CHINESE OPTICS LETTERS

Vol. 21, No. 6 | June 2023

400 Gb/s physical random number generation based on deformed square self-chaotic lasers

Jiancheng Li (李建成)[1,2], Yali Li (李亚理)[1,2], Yunxiao Dong (董云晓)[1,2], Yuede Yang (杨跃德)[1,2], Jinlong Xiao (肖金龙)[1,2*], and Yongzhen Huang (黄永箴)[1,2]

[1] State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China

[2] Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing 100049, China

*Corresponding author: jlxiao@semi.ac.cn

Received January 23, 2023 | Accepted March 24, 2023 | Posted Online June 6, 2023

A circular-sided square microcavity laser etched a central hole has achieved chaos operation with a bandwidth of 20.8 GHz without external optical feedback or injection, in which the intensity probability distribution of a chaotic signal with a two-peak pattern was observed. Based on the self-chaotic microlaser, physical random numbers at 400 Gb/s were generated by extracting the four least significant bits without other complex post-processing methods. The solitary chaos laser and minimal post-processing have predicted a simpler and low-cost on-chip random number generator in the future.

Keywords: microcavity laser; self-chaos; physical random number generation.
DOI: 10.3788/COL202321.061901

1. Introduction

Random numbers play a critical role in Monte Carlo simulation, information cryptography, secure communications, and detection systems[1–7]. An ideal random bit sequence should be unpredictable, unrepeated, and statistically unbiased. In general, random number generation (RNG) can be divided into two classes. The first one is called pseudo-RNG, based on deterministic computer algorithms and initial seeds, which is widely used in modern digital electronic information systems[8]. Although pseudo-RNG has the merits of being fast and easy to implement, these random bit sequences can be solved and forecasted with a high-speed solver or by knowing the "seeds." The second one, physical RNG, is achieved by extracting randomness from natural stochastic phenomena, such as the thermal noise in resistors[9], the phase jitter in oscillators circuits[10], the stochastic switching in memristors[11], and vacuum state fluctuations[12]. However, limited by the intrinsic mechanisms of the physical process, the rate of RNG is only at the Mb/s level. The amplified spontaneous noise[13–16] and intrinsic optical non-linearity in random fiber lasers[17,18] were also investigated for high-rate random numbers generation, but complex systems were required.

In recent years, physical RNG based on optical chaos from a semiconductor laser, with random intensity and a large radio-frequency spectrum, has been widely researched. The first optical physical RNG of 1.7 Gb/s based on two optical-feedback chaotic lasers is demonstrated by 1-bit analog-to-digital transform with exclusive OR (XOR) processing[8]. Since then, various post-processing methods, such as multi-bit extraction[19–21], time-shift[22], and high-order derivative[23], were adopted to generate high-rate chaotic RNG. A chaotic bandwidth was also enhanced with three-cascaded semiconductor lasers for Tb/s level RNG[24]. Moreover, to improve the rate of RNG, parallel physical random bit generators were proposed by expanding bit-stream channels. Tang *et al.* reported a 1.12 Tb/s RNG by interleaving two sets of 0.56-Tb/s random bit stream from mutually coupled lasers[25]. Later, 2.24 Tb/s RNG with seven channels was demonstrated by Xiang *et al.*, consisting of three mutually coupled semiconductor lasers[26]. Li *et al.* demonstrated a Tb/s parallel RNG based on a single quarter-wavelength-shifted distributed feedback laser[27]. Real-time chaotic random number generators were demonstrated by using high-speed electronic devices or all-optical quantization[28-30].

The above-mentioned chaos sources were implemented using discrete devices by optical feedback and injection, which means a complex system and vulnerability to environmental influence. To simplify the system and enhance stability, integrated chaos lasers were developed. Based on a monolithic chaos laser integrated with a short external cavity, amplifiers, and a photodetector, Harayama *et al.* reported a nondeterministic RNG with a rate of 2.08 Gb/s[31]. Argyris *et al.* also implemented a 140-Gb/s random bit generator by using a photonic integrated circuit, including a distributed feedback laser, a phase section, a gain/absorption section, and a passive waveguide[32]. RNG at 500 Mb/s was demonstrated based on a distributed Bragg reflector (DBR) laser with a spiral long-delay on-chip optical feedback[33]. In addition, solitary spontaneous polarization chaos

