IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 May 2024, accepted 7 June 2024, date of publication 11 June 2024, date of current version 20 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3412688

METHODS

Fast Physical Random Bit Generator With Dynamic Post-Processing Based on a Semiconductor Laser Under Multi-Path Optical Feedback

BING CUI[1], WENYAN YANG[2], ZAIFU JIANG[3], DIANZUO YUE[4], AND CHUNXIA HU[5]
[1]School of Statistics and Mathematics, Henan Finance University, Zhengzhou 450046, China
[2]School of Physics, Chongqing University of Science and Technology, Chongqing 401331, China
[3]School of Mathematics and Physics, Jingchu University of Technology, Jingmen, Hubei 448000, China
[4]School of Mathematics and Information Science and Technology, Hebei Normal University of Science and Technology, Qinhuangdao 066004, China
[5]Artificial Intelligence and Big Data College, Chongqing College of Electronic Engineering, Chongqing 401331, China

Corresponding author: Bing Cui (cuibing524@126.com)

This work was supported in part by the Research Start-Up Fund of Henan Finance University under Grant 2024BS003, in part by the Natural Science Foundation of Chongqing City under Grant cstc2021jcyj-msxmX0531 and Grant cstb2022nscq-msx0774, in part by the Natural Science Foundation of Hubei under Grant 2022CFB527, and in part by the Youth Project of Science and Technology Research Program of Chongqing Education Commission of China under Grant KJQN202203125.

ABSTRACT Based on a semiconductor laser (SL) under multi-path optical feedback (MPOF) system, a novel post-processing method for fast physical random bit generation has been proposed and demonstrated. The novel post-processing method is called self-circulating exclusive-or (XOR), and through this post-processing method, all bits of samples are used to produce physical random bits which can pass the National Institute of Standard Technology (NIST) statistical tests and triple standard deviation tests. For the chaotic source of a SL under MPOF system, the influences of feedback intensity on time-delay-signature (TDS) and bandwidth of the produced chaotic signal are experimentally analyzed. The experimental results show that a low TDS chaotic signal with 13 GHz bandwidth can be obtained under appropriate operating parameters and 8 × 80 Gb/s statistically passable physical random bits are produced by using the self-circulating XOR method. In addition, the self-circulating XOR method is robust to the number of samples in delay XOR loop and has a great potential to implement by using up-to-date electronic devices.

INDEX TERMS Multi-path optical feedback (MPOF), physical random bit, self-circulating exclusive-or (XOR), time-delay-signature (TDS).

I. INTRODUCTION

Fast physical random bit generators are crucial ingredients in lots of applications, such as secure communications [1], Monte-Carlo simulations [2], stochastic modeling [3] and even lotteries [4]. For many applications, the generation rate of random bits is of paramount importance [5], [6]. And due to the irregular intensity fluctuation also with large-amplitude of chaotic laser systems output which can be translated to high-speed physical random bits, chaotic laser systems are wildly used as physical random bit generators [7], [8]. For chaotic laser systems, post-processing of the sampled chaotic sequence is often performed to obtain statistically passable physical random bits [6]. As a consequence, the post-processing will ultimately play a role in determining the final generation rate and quality of the random bits [9]. Over the past years, great efforts have been focused on the post-processing to promote the generation rate of random bits. In 2008, Uchida and colleagues for the first time experimentally demonstrated a generation of 1.7 Gb/s random

The associate editor coordinating the review of this manuscript and approving it for publication was Stanley Cheung.

bit sequences by using exclusive-or (XOR) of two 1-bit sampling chaotic signals based on two independent chaotic semiconductor lasers (SLs) [10]. In the next year, a novel post-processing method of least significant bits (LSBs) interception have been proposed and the generation rate of random bits reached 12.5 Gb/s by using 5-LSBs interception combined with first-order derivative at 2.5 GSa/s [5]. In 2010, a method of high-order derivative companied with LSBs interception was introduced and 300 Gb/s random bits can be achieved [6]. In 2012, a bit-order-reversal method was proposed and 400 Gb/s random bits have been realized [11]. By merging of two random bit sequences which are operated by bit-order-reversal method, XOR, and LSBs interception, 1.12 Tb/s random bits have been obtained in 2015 [12]. In 2018, Tian et al. proposed self-bit-delay bitwise XOR operation to generate random bits [13]. Recently, a random bit sequence with a rate of 2.5 Tb/s was generated by using time-shift, bit-order-reversal method, and XOR [14].

However, the above post-processing methods are either complex to implement or limitation of the generation rate of random bits by abandoning some bits of samples in order to obtain statistically passable random bits. So, we propose self-circulating XOR operation in this paper.

In our previous work, we have demonstrated that a SL under multi-path optical feedback (MPOF) can produce suppressed time-delay-signature (TDS) chaotic signals [15]. In this paper, taking a SL under MPOF as chaotic entropy source, experiment of fast physical random bits generation by using the self-circulating XOR operation is demonstrated. The experimental results show that a 13 GHz chaotic signal with low TDS can be obtained under appropriate feedback intensity, and 8 × 80 Gb/s statistically passable physical random bits are produced by using the self-circulating XOR operation.

II. METHODS

Before showing the experimental results and conclusion, we first introduce some data analysis methods and the self-circulating XOR method which are used in this paper.

