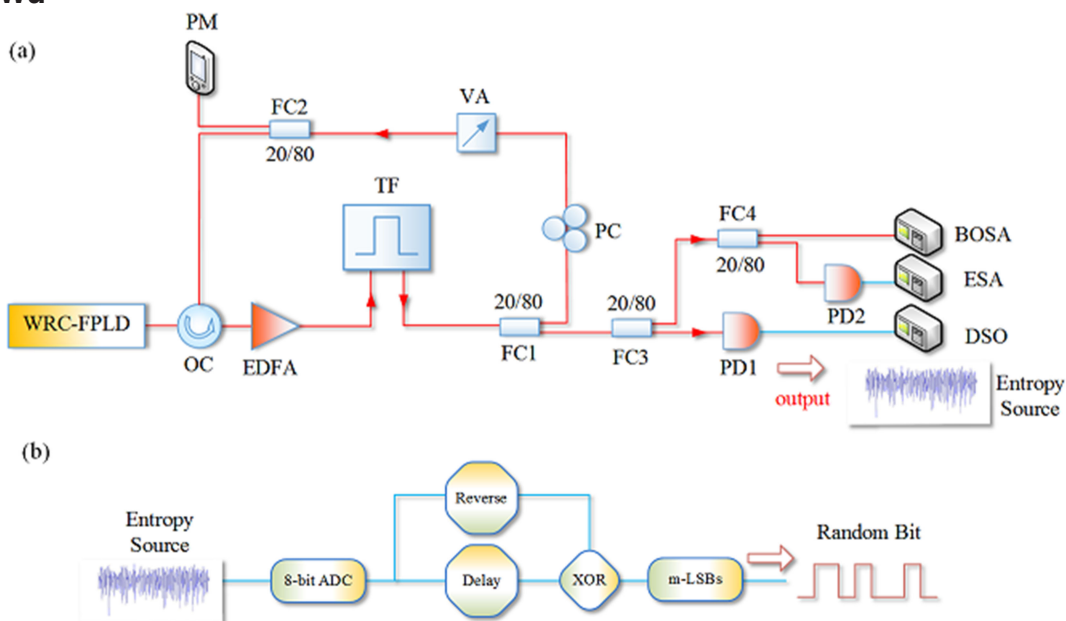


Fast Physical Random Bit Generation Based on a Broadband Chaotic Entropy Source Originated From a Filtered Feedback WRC-FPLD

Volume 11, Number 2, April 2019

Xi Tang
Guang-Qiong Xia
Can Ran
Tao Deng
Xiao-Dong Lin
Li Fan
Zi-Ye Gao
Gong-Ru Lin
Zheng-Mao Wu



DOI: 10.1109/JPHOT.2019.2903535
1943-0655 © 2019 IEEE

Fast Physical Random Bit Generation Based on a Broadband Chaotic Entropy Source Originated From a Filtered Feedback WRC-FPLD

Xi Tang,¹ Guang-Qiong Xia¹, Can Ran,¹ Tao Deng¹,
Xiao-Dong Lin¹, Li Fan,² Zi-Ye Gao¹, Gong-Ru Lin³,
and Zheng-Mao Wu¹

¹School of Physical Science and Technology, Southwest University, Chongqing 400715, China

²School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China

³Graduate Institute of Photonics and Optoelectronics, National Taiwan University, Taipei 10617, Taiwan

DOI:10.1109/JPHOT.2019.2903535

1943-0655 © 2019 IEEE. Translations and content mining are permitted for academic research only.

Personal use is also permitted, but republication/redistribution requires IEEE permission.

See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Manuscript received January 10, 2019; revised February 25, 2019; accepted March 4, 2019. Date of publication March 7, 2019; date of current version March 19, 2019. This work was supported in part by the National Natural Science Foundation of China under Grants 61875167, 61575163, 61775184, and 11704316, in part by the Natural Science Foundation of Chongqing City under Grants CSTC2016jcyjA0082 and CSTC2016jcyjA0575, and in part by the Fundamental Research Funds for the Central Universities of China under Grants XDJK2017B012, XDJK2017B047, and XDJK2017C063. Corresponding authors: Guang-Qiong Xia, Gong-Ru Lin, and Zheng-Mao Wu (e-mail: gqxia@swu.edu.cn; grlin@ntu.edu.tw; zmwu@swu.edu.cn).

Abstract: Taking the broadband chaotic output from a weak-resonant-cavity Fabry–Perot laser diode (WRC-FPLD) under filtered feedback as a chaotic entropy source, we propose and experimentally demonstrate a scheme for generating fast physical random bits (PRBs) at a rate up to 240 Gbits/s. First, we investigate the dependence of the dynamical properties of the filtered feedback WRC-FPLD on the system parameters, and determine the optimized parameter region for generating wavelength-tunable and broadband chaotic signals. Second, a broadband chaotic signal with a bandwidth beyond 20 GHz output from the WRC-FPLD is sampled and transferred to a digital bit sequence by an 8-bit analog-to-digital converter at a rate of 40 GS/s. Finally, by utilizing multi-bit post-processing method, PRBs is generated at a rate up to 240 Gbits/s, which can pass all the 15 NIST statistics tests and meet the strict criteria of the statistical bias and the serial correlation coefficient.

