Self-balanced real-time photonic scheme for ultrafast random number generation

Li, Pu; Guo, Ya; Guo, Yanqiang; Fan, Yuanlong; Guo, Xiaomin; Liu, Xianglian; Shore, K. Alan; Dubrova, Elena; Xu, Bingjie; Wang, Yuncai; Wang, Anbang

APL Photonics

Published: 30/05/2018

Publisher's PDF, also known as Version of record

Self-balanced real-time photonic scheme for ultrafast random number generation

Pu Li, Ya Guo, Yanqiang Guo, Yuanlong Fan, Xiaomin Guo, Xianglian Liu, K. Alan Shore, Elena Dubrova, Bingjie Xu, Yuncai Wang, and Anbang Wang

Citation: APL Photonics **3**, 061301 (2018); doi: 10.1063/1.5029498

View online: https://doi.org/10.1063/1.5029498

View Table of Contents: http://aip.scitation.org/toc/app/3/6

Published by the American Institute of Physics

Self-balanced real-time photonic scheme for ultrafast random number generation

Pu Li,[1,2,3,4] Ya Guo,[1,2] Yanqiang Guo,[1,2] Yuanlong Fan,[3] Xiaomin Guo,[1,2]
Xianglian Liu,[1,2] K. Alan Shore,[3] Elena Dubrova,[5] Bingjie Xu,[4]
Yuncai Wang,[1,2] and Anbang Wang[1,2]
[1]*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan 030024, China*
[2]*Institute of Optoelectronic Engineering, College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China*
[3]*School of Electronic Engineering, Bangor University, Wales LL57 1UT, United Kingdom*
[4]*Science and Technology on Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China*
[5]*School of Information and Communication Technology, KTH Royal Institute of Technology, Stockholm, Kista 16440, Sweden*

(Received 14 March 2018; accepted 4 May 2018; published online 30 May 2018)

We propose a real-time self-balanced photonic method for extracting ultrafast random numbers from broadband randomness sources. In place of electronic analog-to-digital converters (ADCs), the balanced photo-detection technology is used to directly quantize optically sampled chaotic pulses into a continuous random number stream. Benefitting from ultrafast photo-detection, our method can efficiently eliminate the generation rate bottleneck from electronic ADCs which are required in nearly all the available fast physical random number generators. A proof-of-principle experiment demonstrates that using our approach 10 Gb/s real-time and statistically unbiased random numbers are successfully extracted from a bandwidth-enhanced chaotic source. The generation rate achieved experimentally here is being limited by the bandwidth of the chaotic source. The method described has the potential to attain a real-time rate of 100 Gb/s. https://doi.org/10.1063/1.5029498

Random numbers provide the foundation of secure communication, where they are used as the cryptographic keys to encrypt messages for transmission. The "one-time pad" offers unconditional security of communication,[1] but a critical obstacle hindering the adoption of this approach is the need for real-time and ultrafast generation of reliable random numbers.[2] As known, the current communication rate has reached 40 Gb/s and is developing rapidly toward 100 Gb/s.

The quest for true randomness has led to the study of physical random number generators (RNGs). In 2008, Uchida *et al.* made a significant advance in respect of physical RNGs by achieving generation rates of 1.7 Gb/s by exploiting chaotic lasers as the sources of randomness.[3] Since then, there have been numerous proposals, experiments, and improvements on RNGs based on laser chaos.[4–18] However, to date, most of them use off-line random number extraction from stored chaotic time-series and thus do not operate in real time.

Available fast randomness extraction methods share a technical feature: one must first convert the optical chaotic signal to the electrical domain and then enable the random number extraction using electronic 1-bit or multi-bit analog-to-digital converters (ADCs) and also undertake time-consuming post-processing. We notice that some studies once used a sophisticated bit error rate tester or serial data analyzer to perform the function of a clocked comparator for random number production.[19–21] However, a clocked comparator is actually also a 1-bit ADC in practice,[22] just like that in Ref. 3. Due to the bandwidth bottleneck of electronic ADCs, the currently achieved real-time generation rate of RNGs with verified statistical randomness has been commonly limited at several Gb/s.[6]

Three factors are responsible for this limited response speed.[23] They are (i) electronic comparator ambiguity caused by the limited gain bandwidth of the transistors, (ii) sampling error in sample-and-hold (S/H) circuits due to the RF clock jitter (known as aperture jitter), and (iii) the thermal (Johnson) noise and bandwidth of the post-processing electronic components.

