Ultrafast Fully Photonic Random Bit Generator

Li, Pui; Guo, Ya; Guo, Yangqiang; Fan, Yuanlong; Guo, Xiaomin; Liu, Xianglian; Li, Kunying; Shore, K. Alan; Wang, Yuncai; Wang, Anbang

Journal of Lightwave Technology

DOI:
10.1109/JLT.2018.2817512

Published: 15/06/2018

Peer reviewed version

Ultrafast fully photonic random bit generator

Pu Li, Ya Guo, Yanqiang Guo, Yuanlong Fan, Xiaomin Guo, Xianglian Liu, Kunying Li, K. Alan Shore, *Senior Member, IEEE, Fellow, OSA,* Yuncai Wang, and Anbang Wang, *Member, IEEE*

***Abstract*—To achieve complete security of communication, there is a need for *'real-time'* ultrafast physical random bit generators (RBGs). In available physical RBGs, random bit extraction is effected in the electrical domain and therefore cannot directly function beyond frequencies of 10 GHz or so *in real time*. Here we present a fully photonic strategy for *real-time* random number generation and report a proof-of-concept experimental demonstration of an integrated 10 Gb/s RBG system (prototype) based on laser chaos. The use of an ultra-stable mode-locked laser, together with ultrafast optical interactions, gives our method the capability to develop super-high-speed RBGs in practice. The photonic implementation is fully compatible with optical communications so that well-established optical multiplexing techniques can be used to realize Tb/s *real-time* random bit generation.**

***Index Terms*—Chaos, semiconductor laser, random number generation, semiconductor laser amplifier, optical signal processing.**

I. Introduction

Random bit generators (RBGs) have a wide range of applications in science and engineering. For example, RBGs are important tools for Monte Carlo calculations and stochastic simulations, which are employed to solve various problems involved in nuclear physics, molecular biology, computational chemistry, material science and financial economics. Also, RBGs are commonly used to evaluate the system performance of high-speed optical/electrical components in optical transmission links. In particular, RBGs lay the essential foundation of secure communications, used as cryptographic key sources to protect the privacy of data transmission.

For the ultimate security of communication, one must resort to the theoretically unbreakable 'one-time pad' cipher. This cipher requires the plaintext be encrypted by a fully random bit sequence with a length not shorter than itself. Moreover, the random bits can be used only once. To achieve this perfect cipher in practice, one must find a way to continuously produce reliable random bits *in real time*, whose generation rate should not be lower than the present communication rate. With the rapid development of optical fiber communication, the current data transmission rate typically operate at 40 Gb/s.

Computational algorithms offer an inexpensive means to generate pseudo-random bits and thus are the widely adopted RBG scheme in modern cryptography. However, as its name implies, the output of this type of RBG can be totally predicted or even reproduced, once partial knowledge about the algorithm or initial seed is acquired. Thus, they do not satisfy the property of randomness and are therefore vulnerable to attack. In view of this, John von Neumann said, "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. [1]" Such vulnerability of computational algorithms is the root cause of information security incidents which occur too frequently in our Internet age.

To circumvent this issue, another type of RBGs has emerged, and has been called physical RBGs. They employ inherently random or unpredictable phenomena in the physical world to produce reliable random bits. Unfortunately, traditional physical RBGs are often limited to a very slow generation rate at the level of megabit per second (Mb/s). That is mainly caused by the small bandwidth of conventional randomness sources, such as thermal noise in resistors [2], frequency jitter in RF oscillators [3] and photon events in attenuated light [4].

A significant breakthrough in high-speed generation of physical random bits was made in 2008 with the use of a novel broadband source of randomness —— 'laser chaos' [5]. In this scheme, a continuous random bit stream up to 1.7 gigabit per second (Gb/s) was obtained through exclusive OR (XOR) processing the sampled and quantized chaotic outputs of two optical feedback laser diodes (LDs) by 1-bit electrical analog-to-digital converters (ADCs). In addition, a carefully tuned threshold voltage is required to avoid the bias induced by the non-uniform chaotic laser intensity distribution with a varying average value.

Since then, chaotic LDs have been regarded as a highly promising source of randomness for ultrafast physical RBGs with much significant work having been reported over the past ten years or so [6-18]. So, for example, Reidler *et al.* demonstrated that 12.5 Gb/s random bits could be extracted

This work was supported by National Natural Science Foundation of China (NSFC) (61505137, 61775158, 61527819, 61405138, 61505136, 61475111, and 61705159); U. K. Engineering and Physical Sciences Research Council (EPSRC) (EP/P006027/1); National Cryptography Development Fund (MMJJ20170127); Natural Science Foundation of Shanxi (2015021088); Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (2015122).

Pu Li, Ya Guo, Yanqiang Guo, Xiaomin Guo, Xianglian Liu, Kunying Li, Yuncai Wang, and Anbang Wang are with Key Laboratory of Advanced Transducers & Intelligent Control System, Ministry of Education, Taiyuan University of Technology, and Institute of Optoelectronic Engineering, College of Physics& Optoelectronics, Taiyuan University of Technology, Taiyuan, 030024 China (e-mail: lipu8603@126.com; guoyacekong@163.com; guoyanqiang@tyut.edu.cn;guoxiaomin@tyut.edu.cn;liuxianglian@tyut.edu.cn ;lkyinga@163.com;wangyc@tyut.edu.cn;wanganbang@tyut.edu.cn).

Pu Li, Yuanlong Fan, and K. Alan Shore are with School of Electronic Engineering, Bangor University, Wales, LL57 1UT U. K. (e-mail: lipu8603@126.com;y.fan@bangor.ac.uk;k.a.shore@bangor.ac.uk).

from the first-order derivative between a digitized chaotic signal from a single optical feedback LD by a virtual 8-bit ADC and its time-shifted version [7]. Further, Kanter et al. enhanced this rate into 300 Gb/s using high-order derivatives of the digitized chaotic signal [8]. Very recently, the generation rates of RBGs have shown the potential to reach a level of terabit per second (Tb/s) using similar multi-bit extraction [14-17]. We also demonstrated a 320 Gb/s random bit generation using physical white chaos [18].

However, it should be noticed that *none* of the ultrafast RBG proposals described above operates *in real time*. In those demonstrations, the outputs of chaotic LDs were first converted into electrical signals via photo-detectors; then the electrical chaotic waveforms were measured and stored in the limited memory of a sophisticated oscilloscope; finally random bits were obtained through offline digitizing and post-processing of the stored chaotic time-series. Generally speaking, all of the above approaches are based on the supposition that all high-frequency signal processing procedures for random bit extraction are performed in the electrical domain.

