Real-Time 2.5-Gb/s Correlated Random Bit Generation Using Synchronized Chaos Induced by a Common Laser with Dispersive Feedback

Wang, Longsheng ; Wang, Damiang; Gao, Hua; Guo, Yuanyuan; Hong, Yanhua; Shore, Alan

IEEE Journal of Quantum Electronics

DOI:
10.1109/JQE.2019.2950943

Published: 01/02/2020

Peer reviewed version

Real-Time 2.5-Gb/s Correlated Random Bit Generation Using Synchronized Chaos Induced by a Common Laser with Dispersive Feedback

Longsheng Wang, Daming Wang, Hua Gao, Yuanyuan Guo, Yuncai Wang, Yanhua Hong, K. Alan Shore, *Senior Member*, *IEEE*, Anbang Wang, *Member*, *IEEE*

***Abstract*—We experimentally demonstrate high-speed correlated random bit generation in real time using synchronized chaotic lasers commonly driven by a laser with dispersive feedback. The dispersive feedback from a chirped fiber Bragg grating induces frequency-dependent feedback delay and thus no longer causes time-delay signature, and resultantly ensures the signal randomness and security of chaotic laser. Driven by the time-delay signature-free chaotic signal, the two response lasers are routed into chaotic states and establish a synchronization with correlation beyond 0.97 while they maintain a low correlation level with the drive signal. Through quantizing the synchronized laser chaos with a one-bit differential comparator, real-time 2.5-Gb/s correlated random bits with verified randomness are experimentally obtained with a bit error ratio of 0.07. Combining with a robust sampling method, the BER could be further decreased to 1×10^{-4} corresponding to an effective generation rate of 1.7 Gb/s. Bit error analysis indicates that the bit error ratio between the responses is lower than that between the drive and responses over a wide parameter region due to the synchronization superiority of the responses over the drive.**

***Index Terms*—Chaos synchronization, dispersive feedback, random bit generation, semiconductor laser.**

I. Introduction

Chaotic semiconductor lasers with delayed coupling have excellent nonlinear dynamics [1]. Their outputs are characterized with wide bandwidth, large amplitude noise-like oscillation and synchronization possibility [2]. Such merits make them attractive for security-oriented applications, such as high-speed physical random bit generation [3-11], secure communication [12-19] and key distribution [20-26].

For chaos-based key distribution, establishing high-speed correlated random bits between legitimate users is the foundation, which relies on the synchronization of chaotic lasers. For example, Kanter *et al.* numerically verified correlated random bit generation exceeding Gb/s using the identical synchronization between two bidirectionally coupled chaotic lasers [27]. Argyris *et al.* later experimentally demonstrated its feasibility in generating the correlated random bits at Gb/s by using an offline quantization method [28]. Nonetheless, above schemes need to establish chaos synchronization through bidirectional signal coupling over a public channel leading to a risk of exposure of legitimate users' information. An alternative method is to construct the high-speed correlated random bits using chaos synchronization induced by a common drive signal. This kind of synchronization is achieved by injecting a random drive signal into response lasers without bidirectional coupling over the public channel [29-31], whereby the information leakage is avoided.

Considering the drive source used for inducing chaos synchronization, a semiconductor laser with external-cavity feedback is the most attractive choice in view of its simple and integratable setup. For example, Uchida *et al.* experimentally demonstrated the chaos synchronization induced by a common laser subject to mirror optical feedback [29]. Unfortunately, this synchronization scheme has intrinsic defect in extracting the high-speed correlated random bits because the drive signal has time-delay signature (TDS) caused by the mirror external-cavity resonance [32]. Such a signature makes the laser chaos correlated to its previous state at the external-cavity delay time and renders the laser chaos weakly periodic. It can even be inherited by the response lasers thus deteriorating the signal randomness, which impairs random bit generation [5]. Even worse, the TDS induces a security flaw because the drive system may be reconstructed if the delay time is identified [33]. Note that, although many chaotic sources with suppressed TDS have been proposed [34-45], their experimental utilization as drive signals to induce chaos synchronization for generating

Manuscript received April 1, 2019. This work was supported in part by the National Science Foundation of China under Grants 61805170, 61822509, 61731014, 61671316, 61805171, 61705160, 61475111, in part by the National Cryptography Foundation under Grant MMJJ20170207, and in part by the International Cooperation Program and Natural Science Foundation of Shanxi Province under Grants 201603D421008, 201801D221189, 201701D1211362, 201802044.

L. S. Wang, D. M. Wang, H. Gao, Y. Y. Guo, Y. C. Wang, and A. B. Wang are with the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, and College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China. Y. C. Wang is also with Institute of Advanced Photonics Technology, Guangdong University of Technology, Guangzhou 510006, China. (e-mail: wanglongsheng@tyut.edu.cn; wangdaming0910@link.tyut.edu.cn; gaohua0130@link.tyut.edu.cn; guoyuanyuan@tyut.edu.cn; wangyc@tyut.edu.cn; wanganbang@tyut.edu.cn).

K. A. Shore and Y. H. Hong are with the School of Electronic Engineering, Bangor University, Bangor LL57 1UT, U.K. (e-mail: k.a.shore@bangor.ac.uk; y.hong@bangor.ac.uk).

Corresponding author: Anbang Wang (email: wanganbang@tyut.edu.cn)

correlated random bits has not yet been reported.

Approaches in the literature have focused on employing optical sources which are naturally free of the TDS to induce chaos synchronization and then construct correlated random bits. For example, Chan *et al.* numerically verified optical-injection chaos induced synchronization and generated correlated random bits at a tunable rate up to about 2 Gb/s [46]. Uchida *et al.* experimentally achieved constant-amplitude randomly phase-modulated light induced synchronization and demonstrated secure generation of correlated random bits at Mb/s by switching the synchronization states [21]. However, as a compromise, complex structures and delicate operations in these systems are inevitably introduced. Moreover, to the best of our knowledge, the correlated random bits in present schemes are obtained by quantizing synchronized laser chaos with offline methods imposing limitations on the practical tasks.