Firstly, the autocorrelation function (ACF) is a simple and common method to identify the TDS [16]. The ACF is defined as follows:

$$C(\Delta t) = \frac{\langle [I(t+\Delta t) - \langle I(t+\Delta t)\rangle][I(t) - \langle I(t)\rangle]\rangle}{\sqrt{\left\langle [I(t+\Delta t) - \langle I(t+\Delta t)\rangle]^2\right\rangle \left\langle [I(t) - \langle I(t)\rangle]^2\right\rangle}}. \tag{1}$$

where $I(t)$ represents the intensity of the laser output, $< \cdot >$ denotes the time average, and Δt is the lag time. The TDS can be identified by evaluating the height of peak around the feedback time in ACF curve.

Secondly, statistical bias is a very useful method to judge the statistical characteristics of random bits [11]. Statistical bias is defined as the probabilistic deviation of the occurrence of bit 1 from the uniform distribution for binary sequence, which is described as:

$$\varepsilon[N] = \left| \langle p[N] \rangle - 1/2 \right|. \tag{2}$$

where $p[N]$ represents the probability of the occurrence of bit 1 for the binary sequences with N-bit length.

Thirdly, the procedure of the self-circulating XOR method is shown in Fig. 1. Firstly, Chaotic signal is digitized by an analog-to-digital converter (ADC). Then, the digital signal is operated by XOR with the nth previously output digital signal. Here, the number n can be arbitrary non-zero integer. This n samples form a structure called delay XOR loop here. Fig. 1(b) shows the proposed postprocessing method can be implemented in a field programmable gate array (FPGA) electronic board [7]. Through the self-circulating XOR method, the random bits are produced by samples operate a bitwise XOR with other samples which are digitized earlier before. It is obviously that no bits are abandoned in this method and the generation rate of the random bit sequences is equal to the number of sample rate multiply by the vertical resolution of ADC.

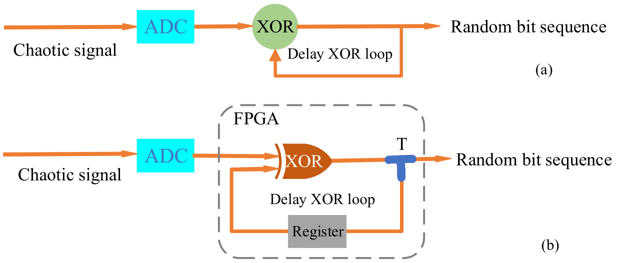


FIGURE 1. Procedure of self-circulating exclusive-or (XOR) method. (a) the profile of self-circulating XOR, and (b) the schematic of self-circulating XOR implemented in a field programmable gate array. ADC: analog-to-digital converter. XOR: exclusive-or. T: T-type connector. FPGA: field programmable gate array.

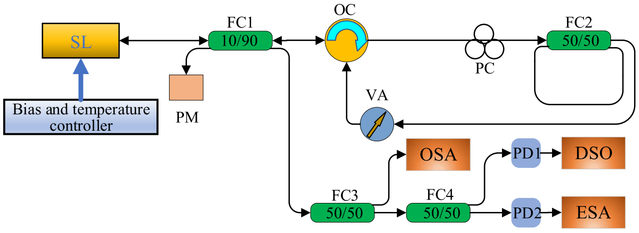


FIGURE 2. Experimental setup. SL: semiconductor laser. PM: power meter. FC: fiber coupler. PC: polarization controller. VA: variable attenuator. OC: optical circulator. PD: photoelectric detector. OSA: optical spectrum analyzer. ESA: electronic spectrum analyzer. DSO: digital storage oscilloscope.

III. EXPERIMENTAL SETUP

The experimental configuration is presented in Fig. 2. A distributed feedback laser diode is used as the SL, and its bias current and temperature is controlled by a current-temperature controller (ILX-Lightwave, LDC-3724). The bias current is set at 30.30 m (3 times the threshold current), while the temperature is maintained at 22.00°C. In this case, the SL sends out light at a wavelength of 1548.45 nm. The light is split into two parts by a 10/90 fiber coupler (FC1) firstly. Then, through an optical circulator (OC), one part of the light (the 90.0% of optical power) is sent to a MPOF module while the state of polarization and intensity of the feedback light are adjusted by a polarization controller (PC) and a variable attenuator (VA) respectively. The MPOF module is composed of a 2 × 2 fiber coupler (FC2) in the feedback loop. For comparison, single optical feedback (SOF) is formed if the loop of FC2 is broken and the delay time of SOF is marked as τ. In this experiment, τ is fixed at 76.25 ns. The extra feedback delay time which is introduced by the loop of FC2 is marked as τ_l, and τ_l is maintained at 10.39 ns. At the same time, the feedback intensity is monitored by a power meter (PM) through the FC1. Here, the feedback intensity is defined as the ratio of feedback optical power to the output power of SL under free-running. The other part of the light (the 10.0% of optical power) is recorded by a digital storage oscilloscope (DSO, Agilent DSO-X 91604A, 80.0 GSa/s sample rate, 16 GHz bandwidth) via a photoelectric detector (PD1, New Focus 1544B, 12 GHz bandwidth). While, the output power spectrum is recorded by an electrical spectrum analyzer (ESA, R&S FSW67, 67 GHz bandwidth) through another photoelectric detector (PD2, U2T-XPDV2120R, 50 GHz bandwidth), and the output optical spectrum is monitored by an optical spectrum analyzer (OSA, Aragon Photonics BOSA lite +, 20 MHz resolution).

