Fast and Tunable All-Optical Physical Random Number Generator Based on Direct Quantization of Chaotic Self-Pulsations in Two-Section Semiconductor Lasers

Pu Li, Yun-Cai Wang, An-Bang Wang, and Bing-Jie Wang

***Abstract*—We present numerically an all-optical approach to generate fast physical random numbers. This approach is based on chaotic self-pulsations, a kind of chaos superimposed on periodic pulse trains. Two-section semiconductor lasers (TSSLs) can exhibit this phenomenon of chaos, under an appropriate external optical injection. Simulations demonstrate that, without sampling and postprocessing procedures, this technique can produce random numbers at gigabit per second rates through directly quantizing the chaotic self-pulsations via an all-optical flip-flop. Further simulation results show that the random number generation rate can be continuously and easily tuned in a large range from 5 to 10 Gb/s by adjusting some control parameters of the TSSL subject to continuous-wave optical injection, such as injection strength, frequency detuning, gain current, and absorber bias. Moreover, our numerical studies show that these generated random numbers sequences above with the proposed method can pass successfully standard benchmark tests for randomness.**

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

I. Introduction

RANDOM number or bit generators (RNGs) are the nuts and bolts for many applications from science to commerce: cryptography and security protocols [1]–[5], Monte Carlo (MC) simulations [6], stochastic experiments [7], and lottery games [8], for instance.

Deterministic algorithm-based pseudorandom number generators (PRNGs) are well known and widely used in various fields aforementioned, because they show the merits of high-speed bit generation rate and ease of implementation. However, there exists a fatal defect in PRNGs that their output sequences are periodic. Once the seeds and generation algorithms are known, one can predict completely their outputs (i.e., pseudorandom bits). If PRNGs are applied in a secure system, disastrous consequences can be caused [9]. Even in the large-scale MC simulations where the security is not crucial, PRNGs can lead to systematic errors [10]. "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin," said by J. von Neumann [11].

The quest for true randomness engenders the other kind of RNGs: true random number generators (TRNGs). TRNGs, also called as physical RNGs, produce random numbers or bits by digitizing stochastic physical processes in the natural world. There have existed many different proposals for TRNGs based on the foundational unpredictability, such as thermal noise in resistors [12], single photon splitting on a beam splitter [13], the continuous variable vacuum fluctuations [14], [15], amplified spontaneous emissions from superluminescent LEDs [16], erbium-doped fiber amplifiers (EDFAs) [17] or semiconductor optical amplifiers [18], and chaotic dynamics in semiconductor lasers [19]–[28] or electrical circuits [29]–[32], but most of them have a common feature that their entropy sources are stochastic continuous variables. In the transformation from stochastic signals to discrete random bit sequences, TRNGs usually need achieve three steps: sampling, quantizing, and postprocessing. In the sampling procedure, the aperture jitter of the external triggered clock can result in great deterioration of the conversion accuracy and signal-to-noise ratio (SNR) [33], especially when it works at a high speed. To obtain statistically passable random sequences, the postprocessing procedure (e.g., hash function [13], [14], exclusive OR (XOR) operation [19], or least significant bits (LSBs) algorithm [21]) is often performed. Finally, the complexity of TRNGs is significantly increased and the bit rates become not easily tunable.

Recently, we have proposed and demonstrated a simple method of a TRNG using discrete-time stochastic systems as physical entropy sources [34]. In this method, a discrete pulse amplitude chaos from a fiber ring laser passively mode locked by nonlinear polarization rotation is directly quantized into high-quality random number sequences in the absence of sampling and postprocessing procedures. Therefore, this method can avoid the aliasing problem induced by the sampling procedure and thus attain a reduction in structure complexity. However, it has an inevitable drawback in the limited rate of 20 Mb/s. For many applications such as secure communications, the generation speed of random numbers is of paramount importance.

In this paper, we show numerically that the high-speed all-optical TRNG based on discrete-time chaotic systems can be achieved with optically injected two-section semiconductor

Manuscript received July 17, 2012; revised September 1, 2012; accepted September 7, 2012. This work was supported by the National Natural Science Foundation of China under Grants 60927007 and 61001114 and by the State Key Laboratory of Quantum Optics and Quantum Optics devices of China under Grant 200903.

The authors are with the College of Physics and Optoelectronics and the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education of China, Taiyuan University of Technology, Taiyuan 030024, China (e-mail: lipu8603@126.com; wangyc@tyut.edu.cn; anbang82w@yahoo.com.cn; wbj1131@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2012.2219298

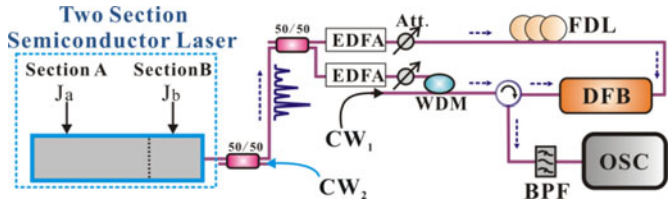

Fig. 1. Schematic diagram of the proposed all-optical TRNG based on chaotic self-pulsations produced by an optically injected TSSL. Sections A and B are the gain and absorber section of TSSL, and J_a and J_b are their respective pump currents. 50/50: 3-dB optical coupler; EDFA: erbium-doped fiber amplifier; Att.: optical attenuator; FDL: fiber delay line; WDM: wavelength-division-multiplexing coupler; CW_1/CW_2: CW lights; DFB: distributed-feedback laser diode; BPF: optical bandpass filter; and OSC: oscilloscope.

lasers (TSSLs). In this new method, the TSSL is used as a slave laser injected by an external continuous-wave (CW) light from the other laser (the master laser). By adjusting the injection strength and the frequency detuning from the master laser to the slave, the TSSL can exhibit chaotic self-pulsations which consist of pulse streams with a high repetition frequency but stochastic intensities. Then, through directly quantizing chaotic self-pulsations with an all-optical flip-flop (AOFF), physical random number sequences with verified randomness can be obtained.