induced by polarization mode competition was utilized to achieve 100 Gb/s RNG[34,35]. Cao *et al.* also reported ultrafast RNG with a broad area semiconductor laser under a large pulse operation[36]. Recently, a self-chaos phenomenon was first reported in a solitary circular-sided hexagonal microlaser based on dual-mode internal interaction[37]. Furthermore, a bandwidth-enhanced tri-mode self-chaotic microlaser was demonstrated based on photon–photon resonance[38]. These solitary self-chaotic lasers have the advantage of a simple fabrication process and no time-delayed signature induced by optical feedback or injection. In our prior work, 10 Gb/s random bit generation was obtained under a small chaos bandwidth[37]. Although RNG at 500 Gb/s was achieved based on bandwidth-enhanced tri-mode chaotic lasers, complex post-processing methods were required, including delay-difference and multiple least significant bits (LSBs) retaining[38].

In this Letter, a circular-sided square microlaser with an optimized size operates in a chaotic state without external permutation, which has a chaos radio-frequency (RF) bandwidth of 20.8 GHz and an intensity probability distribution with a two-peak structure. Based on the solitary self-chaotic microlaser, 400 Gb/s physical random numbers are generated with retaining 4-LSBs at 100 GSa/s sampling.

2. Experimental Setup

Figure 1 shows the schematic of fast physical random number generation based on a self-chaotic microcavity laser. First, the chaos light from a solitary self-chaotic microlaser is amplified by an erbium-doped fiber amplifier (EDFA) and filtered by an optical band-pass filter (OBPF). Then, a high-speed photodetector (PD, Finisar XPD2120RA, 50 GHz bandwidth) is utilized to convert optical chaos into an electrical domain. Finally, the electrical signal is quantized into binary digits via an 8-bit analog-to-digital converter (ADC). In this experiment, the 8-bit ADC is provided by a real-time oscilloscope (OSC, Tektronix DPO77002SX, 100 GSa/s with 33 GHz bandwidth, 8-bit vertical resolution). By discarding the most significant bits and retaining the multiple least significant bits, high-rate physical random numbers are generated, as described in the red dashed box in Fig. 1.

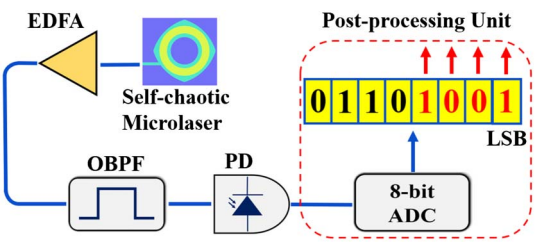

Fig. 1. Schematic of fast physical random number generation with retaining multiple least significant bits. EDFA, erbium-doped fiber amplifier; OBPF, optical band-pass filter; PD, photodetector; ADC, analog-to-digital converter; LSB, least significant bit.

3. Results

3.1. Self-chaotic characteristics of microlaser

A schematic diagram of the two-dimensional (2D) circular-sided square microcavity is shown in the inset of Fig. 2(a), in which the flat-side length $a = 20\ \mu m$, the circular-side deformation $\delta = 2.17\ \mu m$, the width of output waveguide $d = 1.5\ \mu m$, the shift of the output waveguide $h = 4\sqrt{2}\ \mu m$, the radius of the central hole $R_{in} = 6.5\ \mu m$, and the width of ring p-electrode $w = 3.5\ \mu m$ are used in the experiment. The manufacturing process for the microcavity lasers is the same as that described in Ref. [37]. The broadband chaotic light is generated by the self-chaotic microlaser based on the internal interaction of modes as in Refs. [37,38]. The chaos characteristics are first investigated by an optical spectrum analyzer (Yokogawa, AQ6370D, 0.02 nm resolution), an electrical spectrum analyzer (Rohde & Schwarz, FSW50), and a real-time oscilloscope before the RNG application. Figure 2(a) shows the power collected by a single-mode fiber (SMF) and the voltage applied versus the continuous-wave (CW) injection current at 289 K. The threshold current is 3 mA, and the maximum output power is 33 μW at 35 mA. By fitting the *V-I* curve, an 18 Ω serial resistance of the laser is obtained. When the injection current is 32 mA, the laser operates in a chaotic state with a broadened optical spectrum of around 1559 nm shown in Fig. 2(b). A corresponding chaotic RF spectrum is illustrated in Fig. 2(c). We can find that the signal curve is far from the noise floor represented by the black line in Fig. 2(c), and the energy is distributed over a very large range without obvious sharp peaks. By accumulating power from the DC to the frequency where 80% of the total energy is contained within, the calculated chaos standard bandwidth is about 20.8 GHz[39]. Figure 2(d) shows the irregular real-time intensity series at 32 mA with a 100 GSa/s sampling rate, and a two-peak structure of intensity distribution similar to that reported in Ref. [35] is observed in Fig. 2(e). Meanwhile, an autocorrelation function (ACF) curve is depicted in Fig. 2(f), and the overall ACF curve for 1 μs is displayed in the inset of Fig. 2(f). The ACF can rapidly decay within 0.8 ns and without peaks caused by fixed delayed feedback or injection[40–42]. The local peaks of the ACF curve below 0.4 ns are related to the residual high-frequency oscillation components, which is coincident with the poor flatness of the chaotic RF spectrum in Fig. 2(c). By optimizing mode intervals and mode numbers in subsequent microcavity designs, or by introducing external optical feedback or optical injection, these high-frequency oscillations may be suppressed.