IV. EXPERIMENTAL RESULTS

A. CHAOTIC SIGNAL GENERATION

Fig. 3 displays the experimental profiles of time series (first column), the corresponding ACF curves (second column), optical spectra (third column), and power spectra (fourth column) of the output from the SL under SOF (first row) and the SL under MPOF (second row) with identical parameter conditions. As we can see, the optical spectra are clearly wide and the corresponding time series vary erratically in Fig. 3. According the time series and optical spectra, this allows the conclusion that the output signals are chaotic in the two situations. Fig. 3(a2) have an obvious peak appearing at 76.25 ns, which means the TDS is easy to identify using ACF in the SL under SOF case. In the following part, we refer to the height of this peak in ACF curve as the TDS value ρ. In SL under MPOF case, the TDS value ρ in Fig. 3(b2) is relatively small, which means the TDS is effectively suppressed. The power spectra of Fig. 3 show that the bandwidth of the SL under MPOF is not obviously different with that of the SL under SOF and both are about 13 GHz. Because the energy is concentrated nearby the relaxation oscillation in both cases. Here, the bandwidth means the effective bandwidth (EBW) which is defined as the frequency range containing 80% of the total energy in the power spectrum [17].

In order to systematic analysis the influence of feedback intensity on TDS and bandwidth, Fig. 4 presents the TDS value ρ and EBW in the two cases versus the feedback intensity. Obviously, the ρ of the SL under MPOF always maintain at a lower level than that of the SL under SOF and the EBW trend of former have no obviously different with that of latter. In detail, for the TDS value ρ in the two cases, the values decrease firstly as the increase of feedback intensity and then increase with the continually increase of feedback intensity, which is in keeping with our former work [15]. In the SL under MPOF case, the TDS peak is very indistinguishable under proper feedback intensity. Apparently, the SL under MPOF shows better TDS suppression compared with the SL under SOF case. For the bandwidth of the two cases, the values of EBW increase with the increase of feedback intensity and then decrease with the continually increase of feedback intensity. And the biggest EBW is about 13 GHz in both cases. As can be seen from Fig. 4, the chaotic EBW is the largest and the TDS is relatively small under −12 dB feedback intensity, so the feedback intensity is fixed at −12 dB in the following experiment to generate a stable chaotic entropy source for physical random bits generation.

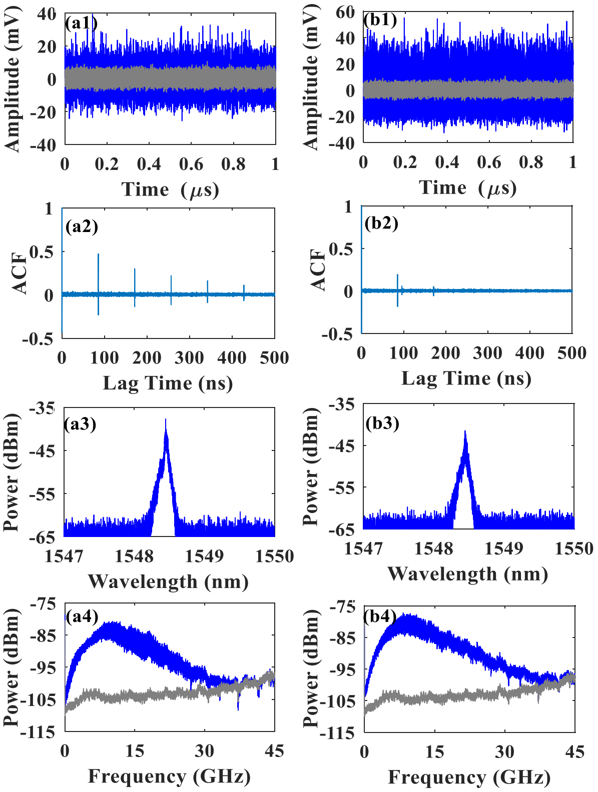


FIGURE 3. Experimentally measured time series (first row), calculated ACF curves (second row), optical spectra (third row) and power spectra (fourth row) of the output from the SL under SOF (first column), and the SL under MPOF (second column). Feedback intensity: - 12 dB. The gray curves are the background noise floor.

B. FAST PHYSICAL RANDOM BIT GENERATION

In this work, the self-circulating XOR operation is done off-line after sampling the chaotic signal by the oscilloscope with 80 GSa/s. The number of samples in delay XOR usually