The introduction of parallel processing technology is helpful in reducing the pressures induced by the necessity of electronic ADCs,[24–26] but this cannot solve the rate limitation by the roots. Using optical sampling can overcome the electronic sampling error as done by us in Ref. 21, but the comparator problem and the post-processing procedure still remains.

In our prior work,[27] we eliminated the need for post-processing by using a differential comparison method in the quantization procedure. However, the cardinal comparator problem still remains unresolved. Specifically, in the quantization process, two identical photo-detectors are utilized to first convert two self-delayed optically sampled chaotic signals into the associated electrical signals. Then, an electronic comparator (a 1-bit ADC without the embedded S/H circuit) is required to differentially quantize the two chaotic signals into a raw random number stream. However, due to the fatal electronic comparator ambiguity, the state of the art electronic comparator used has a severely limited analog bandwidth of not more than 10 GHz. That causes the obtained raw random number waveform to suffer from serious distortion. Finally, the raw random numbers have to be further modulated into the mode-locked optical pulse to observe the final random number output.

In contrast to all the aforementioned RNG schemes using ADCs, the work reported here eliminates the requirement of the speed-limiting electronic ADC and directly utilizes a balanced photo-detector to extract random number streams in real time. This new method simultaneously brings several advantages: (i) Using an optical sampler driven by mode-locked optical pulses to sample the chaotic signal in the optical domain can overcome the electronic jitter bottleneck confronted by electrical ADCs[28] because the timing jitter of the current mode-locked lasers is now of the order of femtosecond (fs).[29,30] (ii) Using photo-detection to quantize the chaotic signal solves the bandwidth bottleneck of the electrical ADCs because the response bandwidth of off-the-shelf photo-detectors has reached 100 GHz.[31] That means that, when a chaotic source with a sufficient bandwidth is used, our new method has the ability to reach a level of 100 Gb/s in real time. It should be noted that the demonstrated RNG rate of 10 Gb/s in our proof-of-principle experiment is limited by the bandwidth of the chaos source. (iii) The entire randomness extraction procedure is greatly simplified. For instance, in our prior work,[27] the RNG scheme contained an all-optical sampling gate, two photo-detectors, an electronic comparator, and an electro-optic modulator. By contrast, the RNG scheme in this work is composed only of an all-optical sampling gate and a balanced photo-detector. Moreover, the approach is self-balanced, i.e., the generation of statistically unbiased random numbers is accomplished with no need of threshold setting or post-processing, despite the chaotic source usually having an asymmetric amplitude distribution. Finally, we want to point that to our knowledge, this paper reports for the first time the use of a balanced photo-detector to play the role of directly quantizing stochastic signals into random numbers (although it has been widely used to measure quantum noise such as vacuum states[32,33] and amplified spontaneous emission[19]). The significant innovation using a balanced photo-detector as the direct quantizing device in the RNG opens new opportunities for further development of techniques for ultrafast real-time random number generation.

Figure 1(a) illustrates the principle of the proposed RNG scheme based on balanced photo-detection. The system consists of an optical chaos source, a mode-locked laser (MLL), an optical sampler, and a balanced photo-detector (BPD). Ultralow jitter optical pulses from the MLL are used as the control clock to periodically open the optical sampler so that the incident laser chaos can be sampled in the optical domain with high fidelity. The optically sampled chaotic pulses are then equally split into two branches and detected by the "+" and "–" inputs of the BPD, respectively. By adjusting the relative time delay τ between the two chaotic pulse trains [named $I(t)$ and $I(t-\tau)$] via an optical delay line (ODL), we can obtain statistically unbiased random number streams [i.e., the difference $I(t)$ and $I(t-\tau)$] at the output of the BPD with no need of threshold setting and post-processing: when the chaotic pulse $I(t)$ is larger than $I(t-\tau)$, the BPD output is a positive pulse and coded as "1"; otherwise the BPD output is a negative pulse and coded as logic "0."