3.2. RNG with minimal post-processing

The chaotic microcavity laser is utilized to generate random bits, as Fig. 1 shows. To eliminate the residual correlation and bias for RNG, an effective post-processing method is required for chaotic output waveform. Here, retaining multiple LSBs is conducted. Figure 3 shows the probability distribution histogram of the 50 million digitalized chaotic signals at 32 mA with LSBs ranging from 4 to 7. When 7 LSBs are selected, the probability

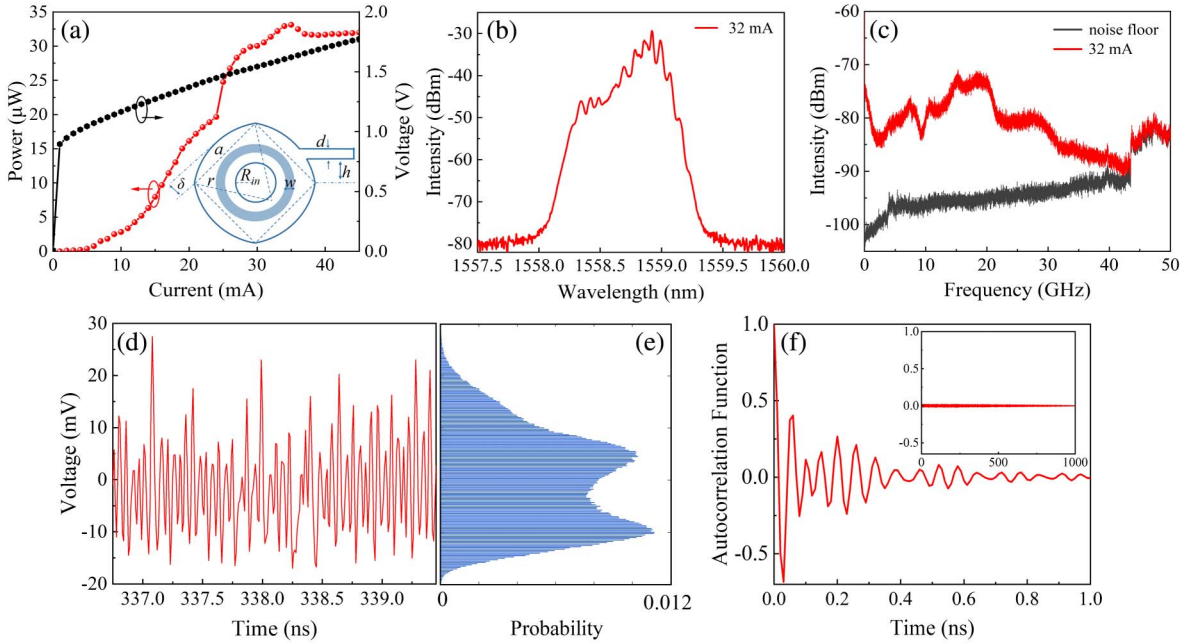

Fig. 2. (a) The output power and applied voltage versus the injection current. Inset in (a), schematic diagram of the 2D circular-sided square microcavity. (b) The optical spectrum, (c) the RF spectra, (d) the time series, (e) the intensity distribution of the time series, and (f) the autocorrelation function of the time signal for the chaos state at 32 mA. Inset in (f), overall ACF curve within 1 μs.