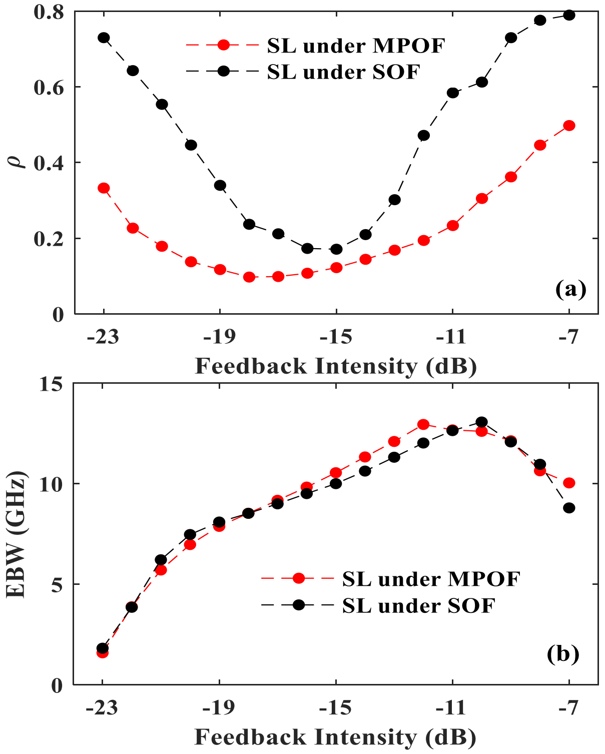


FIGURE 4. Experimentally measured TDS value ρ curves (a), and EBW curves (b) in the two scenarios as a function of feedback intensity. The red points represent SL under MPOF, while the black points stand for SL under SOF.

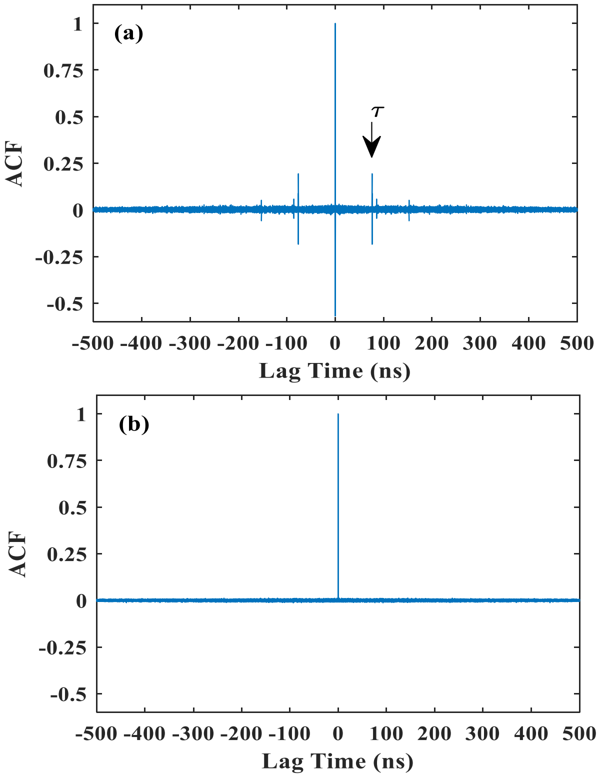


FIGURE 5. ACF curves of (a) raw 8-bit sampling data and (b) produced 8-bit data by using the self-circulating XOR method.

avoid the feedback delay time of chaos laser system to avoid cross-correlation between the two signals [11]. To sufficiently exhibit the robust of this self-circulating XOR method to the number of samples in delay XOR loop, we choose a special number of samples in delay XOR loop to operate the self-circulating XOR method, and the special number is 6100 (76.25 ns) which is equal to the main feedback delay time of MPOF structure [5], [8], [11], [18], [19], [20], [21], [22].

In order to assess the effect of TDS suppression of the self-circulating XOR method, Fig. 5 shows the ACF curves before and after using the self-circulating XOR. It is clear that ρ is 0.1939 at τ before using the method (Fig. 5(a)), and no peaks appear after using the method (Fig. 5(b)). It is means that the TDS is perfectly suppressed by using the self-circulating XOR method even the number of samples in delay XOR loop is equal to the main feedback delay time of MPOF structure.

Next, we investigate the probability distribution of 8-bit data before and after using the self-circulating XOR operation. Fig. 6 shows the probability distribution histogram of raw 8-bit sampling data and produced 8-bit data by using the self-circulating XOR. The produced 8-bit data in Fig. 6(b) has a uniform distribution, whereas the raw sampling data has a nonuniform distribution (Fig. 6(a)). The probability for each 8-bit binary number produced by using the self-circulating XOR is very close to $1/256$. It is clear that the self-circulating XOR method is very helpful to produce data with a uniform distribution from the raw sampling data with a nonuniform distribution. This is because the unbiasedness of the produced data by using the self-circulating XOR. The effectiveness of the bias elimination by the self-circulating XOR method can be proved theoretically. Ideally but not loss of generality, our chaotic SL system is supposed to be a stationary chaotic source, and for simplicity, the chaotic source is supposed to produce binary bits which are statistically independent but bias. The probability of "1" in the raw binary sequence is marked by P. So, the statistical bias is $\varepsilon = |P{-}1/2|$ for the raw sampling data [23]. Though the self-circulating XOR operation, the probability of "1" is changed to P'. Based on the self-circulating XOR operation, the following equation holds: $(1/2+\varepsilon)\times\left(1-P'\right)+(1/2-\varepsilon)\times P' = P'$. As a result, $P' = 1/2$, which means the produced data by using the self-circulating XOR is unbiased. Furthermore, by introducing Hamming weight ω, the probability of every produced 8-bit data by using the self-circulating XOR can also be computed, and the results is 1/256 which is consistent with Fig. 6(b).