There are at least two main technical challenges that obstruct their practical implementation. One is the limited response bandwidth of both electrical ADCs and the digital post-processing radiofrequency (RF) components (including logic gates, memory buffers, multi-bit shift registers and parallel-serial converters). For instance, due to the aperture jitter of the sampling process, the analog bandwidth of the state-of-the-art ADCs embedded by digital oscilloscopes is typically limited to the level of gigahertz (GHz). Secondly, fast processing circuits beyond GHz frequencies are either highly complex or indeed may not be capable of realization. So, for example, to generate say 5 bits there may be a need to perform of order 10 time-shifts in Ref. [7]. As such, generating a random bit stream may require an extremely large number of time-shifts. In particular when attention is given to high-bit range generation where the time-shifts are very short (of order picoseconds or femtoseconds) those time-shifts will need to be set and synchronized to a high degree of accuracy. In respect of synchronization it is noted that state-of-the-art RF clocks deliver a timing jitter of order picoseconds (ps) even when working in the low frequency range between 100 and 400 megahertz (MHz), and more critically this electronic jitter deteriorates rapidly with increasing operating frequency [19]. According to the prediction for electrical ADCs in the future, it will take at least a decade to improve the electronic jitter performance by an order of magnitude [20].

Optical sampling can overcome the bottleneck of electronic jitter [21, 22]: a train of short optical clock pulses are used to sample the chaotic light in the optical domain, and then the sampled chaotic pulses can be detected and digitized. In Refs. [21] and [22], we have demonstrated 5 Gb/s and 7 Gb/s physical random number generation utilizing optically-feedback LD or optically-injected LD as the laser chaos source, respectively.

Nevertheless, limited by the relaxation oscillation of LDs, this two kinds of chaotic LDs used in Refs. [21, 22] commonly has a very low effective bandwidth about few GHz and an uneven power spectrum with a sharp peak around the relaxation oscillation frequency. That is one of the main reasons why their real-time bit rates are limited at several Gb/s. The other limitation factor comes from the thermal (Johnson) noise and comparator ambiguity of the electronic component in the digitizing procedure [23, 24], which cause severe waveform distortion and inter-symbol interference especially in the high frequency operation.

The achievement of the present paper is to report a prototype of integrated fully photonic RBG built on discrete optical and fiber-based elements which moves RBG capabilities close to the requirements of current communication systems. Through introducing the bandwidth enhancement technology [25, 26] into the laser chaos source and photonic technologies into the random bit extraction (including both the sampling and digitizing procedures), we make the physical RBG system reach a *real-time* rate at the level of 10 Gb/s for the first time. We also noticed that, very recently, several works based on a state-of-the-art field programmable gate array (FPGA) claimed that random numbers with a total throughput of more than 10 Gb/s could be obtained by introducing parallel technologies [27, 28], but their final random numbers are output through multiple channels in parallel and the fastest real-time rate in each output channel is still limited at a few Gb/s. Besides, the random bit stream used in practical communication networks is expected to be represented in a physical random waveform [29] (which consists of continuous high and low optical/electrical levels, not stored random data).

The implemented real-time speed in our work is higher than commercially available physical RBG products (*e.g.*, 'Quantis-OEM' from ID Quantique Inc. only has a typical rate of 4 Mb/s) by 2-3 orders of magnitude and is consistent with the data rates of modern communication systems. Moreover, the photonic implementation makes our system fully compatible with present-day optical communications. In consequence, well-established optical multiplexing techniques can be adopted to realize real-time random bit generation rates at Tb/s.

II. Architecture Of The Fully Photonic RBG System

Figure 1a is a picture of the integrated fully photonic RBG system, which consists of three layers: the laser chaos source, the photonic sampler and the photonic digitizer. The key idea, as sketched in Fig. 1b, is to use ultra-stable optical pulse trains from a single mode-locked laser (MLL) for the physical random bit extraction from the chaotic laser, *i.e.*, for both photonic sampling and digitizing procedures. The ultralow temporal jitter of the MLL, together with ultrafast optical interactions, gives the proposed photonic approach the confidence to develop ultra-high-speed random bit generation in real time.

Figure 1c shows the details of the integrated fully photonic RBG scheme: (i) In the chaotic laser, two distributed feedback (DFB) LDs are cascaded in a unidirectional master-slave configuration. One (referred to as LD-1) connects with a fiber ring feedback cavity to produce an initial chaotic oscillation, whereas the other (referred to as LD-2) is used to greatly enhance the chaos bandwidth. Note, this bandwidth-enhancement mechanism is intrinsically different with optically feedback or injection chaotic structure like that in Refs. [21] and

[22]. (ii) In the photonic sampler, an optical pulse stream from the MLL is used as the control clock to periodically switch a semiconductor laser amplifier in a loop mirror (SLALOM) [30]. Thus, the chaotic analog input can be discretized in the time domain, converting into chaotic pulse output which carries the amplitude information of wideband chaos. (iii) In the photonic digitizer, the sampled chaotic pulses are first split into two identical streams with a relative time delay. After optoelectronic conversion, a differential comparator (COM) quantizes the two streams of pulse peaks into unbiased random levels. However, due to the thermal noise and comparator ambiguity of the electronic COM, there is strong intersymbol interference and waveform distortion in the obtained random level stream. To solve this problem, these random levels are further pulse-coded into an optical random bit stream in the return-to-zero (RZ) format using an electro-optic modulator (EOM).

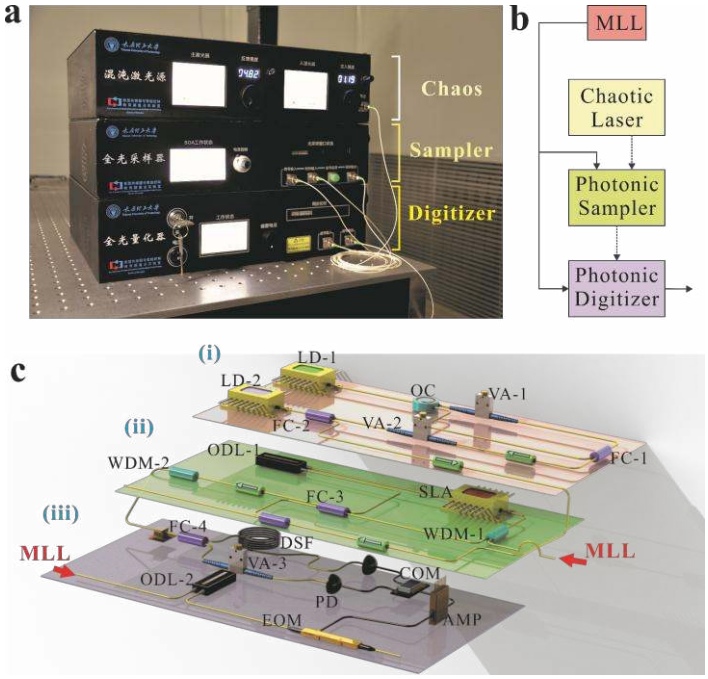

Fig. 1. Architecture of the fully photonic random bit generator (RBG). a, A picture of the integrated fully photonic RBG system. b, Schematic diagram. c, Details of the photonic scheme: (i) laser chaos layer, (ii) photonic sampler layer, and (iii) photonic digitizer layer. MLL, mode-locked laser; LD-1, LD-2, semiconductor distributed-feedback (DFB) laser diode; OC, optical circulator; VA-1, VA-2, VA-3, variable attenuator; FC-1, FC-2, FC-3, FC-4, fiber coupler; ODL-1, ODL-2, optical delay line; SLA, semiconductor laser amplifier; WDM-1, WDM-2, wavelength division multiplexing coupler; DSF, dispersion-shifted fiber; PD, photodiode; COM, comparator; AMP, amplifier; EOM, electro-optic modulator.