This proposed TRNG can not only eliminate the problem induced by sampling procedures, but also has a significantly increased generation rate which can be continuously tuned up to more than 10 Gb/s. Moreover, it is worth mentioning that this new TRNG is directly compatible with the optical communication networks without any electronic-to-optical or optical-to-electronic conversion, because all its signal processing is done in the optical domain. In next generation ultrafast optical networks, all-optical signal processing will be important. The speed limitation of electronic devices is considered to be several tens of gigabits per second. For signal processing at higher speeds, it will inevitably be necessary to use all-optical devices. From this prospect, our work may spur more interests toward realizing ultrafast all-optical TRNGs.

II. Principle and Simulation

The schematic diagram of the proposed TRNG is shown in Fig. 1, which mainly includes a TSSL subject to CW optical injection (CW_2) and a distributed-feedback laser diode (DFB). In this system, the TSSL is the physical entropy source, while the DFB plays the role of an AOFF used to quantize the outputs of the entropy source. Under appropriate injection strength and frequency detuning, the TSSL will exhibit chaotic self-pulsations which are output via a 3-dB coupler (50/50). Then, they are split by another 3-dB coupler (50/50) resulting in two identical pulse streams, whose powers are controlled through a set of EDFAs and optical attenuators (Att.), respectively. One of the two identical trains is injected into the right-hand side of the DFB laser through a fiber delay line (FDL). On the left-hand side of the DFB laser is the other pulse stream combined with a CW light (CW_1) at the same wavelength through a wavelength-division multiplexing (WDM) coupler (WDM). At last, we employ an optical circulator and an optical bandpass filter (BPF) to separate the light of the DFB laser from the injected lights. The obtained random bit sequence can be visualized on an oscilloscope (OSC). We describe detailed numerical simulations as follows.

A. Chaotic Self-Pulsations and Their Characteristics

As the physical random entropy source of the all-optical TRNG, chaotic self-pulsations are generated by a TSSL subject to CW optical injection, as illustrated in Fig. 1. The TSSL is comprised of two sections: the longer section is biased well into gain, named as a gain section, while the shorter section is unbiased or reverse-biased, termed as an absorber section. Each section is individually biased by a direct current (J_a or J_b). Note, all the subscripts a and b in this paper refer to the gain and absorbing media, respectively. When the injection strength and the frequency detuning from the master laser (CW_2) to the slave TSSL are appropriate, chaotic self-pulsing takes place.

Chaotic self-pulsation is a kind of chaos superimposed on a periodic system, which exists commonly in the Rossler dynamical systems [35]. Such chaos in optically injected TSSLs are first reported by Chlouverakis and Adams [36]. In their work, the region of chaotic self-pulsations (named as C_2 region by them in [36]) for an optically injected TSSL with two different linewidth enhancement factors (α_a and α_b) has been determined and they pointed out the chaotic self-pulsation region can be enhanced when $\alpha_a < \alpha_b$.

In this paper, we discuss the characteristics of chaotic self-pulsations in optically injected TSSLs and demonstrate that it is a suitable physical entropy source for TRNGs. The applied model and associated parameters for the TSSL subject to external CW optical injection are the same as those in [36]–[38], expressed as follows:

$$\frac{dE}{dt} = \frac{1}{2}\{n_a(1-h) - n_b h\}E + K\cos\theta \tag{1}$$

$$\frac{d\theta}{dt} = \omega - \frac{1}{2}\{n_a\alpha_a(1-h) - n_b\alpha_b h\} - K\frac{\sin\theta}{E} \tag{2}$$

$$\frac{dn_a}{dt} = J_a - e_1E^2 - e_2n_a(1+E^2) \tag{3}$$

$$\frac{dn_b}{dt} = J_b - e_3E^2 - e_4n_b(1+\gamma E^2) \tag{4}$$

where E is the normalized slave TSSL electronic complex amplitude and θ is the corresponding phase. K and ω denote the injection strength and the frequency detuning from the master laser to the slave TSSL, respectively. n_a and n_b give the normalized carrier densities for both sections in the TSSL, respectively. The following parameters are used in the simulation: the normalized length of the absorber section $h = 0.1$, the normalized pump currents $J_a = 0.0109$ and $J_b = 0.065$, the corresponding linewidth enhancement factors $\alpha_a = 3$ and $\alpha_b = 4$, the material parameters for the TSSL $e_1 = 0.002356$, $e_2 = 0.002$, $e_3 = 0.0036$, $e_4 = 0.005$, and $\gamma = 1.2$. For more details, see [36].

With the aforementioned parameters selected, the TSSL subject to optical injection can emit chaotic self-pulsations in an appropriate injection strength K and frequency detuning ω range. Fig. 2 shows a detailed dynamics of an optically injected TSSL with $\alpha_a = 3$ and $\alpha_b = 4$, where the colored region denotes

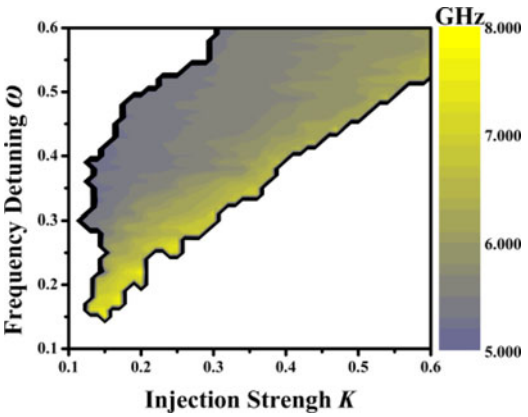

Fig. 2. Stability map for an optically injected TSSL with $\alpha_a = 3$ and $\alpha_b = 4$. The colored region denotes chaotic self-pulsations. The color represents the repetition rate of chaotic pulsations. The rest of the map, i.e., the clear region, represents period states, quasi-period states, or conventional chaos.

chaotic self-pulsations. The rest of the map represents period or quasi-period states or conventional chaos.