Fig. 7 shows the bitmap image of the produced bit sequence by using the self-circulating XOR. It is 1000 by 1000 bits which are plotted in Fig. 7, and white and black dots represent bits "1" and "0" respectively. No obvious pattern can be observed from Fig. 7, which means the distribution of bits "1" and "0" is roughly random.

Triple standard deviation tests are useful examination to quantitatively demonstrate the randomness of bit

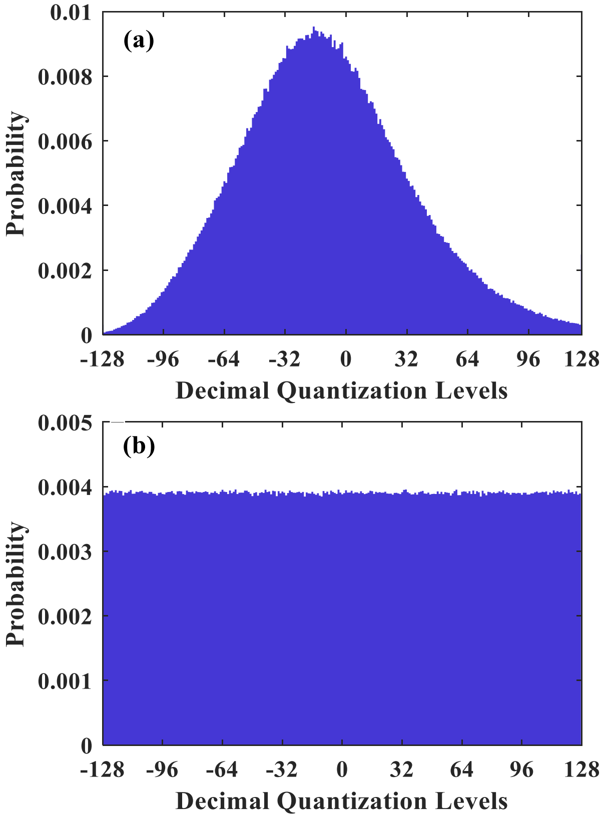


FIGURE 6. Probability distribution histogram of (a) raw 8-bit sampling data and (b) produced 8-bit data by using the self-circulating XOR method.

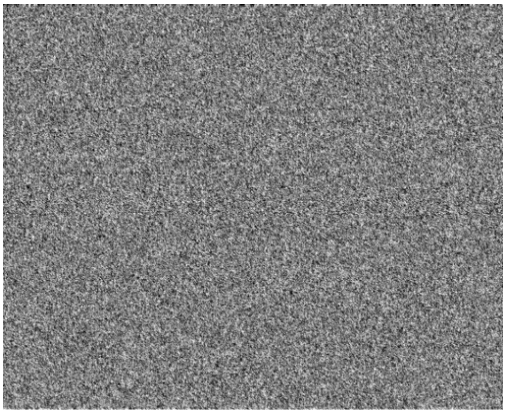


FIGURE 7. Example of produced bit sequence by using the self-circulating XOR plotted in two-dimensional dot diagram. Bits "1" and "0" are converted into white and black dots respectively, and 1000 by 1000 bits are shown.

sequence [24]. According to the examination, the statistical bias $\varepsilon[N]$ of a random sequence of length N falls within the range $[-3\delta_\epsilon, 3\delta_\epsilon]$ has a probability of 99.7% (the standard deviation $\delta_\epsilon = 0.5/\sqrt{N}$), and serial autocorrelation coefficient C_k of the random sequence should fall within the range $[-3\delta_a, 3\delta_a]$ with the same probability (the standard deviation $\delta_a = 1/\sqrt{N}$). By computing the statistical bias and serial autocorrelation coefficient of a bit sequence, it is very convenient to determine whether the sequence meets the triple standard deviation tests. Fig. 8(a) displays the statistical bias as a function of sample size N, which ranges from 1 Mbit to 5 Gbit. It can be seen that the curve of the statistical bias keeps below its triple standard deviation versus different sample sizes. While Fig. 8(b) plots the serial autocorrelation coefficient as a function of delay bit. It is clear that the values of serial autocorrelation coefficient also fall within its triple standard deviation range. Therefore, it is clear that the produced bit sequence by using the self-circulating XOR method can pass the triple standard deviation tests.