To validate our scheme, an external cavity laser diode (referred to as M-LD) cascaded by another solitary laser diode (referred to as S-LD) is used to generate broadband laser chaos. Both the M-LD

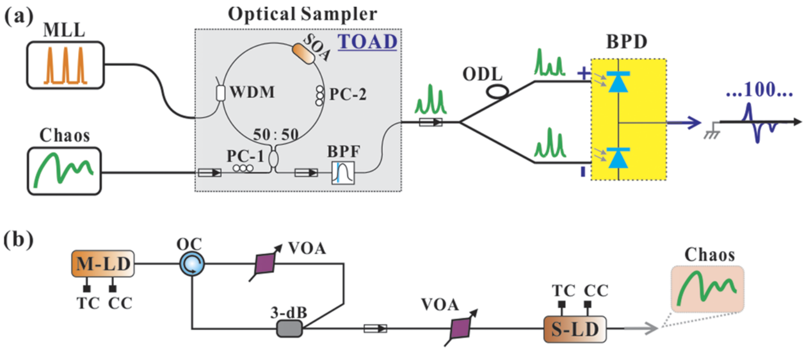

FIG. 1. (a) Schematic of the proposed RNG scheme based on balanced photo-detection and (b) the setup of the laser chaos source used in the proof-of-principle experiment. MLL, mode-locked laser; Chaos, optical chaos source; TOAD, a terahertz optical asymmetric demultiplexer; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; PC-1, and PC-2, polarization controllers; BPF, optical band-pass filter; ODL, optical delay line; BPD, balanced photo-detector; M-LD, master laser diode; S-LD, slave laser diode; OC, optical coupler; VOA, variable optical attenuator; 3-dB, 3-dB optical coupler; TC, temperature controller; CC, current controller.

and S-LD (WTD, LDM5S752, 07R6300352, and 07R6300353), shown in Fig. 1(b), have the same threshold current of 22 mA but in the experiment are biased at 37.4 mA and 35.2 mA, respectively, via two independent current controllers (CCs). The 9 m long external cavity of the M-LD includes an optical circulator (OC), a variable optical attenuator (VOA), and a 3-dB optical coupler (3-dB) and provides a 10.5% feedback to drive the M-LD into a chaotic oscillation state. This chaotic signal is then injected into the S-LD to obtain an enhanced chaos bandwidth.

Figure 2 is the RF spectrum of the bandwidth-enhanced laser chaos measured by a 26.5 GHz spectrum analyzer (Agilent Technologies, N9020A) via a 45 GHz photo-detector (U^{2}T, XPDV2120RA). Here, the injection strength from the M-LD to the S-LD is set at 20.7% using a VOA, and their optical frequency detuning is adjusted to 8.45 GHz using individual temperature controllers (TCs). The final broadband chaotic laser output is at a center wavelength of 1554.08 nm. Comparing with the noise floor, one can clearly observe that the generated chaotic signal exhibits a large intensity fluctuation in a wide frequency domain from 0 to 20 GHz. The chaos bandwidth is calculated to be about 11.89 GHz. It should also be noted from Fig. 2 that the chaotic signal possesses a relatively flat spectrum in the range from 3 to 11 GHz. This flatness feature is very different to that of the pure optical injection or feedback chaotic system,[21] where typically a main peak around the relaxation frequency is seen in their RF spectra. Both the large bandwidth and flatness of the RF spectrum found here assist the fast generation of real-time random numbers from the source.