We arbitrarily select an operating point in the chaotic self-pulsations region (see Fig. 2) with $K = 0.15$ and $\omega = 0.3$ to analyze the characteristics of chaotic self-pulsations. Fig. 3(a) shows a typical chaotic self-pulsations time series in the selected state, composed of chaotic pulse streams with a 5.4-GHz repetition frequency but random intensities. Fig. 3(b) shows the autocorrelation function curve of the chaotic pulse powers. The delta-profile curve in Fig. 3(b) indicates that the chaotic self-pulsations are aperiodic and have a statistically insignificant correlation. This feature is crucial to generate high-quality random bits. For identifying the complexity of chaotic self-pulsations and the nonlinear correlation they embrace, a further analysis is performed. We first reconstruct a pseudophase space from the successive chaotic pulse power data by means of the delay-coordinate technique and then employ Grassberger–Procaccia algorithm (GPA) [39] to acquire their correlation dimensions (D_2) and embedding dimensions (m). Fig. 3(c) shows a plot of D_2 as a function of m based on 20 000 power points. As expected for chaos, D_2 clearly converges to a value corresponding to the correlation dimension. The higher the value, the larger the dimension of the space required to completely unfold the chaotic attractor, and the more complex the dynamic output. From Fig. 3(c), we can confirm that the correlation dimension of the generated chaotic self-pulsations is a fractional number around 5 which implies significant complexity. Finally, we consider the distribution of chaotic pulse powers. As shown in Fig. 3(d), the stochastic histogram of the chaotic pulse peak intensities indicates that chaotic self-pulsations have a highly symmetric distribution. Such a distribution is very useful for a TRNG.

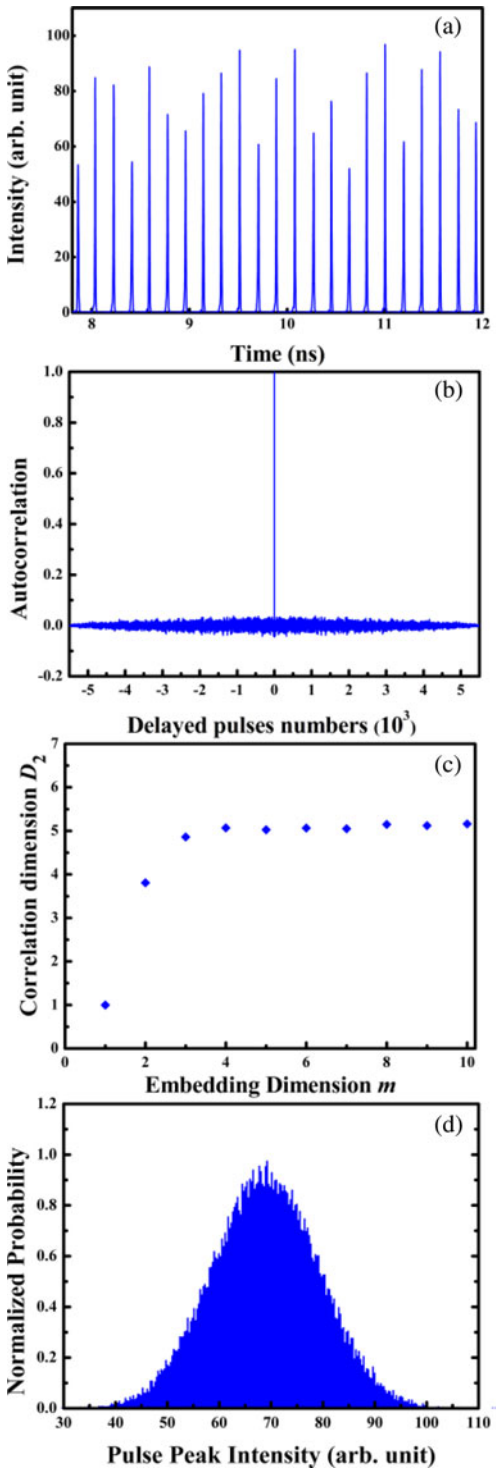

Fig. 3. Characteristics of chaotic self-pulsations. (a) Time series of the chaotic self-pulsations. (b) Autocorrelation curve of the chaotic pulse powers. (c) Result of GPA analysis on chaotic pulse powers. (d) Stochastic histogram of the chaotic pulse peak intensities.

B. All-Optical Quantization for Random Number Generation

We quantize the generated chaotic self-pulsations with the same method as that in [28] and [34], which is implemented using a DFB laser functioning as an AOFF. Through injecting a CW light into such a laser diode, a bistability phenomenon can appear due to the spatial hole burning effect, which is the base of AOFF operation. By adjusting the intensity of the injected CW light into an appropriate value, the DFB laser will be held in the bistable regime. In this condition, the two states of the bistability can be switched by the random pulses injected into the right and left side of the DFB laser, as shown in Fig. 1. Herein, it must be pointed out that only when the injected pulse power is higher above a certain threshold determined by the hysteresis curve width (expressed as $\Delta P = P_{\mathrm{th2}} - P_{\mathrm{th1}}$ in [28] and [34]),

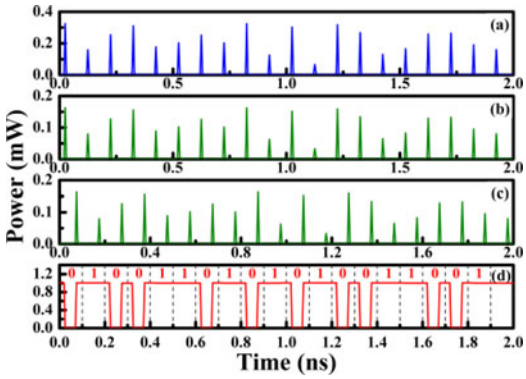

Fig. 4. Temporal waveforms. (a) Chaotic self-pulsations from the optically injected TSSL. (b) Chaotic self-pulsations injected into the left hand of the AOFF. (c) Delayed chaotic self-pulsations injected into the right-hand of the AOFF. (d) Random bit sequence.

