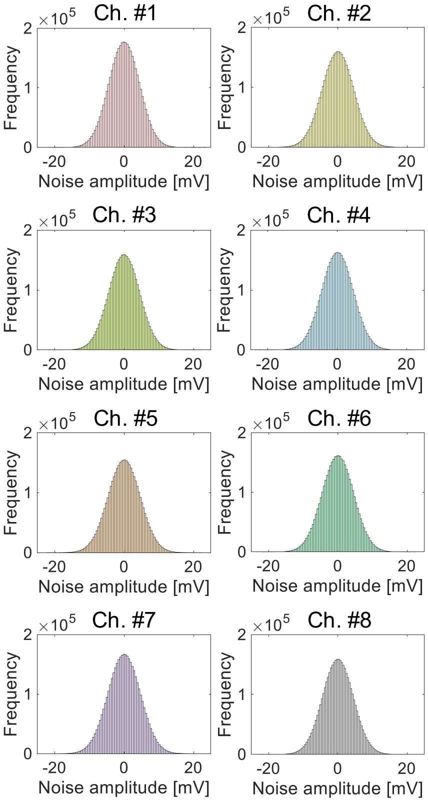

Fig. 4. Histograms of noise amplitude for eight channels.

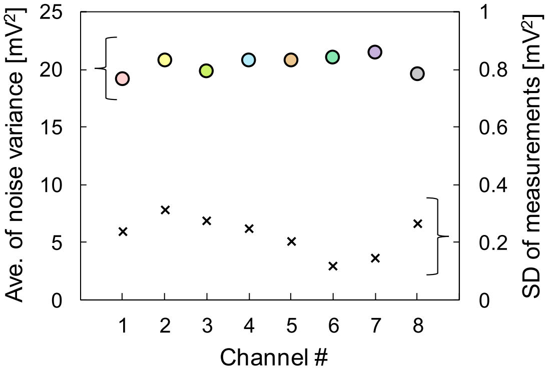

Fig. 5. Average and standard deviation (SD) of the noise variances in the eight-channel parallel QES.

In method 1), a Toeplitz matrix consisting of random seed bits was multiplexed by the raw bits. The compression ratio of the hashing η is expressed as the ratio of the length of the row of the matrix to that of its column. Hence, the aggregated RN generation rate is $\eta \times N \times m / T$. The matrix size was set to 4000 × 2500 ($\eta = 0.625$) and 4000 × 2000 ($\eta = 0.5$), such that 6.25 and 5 random bits, respectively, were extracted from a sample. In method 2), the XOR of raw random bit sequences of two channels was calculated. This method is achievable because each channel is IID in the spatially multiplexed QES. The compression ratio η of XOR operation is fixed at 0.5, whereas the computational cost of the post-processing reduces.

The randomness of raw bits is evaluated based on the min-entropy analysis [13]. The min-entropy is calculated as $H_\infty(X) = -\log_2 P_{\max}$ where $P_{\max} = \max_{x\in\{0,1\}^n} Pr[X = x]$. $P_{\max}$ is obtained from the variances of quantum and classical

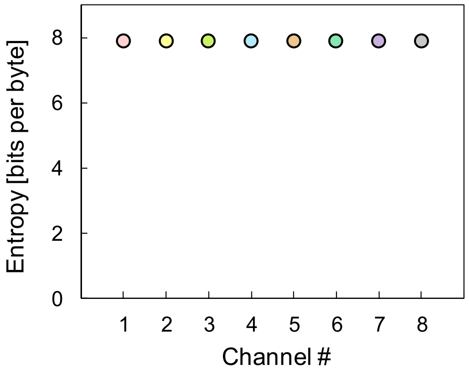

Fig. 6. Entropy of the randomness test for each channel when RNs are extracted utilizing hashing with Toeplitz matrix with a size of 4000 × 2500 ($\eta = 0.625$).

TABLE I
RESULTS OF RANDOMNESS TEST (NIST SP800-90B)

	Method 1) Hashing 4000 × 2500	**Method 1)** Hashing 4000 × 2000	**Method 2)** XOR
Compression ratio: η	0.625	0.5	0.5
Entropy (average of 8 channels)	7.8765 bits per byte	7.8777 bits per byte	7.8724 bits per byte
NIST test	Passed	Passed	Passed
Aggregated rate (offline)	200 Gbit/s	160 Gbit/s	160 Gbit/s

noises, bit resolution of digitization, and amplitude range of measurement. This study focuses on trusted quantum random number generation, and the min-entropy assuming a non-adversary model is employed. The average min-entropy of eight channels in the experimental condition was calculated to be 8.76 bits/sample. This value indicates the maximum number of true random bits extractable from one sample. Thus, it was reasonable to extract 6.25 and 5 bits/sample in the post-processing.