In this paper, we experimentally demonstrated real-time high-speed correlated random bit generation from two semiconductor lasers commonly driven by a third laser with dispersive feedback. The dispersive feedback comes from a chirped fiber Bragg grating (CFBG). As our previous work demonstrated, the CFBG leads to frequency-dependent feedback delay and does not cause the TDS like mirror feedback [47] thus ensuring the signal randomness and security. By harnessing the CFBG-feedback laser as drive, we experimentally achieved high-correlation synchronization between two response lasers, whilst the drive and responses maintain a low correlation level. Through quantizing the synchronized laser chaos with a one-bit differential comparator, real-time 2.5-Gb/s correlated random bits with verified randomness are obtained with a bit error ratio (BER) of 0.07. Bit error analysis indicates that the BER between the responses is lower than that between the drive and responses over a wide parameter region due to the synchronization superiority of the responses over the drive.

II. Experimental Setup

Figure 1 shows the experimental setup for implementing the real-time correlated random bit generation. A distributed feedback semiconductor laser (Drive) subject to CFBG feedback is used as the common drive light source. The CFBG reflects light into the semiconductor laser to induce laser chaos. To adjust the polarization and strength of laser chaos, a polarization controller (PC) and a variable optical attenuator (VOA) are arranged in the feedback path. The laser chaos is then amplified by an optical amplifier (EDFA) and split into two branches, each of which is unidirectionally injected into response lasers (Res1,2) to induce chaos synchronization. The output of each response laser is converted into electrical signal by a photodetector (PD) and then is quantized as a binary stream by a one-bit differential comparator (COM) and a D-type flip-flop (DFF) triggered by a clock (CLK). Correlated random bits can be achieved as long as high-quality chaos synchronization is established between the two response lasers.

In experiments, the threshold currents of drive, response1, and response2 (Eblana, EP1550-DM-B05-FM) are 12.2 mA, 10.8 mA, and 11.0 mA, respectively. They are individually biased at 18.7 mA, 17 mA, and 17 mA by laser drivers (ILX Lightwave, LDX-3412). The wavelengths of lasers are adjusted by temperature controllers (ILX Lightwave LDT-5412). The CFBG has a length of 10 cm, which forms a feedback round-trip time of 61.6 ns with the drive laser pigtailed to optical fiber of several meters. The photodetector (FINISAR, XPDV2120RA) and comparator (Analog Devices, ADCMP567) have bandwidths of 45 GHz and 5 GHz, respectively. The maximum triggered frequencies of clock (Agilent, N4963A) and D-type flip-flop (ON Semiconductor, MC10EP52) are 13.5 GHz and 6 GHz, respectively. The optical spectra of lasers are measured by a spectrum analyzer with a resolution of 1.12 pm (APEX, AP2041-B). Their power spectra and temporal waveforms are measured by a 26.5-GHz radio-frequency spectrum analyzer (Agilent, N9010A) and a 36-GHz real-time oscilloscope (LeCroy, LABMASTER10ZI), respectively.

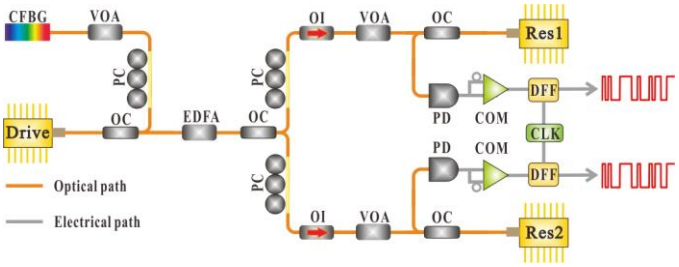

Fig. 1. Experimental setup. Drive: drive laser, Res1,2: response lasers, CFBG: chirped fiber Bragg grating, OC: optical coupler, PC: polarization controller, VOA: variable optical attenuator, EDFA: erbium-doped fiber amplifier, OI: optical isolator, PD: photodetector, COM: one-bit differential comparator, DFF: D-type flip-flop, CLK: trigger clock.

III. Experimental Results

A. Characteristics and Synchronization of Chaotic Signals

Figures 2 shows the spectral characteristics of the drive laser and response lasers. In Fig. 2(a1), the black solid curve and dash curve present the optical spectra of the drive laser with and without CFBG optical feedback, respectively. In experiments, the optical feedback strength of CFBG is adjusted to 0.10, which equals the light power ratio of the feedback signal to the drive laser output. It is found that, due to the optical feedback, the center wavelength of solitary drive is red shifted from 1549.816 nm to 1549.836 nm with the spectrum broadened. The broadened spectrum locates within the main envelope of the CFBG's reflection spectrum as shown by the green curve, which imposes a frequency-dependent feedback delay on the optical components of laser chaos. These additional delays can induce irregular separations of external-cavity modes and destroy their resonance thus causing no TDS [47]. Figure 2(b1) gives the power spectrum of drive laser, which has a bandwidth 6.87 GHz calculated using the 80%-energy bandwidth definition [48]. Its magnified spectrum is shown in the inset, which no longer has the periodic modulation caused by the resonance of

external-cavity modes.

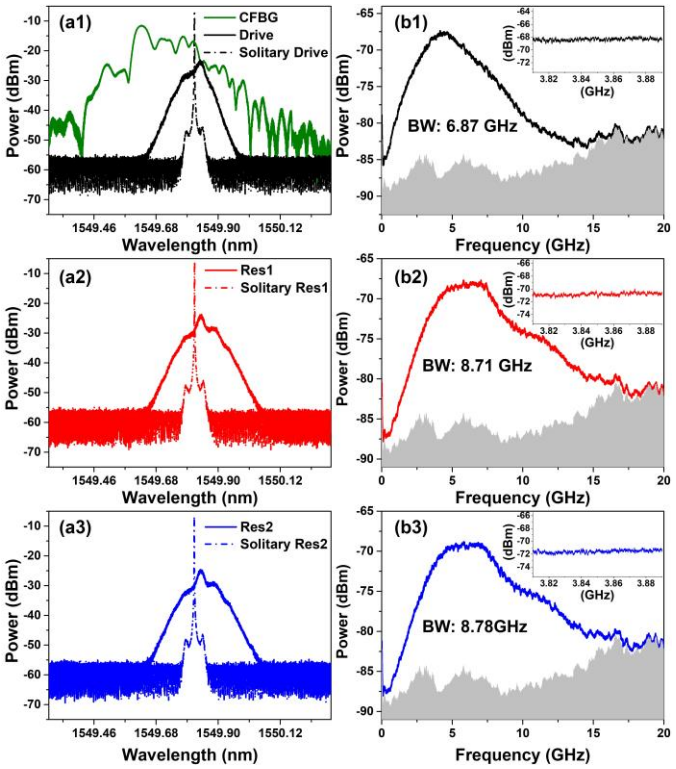

Fig. 2. (a1)-(a3) Optical spectra, (b1)-(b3) power spectra of drive, resonse1,2. The green curve in (a1) plots the reflection spectrum of CFBG. The insets in (b1)-(b3) plot power spectra in a scale of 80 MHz.