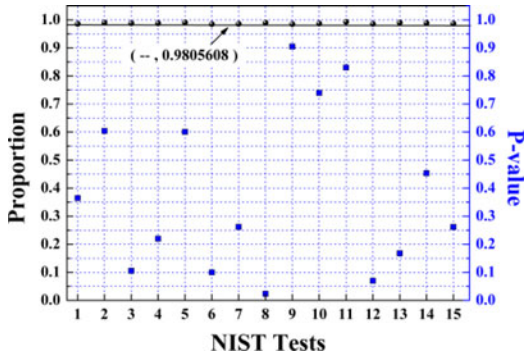

Fig. 5. Typical results of NIST statistical tests. Using 1000 samples of 1-Mb data and significance level $\beta = 0.01$, for "Success," the P-value (uniformity of p-values) should be larger than 0.0001 and the proportion should be greater than 0.9805608. Blue squares and black circles represent the P-value and passed proportion of each tests, respectively.

the switch between the two output states happens. In addition, it should be noted that this kind of AOFF is proposed and demonstrated from both experiment and simulation by Huybrechts *et al*. [40]–[42]. Their studies show that the AOFF requires low trigger pulse energies below 200 fJ and has a rising time of 40 ps in experiments and can be shorten to 10 ps in theory, corresponding to a bandwidth larger than 30 GHz. Therefore, this kind of AOFF is feasible enough to respond to the chaotic self-pulsing train with high repetition frequencies around 10 GHz. On the basis of the aforementioned phenomena, the quantizing to the chaotic self-pulsations can be achieved numerically. For more details, see [28] or [34].

Fig. 4 shows the quantizing results to chaotic self-pulsations. In the simulation, the CW light [CW_1 in Fig. 1] has a power of 1.6 mW. In this case, the AOFF threshold corresponds to 0.1 mW which is equal to the mean power of the chaotic self-pulsation. Fig. 4(a) shows the chaotic self-pulsations time series from 0 to 2 ns emitted by the TSSL subjected to CW optical injection. Different with the state in Fig. 3(a), the chaotic self-pulsations here lie on a higher repetition frequency of 10 GHz. The increase in the repetition frequency is induced by the variations of some parameters J_a, J_b, K, and ω. Herein, $J_a = 0.0118$, $J_b = 0.0624$, $K = 0.2$, and $\omega = 0.35$, and other parameters are the same as that in Section II-A. Specific affection of J_a, J_b, K, and ω on the repetition rate will be analyzed in Section III. The chaotic self-pulsations with an average power of 0.1 mW after through the 3-dB coupler are illustrated in Fig. 4(b), which will be injected into the left side of the DFB laser. Fig. 4(c) shows the other identical stream which is delayed by about 50 ps via the FDL and injected into the DFB laser from its right hand. Fig. 4(d) shows the final AOFF output (i.e., the random bit sequence) after through the BPF separating the lasing light of the AOFF from the injecting lights. The "hollows" in the output waveform represent "0 s" and other parts are coded as "1 s." It is obvious that the bit rate of the generated random sequence is also 10 Gb/s corresponding to the repetition frequency of the chaotic self-pulsations.

C. Randomness Verification

After these aforementioned procedures, the theoretical model of our all-optical TRNG has been constructed. In this section, we provide detailed quality test results of the proposed TRNG.

There are numerous statistical test suites to assess the quality of the statistical randomness of RNGs. However, the statistical test suite of the National Institute of Standards and Technology (NIST) [43] and the Diehard test suite [44] are widely accepted to be more stringent in detecting the deviation of a data stream from randomness and have become the standards.

The NIST test suite contains 15 types of statistical tests and each test is based on a calculated statistical p-value, a function of the data being tested. The passing criterion is determined by the length of the tested bit sequence n and the significant level β. In our tests, $n = 1000$ samples of 1-Mb data are applied and α is chosen to be 0.01. In this case, when the proportion of the sequences satisfying p-value $> \beta$ is in the range of $(1-\beta) \pm 3\sqrt{(1-\beta)\beta/n} = 0.99 \pm 0.0094392$ and the uniformity of the p-values (i.e., the P-value) is larger than 0.0001, the sequences are considered to be random. Fig. 5 shows a typical result of NIST tests, where blue squares and black circles represent the P-value and passed proportion of each tests, respectively. The numbers from 1 to 15 on the horizontal axis represent 15 different statistical tests in NIST test suite, which are named as "Frequency," "Block frequency," "Cumulative sums," "Runs," "Longest-run," "Rank," "FFT," "Nonperiodic templates," "Overlapping templates," "Universal," "Approximate entropy," "Random excursions," "Random excursions variant," "Serial," and "Linear complexity," respectively.

On the other hand, the Diehard test suite is a statistical package involving 18 statistical tests. The 18 tests have been applied to 74 Mb random number sequences. The significant level β has been chosen to be 0.01, which means that each test is considered to be successfully passed when the P-value (i.e., uniformity of the p-values) of each test lies in the range from 0.01 to 0.99. A typical Diehard test result is shown in Fig. 6, where blue squares denote the P-value of each test in Diehard test suite and the numbers from 1 to 18 on the horizontal axis represent 18 different statistical tests, which are named as "Birthday spacing," "Overlapping 5-permutation," "Binary rank for 31 × 31 matrices," "Binary rank for 32 × 32 matrices," "Binary rank for 6 × 8 matrices," "Bitstream," "Overlapping-Pairs-Space-Occupancy," "Overlapping-Quadruples-Space-Occupancy," "DNA," "Count the 1's on a stream of bytes," "Count the 1's for specific bytes," "Parking lot," "Minimum distance," "3D-spheres,"

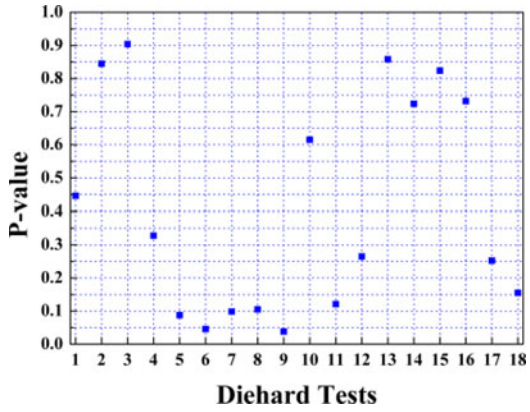

Fig. 6. Typical results of Diehard statistical tests. Using 74-Mb data and significance level $\beta = 0.01$, for "Success," the P-value (uniformity of p-values) should be within [0.01, 0.99]. Blue squares denote the P-values of each test, respectively.