III. Experimental Results

A. *Laser Chaos Layer*

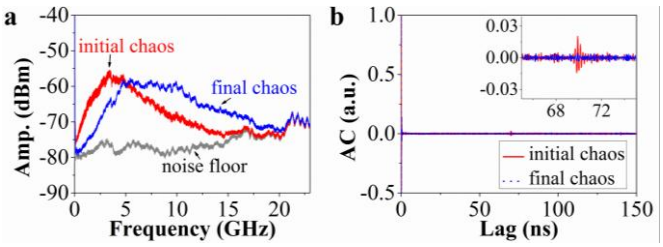

Fig. 2. Test results of the laser chaos layer. a, Radio-frequency spectra for the initial chaotic oscillation (initial chaos, red line), the final high-frequency broadband chaotic output (final chaos, blue line) and the noise floor. b, Autocorrelation (AC) functions of the initial chaotic signal (red solid line) and the final chaos signal (blue dash line). The inset is the partial enlargement of Fig. 2b from 65 to 75 ns.

Figure 2 shows results obtained when testing the chaotic laser (Fig. 1c-i). The master LD-1 at 1554.0660 nm is biased at 1.8 times threshold. Its external 6.99 m fiber ring cavity, constructed by an optical circulator (OC), a variable attenuator (VA-1) and a 50:50 fiber coupler (FC-1), provides a partial optical feedback with a ratio of 6.2%. The red curve in Fig. 2a shows the RF spectrum of the initial chaotic output from the master LD-1, whose main energy is concentrated in the region around the laser relaxation frequency. To obtain a higher chaos bandwidth, the initial chaotic light is injected into the free-running slave LD-2, which is stabilized at 1554.1340 nm and biased at 2 times its threshold current. Setting the injection strength to 7.0% via another variable attenuator (VA-2), one can obtain high-frequency broadband laser chaos from the LD-2 output, whose RF spectrum is the blue curve in Fig. 2a. In contrast to the initial chaos, the enhanced chaos exhibits a flat spectrum with a high plateau from 5 to 10 GHz. The associated chaos bandwidth is about 11.2 GHz, roughly twice that before optical injection. The bandwidth available in the present experimental arrangement enables a random bit generation rate with verified randomness of 10 Gb/s. Further enhancement of the chaos bandwidth may enable an even higher generation rate.

Here, we must point that in this system, the mechanism of chaos bandwidth enhancement is mainly induced by the high-frequency oscillations owing to the beating between the chaotic master laser and the steady slave laser. The current bandwidth of the laser chaos can be further optimized by controlling two critical parameters: the injection strength and the frequency detuning from the master to the slave laser. The maximum bandwidth is expected when the injected chaotic light of the master laser is positive detuned into the edge of the optical spectrum of the slave laser. Detailed maps for oscillation frequency and chaos bandwidth have been systematically studied in Refs. [25, 26]. However, it should be mentioned that when the frequency detuning is too large, the RF spectrum of the chaotic signal will lose its flatness and have two strong resonances around the laser relaxation frequency and the beating frequency, respectively. The existence of the two characteristic oscillations is harmful for high-quality random bit generation. Considering both the flatness and bandwidth of the chaotic RF spectrum, we thus set the frequency detuning at 8.6 GHz in our experiment.

Further, we confirm by comparing the autocorrelation (AC) characteristics of the initial (red solid curve) and the enhanced chaos (blue dash curve) in Fig. 2b that the redundant correlation components of the initial chaotic oscillation (that is, the weak periodicities [7] induced by the external cavity of the master LD-1) have been eliminated by the optical injection. Both the flat top-hat-like spectrum and δ-function-shaped AC characteristic of the chaotic laser enable the high-quality generation of random bits. It is pointed out that polarization maintaining fibers are used for all the optical fiber components in the system. For specifications of the used components in this layer see section V APPENDIX *A*.

B. Photonic Sampler Layer

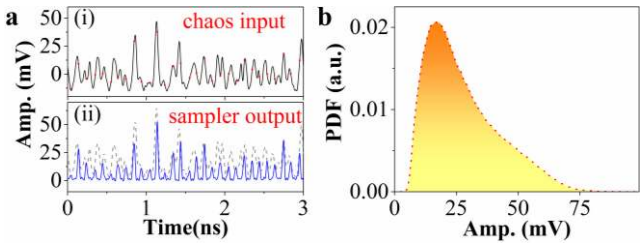

Fig. 3. Test results of the photonic sampler layer. a, (i) Chaos input, i.e., continuous-time chaotic waveform to be sampled; (ii) Sampler output, i.e., discrete-time chaotic pulses after the optical sampling procedure, where the dash line is the envelope of the chaotic pulse peaks. b, A probability density function (PDF) of the sampled chaotic pulse peaks with a size of 1 million data.

Figure 3 reports the results obtained by testing the photonic sampler based on the SLALOM (Fig. 1c-ii). The SLALOM consists of a 50:50 fiber coupler (FC-3) with two branches forming a loop, where a wavelength division multiplexing coupler (WDM-1), a semiconductor laser amplifier (SLA) and an optical delay line (ODL-1) are contained. The chaotic light is split in the FC-3 and travels in clockwise (CW) and counterclockwise (CCW) direction through the SLA. Having traversed the whole loop, the CW and the CCW traveling signals interfere at the FC-3. To achieve the desired sampling function and match the photodiode bandwidth in the subsequent photonic digitizer, the SLA is asymmetrically placed about 20 ps off the center of the loop mirror by accurately adjusting the ODL-1. The MLL used as the triggered optical clock generates ultra-short pulses with a repetition rate of 10 GHz to periodically saturate the SLA, so that the chaotic analog input is sampled at 10 gigasamples per second (GSa/s), which is refined by another WDM coupler (WDM-2). Comparing the broadband chaotic input (Fig. 3a-i) with the discrete sampled output (Fig. 3a-ii), one can see clearly that the sampled chaotic pulse peaks match the analog chaotic envelope very well. This confirms the efficacy of the photonic approach to sample high-frequency and wideband random signals without distortion. Moreover, it should be mentioned that this is the first demonstration that the SLALOM can be used to sample a bandwidth-enhanced chaotic signal with a large optical frequency detuning. Note, polarization maintaining fibers are used for all the optical fiber components in the system. For specifications of the used components mentioned above see section V APPENDIX *A*.

However, it is pointed out that the sampled chaotic pulse peaks inevitably inherit the unwanted asymmetric amplitude distribution from the chaotic laser. Figure 3b shows a typical probability density function (PDF) of the chaotic pulse peaks. For such a distribution, any attempt to make an even division by a fixed threshold will induce some bias in the generated random sequence. Moreover, it should be appreciated that, due to the inherent sensitivity of chaotic systems to external perturbations, the amplitude distribution fluctuates with time.