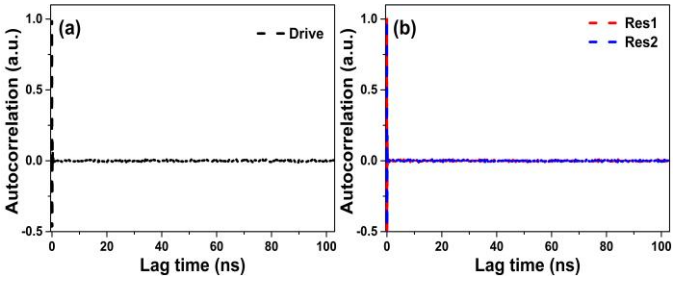

Fig. 3. Autocorrelation traces of (a) drive and (b) resonse1,2. Data length for the autocorrelation trace is 1×10^6 points at 40-GS/s sampling rate.

The optical spectra of response lasers are plotted in Figs. 2(a2) and 2(a3). The red dash curve and blue dash curve present the optical spectra of response1 and response2 without the injection of drive laser, respectively. In experiments, the optical injection strength of drive laser is fixed at 0.33, which equals the light power ratio of the drive signal to the response laser output. The center wavelengths of response lasers are both adjusted to 1549.816 nm which has a -0.020 nm detuning with that of drive laser. With the injection of drive laser, the response lasers have similar optical spectra and their center wavelengths are both locked at that of drive laser~1549.836 nm, as shown by the red solid curve and blue solid curve. But it is noted that, the optical spectrum spans of the response lasers are wider than that of the drive laser, which leads to wider power spectra of the responses corresponding to 8.71 GHz and 8.78 GHz as shown in Figs. 2(b2) and 2(b3), respectively. This is because of the transient interference of the fields of drive laser and response lasers, which increases the response laser' relaxation oscillation frequency and enhances the signal bandwidth [49]. Moreover, benefitting from destroying the external-cavity resonance in the drive laser, the response lasers also inherit no periodic modulation in the magnified spectra as shown by insets of Figs. 2(b2) and 2(b3). Consequently, as shown by autocorrelation traces of the temporal waveforms in Fig. 3, no correlation peak is found at the external-cavity delay~61.6 ns for the drive and responses, which verifies the elimination of TDS and assures the randomness and security of laser chaos.

Figure 4 shows the temporal waveforms of drive, response1, response2 and the correlation plots between them. See from the temporal waveforms shown in Figs. 4(a1)-4(a3), we found that the response lasers have faster irregular oscillation than the drive laser. This is due to the bandwidth enhancement of response lasers caused by injection of drive laser, which introduces more high-frequency oscillation components. These oscillations are different from those of drive laser, causing that the responses establish a high-correlation synchronization (0.975) while they maintain low correlation levels (0.671, 0.727) with the drive, as shown by the correlation plots in Figs. 4(b1)-4(b3). In practice, to verify the response lasers are actually synchronized, the legitimate users can send some recorded chaotic temporal waveforms to the counterpart at set intervals. By quantitatively calculating the cross-correlation between the temporal waveforms, whether the response lasers are synchronized or not can be verified: the correlation with a high value indicates that the response lasers are synchronized, otherwise they are not synchronized. But it is noted that, the temporal waveforms sent to the counterpart of legitimate users cannot be used for generating the correlated random bits anymore because they are exposed in the public channel.

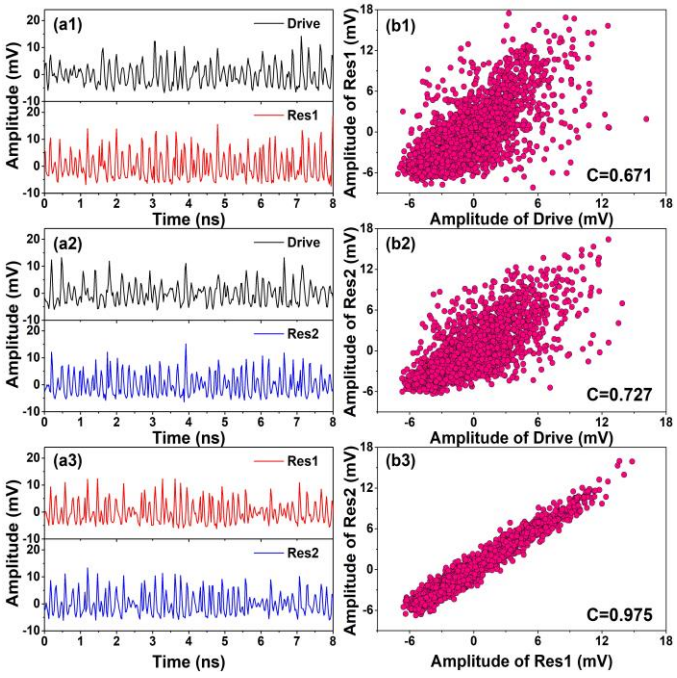

Fig. 4. Temporal waveforms and corresponding correlation plots for (a1), (b1) drive and response1, (a2), (b2) drive and response2, and (a3), (b3) response1,2.

B. Generation and Analysis of Correlated Random Bits

Through differentially quantizing the synchronized temporal waveforms shown in Fig. 4(a3), real-time correlated random bits are achieved for response1 and response2. Figure 5(a) shows the generated non-return-to-zero-formatted bit streams at a 2.5-GHz clock rate acquired by the real-time oscilloscope. It is seen that highly-correlated random bits are achieved for the responses. Their BER is calculated to be 0.07 which is defined as the proportion of unequal bits amongst 1×10^6 bits. The eye diagrams of the correlated random bits are presented in Fig. 5(b), which are well-opened qualitatively indicating a good performance.