Index Terms: Physical random bit (PRB), weak-resonant-cavity Fabry-Perot laser diode (WRC-FPLD), filtered feedback, broadband chaotic entropy source.

1. Introduction

Chaos dynamics has received widespread attention in the past decades due to its emblematic properties such as the ergodicity, the sensitivity to initial conditions, the irregular motion in phase space and so on, and then is suitable for such applications as secret communication, stream cipher, image encryption, multimedia copyright protection, etc [1]–[8]. Specially, compared with the

digital chaotic system, the optical chaotic outputs from laser diodes (LDs) are more suitable to be utilized as the entropy sources for generating fast physical random bits (PRBs) due to their unique virtues including fast irregular amplitude fluctuation, largely spectral bandwidth over GHz level, unpredictability, and statistical randomness. In 2008, Uchida *et al.* innovatively proposed a technical scheme of 1.7 Gbits/s nondeterministic random bit generation based on two chaotic external-cavity LDs with mono-bit generation method [9]. Since then, plenty of schemes based on LD chaotic systems have been proposed for the random bit generation [10]–[28]. In general, there are two main ways to enhance the performances of a chaos-based random bit generator (RBG). One is to optimize the post-processing technique of bit sequences. For examples, in 2009, Reidler *et al.* proposed a novel approach of multi-bit generation, where the chaotic output was sampled by an 8-bit ADC with least significant bits (LSBs) extraction [10]. Comparing with the mono-bit generation method, the bit-rate is manifold raised through multiple-bit sampling. Hence, the random bit rate was raised up to 12.5 Gbits/s with 5-LSBs extraction at 2.5 GS/s sampling rate. Shortly afterwards, Kanter *et al.* utilized high derivatives and LSBs extraction in post-processing, and the random bits at a rate of 300 Gbits/s were obtained (16th derivative, 20 GS/s, 15-LSBs) [11]. In 2012, Akizawa *et al.* proposed a bit-order-reversal method for post-processing, and 400 Gbits/s random bits were generated [12]. In 2014, Li *et al.* obtained 2.2 Tbits/s random bits with high derivatives method (62th derivative, 40 GS/s, 55-LSBs) [13]. In 2015, our group adopted a post-processing scheme by combining Von Neumann unbiased method with exclusive-OR (XOR) method, and 0.96 Tbits/s random bits were achieved under the strict criteria of mainstream information-theoretic assessment [14]. The other feasible way is to optimize the properties of the chaotic entropy sources. In 2010, Argyris *et al.* utilized a photonic integrated circuit LD with optical feedback to enhance the robustness of chaos-based entropy source, and 140 Gbits/s random bits were obtained [15]. In 2012, Li *et al.* adopted optically injected LD instead of optical feedback LD to avoid the time-delay signature of the entropy source, and 30 Gbits/s random bits were generated [16]. In 2014, Virte *et al.* demonstrated a 100 Gbits/s RBG using a polarization chaos from a solitary laser diode without external disturbance, which obviously simplifies the chaotic systems [17]. In 2017, Wang *et al.* demonstrated a 320 Gbits/s RBG using a physical broadband white chaos generated by the optical heterodyning of two external-cavity LDs [18], where only minimal-post-processing is adopted due to the excellent statistical properties of white chaos. Among various methods to optimize the properties of the chaotic entropy sources, directly enhancing bandwidth of a chaos-based entropy source is one of the most effective ways. In 2010, Hirano *et al.* raised the standard bandwidth of chaotic waveforms up to 16 GHz by using a LD with chaotic optical injection, and a 75 Gbits/s random bit was obtained [19]. In 2015, Sakuraba *et al.* achieved a 35.2 GHz standard bandwidth chaotic signal in three-cascaded LDs, and the rate of RBG is greatly increased to 1.2 Tbits/s [20]. In 2017, by using a monolithically integrated dual-mode amplified feedback laser with self-injection, Zhang *et al.* gained a chaotic signal with bandwidth at dozens of GHz and realized a 640 Gbits/s RBG [21].

In this work, we concentrate on obtaining fast PRBs from a wideband chaos-based entropy source by utilizing a weak-resonant-cavity Fabry-Perot laser diode (WRC-FPLD) [29], [30] with filtered optical feedback. Compared with a conventional FPLD, the WRC-FPLD has smaller longitudinal mode spacing due to its longer cavity length ($\sim 630 \mu\text{m}$), and meanwhile the WRC-FPLD possesses broader gain spectrum due to its lower front-facet reflectance ($\sim 1\%$) [29]. Therefore, the WRC-FPLDs are suitable for applying in dense wavelength division multiplexed passive optical network (WDM-PON) system [29]. During our previously preliminary work [31], we have found that the WRC-FPLD under filtered optical feedback can generate broadband chaotic signals. Here, we experimentally investigate the dynamic evolutionary path of the WRC-FPLD with filtered optical feedback under different system parameters, and explore the dependence of the effective bandwidth of the chaotic outputs on feedback parameters. Taking an optimized wideband chaotic signal as an entropy source, we demonstrate the generation of 240 Gbits/s (6-LSBs, 40GS/s) PRBs, which meets the strict criteria of mainstream information-theoretic assessment.