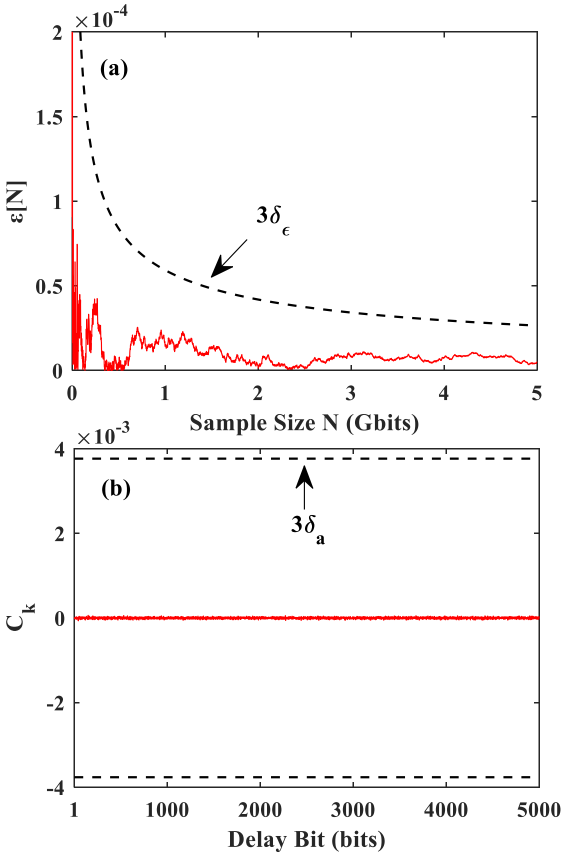


FIGURE 8. (a) Statistical bias as a function of sample size N: N ranges from 1 Mbit to 5 Gbit; (b) serial autocorrelation coefficient as a function of delay bit calculated by ensemble averaging over 5000 sequences of 1 Mbit sample size. The black dashed lines are their triple standard deviation lines.

Moreover, we utilize a strict test suite Special Publication 800-22 with 15 statistical test items from the National Institute of Standards and Technology (NIST statistical tests) to evaluate the statistical randomness of the produced bit sequences by using the self-circulating XOR [25], [26], [27], [28]. These 15 tests focus on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. For each test, a relevant randomness statistic must be chosen and used to determine the acceptance or rejection of the random hypothesis. A theoretical reference distribution of this statistic under the random hypothesis is determined by mathematical methods. If the sequence under test is in fact non-random, the

TABLE 1. Nist special publication 800-22 statistical tests results for 1000 samples of 1-Mbit data.

Statistical test	*P*-value	Proportion	Result
Frequency	0.733899	0.991	Success
Block Frequency	0.022149	0.990	Success
Cumulative Sums	0.587274	0.993	Success
Runs	0.100709	0.992	Success
Longest Run	0.094285	0.995	Success
Rank	0.686955	0.991	Success
FFT	0.316052	0.988	Success
Non-Overlapping Template	0.010310	0.988	Success
Overlapping Template	0.554420	0.989	Success
Universal	0.498313	0.986	Success
Approximate Entropy	0.794391	0.994	Success
Random Excursions	0.121743	0.990	Success
Random Excursions Variant	0.021561	0.994	Success
Serial	0.096000	0.992	Success
Linear Complexity	0.450297	0.993	Success

calculated test statistic will fall in extreme regions of the reference distribution. The passing criterion is determined by the length of the tested bit sequence and the significant level. More in-depth analysis can be performed by using statistical procedures. In our examination, 1000 samples of 1-Mbit data are used and the significant level is set to 0.01. In this situation, when the proportion of sequences satisfying *p*-value larger than 0.01 is in the range of 0.99 ± 0.0094392 and the uniformity of *p*-values (i.e. the *P*-value) is larger than 0.0001, the bit sequences are considered to be random. Table 1 depicts the tests results. For tests that return several *P*-values and proportions, the worst case is given. It can be seen in Table 1 that all of 15 tests are passed indicating that the produced bit sequences have good statistical randomness.

To show the rate and quality of random bits produced by self-circulating XOR, the comparison of self-circulating XOR with other existing random bit generation technologies such as LSB interception [5], [29], delay XOR [30], [31], and bit-order-reversal before delay XOR is made in Fig. 9 and Table 2 [12]. The data used in Fig. 9 and Table 2 is the same as the data used earlier which is sampled from the MPOF system by the oscilloscope with 80 GSa/s. It is show that LSB interception has the worst result. By solely adopting 4-LSBs and 5-LSBs extraction, the bit sequence can't meet all 15 NIST tests. After additionally adopting delay XOR processing, the random bit sequences can meet all 15 NIST tests under 4-LSBs and 5-LSBs extraction. By using bit-order-reversal before delay XOR, the random bit sequences under 7-LSBs extraction can pass all 15 NIST tests. Only by using self-circulating XOR, the random bit sequences produced by all 8 bits of every sample can pass all 15 NIST tests. The maximum random bit generation rate using these post-processing methods are show on Table 2. Under the same data conditions, the maximum random bit generation rate can be obtained by using self-circulating XOR, and all bits of samples are used to produce physical random bits only by using this method.

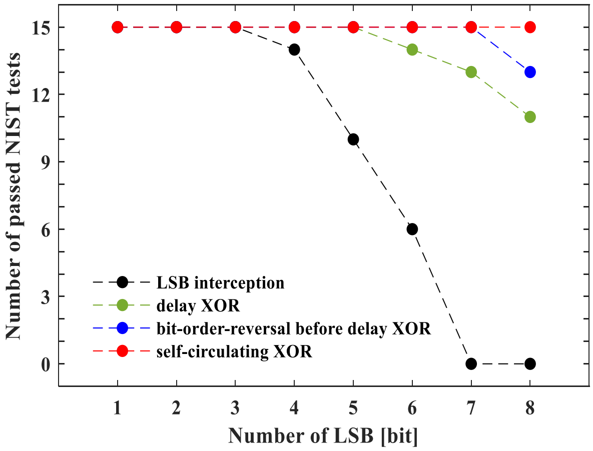


FIGURE 9. The number of passed NIST statistical tests as a function of the number of LSBs used to generate the bit sequence. "15" indicates that all the tests are passed.

TABLE 2. Maximum random bit generation rate by different methods.