Figures 3(a) and 3(b) show the measured chaotic waveforms before and after the optical sampling procedure by a 36 GHz oscilloscope (Lecroy, LabMaster10-36Zi). The optical sampler used in our proof-of-principle demonstration is a terahertz optical asymmetric demultiplexer (TOAD).[34]

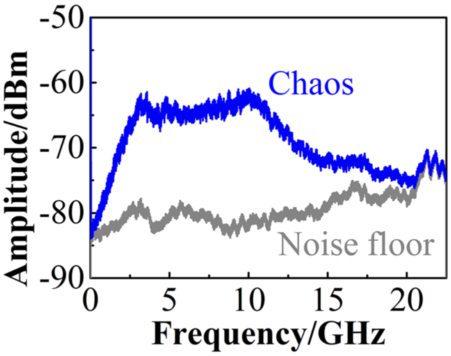

FIG. 2. Measured RF spectrum of the bandwidth-enhanced chaotic laser.

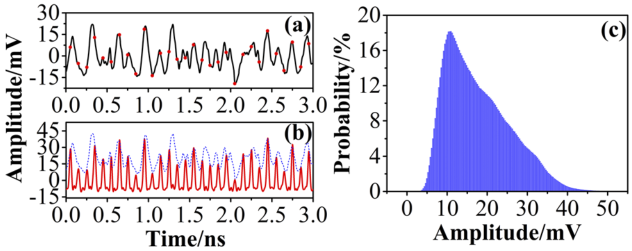

FIG. 3. [(a) and (b)] Measured chaotic waveforms before and after the optical sampling procedure and (c) normalized amplitude distribution of the sampled chaotic pulses with a size of 1×10^6 data.

The TOAD mainly contains a nonlinear semiconductor optical amplifier (SOA) placed asymmetrically from the loop center and an intra-loop wavelength division multiplexer (WDM) coupler for injecting the optical clock pulses from the MLL. With the trigger of the control clock, a sampling window determined by the SOA offset (about 34 ps) will be periodically opened so that the incident chaotic optical signal is sampled at the repetition frequency of the MLL. A band-pass filter (BPF) finally separates the sampled chaotic pulses at the output of the TOAD. In the experiment, the SOA with a gain recovery time of 25 ps (Kamelian, SOA-NL-L1-C-FA) is biased at 300 mA and operates at a peak gain wavelength of 1550 nm with a 3 dB bandwidth of 64 nm. The MLL with a timing jitter less than 50 fs (Pritel, UOC-05-14G-E) operates at 10 GHz and its wavelength is tuned to be 1551.26 nm. From Figs. 3(a) and 3(b), it can be seen that the envelope of the analog chaotic signal [Fig. 3(a)] matches well the peaks of the sampled chaotic pulses [Fig. 3(b)]. This confirms the expected high-fidelity of the sampling. However, from Fig. 3(c), it is apparent that the sampled chaotic pulses also inherit the non-uniform amplitude distribution of the laser chaos.

Such an asymmetry of the distribution introduces a severe bias in the generation of random numbers. To remove that bias, previous physical RNG schemes have generally turned to dynamical threshold tuning and complex post-processing based on electrical ADCs.[3–21] However, both methods will greatly enhance the difficulty of practical implementation, especially when an operating rate beyond GHz is needed. By contrast, as depicted in Fig. 1(a), we exploit a balanced photo-detection technology to quantize the sampled chaotic pulses into a statistically unbiased random number stream. Benefitting from the ultrafast response bandwidth (typically many tens or 100 GHz) of current photo-detectors, this technology can maintain a very high real-time rate.

To effect the balanced photo-detection approach, the relative delay τ is set as 200 ns, which is a high-order integer multiple of the repetition period of the MLL, to ensure that the correlation coefficient between $I(t)$ and $I(\mathrm{t} - \tau)$ is essentially zero. The autocorrelation function of the sampled chaotic pulses is the indicator to instruct this delay. Figure 4 shows results obtained using this photo-detection technique, where a BPD ($\mathrm{u^2t}$, BPDV2120R) with a bandwidth of 45 GHz is used. Figure 4(a) is the generated random number waveform from the BPD, where the positive pulse is coded as logic "1" and the negative pulse as logic "0." There are 10 pulses in a time-slot of 1 ns, which corresponds