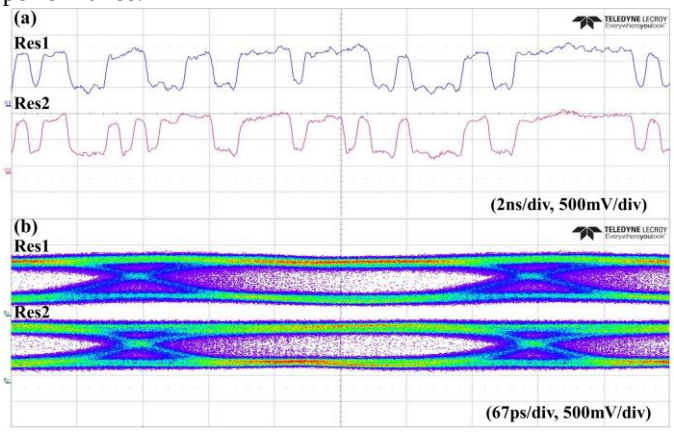

Fig. 5. (a) Correlated random bit streams for response1,2 and (b) the corresponding eyediagrams. The BER is 0.07 calculated as the proportion of unequal bits amongst 1×10^6 bits.

The parameter dependence of BER (with error bars) of correlated random bits is further investigated. Figure 6(a) shows the BERs between the drive, response1 and response2 as a function of the injection strength of drive laser when the wavelength detuning of drive and responses is fixed at -0.020 nm. It is seen that all BERs decrease with gradually reduced rates for increasing the injection strength. And the BER level between the responses is lower than those between the drive and each of responses. As the injection strength increases over 0.2, the BER levels are relatively stable with about 0.07 between the responses and about 0.24 between the drive and responses.

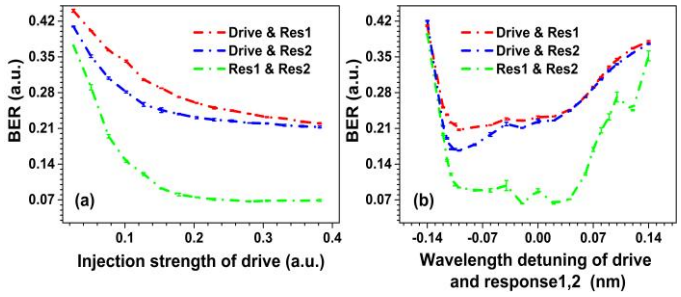

Fig. 6. BERs between drive, response1,2 as a function of (a) injection strength of drive, (b) wavelength detuning of drive and response1,2.

Moreover, we studied the effects of wavelength detuning between the drive and responses on the BERs. For this study, the injection strength and center wavelength of drive are fixed at 0.33 and 1549.836nm, respectively. The center wavelengths of solitary responses are detuned in negative and positive directions with respect to that of the drive laser. Results in Fig. 6(b) show that the BER between the responses (0.07~0.09) is much lower than those (0.17 with minimum value) between the drive and responses within a wide detuning range from -0.10nm to 0.04nm. Outside this range, the BER experiences a rapid increase due to the degradation of chaos synchronization. Aforementioned low BERs between the responses and high BERs between the drive and responses are physically due to the synchronization superiority of the responses over the drive, i.e., high-correlation synchronization between the response lasers and low-correlation synchronization between the drive and response lasers. It is therefore excellent for preventing the eavesdropper intercepting correlated random bits from the drive laser.

It is argued that the eavesdropper can intercept the drive signal from the public channel and reinject it into the response lasers to achieve synchronized temporal waveforms for correlated random bit generation. Indeed, this attack could not be avoided in principle. However, the interception of drive signal may cause asymmetric injection strength to the response lasers. Such an asymmetric injection strength will degrade the synchronization quality and give rise to an unusual high BER between the response lasers as shown in Fig. 7, which uncovers the interception. To avoid this, the eavesdropper will try to reconstruct the same drive laser. Therefore, increasing the difficulty of eavesdropper in obtaining the proper drive system is a solution to improve the security, such as the time-delay signature-free drive laser. Moreover, as we know, chaos synchronization is established based on the parameter match of lasers of legitimate users. Increasing the number of possible parameter values (i.e., key space) for establishing the chaos synchronization can also improve the security, as reported by Yi *et al*. [50] and Wang *et al*. [51]. Except for improving the security from the hardware point of view, the legitimate users can also use the independent and random private keys to switch the synchronization states to increase the difficulty of the eavesdropper in achieving the synchronization, as demonstrated by Uchida *et al*. [20] and Jiang *et al*. [25].

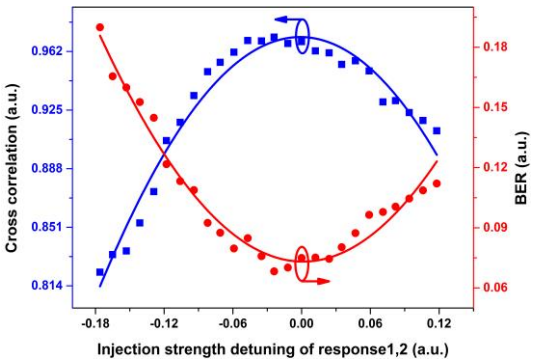

Fig. 7. Cross correlation and BER of the response lasers a function of the injection strength detuning between them.

TABLE I
NIST TESTS FOR 2.5GB/S CORRELATED RANDOM BITS.
"R" DENOTES RESULTS, "S" DENOTES SUCCESS.

Statistical test	Res1			Res2		
	P-value	P	R	P-value	P	R
Frequency	0.534146	0.9920	s	0.899171	0.9850	s
Block Frequency	0.684890	0.9900	s	0.385543	0.9890	s
Cumulative Sums	0.100109	0.9930	s	0.653773	0.9870	s
Runs	0.538182	0.9940	s	0.032923	0.9910	s
Longest Run	0.994005	0.9940	s	0.552383	0.9900	s
Rank	0.112047	0.9950	s	0.585209	0.9880	s
FFT	0.242986	0.9870	s	0.348869	0.9960	s
Non Overlapping Template	0.000890	0.9910	s	0.001544	0.9830	s
Overlapping Template	0.253122	0.9930	s	0.305599	0.9900	s
Universal	0.723804	0.9890	s	0.098330	0.9880	s
Approximate Entropy	0.632955	0.9890	s	0.004802	0.9820	s
Random Excursions	0.025629	0.9832	s	0.040990	0.9884	s
Random Excursions Variant	0.018335	0.9916	s	0.026948	0.9967	s
Serial	0.616305	0.9880	s	0.334538	0.9960	s
Linear Complexity	0.524101	0.9900	s	0.348869	0.9880	s

TABLE II
DIEHARD TESTS FOR 2.5GB/S CORRELATED RANDOM BITS.
"R" DENOTES RESULTS, "S" DENOTES SUCCESS.