Methods	Maximum Random Bit Generation Rate
LSB interception	3 × 80 Gb/s
Delay XOR	5 × 80 Gb/s
Bit-order-reversal before delay XOR	7 × 80 Gb/s
Self-circulating XOR	8 × 80 Gb/s

Besides, to further exhibit the robust of the self-circulating XOR method to the number of samples in delay XOR loop, we use 100 arbitrary integers as the numbers of samples in delay XOR loop for the self-circulating XOR operation to produce random bit sequences. So, we can get 100 produced bit sequences by using the self-circulating XOR with 100 different numbers of samples in delay XOR loop, and we divide them into 10 groups equally. The 10 groups bit sequences are tested by NIST statistical tests and Fig. 10 shows the tests results. It can be seen that all produced bit sequences by using the self-circulating XOR have passed the NIST statistical tests. This sufficiently displays the number of samples in delay XOR loop for the self-circulating XOR operation can be arbitrary nonzero integer in order to produce physical random bits, and the number of samples in delay XOR loop has no influence on the quality of physical random bits if the number is non-zero integer.

It should be noticed that the bit rate is 640 Gbit/s based on the self-circulating XOR under 8-bit vertical resolution

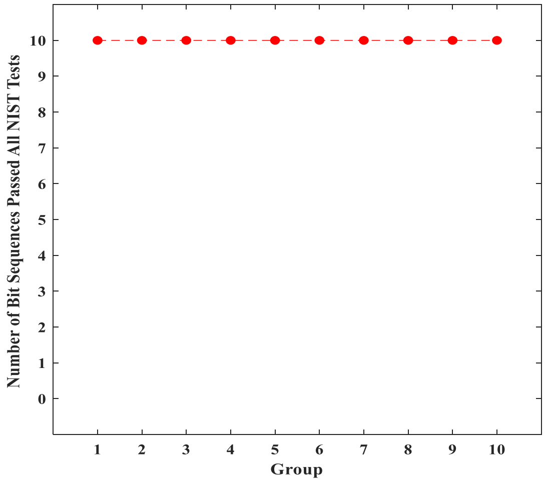


FIGURE 10. NIST statistical tests results for 10 groups of 10 bit-sequences.

ADC sampling at 80 GSa/s, and all bits of samples are used to produce physical random bits. Also, it should be mentioned that if improve the sampling rate or vertical resolution of ADC, the generation rate of physical random bits can be further increased by using the self-circulating XOR.

V. CONCLUSION

In summary, in order to achieve fast physical random bit sequences, a novel and useful post-processing method the self-circulating XOR have been proposed and demonstrated. By adopting the self-circulating XOR method which use all bits of samples, the physical random bits are produced and the produced bits are proved to be unbiased. Furthermore, the produced 640 Gbit/s physical random bits by using the self-circulating XOR method can pass all NIST statistical tests. This post-processing method is simple and it has a great potential in electronic systems.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] N. Metropolis and S. Ulam, "The Monte Carlo method," *J. Amer. Statist. Assoc.*, vol. 44, no. 247, pp. 335–341, 1949.

[3] S. Asmussen and P. W. Glynn, "Markov Chain Monte Carlo methods," in *Stochastic Simulation: Algorithms and Analysis*. New York, NY, USA: Springer-Verlag, 2007, pp. 350–380.

[4] N. Ferguson, B. Schneier, and T. Kohno, "Key negotiation," in *Cryptography Engineering: Design Principles and Practical Applications*. Indianapolis, IN, USA: Wiley, 2010, pp. 135–243.

[5] 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, Jul. 2009, Art. no. 024102.

[6] 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, Jan. 2010.

[7] K. Ugajin, Y. Terashima, K. Iwakawa, A. Uchida, T. Harayama, K. Yoshimura, and M. Inubushi, "Real-time fast physical random number generator with a photonic integrated circuit," *Opt. Exp.*, vol. 25, no. 6, p. 6511, Mar. 2017.

[8] L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, "Random bit generator using delayed self-difference of filtered amplified spontaneous emission," *IEEE Photon. J.*, vol. 6, no. 1, pp. 1–9, Feb. 2014.

[9] T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, "Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser," *Opt. Lett.*, vol. 41, no. 2, p. 388, Jan. 2016.

[10] 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, no. 12, pp. 728–732, Dec. 2008.

[11] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "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.

[12] X. Tang, Z.-M. Wu, J.-G. Wu, T. Deng, J.-J. Chen, L. Fan, Z.-Q. Zhong, and G.-Q. Xia, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," *Opt. Exp.*, vol. 23, no. 26, p. 33130, Dec. 2015.

[13] W. Tian, L. Zhang, J. Ding, S. Shao, X. Fu, and L. Yang, "Ultrafast physical random bit generation from a chaotic oscillator with a silicon modulator," *Opt. Lett.*, vol. 43, no. 19, p. 4839, Oct. 2018.

[14] Z. Ge, Y. Xiao, T. Hao, W. Li, and M. Li, "Tb/s fast random bit generation based on a broadband random optoelectronic oscillator," *IEEE Photon. Technol. Lett.*, vol. 33, no. 22, pp. 1223–1226, Nov. 2021.

[15] B. Cui, G. Xia, X. Tang, F. Wang, Z. Jiang, Y. Zheng, F. Zhang, and Z. Wu, "Generation of chaotic signals with concealed time-delay signature based on a semiconductor laser under multi-path optical feedback," *IEEE Photon. J.*, vol. 14, no. 1, pp. 1–5, Feb. 2022.