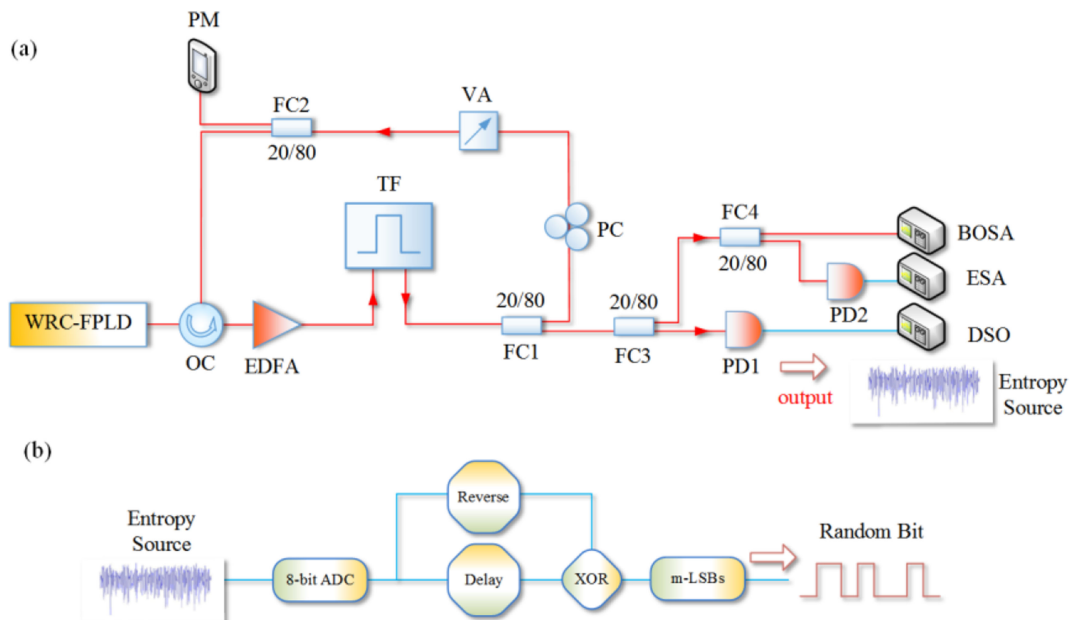


Fig. 1. (a) Experimental setup of the chaotic signal generation, (b) Random bit generation based on the post-processing of a chaotic entropy source. WRC-FPLD: weak-resonant-cavity Fabry-Perot laser diode; OC: optical circulator; EDFA: erbium-doped fiber amplifier; TF: tunable optical filter; FC: fiber coupler; PC: polarization controller; VA: variable attenuator; PM: power meter; PD: photo-detector; BOSA: photonic Brillouin high resolution optical spectrum analyzer; ESA: electrical spectrum analyzer; DSO: digital storage oscilloscope.

2. Experimental Setup

Figure 1 shows a schematic diagram of our experimental system. As shown in Fig. 1(a), the chaotic entropy source is originated from a filtered feedback WRC-FPLD, where the laser is driven by an ultra-low-noise laser controller (LC, ILX-Lightwave LDC-3724C). The output signal from the WRC-FPLD is sent to a 20:80 fiber coupler (FC1) after passing through an optical circulator (OC), an erbium-doped fiber amplifier (EDFA, FIPHENE BML01-EDFA), and a tunable filter (TF, EXFO XTM-50). The central wavelength and bandwidth of the TF can be tuned within 1450 nm–1650 nm and 6.25 GHz–120 GHz, respectively. The 80% part output from FC1 is fed back to the WRC-FPLD via a polarization controller (PC), a variable attenuator (VA), another fiber coupler 2 (FC2) and the OC. The 20% part output from FC1 is utilized as an entropy source, whose characteristics are monitored by a photonic Brillouin high resolution optical spectrum analyzer (BOSA, Aragon photonics BOSA Lite+C), an electronic spectrum analyzer (ESA, Rohde & Schwarz FSW67) and a digital storage oscilloscope (DSO, Agilent X91604A). In addition, an optical power meter (PM, Thorlabs PM100D) is utilized to detect the filtered feedback power ξ_f . In the post-processing part (Fig. 1(b)), a chaotic optical signal, taken as the entropy source, is converted to an electric signal through a photo-detector (PD, Finisar XPDV2120R), and then is sampled and transferred to a digital bit sequence through 8-bit analog-digital conversion (8-bit ADC). The original bit sequence is divided into two paths. One path is dealt with a time-delay operation, and the other path is dealt with a bit-order-reversal procedure. As a result, a bit-wise XOR operation is carried out between the two paths. After adopting an m-LSBs extraction, final random bit sequence can be achieved.