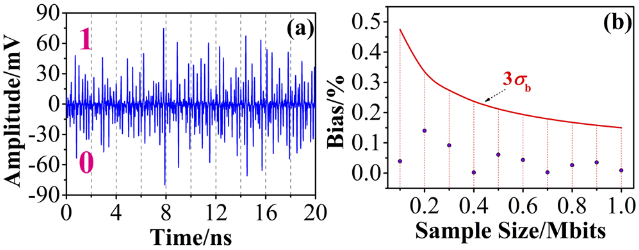

FIG. 4. (a) Measured 10 Gb/s random number waveform from the output of the balanced photo-detector, where positive and negative pulses are coded as "1" and "0," respectively. (b) Biases (blue dots) of the coded random number sequences with different sample sizes of $N = 0.1, 0.2, \ldots, 1.0 \times 10^6$ bits, where the red line represents the associated three-standard-deviations for ideal unbiased random number sequences, $3\sigma_b = (3N^{-1/2})/2$.

to a generation rate of 10 Gb/s determined by the clocking rate of the MLL. Note, to guarantee the balancing in the BPD, a variable attenuator is used in the down branch of the spliced fiber in the experiment, and the power ratio between the two channels is controlled in the range 50% ± 0.1%. The different amplitudes in final 0 or 1 bit can be further reshaped to be uniform through a limiting amplifier. Figure 4(b) depicts the calculated biases $|B[N]|$ of the coded random number sequences $a[n]$ with different sample sizes $N = 0.1, 0.2, \ldots, 1.0$ Mbits, respectively. Herein, $|B[N]|$ is defined as $|B[N]| = |\langle a[n]\rangle - 0.5|$, where $\langle\cdot\rangle$ represents the statistically evaluated proportion of "1" in the random number sequences $a[n]$. For a finite length of an ideal independent random number sequence, the estimate of $|B[N]|$ should follow the Gaussian distribution $\boldsymbol{N}(0, {\sigma_b}^2)$ where $\sigma_b = (N^{-1/2})/2$. From Fig. 4(b), it can be seen clearly that the estimates of $|B[N]|$ keep below the three-standard-deviation line $3\sigma_b$. That indicates our generated random numbers can be considered to be statistically unbiased.

To verify the quality of the random numbers, we first examine the normalized correlation as a function of the time delay for the 1×10^6 random bit streams, as shown in Fig. 5(a). The normalized correlation $C\,[k]$ is defined as $C\,[k] = (\langle a[n]a[n+k]\rangle - \langle a[n]\rangle^2)/(\langle a[n]^2\rangle \cdot \langle a[n]\rangle^2)$, where $\langle\cdot\rangle$ represents the statistically evaluated proportion of "1" in the random number sequence $a[n]$ with a sample size of N 2 1×10^6 bits and k represents the delay bits. Note, every delay bit corresponds to one delay time interval 100 ps in the horizontal axis of Fig. 5(a). For a finite length of an ideal independent random number sequence, the estimate of $C[k]$ should follow the Gaussian distribution $\boldsymbol{N}(0, {\sigma_c}^2)$, where $\sigma_{\mathrm{c}} = N^{-1/2}$ for $C[k]$. Because the estimates of $C[k]$ keep below the three-standard-deviation line $3\sigma_c$ [Fig. 5(a)], the obtained random number sequences can be viewed to be statistically independent. More stringent evaluation is made by the use of the state-of-the-art statistical test suite of the National Institute of Standards and Technology (i.e., NIST SP800-22-rev1a[35]), which is proposed to determine whether a RNG is suitable for cryptographic applications. This suite contains 15 test items, named "Frequency," "Frequency within a Block," "Runs," "Longest Run of Ones in a Block," "Binary Matrix Rank," "Discrete Fourier Transform," "Non-overlapping Template Matching," "Overlapping Template Matching," "Maurer's Universal Statistical," "Linear Complexity," "Serial," "Approximate Entropy," "Cumulative Sums," "Random Excusions," and "Random Excursions Variant," respectively. As advised by the NIST, all 15 test items are executed using 1000 samples of 1×10^6 data with a significance level $\alpha = 0.01$. There are two requirements for passing each test item: (i) the proportion of the tested random numbers satisfying the condition for the p-value larger than α should be larger than 0.980 560 8; (ii) the uniformity of the p-values (denoted as P-value) should be larger than 0.0001. Figure 5(b) is a typical NIST test result, where the numbers from 1 to 15 on the x axis correspond to the 15 test items, respectively. As can be seen, all the test items are successfully passed. This indicates that the generated bit stream can be statistically regarded to be random.