Statistical test	Res1		Res2	
	P-value	R	P-value	R
Birthday Spacings	0.017847 (KS)	s	0.749065 (KS)	s
Overlapping 5-Permutations	0.617219	s	0.086990	s
Binary rank of 31x31 matrices	0.712286	s	0.321032	s
Binary rank of 32x32 matrices	0.783489	s	0.617963	s
Binary rank of 6x8 matrices	0.086380 (KS)	s	0.649114 (KS)	s
Bitstream	0.017010	s	0.018430	s
Overlapping-Pairs-Sparce-Occupancy	0.033000	s	0.012200	s
Overlapping-Quadruples-Sparce-Occupancy	0.067300	s	0.029000	s
DNA	0.023000	s	0.017200	s
Count-the-1's on a stream of bytes	0.680979	s	0.275463	s
Count-the-1's for specific bytes	0.010811	s	0.015408	s
Parking lot	0.102055 (KS)	s	0.014273 (KS)	s
Minimum distance	0.517996 (KS)	s	0.539410 (KS)	s
3D spheres	0.111441 (KS)	s	0.442617 (KS)	s
Sqeeze	0.152029	s	0.199858	s
Overlapping sums	0.087295 (KS)	s	0.794069 (KS)	s
Runs	0.148026 (KS)	s	0.238916 (KS)	s
Craps	0.385874	s	0.594423	s

At last, we examined the statistical randomness of the two correlated random bit streams by using the NIST and Diehard test suites. The NIST has fifteen test items. To test once, one thousand samples of 1×10^6 random bits are required at the significance level of 0.01. For "Success" of each test item, the P-value should be beyond 0.0001 and the proportion (P) should range from 0.9805608 to 0.9994392 [52]. The Diehard has eighteen test items, in which KS means that a Kolmogorov-Smirnov test was applied. To test once, 1×10^9 random bits are needed at the significance level of 0.01. For "Success" of each test item, the P-value should be within the range from 0.01 to 0.99 [53]. Tables I and II show the test results. It can be seen that all tests in both NIST and Diehard can be passed for the two correlated random bit streams indicating a good statistical randomness. We attribute firstly the good statistical randomness to the differential comparison which yields statistically unbiased random bits 0 and 1. Moreover, the good statistical randomness also comes from the internal independence of random bits, which is due to that the extraction rate of random bits is lower than the entropy bandwidths of the response lasers, as well as that the response lasers inherit no TDS from the drive laser thereby assuring the randomness of chaotic signals.

IV. DISCUSSION

In experiment, the BER of the real-time correlated random bits between the responses is 0.07, which is relatively large. We identify the main driver responsible for these errors is the synchronization degradation after the processing of differential comparison: the cross correlation of the temporal waveforms of the response lasers is decreased to the 0.90 from the 0.975 after the differential comparison and these synchronization -degraded temporal waveforms locate mainly around the mean value used for determining the bit 0 or 1, thus causing the native BER of 0.07. It is suspected that the main reason for the synchronization degradation is that the two comparators are not perfectly consistent. The inconsistency mainly comes from that the delay time of differential inputs of the two comparators has a little difference. As shown in Fig. 8(a), with increasing the difference of the delay time of differential inputs of the two comparators, the synchronization quality of the response lasers reduces rapidly, where $\Delta\tau_i$ (i=1,2) represents the delay time of the differential inputs of the comparators, and their difference can be expressed as $\Delta\tau=|\Delta\tau_1-\Delta\tau_2|$.

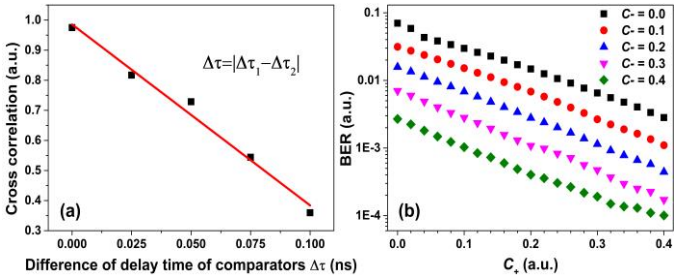

Fig. 8. (a) Cross correlation of the response lasers as a function of the difference of delay time of comparators, (b) BER of the correlated random bits as a function of the threshold coefficients C_+ when different values of C_- are set.

To reduce the BER caused by the synchronization degradation, one method is customizing two comparators to minimize the difference of delay time in the differential inputs. Another method is storing the synchronized temporal waveforms and then quantizing them offline with the robust sampling method [21]. In this method, two thresholds including the upper and lower threshold values are used and set as $I_u=m+C_+\sigma$ and $I_l=m-C_-\sigma$ respectively, where m and σ represent the mean value and standard deviation of the temporal waveforms respectively, C_+ and C_- denote the threshold coefficients for adjusting the threshold values. Bit 1 (0) is generated when the amplitude of temporal waveforms is larger (lower) than the upper threshold I_u (lower threshold I_l), and no

bit is generated when the amplitude is located between I_u and I_l. This method can yield a low BER because the temporal waveforms that locate away from the mean value and are more likely to be synchronized are used to extract the correlated random bits. Figure 8(b) shows the BER of the generated correlated random bits as a function of the threshold coefficients C_+ when different values of C_- are set. It is found that the BER can be decreased as low as 1×10^{-4} when the values of C_+ and C_- are both set as 0.4. Under this scenario, the retained ratio of random bits is 0.68, and the corresponding effective generation rate of random bits is 1.7 Gb/s.

For the simplicity of discussion, we adopted the symmetric transmission spans between the common laser and response lasers to establish the chaos synchronization. Under the real-world implementation conditions, it is highly probable that the transmission spans are asymmetric. To verify whether the chaos synchronization can be established under this scenario, we arranged transmission fibers with different lengths and dispersion compensation modules (DCMs) on the path of one of the response lasers, and then evaluated the synchronization quality by calculating the cross correlation of the response lasers. Results in Fig. 9(a) indicate that although the synchronization quality is slightly degraded as increasing the asymmetric fiber spans, the high-quality chaos synchronization (>0.90) between the response lasers can still be established, which proves the feasibility of the proposed scheme under the real-world implementation conditions. Note that, limited by the DCMs, the asymmetric fiber length is not increased uniformly.