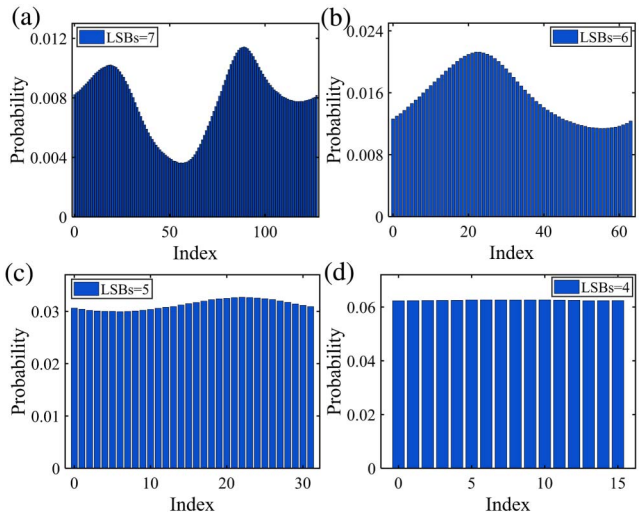

Fig. 3. Probability distribution histogram of the digitalized chaotic signal with (a) LSBs = 7, (b) LSBs = 6, (c) LSBs = 5, and (d) LSBs = 4.

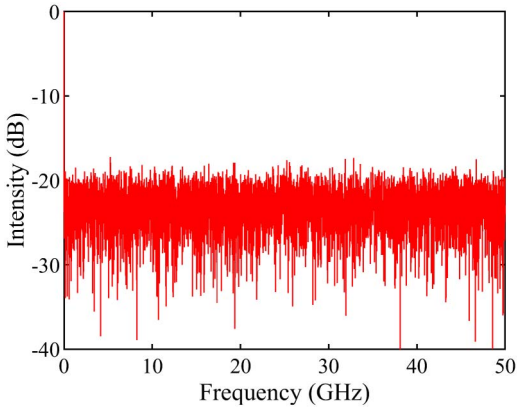

Fig. 4. RF spectrum of the recovered time series with retaining 4-LSBs.

for a different quantized index presents large fluctuation. With more most significant bits discarded, the uniformity is improved for LSBs = 6 and 5, as in Figs. 3(b) and 3(c), owing to the consequent logical "0" or "1" block removed. When four LSBs of each 8-bit sample are retained, an equal-probability histogram can be observed, as depicted in Fig. 3(d). The RF spectrum of the temporal signal recovered by digital-to-analog conversion with 4-LSBs binary digits is extracted by Fourier transform. As Fig. 4 shows, nearly equal intensity energy is distributed over a 50 GHz bandwidth, which indicates that discarding the most significant bits is equivalent to bandwidth enhancement[43].

To evaluate the randomness of the random bit sequence, statistical bias and autocorrelation functions are investigated with LSBs = 4. Here, the bias for an N-bit sequence is defined as $|p_N(1) - 0.5|$, where $p_N(1)$ represents the probability of "1" with N-bit binary numbers. For high-quality random number sequences, the bias should follow the Gaussian distribution $N(0, \sigma_b^2)$ with $\sigma_b = 0.5N^{-0.5}$. As Fig. 5(a) shows, the calculated bias remains below their three-standard-deviations ($3\sigma_b$) line, indicating that it is statistically unbiased[44]. The absolute value of the autocorrelation function of the 200-Mbits bit stream with the first 100 points intercepted is illustrated in Fig. 5(b), where