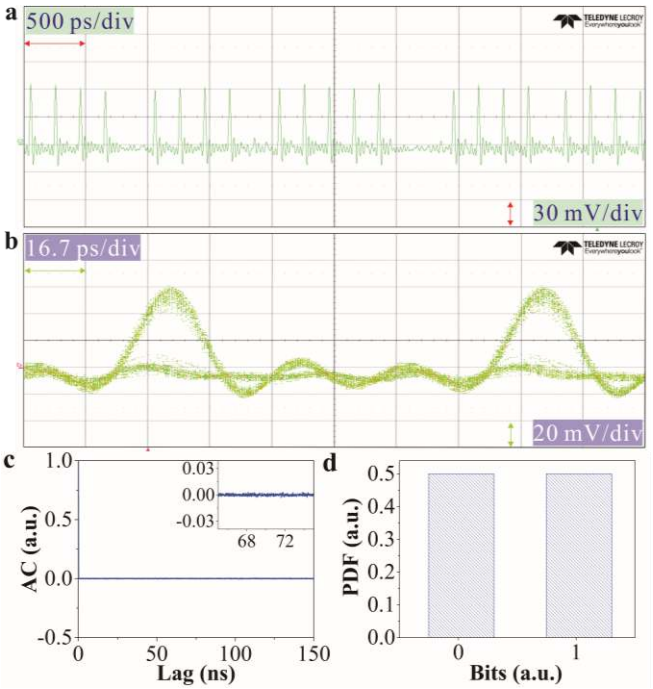

Fig. 4. Test results of the photonic digitizer layer. a, Temporal waveform of the obtained optical bit stream. b, An eye-diagram of the optical bit stream. c, Autocorrelation (AC) function of the random sequence with a size of 1 million bits. d, Corresponding probability density function (PDF) of the random sequence with a size of 1 million bits.

C. Photonic Digitizer Layer

Figure 4 includes all tested results from the photonic digitizer (Fig. 1c-iii). Through two 45 GHz photodiodes (PD), the discrete chaotic pulse peaks $V(t)$ and its delay $V(t-\tau)$ are coupled to the differential input ports of the COM. The output of the COM, referred to as $S(n)$, are high levels when the difference $V(t)$-$V(t-\tau)$ is larger than zero, and low levels otherwise. In our setup, the relative delay τ is realized by a length of dispersion-shifted fiber (DSF) with an extremely long delay of 200 μs. Having been amplified by a 40 GHz RF amplifier (AMP), the binary output $S(n)$ are pulse-coded into an optical random bit stream in the RZ modulation format (with a duty cycle of 33%) by means of the 40 GHz EOM. Note, the modulated optical pulses are from the same MLL, but the pulse-width is broadened with a dispersion compensating fiber (DCF) module to match the 33% duty cycle standard of RZ format.

Herein, we must point out that the conversion from electrical random levels to optical random bits using a EOM is not only to simply make our RBG system applicable to optical fiber communications, but more importantly, is for suppressing the effect of the Johnson noise and comparator ambiguity from the electronic components (*i.e.*, COM). Figure 4a and 4b show the waveform and the eye diagram of the optical random bit stream, respectively. The measured eye has an extinction ratio greater than 10 dBm. Figure 4c and 4d give, respectively, the normalized AC function and PDF of the optical random bits. Compared with Fig. 2b, the ripples on the AC curves have been further suppressed. The 0/1 ratio of the generated random bit is obtained simply by dividing the number of "0s" by the number of "1s" in a bit sequence. Here a 0/1 ratio bits of 0.9994 is obtained. This indicates that the obtained optical bits can be statistically viewed to be independent and unbiased. When we switch off the laser chaos source, only a train of clock pulses (not the random bit waveform in Fig. 4a) is obtained at the final output port of the photonic digitizer. This confirms that the RBG is directly induced by the source chaos and not the consequence of the noise properties of other photonics components within the photonics digitizer and sampler. For specifications of the used components in this part see Section V APPENDIX *A*.

The digitization method used here is termed by us 'discrete self-delay differential comparison'. The key for the discrete self-delay differential comparison approach to guarantee that the obtained random bits are bias-free is the selection of the relative delay (τ). There are two requirements for the delay: (i) The delay must be a high-order integer multiple of the clock period; (ii) The AC coefficient of the chaotic pulses at the delay should be infinitesimally close to zero. The means by which the delay can adaptively eliminate the bias induced by the non-uniform chaotic intensity are explained in Section V APPENDIX *B*.

D. Randomness Verification

We perform more stringent randomness verification using the state-of-the-art statistical test suite of the National Institute of Standards and Technology (NIST SP800-22-rev1a) [31], widely accepted to be the benchmark in the field of cryptographic applications. Table I illustrates a typical result of the 15 NIST test items. As advised by NIST, all the test items are executed using 1000 instances of 1 million bits with a significance level α=0.01. In each test, a p-value is first calculated, which represents the probability that a perfect randomness generator would have produced a random sequence less random than the tested random stream. The criteria for passing the tests are as follows: (i) the proportion of the tested random bit samples satisfying the condition for the p-value larger than α should be in the confidence interval of 0.99 ± 0.0094392; (ii) the uniformity of the p-values (denoted as P-value) should be larger than the failure level of 0.0001. All test results confirm that the generated optical bit stream can be statistically regarded to be random.

TABLE I
TYPICAL RESULTS OF NIST SPECIAL PUBLICATION 800-22-REV1A STATISTICAL TESTS[a]

Statistical test	P-value	Proportion	Result
Frequency	0.522100	0.9920	Success
Block Frequency	0.927677	0.9910	Success
Cumulative Sums	0.924076	0.9920	Success
Runs	0.666245	0.9910	Success
Longest Run	0.426272	0.9890	Success
Rank	0.930026	0.9880	Success
FFT	0.645448	0.9860	Success
Non-Overlapping Templates	0.595549	0.9820	Success
Overlapping Templates	0.134172	0.9900	Success
Universal	0.676615	0.9830	Success
Approximate Entropy	0.866097	0.9910	Success
Random Excursions	0.457557	0.9799	Success
Random Excursions Variant	0.098160	0.9866	Success
Serial	0.731886	0.9910	Success
Linear Complexity	0.645448	0.9910	Success

[a]Using 1000 samples of 1 Mb data and significance level $\alpha = 0.01$, for "Success", the P-value (uniformity of p-values) should be larger than the failure level of 0.0001 and the proportion should be in the confidence interval of 0.99 ± 0.0094392.

IV. CONCLUSIONS AND DISCUSSIONS

We have proposed and demonstrated a fully photonic RBG method. The ultralow temporal jitter of a MLL, together with the utilized ultrafast photonic processes, enables the proposed photonic approach to efficiently overcome the electronic bottlenecks present in previously available physical random bit extraction processes. The present approach thereby possesses a real-time performance exceeding that of all currently available physical RBG systems.