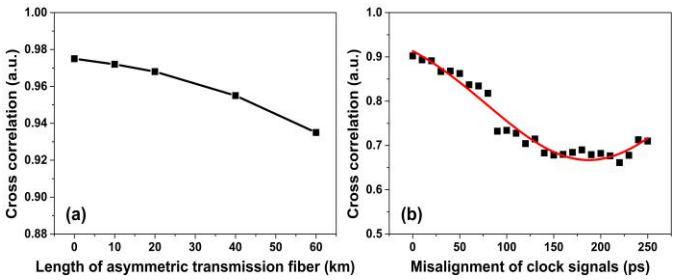

Fig.9. (a) Cross correlation of the response lasers as a function of the length of the asymmetric transmission fiber, (b) Cross correlation of the correlated random bits as a function of the misalignment time of clock signals.

Such an asymmetric and distant scenario will inevitably give rise to another problem to be considered, i.e., the misalignment of clock signals. To check the sensitivity of random bit extraction to the misalignment in the clock signals, an electrical delay line (resolution: 10 ps, delay range: 0~250 ps) is used to control the arrival time of clock signals to the DFFs and thus introduce the misalignment. The tolerance can then be examined by calculating the cross correlation of the correlated random bits as a function of the misalignment time of clock signals. As shown in Fig. 9(b), the cross correlation of the correlated random bits decreases gradually as increasing the misalignment time. When the misalignment time is within 30 ps, the cross correlation of generated random bits is relatively stable at 0.90, which corresponds to the BER of 0.07. As increasing the misalignment time beyond 30 ps, the cross correlation experiences a fast decrease and then is stable around 0.70 when the misalignment time is further beyond 80 ps, which undoubtedly enlarges the BER. Therefore, according the experimental results, the tolerance time for the clock misalignment in the current scheme can be 30 ps.

V. Conclusion

In conclusion, based on chaos synchronization induced by a common chaotic laser with dispersive feedback from a CFBG, we experimentally demonstrated real-time correlated random bit generation at a 2.5-Gb/s rate. Benefitting from the dispersive feedback, the common chaotic laser has no TDS ensuring the randomness and security. Driven by the TDS-free chaotic signal, we obtained a high-correlation synchronization between the response lasers and a low correlation level between the drive and responses. After quantizing the synchronized laser chaos with a one-bit differential comparator, real-time 2.5-Gb/s correlated random bits with verified randomness are obtained with a BER of 0.07. The BER could be further decreased to 1×10^{-4} using the robust sampling method at the cost of sacrificing the effective generation rate to 1.7 Gb/s. Bit error analysis indicates that the BER between the responses is lower than that between the drive and responses over a wide parameter region because of the synchronization superiority of response lasers. It is believed this demonstration will pave a way for real-time fast correlated random bit generation and promote its practical tasks in the key distribution.

References

[1] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photon.*, vol. 9, no. 3, pp. 151-163, Feb. 2015.

[2] M. C. Soriano, J. García-Ojalvo, C. R. Mirasso, and I. Fischer, "Complex photonics: Dynamics and applications of delay-coupled semiconductor lasers," *Rev. Mod. Phys.*, vol. 85, no. 1, pp. 421-470, Jan. 2013.

[3] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers", *Nat. Photon.*, vol. 2, no. 12, pp. 728-732, Dec. 2008.

[4] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, no. 2, pp. 024102-1–024102-4, Jul. 2009.

[5] I. Kanter1, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nat. Photon*., vol. 4, no. 1, pp. 58-61, Dec. 2010.

[6] 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.

[7] 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.

[8] 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.

[9] A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, "45 Gbps high-speed real-time physical random bit generator." *Opt. Express*, vol. 21, no. 17, pp. 20452-20462, Aug. 2013.

[10] L. S. Wang, D. M. Wang, P. Li, Y. Y. Guo, T. Zhao, Y. C. Wang, and A. B. Wang, "Real-time 14-Gbps physical random bit generator based on

time-interleaved sampling of broadband white chaos," *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7201412.

[11] X. Tang, G. Q. Xia, E. Jayaprasath, T. Deng, X. D. Lin, L. Fan, Z. Y. Gao, and Z. M. Wu, "Multi-channel physical random bits generation using a vertical-cavity surface-emitting laser under chaotic optical injection," *IEEE Access*, vol. 6, pp. 3565-3572, Jan. 2018.

[12] G. D. VanWiggeren and R. Roy, "Communication with chaotic lasers," *Science*, vol. 279, no.5354, pp. 1198–1200, Feb. 1998.

[13] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links" *Nature*, vol. 437, no. 7066, pp. 343-346, Nov. 2005.

[14] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, and S. Merlo, "Private message transmission by common driving of two chaotic lasers," *IEEE J. Quantum Electron.*, vol. 46, no.2, pp. 258–264, Feb. 2010.

[15] N. Q. Li, W. Pan, L. S. Yan, B. Luo, X. H. Zou, and S. Y. Xiang, ''Enhanced two-channel optical chaotic communication using isochronous synchronization,'' *IEEE J. Sel. Topics Quantum Electron.*, vol. 19, no. 4, Aug. 2013, Art. no. 0600109.

[16] X. Porte, M. C. Soriano, D. Brunner, and I. Fischer, "Bidirectional private key exchange using delay-coupled semiconductor lasers." *Opt. Lett.* vol. 41, no. 12, pp. 2871-2874, Jun. 2016.

[17] N. Jiang, C. Xue, Y. Lv, and K. Qiu, ''Physically enhanced secure wavelength division multiplexing chaos communication using multimode semiconductor lasers,'' *Nonlinear Dyn.*, vol. 86, no. 3, pp. 1937–1949, Aug. 2016.

[18] J. Z. Ai, L. L. Wang, and J. Wang, "Secure communications of CAP-4 and OOK signals over MMF based on electro-optic chaos." *Opt. Lett.*, vol. 42, no. 18, pp. 3662-3665, Sep. 2017.

[19] J. X. Ke, L. L. Yi, G. Q. Xia, and W. S. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate." *Opt. Lett.*, vol, 43, no. 6, pp. 1323-1326, Mar. 2018.

[20] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," *Phys. Rev. Lett.*, vol. 108, no. 7, Feb. 2012, Art. no. 070602.

[21] H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," *Opt. Express*, vol. 21, no. 15, pp.17869-17893, Jul. 2013.

[22] L. S. Wang, Y. Q. Guo, Y. Y. Sun, Q. Zhao, D. D. Lan, Y. C. Wang, and A. B. Wang, "Synchronization-based key distribution utilizing information reconciliation," *IEEE J. Quantum Electron.*, vol. 51, no. 12, pp. 1-8, Dec. 2015.

[23] C. P. Xue, N. Jiang, K. Qiu, and Y. X. Lv, "Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing," *Opt. Express*, vol. 23, no. 11, pp. 14510-14519, Jun. 2015.