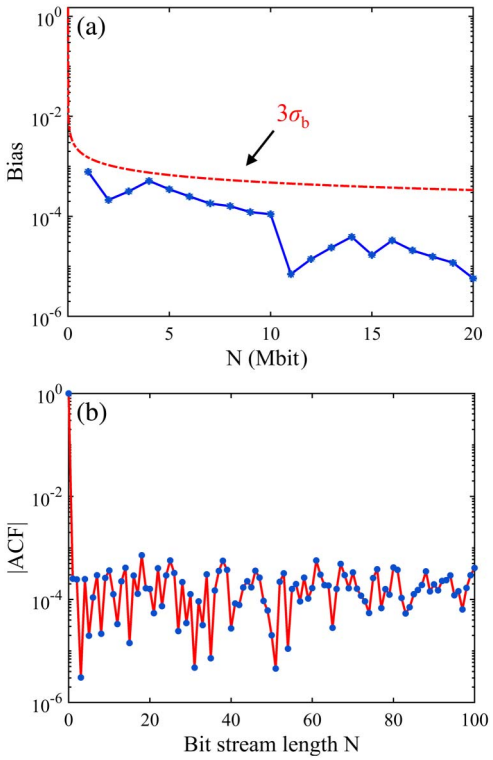

Fig. 5. (a) Statistical bias and (b) absolute autocorrelation function versus the sample size of the generated 400 Gb/s random bit stream. The first 100 points of the 200-Mbits autocorrelation coefficient are shown in (b).

Table 1. Results of the NIST SP 800-22 Statistical Tests for Random Bit Sequence.

Statistical Test	*P*-value	Proportion	Result
Frequency	0.24801	0.992	Success
Block frequency	0.00691	0.994	Success
Runs	0.04422	0.989	Success
Longest run	0.61423	0.992	Success
Rank	0.87399	0.986	Success
FFT	0.74790	0.987	Success
Nonoverlaping template	0.01959	0.994	Success
Overlapping template	0.12813	0.990	Success
Universal	0.36525	0.990	Success
Linear complexity	0.01046	0.989	Success
Serial	0.19798	0.988	Success
Approximate entropy	0.06049	0.987	Success
Cumulative sums	0.29109	0.992	Success
Random excursions	0.22801	0.989	Success
Random excursions variant	0.00961	0.992	Success

the correlation of adjacent bits has dramatically reduced, and the overall ACF is coincident with the background level.

The randomness of these generated random numbers is verified by the National Institute of Standards and Technology Special Publication (NIST SP) 800-22 statistical tests[45]. At the significance level $\alpha = 0.01$, successful tests require a proportion within 0.99 ± 0.0094932 and a *P*-value over 0.0001 for each item. For test items that produce multiple *P*-values and proportions, the worst case is selected. In this experiment, 1000 sequences of 1-Mbit data are set to the standard statistical test suite, and the results are shown in Table 1. The generated bits pass all NIST sub-tests, and RNG at 400 Gb/s (100 GSa/s × 4 bit) is achieved successfully. When the LSBs is more than 4, the generated bit stream cannot pass the NIST SP 800-22 statistical test due to poor randomness. Compared with the RNG system mentioned in Ref. [38], the new random bit generator has a high rate with a simpler configuration.

4. Conclusion

In conclusion, a self-chaotic deformed square microcavity laser was demonstrated with a 20.8-GHz chaotic bandwidth and distinctive dual-peak intensity probability distribution. By retaining 4-LSBs post-processing, a 400-Gb/s physical random bit sequence, which passed the NIST SP 800-22 statistical test of randomness, was generated based on a spontaneous chaotic microlaser. The new RNG system was significantly simplified due to monolithic chaos sources and simpler post-processing configurations.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Nos. 12274407, 61935018, 62122073, and 61874113) and the Strategic Priority Research Program, Chinese Academy of Sciences (No. XDB43000000).

References

1. S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer, 2007).
2. D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995).
3. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
4. H. Gao, A. Wang, L. Wang, Z. Jia, Y. Guo, Z. Gao, L. Yan, Y. Qin, and Y. Wang, "0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry–Perot lasers," Light Sci. Appl. **10**, 172 (2021).
5. X. Lin, R. Wang, S. Wang, Z.-Q. Yin, W. Chen, G.-C. Guo, and Z.-F. Han, "Certified randomness from untrusted sources and uncharacterized measurements," Phys. Rev. Lett. **129**, 050506 (2022).
6. M. Li, Y. Chen, Y. Song, C. Zeng, and X. Zhang, "DOE effect on BER performance in MSK space uplink chaotic optical communication," Chin. Opt. Lett. **18**, 070601 (2020).