The extracted RN sequences for each channel were assessed based on the randomness test according to NIST SP800-90B [11]. Fig. 6 shows the test results of entropy with a unit of bits per byte when the extraction method is the hashing with Toeplitz matrix of 4000 × 2500 ($\eta = 0.625$). The entropy here is a measure of randomness of RNs, which is different from an entropy with a unit of bits/sample used in the previous paragraph. The entropy for each channel was close to the ideal value of 8 bits per byte. This indicates that the RN sequences are sufficiently random. Table I summarizes the results for methods 1) and 2). The average entropies of the eight channels approached the ideal value for all the extraction methods, and the randomness test passed. Thus, unpredictable RNs based on vacuum fluctuation were generated successfully. When $\eta = 0.625$, the aggregated RN generation rate could attain 8 (channels) × 4 (Gsample/s) × 10 (bits) × 0.625 = 200 Gbit/s.

IV. CONCLUSION

An eight-channel spatially multiplexed QES based on vacuum fluctuation with a high-power DFB LD and a low-loss 1 × 16 silica PLC splitter was demonstrated. Eight-channel quantum randomness sources with a bandwidth of 4 GHz each were obtained. Then, RN generation at a four-channel aggregated rate of 100 Gbit/s and scalability up to 200 Gbit/s using eight channels were demonstrated via the offline post-processing. The RN sequences passed the randomness test according to NIST SP800-90B. Although the post-processing was implemented offline, this demonstration indicates that the highest RN generation rate for QRNGs is achievable with the eight-channel parallel QES. Real-time post-processing with the hashing at a Gbit/s class throughput had been a challenge. The recent progress of high-speed FPGAs has rendered such high-speed real-time post-processing feasible. A real-time QRNG at a rate of 100 Gbit/s or higher will be realized using the spatially multiplexed broadband QES and multiple high-speed FPGAs.

REFERENCES

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *NPJ Quantum Inf.*, vol. 2, no. 1, p. 16021, Nov. 2016.

[2] M. H. Collantes and J. C. G.-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, Feb. 2017, Art. no. 015004.

[3] L. Huang, H. Zhou, K. Feng, and C. Xie, "Quantum random number cloud platform," *NPJ Quantum Inf.*, vol. 7, no. 1, p. 107, Jul. 2021.

[4] ETSI Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD), "Quantum key distribution (QKD); components and internal interfaces," ETSI, Sophia Antipolis, France, Tech. Rep. ETSI GR QKD 003 V2.1.1, Mar. 2018.

[5] F. Futami, K. Tanizawa, and K. Kato, "Experimental demonstration of quantum deliberate signal randomization for Y-00 quantum noise stream cipher," in *Proc. Conf. Lasers Electro-Optics*, May 2022, pp. 1–2.

[6] C. Gabriel et al., "A generator for unique quantum random numbers based on vacuum states," *Nature Photon.*, vol. 4, no. 10, pp. 711–715, Oct. 2010.

[7] B. Bai et al., "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," *Appl. Phys. Lett.*, vol. 118, no. 26, Jun. 2021, Art. no. 264001.

[8] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, "Multiplexed quantum random number generation," *Quantum*, vol. 3, p. 141, May 2019.

[9] K. Tanizawa, K. Kato, and F. Futami, "Four-channel parallel broadband quantum entropy source for true random number generation at 100 Gbps," in *Proc. Conf. Lasers Electro-Optics*, 2022, pp. 1–2.

[10] A. Aratake, "Field reliability of silica-based PLC splitter for FTTH," in *Proc. Opt. Fiber Commun. Conf.*, 2015, pp. 1–3.

[11] M. S. Tura, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," NIST, Gaithersburg, MD, USA, NIST Special Publication 800-90B, 2018.

[12] S. Prasad, M. O. Scully, and W. Martienssen, "A quantum description of the beam splitter," *Opt. Commun.*, vol. 62, no. 3, pp. 139–145, May 1987.

[13] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 6, Jun. 2013, Art. no. 062327.

[14] Y. Kurata et al., "Silica-based PLC with heterogeneously-integrated PDs for one-chip DP-QPSK receiver," *Opt. Exp.*, vol. 20, no. 26, pp. B264–B269, 2012.