A proof-of-concept fully photonic *real-time* RBG system (prototype) has been implemented using commercially-available photonic devices and has succeeded in generating a 10 Gb/s optical random bit stream. State-of-the-art electrical counterparts cannot directly reach such a high bandwidth.

In the present photonic RBG system, the generation rate is determined by the clock rate of the MLL in the SLALOM based sampler. Considering the ultrafast gain recovery time (below 25

ps) of the semiconductor laser amplifier (SLA) used, our RBG has the ability to be tuned to at least 40 Gb/s. The current maximum secure random bit rate is limited by an information theoretical upper bound on the entropy rate h_{SH} [32], which is given by the Shannon-Hartley limit as below.

$$h_{SH} = 2\mathrm{BW} \times N_{\varepsilon}$$

, where N_{ε} is the number of bits of the digitizer and BW is the bandwidth of the chaotic signal measured by the digitizer. Note, the bandwidth (BW) here means the effective bandwidth of the chaos [33], not the aforementioned chaos bandwidth (i.e., standard bandwidth [34]). In our current experiment, the measured effective bandwidth of chaotic signal is about 5 GHz, which just corresponds to the flat high plateau from 5 to 10 GHz in Fig. 2(a). Considering the number of bits of our photonic digitizer is 1-bit, we thus can get the entropy rate h_{SH}=2BW×N_{ε}=2×5 (GHz)×1 (bit)=10 (Gb/s), which finally limits the maximum bit rate of secure random bits. Secure random bits with real-rates of order 40 Gb/s are expected by using chaotic optical sources constructed by photonic integrated circuits [35-37], fiber ring resonators [38-39] or their combinations [40]. Higher real rates such as 100 Gb/s can be realized, if the SLA used can be replaced by a faster SLA with a recovery time less than say 10 ps [41].

The stability of our generator is quantitatively analyzed by monitoring the frequency of '0' bits, which is a good real-time indicator of the randomness of the bit sequence [42]. In the experiment, we recorded a 1 Mb random bit sequence every half hour to measure its frequency. According to the NIST tests, only a deviation value of 0.13% in the frequency is allowed in this condition. Figure 5 is a typical frequency of '0' bits for the 10 Gb/s physical random bit generator as a function of time, where the dash lines show the range 50.00 ± 0.13%. This demonstrates that our system can operate stably at least 24 hours. In addition, we point out that we use the DC bias control (Model No. MBC-3) from YYLabs Inc. to compensate the bias drift of the EOM in our RBG system.

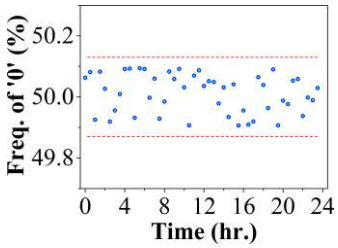

Fig. 5. Measured frequency of '0' bits (the blue circles) for the 10 Gb/s RBG system. Note that the dash lines show the range 50.00 ± 0.13%.

The use of photonics in RBG systems introduces several practical advantages. For instance, the complicated high-precision time shift control needed in the RF domain can be easily realized using tunable optical delay techniques. More generally, the photonic RBG technique is fully compatible with current optical communication systems. As such, well-established optical multiplexing techniques can be directly applied to greatly enhance the random bit generation rate. Currently, 40 Gb/s and 100 Gb/s optical multiplexing systems are commercially available and the systems operating at higher bit rates of 400 Gb/s or 1 Tb/s have been under investigation for telecommunication applications [43]. Considering this point, we think the introduction of parallelism in the optical domain may improve the real-time rate of our photonic RBG method into a level of Tb/s.

With the rapid development of photonic integration circuits (PICs), monolithic integrated chaotic laser chips [35-37] and commercial hybrid-integrated SLA-based interferometric switches [41] have also appeared. This brings an opportunity to construct a compact photonic RBG with high performance for advanced applications, such as large-scale scientific calculations, secure communications and quantum key distributions. Moreover, appropriately designed PICs for this job will greatly reduce the cost and make this fully photonic RBG method be radically innovative. The development of fully photonic integrated RBG modules is our next objective.

Considering that the processed entropy signal (*i.e.*, laser chaos) is a kind of intensity fluctuation in our system, we think the randomness extraction method can be directly applied to other intensity entropy sources such as amplified spontaneous noise [44]. In addition, laser phase noise is always measured by converting phase variation into the intensity fluctuation by the delayed self-homodyne technique [45], so our method should also be expected to be applicable for these phase entropy sources.

At last, we want to emphasize that the optical random bits at least can be used as the cryptographic keys to protect the privacy of data transmission in current optical communication and future all-optical communication. Moreover, if it is wished to apply our optical random bits in electronics, the only requirement is to effect a conversion using a broadband photo-detector. As far as we know, commercially available photo-detectors have reached a response bandwidth of order 100 GHz [46].

APPENDIX

A. *Specifications of Components*

The mode-locked laser (MLL) used is an actively mode-locked fiber-optic laser (Pritel, UOC-05-14G-E). In our system, the MLL works at a 10 GHz repetition frequency and a 1551.2 nm operation wavelength. Its measured pulse width is 2.02 ps (=2.87 ps×0.707) and the associated timing jitter is less than 50 fs. Its RF spectrum, optical spectrum and autocorrelation at 10 GHz are shown in Fig. 6.

In the laser chaos layer, both LD-1 and LD-2 are distributed feedback laser diodes (WTD, LDM5S752 and LDM5S753). The wavelength detuning between them is realized by adjusting their individual temperature controllers. In the associated measurements, a 26.5 GHz spectrum analyzer (Agilent, N9020A, 3 MHz RBW, 3 KHz VBW) and a 36 GHz oscilloscope (Lecroy, LabMaster10-36Zi, 80 GSa/s triggering rate) are used.

In the photonic sampler, the nonlinear semiconductor laser amplifier (SLA, Kamelian, SOA-NL-L1-C-FA) is biased at 300 mA and operates at a peak gain wavelength of 1550 nm with a

small-signal gain of 26 dB, a 3 dB bandwidth of 64 nm and a gain recovery time of 25 ps. The sampling results are monitored by the same 36 GHz oscilloscope, but the triggering rate is set at 800 GSa/s.

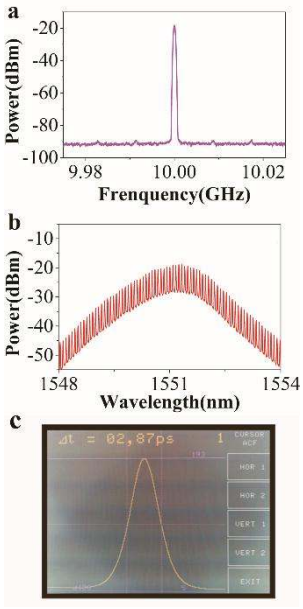

Fig. 6. (a) RF spectrum, (b) optical spectrum and (c) autocorrelation of the mode-locked laser (MLL) at 10 GHz, which are, respectively, measured by the 26.5 GHz spectrum analyzer (Agilent, N9020A, 1.0 KHz VBW, 300 KHz RBW), the optical spectrum analyzer (YOKOGAWA, AQ6370C, 0.02 nm wavelength resolution), and the autocorrelator (APE, Autocorrelator PulseCheck TC).