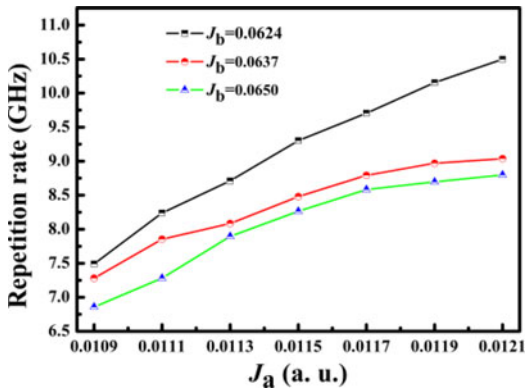

Fig. 7. Typical variation of chaotic self-pulsation frequency with gain current J_a and absorber bias J_b.

"Squeeze," "Overlapping sums," "Runs," and "Craps," respectively. Among them, the P-values of "Binary rank for 6×8 matrices"/"3D-spheres"/"Overlapping sums"/"Runs"/"Parking lot"/"Minimum distance" are obtained by applying the Kolmogorov–Smirnov (KS) test to the P-values of all the subtests.

As shown in Figs. 5 and 6, the obtained binary strings with our method pass all the statistical tests of NIST and Diehard. That indicate that the proposed TRNG has high-quality randomness and its outputs are truly independent random bits.

III. Tunable Bit Generation Rate of the TRNG

The generation rate of the proposed all-optical TRNG is primarily determined by the repetition frequency of chaotic self-pulsations from the optically injected TSSL, as described in Section II. Therefore, if the repetition rate of chaotic self-pulsations is tunable, the tunability of bit rate of TRNG can be realized correspondingly.

There are two methods to tune the repetition rate of chaotic self-pulsations.

One is to vary the injection strength K and frequency detuning ω, through adjusting the master laser [CW_2 in Fig. 1] in the master–slave configuration of optically injected TSSL on the repetition rate of chaotic self-pulsations. The calculated mapping of the repetition rate of chaotic pulsations as a function of the injection strength K and frequency detuning ω has been given beforehand in Fig. 2 (see Section II-A). On the mapping, two characterizations are apparent. When the frequency detuning ω is fixed, the chaotic pulsation repetition rate will increase with the increase of the injection strength K. In contrast, by increasing the frequency detuning ω, the repetition rate of chaotic pulsations falls down while the injection strength K is constant. Typically, the repetition rate of chaotic pulsations can be tuned up to 8 GHz at the bottom of the chaotic self-pulsation region (see Fig. 2).

The other is to simultaneously varying both bias currents of the slave TSSL. We consider the effects of bias currents of the TSSL on the repetition rate of chaotic pulsations by arbitrarily selecting an operating point in the chaotic self-pulsations region (see Fig. 2) with $K = 0.2$ and $\omega = 0.35$. Other parameters in the simulation keep the same as that in Section II-A. Fig. 7 shows the typical variation of chaotic self-pulsation frequency with gain current J_a and absorber bias J_b. Continuous tuning can be observed. When absorb bias is fixed, increasing gain current increases the repetition rate of chaotic self-pulsations. On the other hand, the chaotic self-pulsation frequency shows a linear dependence on the absorber bias: increasing the positive bias will increase the pulsation frequency for a constant gain current. Meanwhile, it is clear from Fig. 7 that chaotic self-pulsations at frequencies above 10 GHz are possible, and the repetition frequency can be continuously tuned in a large range of several gigahertz. In fact, if the selected operating point is located at the bottom of the chaotic self-pulsation region (see Fig. 2), the chaotic self-pulsations can reach a higher repetition rate. Here, it should be noted that the gain current J_a and absorber bias J_b only can vary in a limited range. If the pump currents increase further, the chaotic self-pulsation state may break up.

In addition, we point out that the statistical randomness of random bit sequences extracted from the chaotic self-pulsations with different repetition rates by means of the same method in Section II-B can also pass successfully the statistical test suite of NIST and DIEHARD. Those detailed test results are omitted in this paper, because they are similar with the ones in Figs. 5 and 6. Herein, we only list some typical final test results of random sequences with different rates and their corresponding working states of the TSSL where only J_a, J_b, K, and ω are variables, while the other parameters are the same as that in Section II-A. As shown in Table I, the random sequences working at the bit rates from 5 to 10 Gb/s can pass all tests. The maximum passable bit rate is 10.15 Gb/s, corresponding to the repetition frequency of chaotic self-pulsations from the TSSL working at the condition where $J_a = 0.0119$, $J_b = 0.0624$, $K = 0.20$, and $\omega = 0.35$. Note, NIST and Diehard in Table I denote the final result of the NIST and Diehard test suite, respectively.

IV. Discussions

A. Robustness of the All-Optical TRNG and Its Improvement

Among all signal processing procedures in our system, all-optical quantization to chaotic self-pulsations is a crucial

TABLE I
TYPICAL FINAL TEST RESULTS OF RANDOM SEQUENCES WITH DIFFERENT REPETITION RATES

K	ω	Ja	J_b	Bit rate	NIST	Diehard
0.15	0.41	0.0109	0.065	5.0 Gb/s	pass	pass
0.15	0.28	0.0109	0.065	5.5 Gb/s	pass	pass
0.20	0.30	0.0109	0.065	6.0 Gb/s	pass	pass
0.15	0.25	0.0109	0.065	6.5 Gb/s	pass	pass
0.30	0.30	0.0109	0.065	7.0 Gb/s	pass	pass
0.25	0.26	0.0109	0.065	7.5 Gb/s	pass	pass
0.15	0.15	0.0109	0.065	8.0 Gb/s	pass	pass
0.20	0.35	0.0111	0.0624	8.3 Gb/s	pass	pass
0.20	0.35	0.0113	0.0624	8.7 Gb/s	pass	pass
0.20	0.35	0.0115	0.0624	9.3 Gb/s	pass	pass
0.20	0.35	0.0117	0.0624	9.7 Gb/s	pass	pass
0.20	0.35	0.1118	0.0624	10.0 Gb/s	pass	pass
0.20	0.35	0.0119	0.0624	10.15 Gb/s	pass	pass