[16] 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.

[17] S.-S. Li, X.-Z. Li, and S.-C. Chan, "Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation," *Opt. Lett.*, vol. 43, no. 19, p. 4751, Oct. 2018.

[18] J. Zhang, Y. Wang, L. Xue, J. Hou, B. Zhang, A. Wang, and M. Zhang, "Delay line length selection in generating fast random numbers with a chaotic laser," *Appl. Opt.*, vol. 51, no. 11, p. 1709, Apr. 2012.

[19] T. Yamazaki and A. Uchida, "Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers," *IEEE J. Sel. Topics Quantum Electron.*, vol. 19, no. 4, Jul. 2013, Art. no. 0600309.

[20] R. Takahashi, Y. Akizawa, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation," *Opt. Exp.*, vol. 22, no. 10, p. 11727, May 2014.

[21] 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, p. 1470, Jan. 2015.

[22] X.-Z. Li, S.-S. Li, J.-P. Zhuang, and S.-C. Chan, "Random bit generation at tunable rates using a chaotic semiconductor laser under distributed feedback," *Opt. Lett.*, vol. 40, no. 17, p. 3970, Sep. 2015.

[23] M. Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *Proc. Int. Workshop Fast Softw. Encryption*, vol. 4593, Mar. 2007, pp. 137–152.

[24] Y. Liu, C. Chen, D. D. Yang, Q. Li, and X. Li, "Fast true random number generator based on chaotic oscillation in self-feedback weakly coupled superlattices," *IEEE Access*, vol. 8, pp. 182693–182703, 2020.

[25] L. Wang, T. Zhao, D. Wang, D. Wu, L. Zhou, J. Wu, X. Liu, Y. Wang, and A. 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, pp. 1–13, Apr. 2017.

[26] Y. Guo, W. Liu, Y. Huang, Y. Sun, R. Zinsou, Y. He, and R. Zhang, "Fast physical random bit generation using a millimeter-wave white noise source," *Opt. Exp.*, vol. 30, no. 2, p. 3148, Jan. 2022.

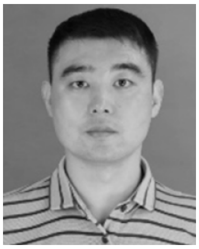
[27] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Opt. Exp.*, vol. 18, no. 23, p. 23584, Oct. 2010.

[28] Y. Xu, P. Lu, S. Mihailov, and X. Bao, "Real-time physical random bit generation at gbps based on random fiber lasers," *Opt. Lett.*, vol. 42, no. 23, p. 4796, Dec. 2017.

[29] 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.

[30] C. Ran, X. Tang, Z.-M. Wu, and G.-Q. Xia, "Dual-channel physical random bits generation by a master-slave vertical-cavity surface-emitting lasers chaotic system," *Laser Phys.*, vol. 28, no. 12, Sep. 2018, Art. no. 126202.

[31] H. Wu, J. Xiong, B. Han, Z. Wang, W. Zhang, X. Jia, and H. Liang, "Ultrahigh speed random bit generation based on Rayleigh feedback assisted ytterbium-doped random fiber laser," *Sci. China Technolog. Sci.*, vol. 64, no. 6, pp. 1295–1301, Jun. 2021.



BING CUI was born in Dengzhou, Henan, China, in 1984. He received the M.S. degree in applied mathematics from Northwest A&F University, Yangling, Shaanxi, China, in 2012, and the Ph.D. degree in applied mathematics from Southwest University, Chongqing, China, in 2023. He is currently a Lecturer with the School of Statistics and Mathematics, Henan Finance University. His current research mainly focuses on the physical random bit generator based on semiconductor lasers.

WENYAN YANG was born in Chifeng, China, in 1978. She received the M.Sc. degree in optics and the Ph.D. degree in applied mathematics from Southwest University, Chongqing, China, in 2005 and 2020, respectively. Her current research interest includes the nonlinear dynamics of semiconductor lasers.

ZAIFU JIANG was born in Jingmen, Hubei, China, in 1981. He received the M.Sc. degree in theoretical physics from Chongqing University, Chongqing, China, in 2007, and the Ph.D. degree in applied mathematics from Southwest University, Chongqing, in 2021. His main research focuses on the nonlinear dynamics of semiconductor lasers.

DIANZUO YUE was born in Tangshan, Hebei, China, in 1982. He received the M.Sc. degree in information processing and automation from Inner Mongolia University of Science and Technology, Baotou, China, in 2014, and the Ph.D. degree in applied mathematics from Southwest University, Chongqing, China, in 2021. He is currently an Associate Professor with the School of Mathematics and Information Science and Technology, Hebei Normal University of Science and Technology. His current research mainly focuses on the reservoir computing based on semiconductor lasers and its applications.

CHUNXIA HU was born in Zhoukou, China, in 1982. She received the M.Sc. degree in optics and the Ph.D. degree in applied mathematics from Southwest University, Chongqing, China, in 2008 and 2021, respectively. She is currently an Associate Professor with Chongqing College of Electronic Engineering. Her research interests include the nonlinear dynamics of semiconductor lasers and optical chaotic secure communication.