In the photonic digitizer, the two photodiodes (PDs) are Finisar XPDV2120RA and the differential comparator (COM) is Hittite HMC675LP3E. The broadband 40 GHz electro-optic modulator (EOM) is the Photline MAXAN-LN-35 with a driver (named in the text as AMP) of Photline DR-AN-40-MO. In the measurement, the oscilloscope used is the same as the aforementioned and its triggering rate is set to 800 GSa/s. The chromatic dispersion of the dispersion compensating fiber module (YOFC DM1011-A) is -350 ps/nm used to match the pulse width to the 33% duty cycle standard of the return-to-zero (RZ) modulation format.

B. Discrete Self-Delay Differential Comparison Method

The discrete chaotic pulse train $V(t)$ and its delay $V(t-\tau)$ are coupled to the differential input ports of the COM. Thereby, a binary sequence $S(n)$ can be obtained at the output of the COM: $S(n)$ are high levels when the difference $D(t)=V(t)-V(t-\tau)$ is larger than zero, and low levels otherwise.

Considering that the chaotic amplitude distribution can become relatively stationary on an extremely large time scale, one can regard the chaotic process as a generalized stationary random process. Supposing the amplitude probability density functions of $V(t)$ and $V(t-\tau)$ are $f(x)$ and $f(y)$, we can obtain their joint probability density function $f(x-y)$. Thus, the amplitude distribution function $F(z)$ of their difference signal $D(t)$ can be expressed a

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

Making a variable substitution by $x=u+y$, we can get:

$$\begin{aligned} F(z) &= \int_{-\infty}^{+\infty}[\int_{-\infty}^{z} f(u+y, y)du]dy \\ &= \int_{-\infty}^{z}[\int_{-\infty}^{+\infty} f(u+y, y)dy]du \end{aligned} \tag{2}$$

Taking the derivative of Eq. (2), we can obtain its probability density function:

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

If $V(t)$ and $V(t-\tau)$ are statistically independent, $f(x-y)$ can be equivalent with $f(x)\,f(y)$. Thus, Eq. (3) will be translated into the following:

$$f_z(z) = \int_{-\infty}^{+\infty} f(z+y)f(y)dy \tag{4}$$

Then,

$$f_z(-z) = \int_{-\infty}^{+\infty} f(-z+y, y)dy \tag{5}$$

Defining $v=-z+y$, we have:

$$\begin{aligned} f_z(-z) &= \int_{-\infty}^{+\infty} f(v, v+z)dv \\ &= \int_{-\infty}^{+\infty} f(v)f(v+z)dv \end{aligned} \tag{6}$$

According to Eq. (4) and Eq. (6), we get this result below:

$$f_z(z) = f_z(-z) \tag{7}$$

This means that unbiased random bit sequences can be obtained only if one can guarantee that the correlation coefficient between the two sampled chaotic peaks is close to zero.

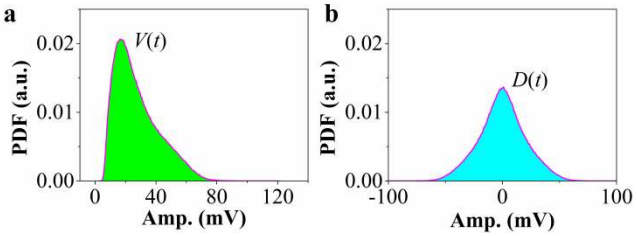

Fig. 7. (a) Probability density functions (PDF) of the chaotic pulse peaks $V(t)$ and (b) PDF of the calculated difference $D(t)$. Note, 1 million samples are used here.

To demonstrate this conclusion, we experimentally recorded the chaotic pulse peaks $V(t)$ and its delay $V(t-\tau)$ and then calculated their difference $D(t)=V(t)-V(t-\tau)$. In our system, the relative time delay τ is set as 200 μs due to the available equipment, where the correlation coefficient is just infinitesimally close to zero. Figure 7 displays the statistical histogram (probability density function, PDF) of $D(t)$. It can be seen clearly that the histogram has a symmetric profile around 0. Thus, our system can yield balanced logical "0" and "1" bits,

although the measured chaotic signals unavoidably have an asymmetric amplitude distribution with a mean voltage drift mainly induced by thermal or mechanical fluctuations.

ACKNOWLEDGEMENT

Pu Li acknowledges Dr. K. V. Reddy for technical assistance on the actively mode-locked fiber laser.

REFERENCES

[1] J. V. Neumann, "Various techniques used in connection with random digits," *Appl. Math. Ser*., vol. 12, pp. 36-38, 1951.

[2] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circ. Syst. I Fundam. Theory Appl.,* vol. 46, no. 5, pp. 615-621 May 2000.

[3] M. Bucci, L. Germani, R.Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC," *IEEE Trans. Comput*., vol. 52, no. 4, pp. 403-409, Apr. 2003.

[4] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, p. 015004, Feb. 2017.

[5] 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*, vol. 2, no. 12, pp. 728-732, Nov. 2008.

[6] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photonics*, vol. 9, no.3, pp.151-162, Feb. 2015.

[7] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.,* vol.103, no. 2, p. 024102, Jul. 2009.

[8] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nat. Photonics*, vol. 4, no. 1, pp. 58-61, Dec. 2010.

[9] 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.*, vol. 49, no.11, pp. 910-918, Nov. 2013.

[10] 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*, vol. 20, no. 27, pp.28603–28613, Dec. 2012.

[11] 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*, vol. 18, no. 18, pp. 18763–18768, Aug. 2010.

[12] X. Z. Li and S. C. Chan, "Random bit generation using an optically injected semiconductor laser in chaos with oversampling," *Opt. Lett.*, vol. 37, no. 11, pp. 2163–2165, Jun. 2012.

[13] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," *Opt. Express*, vol. 22, no. 14, pp. 17271-17280, July 2014.

[14] 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*, vol. 22, no. 6, pp. 6634-6646, Mar. 2014.

[15] 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*, vol. 23, no. 26, pp. 33130-33141, Mar. 2015.

[16] 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*, vol. 23, no. 2, pp. 1470-1490, Dec. 2015.

[17] 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*., vol. 41, no. 2, pp. 388-391, Sep. 2016.

[18] A. Wang, L. Wang, P. Li, and Y. Wang, "Minimal-post-processing 320-Gbps true random bit generation using physical white chaos," *Opt. Express*, vol. 25, no. 4, pp. 3153-3164, Feb. 2017.

[19] R. Walden, *Analog-to-digital conversion in the early twenty-first century*, Wiley, 2008.