The reason why the balanced photo-detection can remove the inherent bias in the random number output is established theoretically here. Considering the chaotic amplitude distribution is relatively stationary on a large time scale, we can suppose the amplitude probability density functions (PDF)

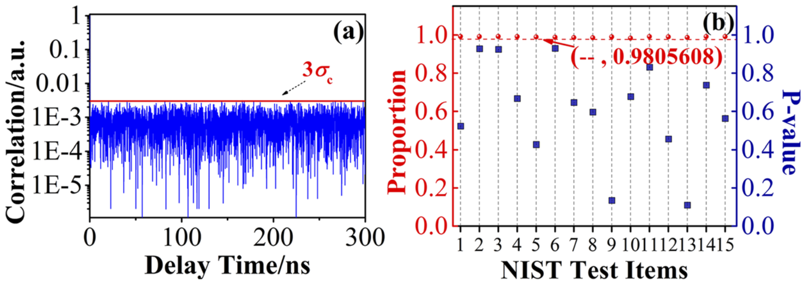

FIG. 5. (a) Normalized correlation function (blue line) of the coded 10 Gb/s random number sequence with a finite length of $N = 1 \times 10^6$ bits, where the red line is the three-standard-deviation for an ideal independent random number sequence, $3\sigma_c = 3N^{-1/2}$; note, every delay time interval in the horizontal axis is 100 ps, which corresponds to one delay bit. (b) NIST test results use 1000 samples of $N = 1 \times 10^6$ bits with a significance level $\alpha = 0.01$, where red circles and blue squares represent the P-value and passed proportion of 15 test items, respectively.

of I(t) and $I(t-\tau)$ to be $f(x)$ and $f(y)$, respectively. Furthermore, their joint PDF can be expressed as $f(x, y)$. Thus, the amplitude distribution function $F(z)$ for the difference signal, $I(t) - I(t-\tau)$, can be written as

$$F(z) = P(x{-}y < z) = \int_{-\infty}^{+\infty}\left[\int_{-\infty}^{z+y} f(x, y)dx\right]dy. \tag{1}$$

Taking the derivative of Eq. (1), we can obtain its PDF,

$$f_z(z) = \int_{-\infty}^{+\infty} f(z+y, y)dy. \tag{2}$$

If $I(t)$ and $I(t-\tau)$ are statistically independent, $f(x, y)$ can be equivalent with $f(x)f(y)$. Thus, Eq. (2) will be transferred into

$$f_z(z) = \int_{-\infty}^{+\infty} f(z+y)f(y)dy. \tag{3}$$

Defining $r = -z + y$, we have

$$f_z(-z) = \int_{-\infty}^{+\infty} f(r)f(r+z)dv. \tag{4}$$

Comparing Eq. (3) with Eq. (4), we can get

$$f_z(z) = f_z(-z). \tag{5}$$

In our experiment, the correlation coefficient between $I(t)$ and $I(t-\tau)$ is about 10^{-4} when $\tau = 200$ ns, a high-order integer multiple of the MLL repetition frequency. That guarantees that $I(t)$ and $I(t-\tau)$ are independent, so a statistically unbiased random sequence is obtained.

This point can also be further confirmed by monitoring the frequency of "1" bits in a long time, which is a good real-time indicator of the quality of the generated random number sequence.[36] In the experiment, we recorded a random number sequence with a size of 1 Mbits every 6 min to calculate the "1" frequency. According to the NIST tests, only a deviation value of 0.13% in the frequency is allowed. Figure 6 is a typical "1" frequency variation with time increasing, where the red lines show the range 50.00% ± 0.13%. This result also demonstrates that statistically unbiased random number streams can be robustly generated for at least 24 h without deteriorating the performance of our RNG.