[24] T. Sasaki, I. Kakesu, Y. Mitsui, D. Rotani, A. Uchida, S. Sunada, K. Yoshimura, and M. Inubushi, "Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution," *Opt. Express*, vol. 25, no. 21, pp. 26029-26044, Oct. 2017.

[25] C. Xue, N. Jiang, Y. Lv, and K. Qiu, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 312-319, Jan. 2017.

[26] N. Jiang, C. P. Xue, D. Liu, Y. X. Lv, and K. Qiu, "Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection," *Opt. Lett.*, vol. 42, no. 6, pp. 1055-1058, 2017.

[27] I. Kanter, M. Butkovski, Y. Peleg, M. Zigzag, Y. Aviad, I. Reidler, M. Rosenbluhet, and W. Kinzelal, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," *Opt. Express*, vol. 18, no. 17, pp. 18292-18302, Aug. 2010.

[28] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators," *J. Lightwave Technol.*, vol. 34, no. 22, pp. 5325-5331, Nov. 2016.

[29] T. Yamamoto, I. Oowada, H. Yip, A. Uchida, and S. Yoshimori, "Common-chaotic-signal induced synchronization in semiconductor lasers." *Opt. Express*, vol. 15, no.7, pp.3974-3980, Apr. 2007.

[30] H. Aida, M. Arahata, H. Okumura, H. Koizumi, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, "Experiment on synchronization of semiconductor lasers by common injection of constant-amplitude random-phase light." *Opt. Express*, vol. 20, no. 11, pp. 11813-11829, May. 2012.

[31] N. Suzuki, T. Hida, M. Tomiyama, A. Uchida, K. Yoshimura, K. Arai, and M. Inubushi, "Common-signal-induced synchronization in semiconductor lasers with broadband optical noise signal." *IEEE J. Sel. Top. Quantum Electron.*, vol. 23, no. 6, Apr. 2017, Art. no. 1800810.

[32] D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A Dynamical Point of View." *IEEE J. Quantum Electron.*, vol. 45, no. 7, pp.879-1891, Jul. 2009.

[33] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta, "Identifying and modelling delay feedback systems." *Phys. Rev. Lett.*, vol. 81, no.3, pp. 558-561, Jul. 1999.

[34] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback,'' *Opt. Lett.*, vol. 32, no. 20, pp. 2960–2962, Oct. 2007.

[35] J. G. Wu, G. Q. Xia, and Z. M. Wu, "Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback." *Opt. Express*, vol. 17, no. 22, pp. 20124-20133, Oct. 2009.

[36] S. Y. Xiang, W. Pan, B. Luo, L. S. Yan, X. H. Zou, N. Jiang, L. Yang, H. N Zhu, "Conceal time-delay signature of chaotic vertical-cavity surface-emitting lasers by variable-polarization optical feedback." *Opt. Commun.*, vol. 284, no. 24, pp. 5758-5765, Dec. 2011.

[37] N. Li, W. Pan, S. Xiang, L. Yan, B. Luo, and X. Zou, "Loss of time delay signature in broadband cascade-coupled semiconductor lasers," *IEEE Photon. Technol. Lett.*, vol. 24, no. 23, pp. 2187–2190, Dec. 2012.

[38] A. B. Wang, Y. B. Yang, B. J. Wang, B. B. Zhang, L. Li, and Y. C. Wang, "Generation of wideband chaos with suppressed time-delay signature by delayed self-interference." *Opt. Express*, vol. 21, no. 7, pp. 8701-8710, Apr. 2013.

[39] S. Priyadarshi, Y. Hong, I. Pierce, and K. A. Shore, ''Experimental investigations of time-delay signature concealment in chaotic external cavity VCSELs subject to variable optical polarization angle of feedback,'' *IEEE J. Sel. Topics Quantum Electron.*, vol. 19, no. 4, Jan. 2013, Art. no. 1700707.

[40] N. Q. Li, W. Pan, A. Locquet, and D. S. Citrin, ''Time-delay concealment and complexity enhancement of an external-cavity laser through optical injection,'' *Opt. Lett.*, vol. 40, no. 19, pp. 4416–4419, Sep. 2015.

[41] C. H. Cheng, Y. C. Chen, and F. Y. Lin, "Chaos time delay signature suppression and bandwidth enhancement by electrical heterodyning." *Opt. Express*, vol. 23, no. 3, pp. 2308-2319, Feb. 2015.

[42] M. F. Cheng, X. J. Gao, L. Deng, L. F. Liu, Y. S. Deng, S. N. Fu, M. M. Zhang, and D. M. Liu, "Time-delay concealment in a three-dimensional electro-optic chaos system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 9, pp. 1030-1033, May 2015.

[43] P. H. Mu, W. Pan, L. S. Yan, B. Luo, N. Q, Li, and M. F. Xu, ''Experimental evidence of time-delay concealment in a DFB laser with dual-chaotic optical injections,'' *IEEE Photon. Technol. Lett.*, vol. 28, no. 2, pp. 131–134, Jan. 2016.

[44] Z. Q. Zhong, Z. M. Wu, and G. Q. Xia, "Experimental investigation on the time-delay signature of chaotic output from a 1550 nm VCSEL subject to FBG feedback," *Photon. Res.*, vol. 5, no. 1, pp. 6–10, Feb. 2017.

[45] P. H. Mu, P. F. He, and N. Q. Li, "Simultaneous chaos time-delay signature cancellation and bandwidth enhancement in cascade-coupled semiconductor ring lasers," *IEEE Access*, vol. 7, pp. 11041-11048, Jan. 2019.

[46] X. Z. Li, S. S. Li, and S. C. Chan, "Correlated random bit generation using chaotic semiconductor lasers under unidirectional optical Injection," *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no.1505411.

[47] D. M. Wang, L. S. Wang, T. Zhao, H. Gao, Y. C. Wang, X. F. Chen, and A. B. Wang, "Time delay signature elimination of chaos in a semiconductor laser by dispersive feedback from a chirped FBG." *Opt. Express*, vol. 25, no. 10, pp. 10911-10924, May. 2017.

[48] 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, Aug. 2012.