3. Experimental Results and Discussion

3.1 Dynamical Properties of the Filtered Feedback WRC-FPLD

Since the characteristics of an entropy source seriously affect the performance of the generated PRBs, it is necessary to investigate the dynamical properties of the system for providing the entropy

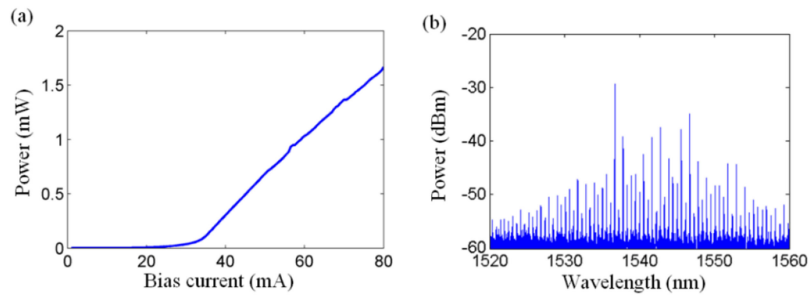


Fig. 2. (a) Power-current curve of a free-running WRC-FPLD; and (b) the optical spectrum for the laser biased at 40.00 mA.

source. In this work, the entropy source is provided by a WRC-FPLD under filtered feedback. During the experiment, the temperature of the WRC-FPLD is stabilized at 21.08 °C. Under this condition, the power-current curve for the free-running WRC-FPLD is measured as shown in Fig. 2(a). Obviously, the threshold current (I_{th}) of the WRC-FPLD is about 31.50 mA. During this experiment, the bias current of the WRC-FPLD is fixed at 40.00 mA, and the corresponding optical spectrum is displayed in Fig. 2(b). As can be seen, the output of the WRC-FPLD includes dozens of longitudinal modes, and the mode interval is about 0.55 nm.

Usually, for acquiring a LD-Based chaotic entropy source, one or more external disturbances are necessary to act on the LD. In this work, the external disturbance is a filtered optical feedback to be implemented by a TF. For convenient, the central wavelengths of the TF are always set at the resonant wavelengths of the longitudinal modes in the range of 1535–1555 nm, in which there are 35 longitudinal modes of the free-running WRC-FPLD as shown in Fig. 2(b). In order to investigate the impact of the filter bandwidth variation on the dynamical properties of the WRC-FPLD, three different bandwidths of the filter are selected at 60 GHz, 80 GHz and 100 GHz, respectively.

Figure 3 displays the optical spectra and the power spectra of the WRC-FPLD under filtered feedback at 1554.64 nm with an 80 GHz bandwidth and different feedback strength ξ_f . When $\xi_f = 0.06$ mW, the filtered feedback provided by the TF works, only the longitudinal mode oscillating at 1554.64 nm lases and the others are suppressed (Fig. 3(a1)), and the power spectrum enhances within the low frequency region (Fig. 3(b1)). Under this case, the dynamical state is a stable state. For $\xi_f = 0.21$ mW, the system is driven into the period state, where a strong oscillation peak can be observed at the fundamental frequency ~ 9.95 GHz in the power spectrum (Fig. 3(b2)). With the enhancement of ξ_f , the longitudinal mode located at the center wavelength of the filter may oscillate in chaos state. In the meantime, due to the small longitudinal mode spacing, the adjacent longitudinal modes may also oscillate and make a contribution to the broadening of chaotic bandwidth. For $\xi_f = 0.60$ mW, the optical spectrum (Fig. 3(a3)) is broadened, and the laser is driven into chaos. For the random bit generation, the effective bandwidth (EBW) is one of the important parameters to determine the maximum rate of PRBs. Hence, we adopt the EBW to qualify the chaotic spectra obtained in our experiment, where the EBW is defined as the summation of the discrete spectral segments of the chaos power spectrum accounting for 80% of the total power. Thus, the EBW is 12.8 GHz for $\xi_f = 0.60$ mW, in which the flatness of the power spectrum [20] is 12.1 dB. For $\xi_f = 2.20$ mW (as shown in Fig. 3(a4)–(b4)), the optical spectrum and the power spectrum further broaden, and the EBW of the power spectrum is 23.6 GHz, in which the flatness of the power spectrum is only 6.5 dB. However, when $\xi_f = 3.2$ mW (as shown in Fig. 3(a5)–(b5)), the optical spectrum narrows and the power spectrum is near to the noise background. As a result, the dynamical state of the laser returns into a stable state. Additionally, comparing the inset in Fig. 3(a5) with that in Fig. 3(a1), it can be seen that a stronger feedback would be helpful for improving the laser linewidth [32]. Further experiments show that for the TF under 60 GHz and 100 GHz filter bandwidths, the filtered feedback WRC-FPLD behaves similar dynamic evolution routes.