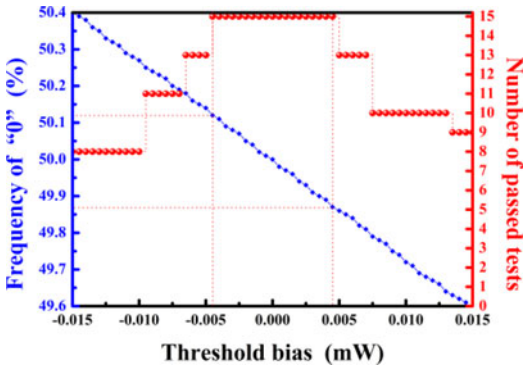

Fig. 8. Frequency of "0" in a random bit sequence (blue squares) and the number of passed NIST tests (red circles) as a function of the threshold bias. Here, the threshold bias represents the difference between the threshold of the AOFF which is fixed at 0.1 mW and the average power of the chaotic pulse trains.

ingredient to affect the tolerance of the proposed TRNG, because all-optical quantization through the AOFF operation requires a very strictly determined threshold decision in order to maintain good randomness.

Let us take the TRNG with the rate of 5.4 Gb/s (see Section II-A) as an example. In Fig. 8, a graph of the occurrence frequency of "0" and the number of successful NIST tests as functions of the threshold bias is shown. Notice that the threshold bias denotes the difference of the mean value of the chaotic pulse powers from the AOFF threshold which is fixed at 0.1 mW in our simulation. The mean power of the chaotic pulse streams is variable through tuning the set of EDFAs and Att. in Fig. 1. From Fig. 8, it is obvious that the frequency of "0" decreases almost linearly as the threshold bias increases. Only when the frequency of "0" is within [49.87%, 50.13%], the corresponding random sequences can successfully pass all the NIST tests (15 tests in total). To satisfy this condition, the variation range of the threshold bias is allowed from -0.0045 to 0.0045 mW, as shown in Fig. 8. Further, we have also analyzed the robustness of the proposed TRNGs working at other states with different generation rates using the same method above. The analysis results confirm that they also exhibit similar features as shown in Fig. 8. That implies that slight detuning from the threshold value of the AOFF would deteriorate the randomness of the output random bit sequences. Such a limited tolerance of threshold bias is hard to control in a real system. The difficulty mainly comes from one reason that the long-term stability of chaotic entropy source (i.e., chaotic self-pulsations from the TSSL) is not easy to guarantee in experiments. In our simulation on the optically injected TSSL, we find that any tiny change of laser operating parameters such as K and ω will induce to a great fluctuation of mean power of chaotic self-pulsations. This phenomenon is in accordance with that observed by Chlouverakis and Adams in [36]. Therefore, it is predictable that the threshold of AOFF (which is equal to the mean power of chaotic self-pulsation) in experiment will be more difficult to tune so as to avoid the bias in the division, because there are more avoidable perturbations sources. So, the core of the problem to construct a real system in future should be how to strengthen the tolerance of TRNG in the fluctuation of chaotic output.

The reason why the threshold bias for high-quality randomness is only allowed in such a small range is that the AOFF threshold (i.e., the width of the bistability range, $\Delta P = P_{\rm th2} - P_{\rm th1}$ in [28] and [34]) at the quantizing step in our TRNG (see Section II-B) is located at a low level, only 0.1 mW, so that the chaotic pulse streams have to be attenuated to make their mean pulse power in accordance with the threshold. In fact, the AOFF threshold, $\Delta P = P_{\rm th2} - P_{\rm th1}$, has a large room to be increased. As demonstrated by Huybrechts *et al.* in [40] and [41], the hysteresis curve widens and shifts to higher thresholds (such as 5 mW, Fig. 4 in [40]) when the bias current of AOFF is increased. Correspondingly, the threshold bias in our system is able to be tolerated in a wider range where our TRNG remains the high-quality randomness. We confirmed that the sufferable threshold bias in current TRNG would be enhanced to about 0.2 mW when the higher AOFF threshold of 5 mW was applied.

Another method to enhance the TRNG tolerance is introduced: a XOR operation, which can be performed with an all-optical XOR gate based on a hybrid-integrated Mach–Zehnder interferometer [28]. However, we must point out that even though an all-optical XOR gate may appear in the future implementation of our TRNG, its function has essential distinction with that of existing high-speed TRNGs based on chaos single section lasers with optical feedback [19]–[25]. In their system, the physical entropy source is a kind of continuous-time chaos. Such a source is driven by an external feedback cavity into chaos so that its output is nearly repeated at a roundtrip time corresponding to the external cavity length. So, the introduced XOR processing or LSBs algorithm in their system is not only to enhance the system tolerance, but, more crucially, to eliminate these weak periodicities. That means that their generated random bits even with unbiased 0/1 ratio have no way to pass standard randomness tests if they are not post-processed. On the contrary, chaotic self-pulsations in our optically injected TSSL show no correlation [see Fig. 3(b)] and has a high complexity [see Fig. 3(c)]. Theoretically, postprocessing procedures are not required in our system. To some extent, our method may provide a way to construct fast and simple TRNGs without postprocessing.

B. Merits and Prospect of All-Optical TRNGs

We believe our all-optical scheme has several benefits over existing TRNGs as follows:

1) Our TRNG can be directly compatible with the optical networks without any electric-to-optical or optical-to-electric devices, because it does all signal processing with all-optical techniques. This characteristic makes it not only be able to overcome the "electronic bottleneck" limitation [46] but also be more convenient in modern safe communications. Moreover, in future ultrahigh speed all-optical communications, all-optical signal processing will be very crucial and required. An extremely flexible communications network can be created if the optical signal can be directly treated without conversion to an electrical signal. Thus, all-optical TRNGs can also be expected to play important roles in future ultrafast all-optical network security and computing systems.
2) Our TRNG has a simple configuration. Without sampling and postprocessing that are necessities in the existing TRNGs, our method directly quantize chaotic self-pulsations to random sequences with an AOFF. This feature enables our TRNG to avoid the aliasing problem induced by these two procedures and attain a reduction in structure complexity.
3) The bit rate of our TRNG can reach more than 10 Gb/s (see Fig. 7) and has the potential of 1 Tb/s. Moreover, the rate can be continuously tuned in a large range of several gigabits per second by easily adjusting some control parameters of the entropy source (see Section III). Currently, the highest bit rate in our TRNG is of the order of 10 Gb/s, which is mainly limited by the absorption recovery time of the TSSL based on bulk heterostructures. This limitation can be overcome by replacing the ordinary TSSL with quantum-dot (QD) TSSL. QD structures possess ultrafast (of the order of 100 fs) carrier dynamics [47] and thus have the potential to boost the generation rate to beyond 1 THz. In addition, it should be noted that our method is modeled only by extracting one bit from each chaotic pulse with the AOFF functioned as an all-optical one-bit quantizer. If it was replaced with an all-optical multibit quantizer such as that in [48], the bit rates would be much faster.