[49] A. B. Wang, Y. C. Wang, and H. C. He, "Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical

feedback," *IEEE Photon. Technol. Lett.*, vol. 20, no. 19, pp. 1633-1635, Oct. 2008.
[50] T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, "Maximizing the security of chaotic optical communications," *Opt. Express*, vol. 24, no. 20, pp. 23439-23449, Oct. 2016.
[51] D. M. Wang, L. S. Wang, Y. Y. Guo, Y. C. Wang, and A. B. Wang, "Key space enhancement of optical chaos secure communication: chirped FBG feedback semiconductor laser," *Opt. Express*, vol. 27, no. 3, pp. 3065-3073, Feb. 2019.
[52] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dary, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Pub. 800–22 Rev. 1a, 2010.
[53] G. Marsaglia, The diehard test suite, http://www. Csis. hku. hk/diehard, 2003.

Longsheng Wang received the B.S. degree in optical engineering and the Ph.D. degree in physical electronics from the Taiyuan University of Technology, Shanxi, China, in 2013 and 2017, respectively.

In 2018, he joined the Taiyuan University of Technology, where he is currently an Assistant Professor with the College of Physics and Optoelectronics. His research interests include nonlinear dynamics of semiconductor lasers, chaos synchronization, random bit generation, secure communications, and key distribution.

Daming Wang received the B.S. degree in Electronic Information Engineering from Beijing Institute of Graphic Communication, Beijing, China, in 2012. He is now pursuing the Ph.D. degree in physical electronics in the Taiyuan University of Technology.

His research interests include laser dynamics, optical chaos generation, and random bit generation.

Hua Gao received the B.S. degree in Photoelectric Information and Science and Technology from Taiyuan University of Technology, Shanxi, China, in 2015. She is now pursuing the Ph.D. degree in Instrument Science and Testing Technology in the Taiyuan University of Technology.

His research interests include key distribution, chaos synchronization, and random bit generation.

Yuanyuan Guo received the M.S. and Ph.D. degrees from Taiyuan University of Technology, Shanxi, China, in 2009 and 2016, respectively.

Her research interests include secure communication and nonlinear dynamics of semiconductor lasers.

Yuncai Wang 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, Beijing, China, in 1994 and 1997, respectively.

He has been a Professor in the College of Physics and Optoelectronics, Taiyuan University of Technology, where he is also the Chair of the Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi province 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.

Yanhua Hong received the B.Sc. degree in physics from Fujian Normal University, Fuzhou, China, the M.S. degree in physics from Beijing Normal University, Beijing, China, and the Ph.D. degree in optics from the Institute of Physics, Chinese Academy of Sciences, Beijing, in 1987, 1990, and 1993, respectively.

She was a Lecturer with Beihang University, Beijing, from 1993 to 1997. Since 1997, she has been with Bangor University, Bangor, U.K., where she became a Permanent Research Staff in 2007 and a Lecturer in 2013. She is the author or co-author of more than 150 journal and conference papers. Her current research interests include nonlinear dynamics in edge emitting semiconductor lasers, vertical cavity surface-emitting lasers, and semiconductor optical amplifiers and optical communication systems based on optical orthogonal frequency division multiplexing.

K. Alan Shore (M'88–SM'95) received the B.A. degree in mathematics from the University of Oxford, Oxford, U.K., and the Ph.D. degree in applied mathematics from University College, Cardiff, U.K.

He was a Lecturer with the University of Liverpool, Liverpool, U.K., from 1979 to 1983. He joined the University of Bath, Bath, U.K., where he became a Senior Lecturer in 1986, Reader in 1990, and Professor in 1995. He was a Visiting Researcher with the Center for High Technology Materials, University of New Mexico, Albuquerque, NM, USA, in 1987, and the Huygens Laboratory, Leiden University, Leiden, The Netherlands, in 1989. From 1990 to 1991, he was with the Teledanmark Research Laboratory and the Modeling, Nonlinear Dynamics and Irreversible Thermodynamics Center, Technical University of Denmark, Lyngby, Denmark. He was a Guest Researcher with the Electrotechnical Laboratory Tsukuba, Japan, in 1991. He was a Visiting Professor with the Department of Physics, University de les Illes Balears, Palma de Mallorca, Spain, in 1992. He was appointed as the Chair of Electronic Engineering, University of Wales, Bangor, U.K., in 1995, where he has served as the Head of the School of Informatics and the College of Physical and Applied Sciences. He was the Director of Industrial and Commercial Optoelectronics, a Welsh Development Agency Centre of Excellence. From 1996 to 1998, he was a Visiting Lecturer with the Instituto de Fisica de Cantabria, Santander, Spain. In 1996, 1998, 2000, 2002, 2005, and 2008, he was a Visiting Researcher with the Department of Physics, Macquarie University, Sydney, Australia. In 2001, he was a Visiting Researcher with the ATR Adaptive Communications Laboratories, Kyoto, Japan. He held a JSPS Invitation Fellowship with the Nara Institute of Science and Technology, Nara, Japan, in 2011. He has been the Chair of Welsh Optoelectronics Forum and he is currently the Chair of the Photonics Academy for Wales, Bangor. He is the author or coauthor of more than 930 contributions to archival journals, books, and technical conferences. He is a Coeditor with Prof. D. Kane of the research monograph *Unlocking Dynamical Diversity* (Wiley, 2005). His current research interests include semiconductor optoelectronic device design and experimental characterization with particular emphasis on nonlinearities in laser diodes dynamics, vertical cavity semiconductor lasers, and applications of nonlinear dynamics in semiconductor lasers to optical data encryption.

Dr. Shore is a Program Member of several Optical Society of America conferences and was a Coorganizer of the Rank Prize Symposium on Nonlinear Dynamics in Lasers held in the Lake District, U.K., in August 2002. He was a Cofounder, Organizer, and till 2012, Program Committee Chair of the International Conference on Semiconductor and Integrated Optoelectronics, which, since 1987, has been held annually in Cardiff, Wales, U.K. He is a Fellow of the Optical Society of America, the Institute of Physics, and the Learned Society of Wales for which he serves as a Council Member since 2012.

Anbang Wang (M'14) received a B.S. degree in Applied Physics and a Ph.D. degree in electronic circuits and systems from the Taiyuan University of Technology, Taiyuan, China, in 2003 and 2014, respectively. In 2006, he joined the Taiyuan University of Technology, where he is currently an Professor with the College of Physics and Optoelectronics. In 2014, He was a Visiting Scholar with the School of Electronic Engineering, Bangor University, Bangor, U.K. In 2017, he got the National Science Fund for Excellent Young Scholars in China.

His research interests include laser dynamics, wideband chaos generation, optical time-domain reflectometry, random bit generation, secure communication, and key space enhancement.