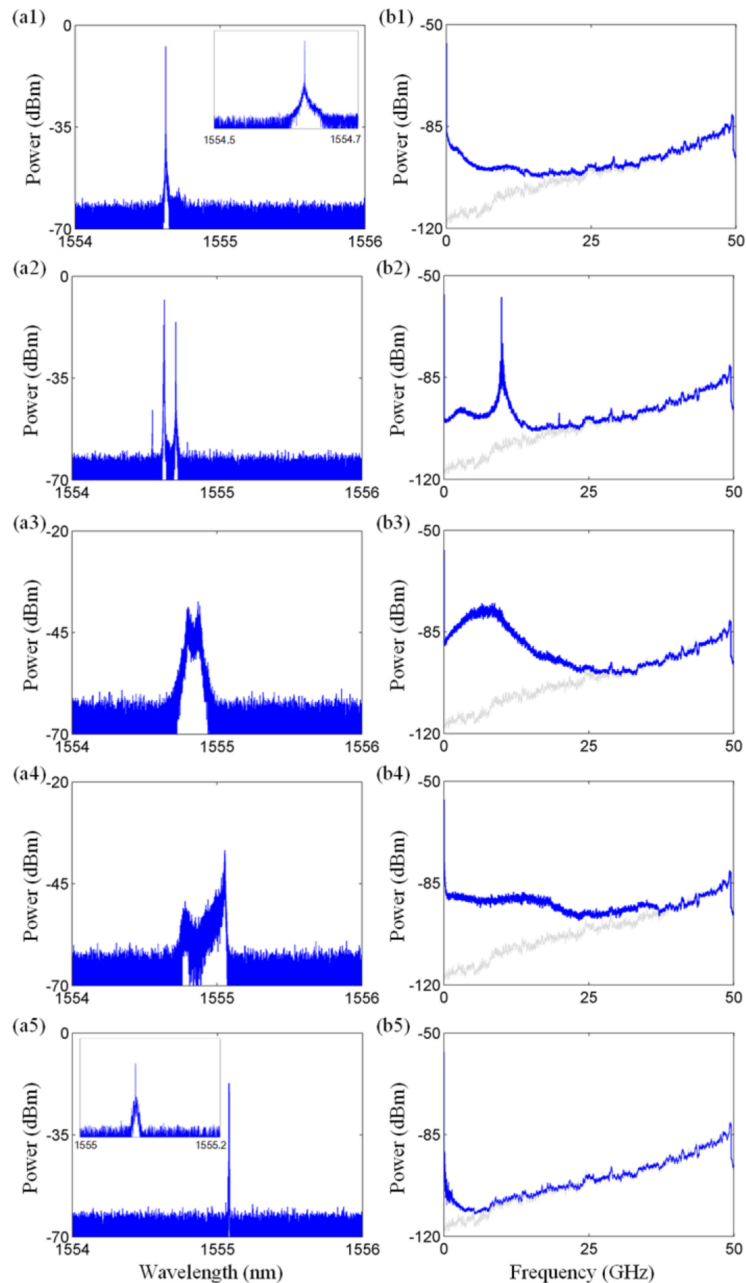


Fig. 3. (a) Optical spectra and (b) power spectra of the WRC-FPLD under filtered feedback with an 80 GHz bandwidth and feedback strength $\xi_f = 0.06$ mW (Row 1), 0.21 mW (Row 2), 0.60 mW (Row 3), 2.20 mW (Row 4) and 3.20 mW (Row 5), respectively. The central wavelength of the TF is set at 1554.64 nm, and the gray lines in power spectra denote the noise floor.

The above results show that, with a filtered feedback of the TF at a given central wavelength of 1554.64 nm, the WRC-FPLD can operate at a chaotic state under suitable feedback power. Moreover, the EBW of the chaotic signal is depended on the feedback power. We have also examined the cases that other central wavelengths of the TF are chosen, and related results are presented in Fig. 4. Here, only the central wavelengths within 1535.00 nm–1555.00 nm are considered, and the feedback power ξ_f is varied from 0.40 mW to 3.20 mW. From this diagram, it can

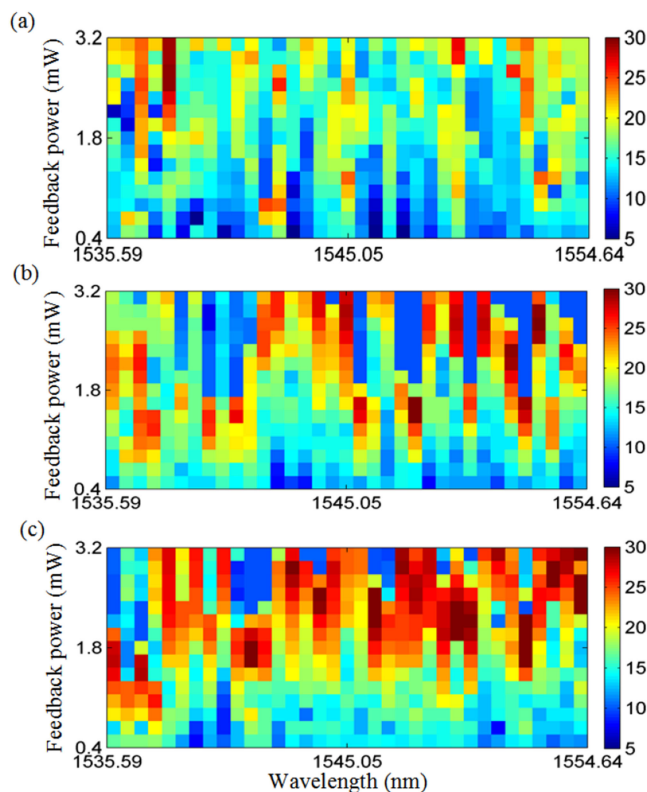


Fig. 4. Variation of the effective bandwidth (EBW) of the chaotic output from the WRC-FPLD with the feedback power under the case that the central wavelengths of the TF match with the oscillation wavelengths of the 35 longitudinal modes within 1535.00 nm–1555.00 nm, respectively, where the filter bandwidth is set at (a) 60 GHz, (b) 80 GHz and (c) 100 GHz, respectively.