We also note that there have been recently a large number of optoelectronic proposals expected to generate ultrahigh speed random bits by applying different multibit extraction for one sample and postprocessing of bits [22]–[26]. However, their ultrafast bit rates are only estimates in theory through offline processing of experimental stochastic time series recorded with multibit ADCs. For example, in [25], Argyris *et al*. demonstrate a 140 Gb/s TRNG based on chaotic laser, but this rate is obtained through offline retaining 14 LSB from the 16-bit ADC whose actual speed in each bit output port is only 10 Gb/s. In practice, it is very hard to realize such ultrafast TRNGs with rates of hundreds of gigabits per second, as their signal processings (such as fast optoelectronic conversion, broadband electronic amplification, electronic ADC, electronic clocks, and the post-processing circuitry of XOR gates or memory buffers) are done in the electrical domain faced with "electrical bottleneck." The speed limitation of electronic devices is considered to be several gigabits per second [45]. Moreover, the conversion accuracy and SNR of electrical ADC are limited severely due to the jitter of the sample clocks and the ambiguity of the electrical comparator [33]. Another difficult challenge to implement these electronic-based systems is to maintain strict synchronization among each electrical components working at such ultrahigh speeds of hundreds of gigabits per second, especially memory buffers used for parallel–serial conversion.

V. Conclusion

A fast all-optical TRNGs based on discrete-time chaotic systems have been demonstrated theoretically, which do not require sampling and postprocessing procedures. Utilizing an optically injected TSSL as a physical entropy source, this new TRNG can reach a high generation rate above 10 GHz. Moreover, a continuous tuning range of several gigahertz can be achieved through controlling external parameters of the optically injected TSSL, such as injection strength K, frequency detuning ω, gain current J_a, and absorber bias J_b. In addition, the whole signal processing in this system is done in the optical domain and thus can overcome "electronic bottleneck." This achievement may spur more interest toward realizing ultrafast all-optical TRNGs for modern fast communications and the next-generation all-optical networks.

References

[1] D. Eastlake, J. Schiller, and S. Crocker, (2005). Randomness requirements for security, RFC4086 [Online]. Available: http://tools.ietf.org/html/rfc4086.

[2] (2001). Security requirements for cryptographic modules, FIPS 140-2 [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[4] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL: CRC Press, 1995.

[5] R. G. Gallager, *Principles of Digital Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[6] N. Metropolis and S. Ulam, "The Monte Carlo method," *J. Amer. Stat. Assoc*., vol. 44, pp. 335–341, Sep. 1949.

[7] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis*. New York: Springer-Verlag, 2007.

[8] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. New York: Wiley, 2010.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys*., vol. 74, pp. 145–195, Mar. 2002.

[10] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, "Monte Carlo simulations: Hidden errors from 'good' random number generators," *Phys. Rev. Lett*., vol. 69, pp. 3382–3384, Dec. 1992.

[11] J. Von Neumann, "Various techniques used in connection with random digits," *Appl. Math. Series*, vol. 12, pp. 36–38, 1951.

[12] 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. 47, no. 5, pp. 615–621, May 2000.

[13] M. A. Wayne and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," *Opt. Exp*., vol. 18, pp. 9351–9357, Apr. 2010.

[14] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Anderson, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photon*., vol. 4, pp. 711–715, Aug. 2010.

[15] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," *Appl. Phys. Lett*., vol. 98, pp. 231103-1–231103-3, Jun. 2011.

[16] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Opt. Lett*., vol. 36, pp. 1020–1022, Mar. 2011.

[17] 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. Exp*., vol. 18, pp. 23584–23597, Oct. 2010.