[20] A. Khilo, S. J. Spector, M. E. Grein, A. H. Nejadmalayeri, C. W. Holzwarth, M. Y. Sander, M. S. Dahlem, M. Y. Peng, M. W. Geis, N. A. DiLello, J. U. Yoon, A. Motamedi, J. S. Orcutt, J. P. Wang, C. M. Sorace-Agaskar, M.A. Popović, J. Sun, G. R. Zhou, H. Byun, J. Chen, J. L. Hoyt, H. I. Smith, R. J. Ram, M. Perrott, T. M. Lyszczarz, E. P. Ippen, and F. X. Kärtner, "Photonic ADC: overcoming the bottleneck of electronic jitter," *Opt. Express*, vol. 20, no. 4, pp. 4454-4467, Feb. 2012.

[21] P. Li, Y. Sun, X. Liu, X. Yi, J. Zhang, X. Guo, Y. Guo, and Y. Wang, "Fully photonics-based physical random bit generator," *Opt. Lett.*, vol. 41, no. 14, pp. 3347-3350, Jul. 2016.

[22] P. Li, J. Zhang, L. Sang, X. Liu, X. Guo, A. Wang, K. A. Shore, and Y. Wang, "Real-time online photonic random number generation," *Opt. Lett.*, vol. 42,no.14, pp. 2699-2702, Jul. 2017.

[23] B. Jalali, and F. M. A. Coppinger, "Data conversion using time manipulation", U.S. Patent 6 288 659, Sep. 11, 2001.

[24] A. Mahjoubfar, D. V. Churkin, S. Barland, N. Broderick, S. K. Turitsyn, and B. Jalali, "Time stretch and its applications," *Nat. Photonics*, vol. 11, no. 6, pp. 341-351, Jun. 2017.

[25] A. Uchida, T. Heil, Y. Liu, P. Davis, and T. Aida, "High-frequency broad-band signal generation using a semiconductor laser with a chaotic optical injection," *IEEE J. Quantum Electron.,* vol. 39, no. 11, pp.1462-1467, Dec. 2003.

[26] A. B. Wang, Y. C. Wang, and J. F. Wang, "Route to broadband chaos in a chaotic laser diode subject to optical injection," *Opt. Lett.*, vol. 34, no. 8, pp. 1144-1146, May 2009.

[27] 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*, vol. 25, no. 6, pp. 6461-6474, Mar. 2017.

[28] 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*, vol. 25, no. 6, pp. 6511-6523, Mar. 2017.

[29] A. Wang, P. Li, J. Zhang, J. Zhang, L. Li, and Y. Wang, "4.5 Gbps high-speed real-time physical random bit generator," *Opt. Express*, vol. 21, no. 17, pp. 20452–20462, Aug. 2013.

[30] M. Eiselt, W. Pieper, and H. G. Weber, "SLALOM: Semiconductor laser amplifier in a loop mirror," *J. Lightwave Technol.*, vol. 13, no. 10, pp. 2099-2112, Nov.1995.

[31] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, N. Heckert, and J. Dray (2010, Apr.). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

[32] 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*, vol. 2, no. 9, p. 090901, Aug. 2017.

[33] F.Y. Lin, Y.K. Chao, and T.C. Wu, "Effective bandwidths of broadband chaotic signals," *IEEE J. Quantum Electron*., vol. 48, no. 8, pp.1010-1014, May 2012.

[34] F. Y. Lin and J. M. Liu, "Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback," *Opt. Commun.*, vol. 221, no. 1, pp. 173-180, Jun. 2003.

[35] A. Argyris, M.Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," *Phys. Rev. Lett.*, vol.100, no.19, p.194101, May 2008.

[36] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Chaos laser chips with delayed optical feedback using a passive ring waveguide," *Opt. Express*, vol.19, no. 7, pp. 5713-5724, Mar. 2011.

[37] J. G.Wu, L. J. Zhao, Z. M. Wu, D. Lu, X. Tang, Z. Q. Zhong, and G. Q. Xia, "Direct generation of broadband chaos by a monolithic integrated semiconductor laser chip," *Opt. Express,* vol. 21, no. 20, pp. 23358-23364, Sep. 2013.

[38] A. Wang, Y. Wang, Y. Yang, M. Zhang, H. Xu, and B. Wang, "Generation of flat-spectrum wideband chaos by fiber ring resonator," *Appl. Phys. Lett.*, vol. 102, no. 3, p.031112, Jan. 2013.

[39] Y. Hong, X. Chen, P. S. Spencer, and K. A. Shore, "Enhanced Flat Broadband Optical Chaos Using Low-Cost VCSEL and Fiber Ring

Resonator," *IEEE J. Quantum Electron*., vol. 51, no. 3, p.1200106, Mar. 2015.
[40] B. W. Pan, D. Lu, and L. Zhao, "Broadband chaos generation using monolithic dual-mode laser with optical feedback," *IEEE Photonics Technol. Lett.,* vol. 27, no. 23, pp. 2516-2519, Aug. 2015.
[41] 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*., vol. 24, no.12, pp. 4903-4911, Dec. 2006.
[42] 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 semiconductor lasers," *Opt. Express*, vol. 17, no. 11, pp.9053-9061, May 2009.
[43] M. Saruwatari, "All-optical signal processing for terabit/second optical transmission," *IEEE J. Sel. Topics Quantum Electron.*, vol.6, no.6, pp.1363-1374, Nov.-Dec. 2000.
[44] 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, vol. 18, no. 23, pp. 23584–23597, Nov. 2010.
[45] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett., vol. 35, no. 3, pp. 312–314, Feb. 2010.
[46] C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an InP photonic integrated circuit for random number generation," *Optica*, vol. 3, no. 9, pp. 989-994, Sep. 2016.

Pu Li received the M. S. degree in physical electronics from Taiyuan University of Technology (TYUT), Shanxi, China, in 2011. In 2014, he received the Ph. D. degree in circuits and systems at the Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China), College of Physics and Optoelectronics, TYUT, Shanxi, China.

In 2014, He joined TYUT. Currently, he is an assistant professor at the College of Physics and Optoelectronics, TYUT. Meanwhile, he is a Visiting Scholar at the School of Electronic Engineering, Bangor University, United Kingdom in 2017. His research interests include nonlinear dynamics of semiconductor lasers and its applications, fast physical random number generation, and all-optical signal processing.

Dr. Li is a Member of the Chinese Optical Society and the Chinese Physical Society. He also serves as a reviewer for journals of the OSA, IEEE and Elsevier organizations.

Ya Guo received the M. S. degree in optical engineering from TYUT, Shanxi, China, in 2017. He is currently working towards Ph. D. degree at the Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China), TYUT, Shanxi, China.

His research interests focus on fast physical random number generation, and all-optical signal processing.

Yanqiang Guo received the B. S. degree in physics from National Science Talent Training Base, Shanxi University, Taiyuan, China, in 2007, and his M.S. and Ph. D. degrees in optics from the State Key Laboratory of Quantum Optics and Quantum Optics Devices, Shanxi University, Taiyuan, China, in 2009 and 2013, respectively.