be seen that, under different central wavelength, the feedback powers required for realizing chaotic outputs with large bandwidths are different. Comparatively speaking, the larger the bandwidth of the filter is, the broader the chaotic bandwidth will be. When the central wavelength and the bandwidth of the TF are set at 1554.64 nm and 100 GHz, respectively, the EBW of the chaotic output from the WRC-FPLD can be up to 31.9 GHz under $\xi_f = 3.20$ mW. Through carefully observing this diagram, it can be found that, for all the longitudinal modes within 1535.00 nm–1555.00 nm, the chaotic outputs with effective bandwidths over 20 GHz can be obtained under suitable parameters. The relatively wide chaotic bandwidth is originated from the small longitudinal mode spacing in the WRC-FPLD. In the following, the chaotic signal at 1546.12 nm with an effective bandwidth of 23.9 GHz, which is obtained under a filtered feedback power $\xi_f = 1.80$ mW with 100 GHz filter bandwidth, is taken as a chaotic entropy source for generating the random bit sequence.

3.2 Random Bit Generation

Via an 8-bit analog-to-digital converter (ADC) in a 16 GHz bandwidth digital storage oscilloscope (DSO), the above chaotic entropy source with 23.9 GHz bandwidth is sampled, and the obtained time series is shown in Fig. 5(a1). Here, the sampling rate of the DSO is set at 40 GS/s after considering that the bandwidth of the DSO is only 16 GHz. Figure 5(b1) displays the corresponding histogram of the waveform. Obviously, the amplitude probability density distribution is inhomogeneous, which is adverse in obtaining unbiased random bit sequence. In order to measure the number of LSBs extracted from the entropy source in a most conservative way [13], we have calculated the min-entropy of the sampled data to be equal to 6.72. Hence, the value of the selected LSBs should

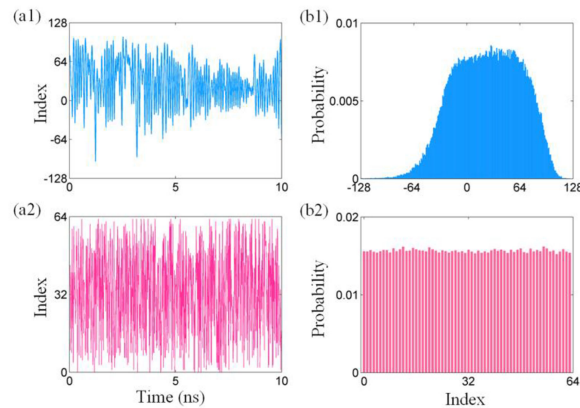


Fig. 5. Time series and the corresponding histograms for original digital sequence with 8 bit sampling (Row 1) and the final digital sequence with post-processing (Row 2).

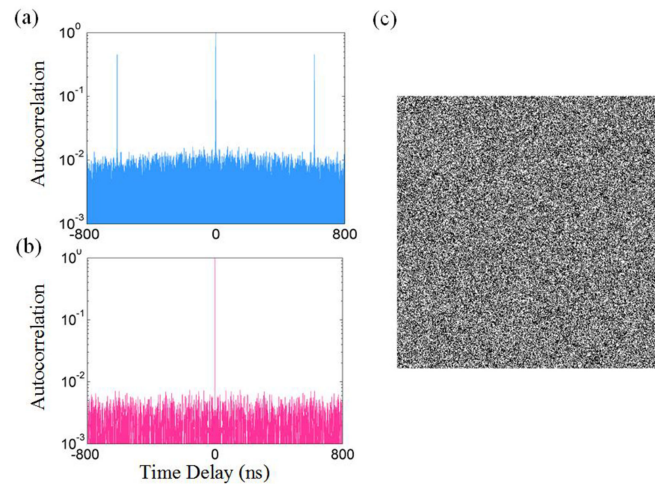


Fig. 6. (a) Autocorrelation result for the original digital sequence. (b) Autocorrelation result for the final digital sequence with 6-LSBs selected. (c) 2D graph of a random bit sequence with 1000×1000 bits, where bits “1” and “0” converted to white and black dots, respectively.

be no more than 6. Figure 5(a2) shows the digital sequence with a 6-bit vertical resolution, which is transformed from the final bit sequence (at 6-LSBs) with the post-processing method shown in Fig. 1(b). As shown in Fig. 5(b2), the amplitude probability density distribution is approximately uniform, which means that the final bit sequence is almost unbiased.