[18] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *J. Lightw. Technol.*, vol. 30, no. 9, pp. 1329–1334, May 2012.
[19] 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," *Nature Photon.*, vol. 2, pp. 728–732, Nov. 2008.
[20] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 45, no. 11, pp. 1367–1379, Nov. 2009.
[21] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," *Phys. Rev. A*, vol. 83, pp. 031803-1–031803-4, Mar. 2011.
[22] 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, pp. 024102-1–024102-4, Jul. 2009.
[23] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photon.*, vol. 4, pp. 58–61, Jan. 2010.
[24] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt. Exp.*, vol. 18, pp. 5512–5524, Mar. 2010.
[25] 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. Exp.*, vol. 18, pp. 18763–18768, Aug. 2010.
[26] X. Li and S. Chan, "Random bit generation using an optically injected semiconductor laser in chaos with oversampling," *Opt. Lett.*, vol. 37, pp. 2163–2165, Jun. 2012.
[27] P. Li, Y. C. Wang, and J. Z. Zhang, "All-optical fast random number generator," *Opt. Exp.*, vol. 18, pp. 20360–20369, Sep. 2010.
[28] Y. C. Wang, P. Li, and J. Z. Zhang, "Fast random bit generation in optical domain with ultrawide bandwidth chaotic laser," *IEEE Photon. Technol. Lett.*, vol. 22, no. 22, pp. 1680–1682, Nov. 2010.
[29] D. S. Ornstein, "Ergodic theory, randomness, and 'chaos'," *Science*, vol. 243, pp. 182–187, Jan. 1989.
[30] G. M. Bernstein and M. A. Lieberman, "Secure random number generation using chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 37, no. 9, pp. 1157–1164, Sep. 1990.
[31] T. Stojanovski and L. Kocarev, "Chaos-based random number generators - Part I: analysis [cryptography]," *IEEE Trans. Circuits Syst. I—Fundam. Theory Appl.*, vol. 48, no. 3, pp. 281–288, Mar. 2001.
[32] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators—II: Practical realization," *IEEE Trans. Circuits Syst. I—Fundam. Theory Appl.*, vol. 48, no. 3, pp. 382–385, Mar. 2001.
[33] R. H. Walden, "Analog-to-digital converter survey and analysis," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 4, pp. 539–550, Apr. 1999.
[34] P. Li, Y.-C. Wang, A.-B. Wang, L.-Z. Yang, M.-J. Zhang, and J.-Z. Zhang, "Direct generation of all-optical random numbers from optical pulse amplitude chaos," *Opt. Exp.*, vol. 20, pp. 4297–4308, Feb. 2012.
[35] O. E. Rossler, "An equation for continuous chaos," *Phys. Lett. A*, vol. 57, pp. 397–398, Jul. 1976.
[36] K. E. Chlouverakis and M. J. Adams, "Two-section semiconductor lasers subject to optical injection," *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 5, pp. 982–990, Sep.–Oct. 2004.
[37] K. E. Chlouverakis and M. J. Adams, "Optoelectronic realisation of NOR logic gate using chaotic two-section lasers," *Electron. Lett.*, vol. 41, no. 6, pp. 359–360, Mar. 2005.
[38] K. E. Chlouverakis and M. J. Adams, "Antimonotonicity and maximal complexity in optically injected two-section lasers," *IEEE J. Sel. Topics Quantum Electron.*, vol. 12, no. 3, pp. 398–404, May–Jun. 2006.
[39] P. Grassberger and I. Procaccia, "Characterization of strange attractors," *Phys. Rev. Lett.*, vol. 50, pp. 346–349, Jan. 1983.
[40] K. Huybrechts, W. D'Oosterlinck, G. Morthier, and R. Baets, "Proposal for an all-optical flip-flop using a single distributed feedback laser diode," *IEEE Photon. Technol. Lett.*, vol. 20, no. 1, pp. 18–20, Jan. 2008.
[41] K. Huybrechts, G. Morthier, and R. Baets, "Fast all-optical flip-flop based on a single distributed feedback laser diode," *Opt. Exp.*, vol. 16, pp. 11405–11410, Jul. 2008.
[42] K. Huybrechts, A. Ali, T. Tanemura, Y. Nakano, and G. Morthier, "Numerical and experimental study of the switching times and energies of DFB-laser based all-optical flip-flops," in *Proc. Int. Conf. Photon. Switch.*. Pisa, Italy, 2009, pp. 15–19.
[43] A. Rukhin, J. Sato, J. Nechvatal, M. Smid, and E. Barker, (2010). "A statistical test suite for random and pseudorandom number generators for cryptographic applications, [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
[44] G. Marsaglia, (1996). "DIEHARD: A battery of tests of randomness, [Online]. Available: http://www.stat.fsu.edu/pub/diehard
[45] K. E. Stubkjaer, "Semiconductor optical amplifier-based all-optical gates for high-speed optical processing," *IEEE J. Sel. Topics Quantum Electron.*, vol. 6, no. 6, pp. 1428–1435, Nov.–Dec. 2000.
[46] L. Venema, "Photonics technologies," *Nature Insight*, vol. 424, p. 809, Aug. 2003.
[47] E. U. Rafailov, M. A. Cataluna, and W. Sibbett, "Mode-locked quantum-dot lasers," *Nature Photon.*, vol. 1, pp. 395–401, Jul. 2007.
[48] K. Ikeda, J. M. Abdul, S. Namiki, and K. Kitayama, "Optical quantizing and coding for ultrafast A/D conversion using nonlinear fiber-optic switches based on Sagnac interferometer," *Opt. Exp.*, vol. 13, pp. 4296–4302, May 2005.

Pu Li received the M.S. degree in physical electronics from the Taiyuan University of Technology (TYUT), Shanxi, China, in 2011, where he is currently working toward the Ph.D. degree in the Key Laboratory of Advanced Transducers and Intelligent Control System (Ministry of Education of China), College of Physics and Optoelectronics.

His research interests include optical communications, all-optical signal processing, and nonlinear dynamics of semiconductor lasers.

Yun-Cai 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 the Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Shaanxi, China, in 1994 and 1997, respectively.

From 2001 to 2002, he was a Visiting Scholar at the Institut für Festkörperphysik, Technische Universität Berlin, Berlin, Germany. In 1986, he joined the Taiyuan University of Technology (TYUT), Taiyuan, China, as a Teaching Assistant, where he was a Lecturer from 1994 to 1998 and an Assistant Professor from 1998 to 2003 in the Department of Physics. Since 2003, he has been a Professor in the College of Physics and Optoelectronics, TYUT, where he is also the Chair of the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education of China. His current research interests include nonlinear dynamics of chaotic lasers and its applications, including optical communications, chaotic optical time-domain reflectometers, chaotic lidars, and random number generation based on chaotic lasers.

Dr. Wang is a Fellow of the Chinese Instrument and Control Society, and a senior member of the Chinese Optical Society and the Chinese Physical Society. He also serves as a Reviewer for journals of the IEEE, Optical Society of America, and Elsevier organizations.

An-Bang Wang received the M.S. degree in physical electronics from the Taiyuan University of Technology (TYUT), Taiyuan, China, in 2006, where he is currently working toward the Ph.D. degree in the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education of China.

In 2006, he joined TYUT, where he is currently a Lecturer in the College of Physics and Optoelectronics. His research interests include nonlinear dynamics of semiconductor lasers, optical/electrical time-domain reflection measurement, and wideband chaos generation.

Bing-Jie Wang received the M.S. degree in physical electronics and the Ph.D. degree in circuits and systems from the Taiyuan University of Technology (TYUT), Taiyuan, China, in 2008 and 2012, respectively.

In 2001, she joined TYUT, where she is currently an Assistant Professor in the College of Physics and Optoelectronics. Her research interests include the field of chaotic semiconductor lasers and its applications to optical communications.