Noting that the RNG rate in our proof-of-principle experiment is 10 Gb/s (limited by the 11 GHz bandwidth of the chaos), we discuss the ultimately achievable real-time rate of the proposed method. The physical RNG scheme can be divided into two parts: a randomness source and its extraction. We notice that the recovery time of the commercial SOA has reached a level of less than 10 ps[37] and the response bandwidth of the commercial product of photo-detection has reached a level of 100 GHz.[31] This means that, with a randomness source of a sufficient bandwidth, the RNG rate has the potential to reach 100 Gb/s in real time, without any parallelization being used. In addition, considering that the chaotic laser in our experiment is an intensity variable, we believe that this method can also apply for the other similar entropy sources such as superluminescent diodes[19,20] or improved external cavity laser diodes.[38]

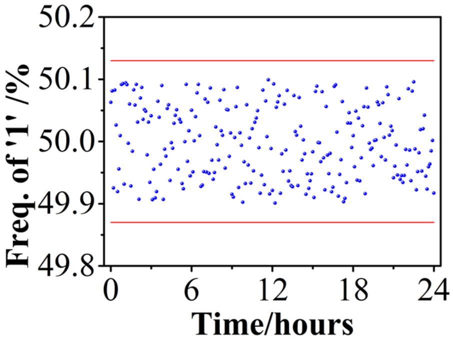

FIG. 6. Measured frequency of "1" bits (the blue dots) for the 10 Gb/s RNG. Note that the red lines show the range 50.00% ± 0.13%.

In conclusion, we have proposed a real-time and self-balanced photonic RNG method. The ultralow temporal jitter of the mode-locked laser, together with ultrafast photo-detection, makes this photonic approach an efficient way to overcome the electronic bottlenecks present in existing fast physical RNGs. Meanwhile, the introduction of balanced photo-detection technique gives our method a self-adaptive ability to generate statistically unbiased random numbers, with no need of dynamical threshold tuning or off-line post-processing. In the proof-of-principle experiment, 10 Gb/s real-time random number extraction is successfully demonstrated using a chaotic source consisting of two cascaded laser diodes. With a sufficient chaos bandwidth, the random number generation rate of our method can be improved to the level of 100 Gb/s.

This work is supported by the National Natural Science Foundation of China (NSFC) (Nos. 61775158, 61505137, 61505136, 61527819, and 61771439), National Cryptography Development Fund (No. MMJJ20170127), China Postdoctoral Science Foundation (No. 2018M630283), U.K. Engineering and Physical Sciences Research Council (EPSRC) (No. EP/P006027/1), and Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (No. 2015122).