Since the chaotic entropy source is originated from a WRC-FPLD with filtered feedback, the chaotic entropy source usually exist a time delay signature (TDS). Fig. 6(a) displays the autocorrelation curve of the original digital sequence, from which the TDS is obvious. By utilizing post-processing method, the TDS can be eliminated. Figure 6(b) displays the autocorrelation result for the final digital sequence at 6-LSBs, and the single peak feature of the autocorrelation demonstrates that there is no TDS at all. Figure 6(c) show a 2D graph of a random bit sequence with 1000×1000 bits to visually indicate the randomness of the final bit sequence, where bits “1” and “0” are converted to white and black dots, respectively. It is clear that there are no obvious patterns in the graph, which indicates that no deterministic relationship exists between “1” and “0”. To further make a quantitative analysis of the final PRBs, we use NIST SP800-22 statistical test suite to verify the statistical randomness of the generated random bits. The results show that the final PRBs at

TABLE 1
Results of the NIST Tests for Final Random Bit Sequence, Where a Set of 1000 Sequences of 1 Mbit is Used for Evaluation

Statistical Test	P-value	Proportion	Result
Frequency	0.383827	0.9880	Success
Block Frequency	0.579021	0.9910	Success
Cumulative Sums	0.554420	0.9880	Success
Runs	0.101311	0.9940	Success
Longest Run	0.382115	0.9880	Success
Rank	0.862883	0.9840	Success
FFT	0.544254	0.9890	Success
Non Overlapping Template	0.019857	0.9820	Success
Overlapping Template	0.622546	0.9860	Success
Universal	0.701366	0.9950	Success
Approximate Entropy	0.245490	0.9850	Success
Random Excursions	0.023243	0.9810	Success
Random Excursions Variant	0.069581	0.9873	Success
Serial	0.278461	0.9920	Success
Linear Complexity	0.350485	0.9900	Success

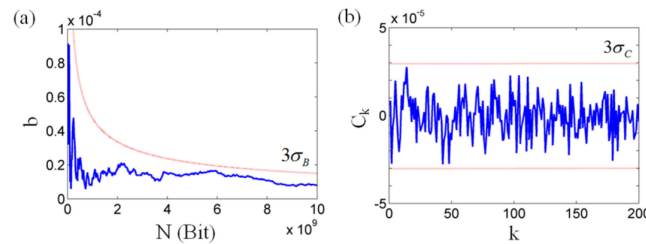


Fig. 7. (a) Variation of the statistical bias b with the sequence length N , and (b) the first 200 serial autocorrelation coefficients for the final binary sequences of 10 Gbits.

6-LSBs can successfully pass all the 15 NIST tests (Table 1). Therefore, referring to Ref. [10], the rate of the generated PRBs can be up to 240 Gbit/s ($40 \text{ GS/s} \times 6 \text{ bits}$).

It is worth noting that for statistical tests, more precise detection of randomness can be executed with a longer bit sequence. However, the length of a random bit sequence checked by the NIST tests is limited to only 1 Gbit. Hence, to evaluate the statistical randomness of a long bit sequence, we calculate the statistical bias b (as a function of the sequence length M) and serial autocorrelation coefficients C_k (as a function of the delay in bits k) for the final PRBs at a 10 Gbit length [14], which are given in Fig. 7. The red lines in this diagram show the bounds of three-standard-deviations of $3\sigma_B$ and $3\sigma_C$, which are determined by $3\sigma_B = 1.5N^{-0.5}$ for bias b and $3\sigma_C = 3N^{-0.5}$ for C_k , respectively. Based on the strict criteria of mainstream information-theoretic assessment, the curve of calculated b should always maintain below the red line of $3\sigma_B$ while the curve of calculated C_k should keep in the range of $\pm 3\sigma_C$ bound. As shown in this diagram, our results can meet these standards. In other words, the final PRBs have good statistical randomness at long range.

4. Conclusion

In summary, we have proposed and experimentally demonstrated a scheme to generate fast PRBs based on a WRC-FPLD subject to filtered optical feedback. We investigate the dynamical properties of the filtered feedback WRC-FPLD. With the increase of the feedback power, the dynamical evolution path of the laser is from a stable state, a period state and then into a chaotic state. However, if the feedback power is large enough, the WRC-FPLD may drop out of the chaotic state and turn back into a stable state. The chaotic signals with effective bandwidths over 20 GHz can be

generated under appropriate system parameters, and the highest effective bandwidth can reach beyond 30 GHz. Considering the electronic bottleneck of our used DSO bandwidth, we only set a sampling rate of 40 GS/s to avoid the short-timescale correlation between adjacent sampling points [14]. With multi-bit post-processing method, we have finally obtained PRBs at a rate up to 240 Gbits/s, which can pass all the 15 NIST tests and meet the strict criteria of mainstream information-theoretic assessment. Additionally, it is worth noting that, through adopting all-optical post-processing technique, such a scheme possesses a potential for generating wavelength-tunable all-optical PRBs [26], which can be compatible with different channels in WDM system. Therefore, this work may provide a tremendous convenience for achieving chaotic secure communication in WDM system.