In 2013, he joined the TYUT, where he is currently an Assistant Professor with the College of Physics and Optoelectronics. He was also an Assistant Professor with the Center for Photonic Innovations, University of Electro-Communications, Tokyo, Japan in 2014-2016. His research interests include nonlinear optics and its applications, physical random number generation, and quantum state generation and measurement.

Yuanlong Fan received the B. E. degree from Dalian University of Technology, China, in 2009 and his M. E. and Ph. D. degrees from the University of Wollongong, Australia, in 2011 and 2016, respectively, all in electronic engineering. He was a recipient of the Australian Endeavour Fellowship to undertake postdoctoral research at the University of Wollongong, Australia in 2016.

He is currently a research officer at the School of Electronic Engineering, Bangor University, United Kingdom. His research interests include nonlinear dynamics of semiconductor lasers, fiber nonlinear optics, and optical signal processing.

Xiaomin Guo received the B. S. degree in physics from Shanxi Normal University, Linfen, China, in 2008, and her Ph. D. degree in optics from the State Key Laboratory of Quantum Optics and Quantum Optics Devices, Shanxi University, Taiyuan, China, in 2014.

Since 2014, she has been an Assistant Professor with the College of Physics and Optoelectronics, TYUT. She undertook postdoctoral research at University of Electro-Communications, Tokyo, Japan, from 2014 to 2016. Her research interests include physical random number generation, secure communication, and quantum information processing.

Xianglian Liu received the Ph. D. degree in the State Key Laboratory of Transient Optics and Photonics, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an 710119, China.

Now, she is with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, College of Physics and Optoelectronics, TYUT. Her research interests include random number and all-optical analog-to-digital conversion.

Kunying Li received the M. S. degree in optical engineering from TYUT, Shanxi, China, in 2017. She is currently working towards Ph. D. degree at the Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China), TYUT, Shanxi, China.

Her research interests focus on fast physical random number generation, and all-optical analog to digital conversion.

K. Alan Shore (SM'95) received the degree in mathematics from the University of Oxford, Oxford, U.K., and the Ph.D. degree from University College, Cardiff, Wales, U. K.

He was a Lecturer with the University of Liverpool from 1979 to 1983 and with the University of Bath, where he became a Senior Lecturer in 1986, a Reader in 1990, and a Professor in 1995. He was a Visiting Researcher with the Center for High Technology Materials, University of New Mexico, Albuquerque, USA, in 1987. In 1989, he was a Visiting Researcher with the Huygens Laboratory, Leiden University, The Netherlands. From 1990 to 1991, he was with the Teledanmark Research Laboratory and the MIDIT Center of the Technical University of Denmark, Lyngby. He was a Guest Researcher with the Electrotechnical Laboratory, Tsukuba, Japan, in 1991. In 1992, he was a Visiting Professor with the Department of Physics, University de les IllesBalears, Palma–Majorca, Spain. He was a Visiting Lecturer with the Instituto de Fisica de Cantabria, Santander, Spain, from 1996 to 1998, and a Visiting Researcher with the Department of Physics, Macquarie University, Sydney, Australia, in 1996, 1998, 2000, 2002, 2005, and 2008. In 2001, he was a Visiting Researcher with the ATR Adaptive Communications Laboratories, Kyoto, Japan. From 2001 to 2008, he was the Director of Industrial and Commercial Optoelectronics, a Welsh Development Agency Center of Excellence. Since 1995, he has been the Head of the School of Informatics, College of Physical and Applied Sciences, Bangor University. He has authored or co-authored more than 1000 contributions to archival journals, books, and technical conferences. With Prof. D. Kane, he co-edited the research monograph Unlocking Dynamical Diversity. His research work has been principally in the area of semiconductor optoelectronic device design and experimental characterization with particular emphasis on nonlinearities in laser diodes and semiconductor optical waveguides. His current research interests include nonlinear optics and its applications, and the design of nano-spin semiconductor lasers. In 1995, he was appointed as the Chair of Electronic Engineering with Bangor University. He was the Chair of the Welsh Optoelectronics Forum from 2006 to 2008 and has chaired the Photonics Academy for Wales, since its establishment in 2005. From 2008 to 2011, he was the Chair of the Quantum Electronics Commission of the International Union of Pure and Applied Physics.

Dr. Shore has been a Program Member for several OSA conferences. He was a Co-Organizer of a Rank Prize Symposium on Nonliear Dynamics in Lasers held at the lake district, U.K., in 2002. He cofounded and from 1987 to 2012 acted as the Organizer and Program Committee Chair for the International Conference on Semiconductor and Integrated Optoelectronics, which is held annually in Cardiff, Wales, U.K. He chaired the Education and Training in Optics and Photonics conference held at the Technium OpTIC, Wales, 2009. He received the Royal Society Travel Grant to visit universities and laboratories in Japan in 1988. From July to December 2010, he held a Japan Society for the Promotion of Science Invitation Fellowship in the Ultrafast Photonics Group, Graduate School of Materials Science, Nara Institute of Science and

Technology, Nara, Japan. He is a Fellow of the Optical Society of America, the Institute of Physics, and the Learned Society of Wales for which he has served as a Council Member (2012-2015; 2016-2019) and General Secretary (2017-2020).

Yuncai Wang was born in Shanxi, China. He received the B.S. degree in semiconductor physics from Nankai University, Tianjin, China, in 1986, and the M. S. and Ph. D. degrees in physics and optics from Xi'an Institute of Optics and Precision Mechanics of Chinese Academy of Sciences (CAS), Shaanxi, China, in 1994 and 1997, respectively.

In 1986, he joined TYUT, as a teaching assistant. He was a Visiting Scholar at the Institut für Festkörperphysik, Technische Universität Berlin, Berlin, Germany, from 2001 to 2002. He was a Lecture (1994-1998) and then an Assistant Professor (1998-2003) at the Department of Physics, TYUT. Since 2003, he has been a Professor at the College of Physics and Optoelectronics, TYUT. Now, he also is the chair of the Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China). His current research interests are nonlinear dynamics of semiconductor lasers and fibers and their applications, including all-optical analog-to-digital conversion, and optical communications.

Dr. Wang is a Fellow of the Chinese Instrument and Control Society, a Senior Member of the Chinese Optical Society and the Chinese Physical Society. He also serves as a reviewer for journals of the IEEE, OSA and Elsevier organizations.

Anbang Wang received the M. S. degrees in physical electronics and the Ph. D degree in electronic circuit and system from TYUT in 2006 and 2014, respectively.

He joined TYUT as a lecture in 2006 and became a professor in 2015 at the College of Physics and Optoelectronics, TYUT. Between Dec. 2014 and May 2015, he was a visiting scholar with the School of Electronic Engineering, Bangor University, U.K. His research interests include nonlinear dynamics of semiconductor lasers and its applications, all-optical analog-to-digital conversion, optical signal processing, fiber nonlinear optics and optical communications.

Dr. Wang is a Member of the IEEE Society. He is a committee member of Opto-Electronic Technology Professional Committee, the Chinese Optical Society. He serves as a topical editor of Acta Optica Sinica, and as a reviewer for journals of the IEEE and OSA organizations.