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).
[2] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604 (2014).
[3] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**(12), 728–732 (2008).
[4] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**(2), 024102 (2009).
[5] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).
[6] A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, "4.5 Gbps high-speed real-time physical random bit generator," Opt. Express **21**(17), 20452–20462 (2013).
[7] P. Li, Y. C. Wang, and J. Z. Zhang, "All-optical fast random number generator," Opt. Express **18**(19), 20360–20369 (2010).
[8] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: Approaching the information theoretic limit," IEEE J. Quantum Electron. **49**(11), 910–918 (2013).
[9] R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, "Fast random bits generation based on a single chaotic semiconductor ring laser," Opt. Express **20**(27), 28603–28613 (2012).
[10] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," Opt. Express **18**(18), 18763–18768 (2010).
[11] X. Z. Li and S. C. Chan, "Heterodyne random bit generation using an optically injected semiconductor laser in chaos," IEEE J. Quantum Electron. **49**(10), 829–838 (2013).
[12] N. Q. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," Opt. Express **22**(6), 6634–6646 (2014).
[13] X. Tang, Z. M. Wu, J. G. Wu, T. Deng, J. J. Chen, L. Fan, Z. Q. Zhong, and G. Q. Xia, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," Opt. Express **23**(26), 33130–33141 (2015).
[14] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," Opt. Express **22**(14), 17271–17280 (2014).
[15] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," Opt. Express **23**(2), 1470–1490 (2015).
[16] T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, "Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser," Opt. Lett. **41**(2), 388–391 (2016).
[17] L. Zhang, B. Pan, G. Chen, L. Guo, D. Lu, L. Zhao, and W. Wang, "640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser," Sci. Rep. **7**, 45900 (2017).
[18] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy, and R. Roy, "Recommendations and illustrations for the evaluation of photonic random number generators," APL Photonics **2**(9), 090901 (2017).
[19] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**(23), 23584–23597 (2010).
[20] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," Opt. Lett. **36**(6), 1020–1022 (2011).
[21] P. Li, Y. Y. Sun, X. L. Liu, X. G. Yi, J. G. Zhang, X. M. Guo, Y. Q. Guo, and Y. C. Wang, "Fully photonics-based physical random bit generator," Opt. Lett. **41**(14), 3347–3350 (2016).
[22] See http://www.analog.com/media/en/training-seminars/tutorials/MT-020.pdf for information about 1-bit ADCs.
[23] A. Mahjoubfar, D. V. Churkin, S. Barland, N. Broderick, S. K. Turitsyn, and B. Jalali, "Time stretch and its applications," Nat. Photonics **11**(6), 341–351 (2017).
[24] D. P. Rosin, D. Rontani, and D. J. Gauthier, "Ultrafast physical generation of random numbers using hybrid Boolean networks," Phys. Rev. E **87**(4), 040902 (2013).
[25] S. Shinohara, K. Arai, P. Davis, S. Sunada, and T. Harayama, "Chaotic laser based physical random bit streaming system with a computer application interface," Opt. Express **25**(6), 6461–6474 (2017).
[26] K. Ugajin, Y. Terashima, K. Iwakawa, A. Uchida, T. Harayama, K. Yoshimura, and M. Inubushi, "Real-time fast physical random number generator with a photonic integrated circuit," Opt. Express **25**(6), 6511–6523 (2017).

[27] P. Li, Y. Guo, Y. Q. Guo, Y. L. Fan, X. M. Guo, X. L. Liu, K. Y. Li, K. A. Shore, Y. C. Wang, and A. B. Wang, "Ultrafast fully photonic random bit generator," J. Lightwave Technol. **36**(12), 2531–2540 (2018).

[28] R. Walden, "Analog-to-digital conversion in the early twenty-first century," in *Wiley Encyclopedia of Computer Science and Engineering* (Wiley, 2008), pp. 126–138.

[29] U. Keller, "Recent developments in compact ultrafast lasers," Nature **424**(6950), 831–838 (2003).

[30] E. U. Rafailov, M. A. Cataluna, and W. Sibbett, "Mode-locked quantum-dot lasers," Nat. Photonics **1**(7), 395–401 (2007).

[31] See https://www.finisar.com/optical-components/xpdv412xr for information about photodetectors.

[32] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A **81**(6), 063814 (2010).

[33] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**(10), 711–715 (2010).

[34] P. Li, L. Jiang, J. G. Zhang, J. Z. Zhang, and Y. C. Wang, "Low-complexity TOAD-based all-optical sampling gate with ultralow switching energy and high linearity," IEEE Photonics J. **7**(4), 7801108 (2015).

[35] See http://csrc.nist.gov/groups/ST/toolkit/rng/index.html for information about the NIST test suite.

[36] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductorlasers," Opt. Express **17**(11), 9053–9061 (2009).

[37] E. Kehayas, D. Tsiokos, P. Bakopoulos, D. Apostolopoulos, D. Petrantonakis, L. Stampoulidis, A. Poustie, R. McDougall, G. Maxwell, Y. Liu, S. Zhang, H. J. S. Dorren, J. Seoane, P. V. Holm-Nielsen, P. Jeppesen, and H. Avramopoulos, "40-Gb/s All-optical processing systems using hybrid photonic integration technology," J. Lightwave Technol. **24**(12), 4903–4911 (2006).

[38] N. Li, W. Pan, A. Locquet, and D. S. Citrin, "Time delay concealment and complexity enhancement of an external-cavity laser through optical injection," Opt. Lett. **40**(19), 4416–4419 (2015).