References

- [1] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Nov. 2005.
- [2] R. Vicente, C. R. Mirasso, and I. Fischer, "Simultaneous bidirectional message transmission in a chaos-based communication scheme," *Opt. Lett.*, vol. 32, no. 4, pp. 403–405, Feb. 2007.
- [3] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nature Photon.*, vol. 9, no. 3, pp. 151–162, Feb. 2015.
- [4] H. E. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," *Informatica*, vol. 31, no. 1, pp. 121–129, Mar. 2007.
- [5] P. Li, Z. Li, W. A. Halang, and G. Chen, "A stream cipher based on a spatiotemporal chaotic system," *Chaos Solitons Fractals*, vol. 32, no. 5, pp. 1867–1876, Jun. 2007.
- [6] A. Cheddad, J. Condell, K. Curran, and P. McKeivitt, "A hash-based image encryption algorithm," *Opt. Commun.*, vol. 283, no. 6, pp. 879–893, Mar. 2010.
- [7] T. Sivakumarc and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos," *Opt. Laser Technol.*, vol. 111, pp. 196–204, Apr. 2019.
- [8] C. Fu, B. B. Lin, Y. S. Miao, X. Liu, and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Opt. Commun.*, vol. 284, no. 23, pp. 5415–5423, Nov. 2011.
- [9] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, Nov. 2008.
- [10] 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.
- [11] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photon.*, vol. 4, no. 1, pp. 58–61, Jun. 2010.
- [12] Y. Akizawa *et al.*, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8×50 Gb/s," *IEEE Photon. Technol. Lett.*, vol. 24, no. 12, pp. 1042–1044, Jun. 2012.
- [13] N. Q. Li *et al.*, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," *Opt. Exp.*, vol. 22, no. 6, pp. 6634–6646, Mar. 2014.
- [14] X. Tang *et al.*, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," *Opt. Exp.*, vol. 23, no. 26, pp. 33130–33141, Dec. 2015.
- [15] 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, no. 18, pp. 18763–18768, Aug. 2010.
- [16] 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.
- [17] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," *Opt. Exp.*, vol. 22, no. 14, pp. 17271–17280, Jul. 2014.
- [18] A. B. Wang, L. S. Wang, P. Li, and Y. C. Wang, "Minimal-post-processing 320-Gbps true random bit generation using physical white chaos," *Opt. Exp.*, vol. 25, no. 4, pp. 3153–3164, Feb. 2017.
- [19] K. Hirano *et al.*, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt. Exp.*, vol. 18, no. 6, pp. 5512–5524, Mar. 2010.
- [20] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Opt. Exp.*, vol. 23, no. 2, pp. 1470–1490, Jun. 2015.
- [21] L. M. Zhang *et al.*, "640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser," *Sci. Rep.*, vol. 7, pp. 45900-1–45900-8, Apr. 2017.
- [22] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation," *Opt. Lett.*, vol. 36, no. 23, pp. 4632–4634, Dec. 2011.
- [23] X. Z. Li and S. C. Chan, "Heterodyne random bit generation using an optically injected semiconductor laser in chaos," *IEEE J. Quantum Electron.*, vol. 49, no. 10, pp. 829–838, Oct. 2013.
- [24] 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.
- [25] 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, no. 3, pp. 031803-1–031803-4, Mar. 2011.
- [26] P. Li, Y. C. Wang, and J. G. Zhang, "All-optical fast random number generator," *Opt. Exp.*, vol. 18, no. 19, pp. 20360–20369, Sep. 2010.

- [27] T. Butler *et al.*, "Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser," *Opt. Lett.*, vol. 41, no. 2, pp. 388–391, Jan. 2016.
- [28] N. Q. Li, W. Pan, S. Y. Xiang, Q. C. Zhao, and L. Y. Zhang, "Simulation of multi-bit extraction for fast random bit generation using a chaotic laser," *IEEE Photon. Technol. Lett.*, vol. 26, no. 18, pp. 1886–1889, Sep. 2014.
- [29] G. R. Lin, H.-L. Wang, G. C. Lin, Y. H. Huang, Y. H. Lin, and T. K. Cheng, "Comparison on injection-locked Fabry–Perot laser diode with front-facet reflectivity of 1% and 30% for optical data transmission in WDM-PON system," *J. Lightw. Technol.*, vol. 27, no. 14, pp. 2779–2785, Apr. 2009.
- [30] G. R. Lin, H. L. Wang, T. K. Cheng, and G. C. Lin, "Suppressing chirp and power penalty of channelized ASE injection-locked mode-number tunable weak-resonant-cavity FPLD transmitter," *IEEE J. Quantum Electron.*, vol. 45, no. 9, pp. 1106–1113, Sep. 2009.
- [31] Z. Q. Zhong *et al.*, "Tunable broadband chaotic signal synthesis from a WRC-FPLD subject to filtered feedback," *IEEE Photon. Technol. Lett.*, vol. 29, no. 17, pp. 1506–1509, Sep. 2017.
- [32] R. W. Tkach and A. R. Chraplyvy, "Regimes of feedback effects in 1.5- μm distributed feedback lasers," *J. Lightw. Technol.*, vol. 4, no. 11, pp. 1655–1661, Nov. 1986.