7. D. Wu, L. Yang, X. Chen, Z. Li, and G. Wu, "Multi-channel pseudo-random coding single-photon ranging and imaging," Chin. Opt. Lett. **20**, 021202 (2022).
8. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**, 728 (2008).
9. C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I **47**, 615 (2000).
10. B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," IEEE Trans. Comput. **56**, 109 (2007).
11. G. Kim, J. H. In, Y. S. Kim, H. Rhee, W. Park, H. Song, J. Park, and K. M. Kim, "Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor," Nat. Commun. **12**, 2906 (2021).
12. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**, 711 (2010).
13. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**, 23584 (2010).
14. P. Li, K. Li, X. Guo, Y. Guo, Y. Liu, B. Xu, A. Bogris, K. A. Shore, and Y. Wang, "Parallel optical random bit generator," Opt. Lett. **44**, 2446 (2019).
15. G. Cao, L. Zhang, X. Huang, W. Hu, and X. Yang, "16.8 Tb/s true random number generator based on amplified spontaneous emission," IEEE Photon. Technol. Lett. **33**, 699 (2021).
16. 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. Express **30**, 3148 (2022).
17. F. Monet, J.-S. Boisvert, and R. Kashyap, "A simple high-speed random number generator with minimal post-processing using a random Raman fiber laser," Sci. Rep. **11**, 13182 (2021).
18. B. C. Lima and J. P. von der Weid, "Fast true random bit generation with an SOA-Based random fiber laser," IEEE Photon. Technol. Lett. **35**, 191 (2023).
19. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**, 024102 (2009).
20. 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. **41**, 388 (2016).
21. L. Zhang, B. Pan, G. Chen, L. Guo, D. Lu, L. Zhao, and W. Wang, "640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser," Sci. Rep. **7**, 45900 (2017).
22. A. Wang, Y. Yang, B. Wang, B. Zhang, L. Li, and Y. Wang, "Generation of wideband chaos with suppressed time-delay signature by delayed self-interference," Opt. Express **21**, 8701 (2013).
23. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**, 58 (2010).
24. R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," Opt. Express **23**, 1470 (2015).
25. X. Tang, Z.-M. Wu, J.-G. Wu, T. Deng, J.-J. Chen, L. Fan, Z.-Q. Zhong, and G.-Q. Xia, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," Opt. Express **23**, 33130 (2015).
26. S. Xiang, B. Wang, Y. Wang, Y. Han, A. Wen, and Y. Hao, "2.24-Tb/s physical random bit generation with minimal post-processing based on chaotic semiconductor lasers network," J. Light. Technol. **37**, 3987 (2019).
27. Q. Cai, P. Li, Y. Shi, Z. Jia, L. Ma, B. Xu, X. Chen, K. A. Shore, and Y. Wang, "Tbps parallel random number generation based on a single quarter-wavelength-shifted DFB laser," Opt. Laser Technol. **162**, 109273 (2023).
28. A. Wang, P. Li, J. Zhang, J. Zhang, L. Li, and Y. Wang, "4.5 Gbps high-speed real-time physical random bit generator," Opt. Express **21**, 20452 (2013).
29. P. Li, Y. Guo, Y. Guo, Y. Fan, X. Guo, X. Liu, K. A. Shore, E. Dubrova, B. Xu, Y. Wang, and A. Wang, "Self-balanced real-time photonic scheme for ultrafast random number generation," APL Photonics **3**, 061301 (2018).
30. Y. Guo, Q. Cai, P. Li, R. Zhang, B. Xu, K. A. Shore, and Y. Wang, "Ultrafast and real-time physical random bit extraction with all-optical quantization," Adv. Photonics **4**, 035001 (2022).
31. 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 **83**, 031803 (2011).
32. S. D. Apostolos Argyris, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," Opt. Express **18**, 18763 (2010).
33. G. Verschaffelt, M. Khoder, and G. Van der Sande, "Random number generator based on an integrated laser with on-chip optical feedback," Chaos **27**, 114310 (2017).
34. M. Virte, K. Panajotov, H. Thienpont, and M. Sciamanna, "Deterministic polarization chaos from a laser diode," Nat. Photonics **7**, 60 (2013).
35. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," Opt. Express **22**, 17271 (2014).
36. K. Kim, S. Bittner, Y. Zeng, S. Guazzotti, O. Hess, Q. J. Wang, and H. Cao, "Massively parallel ultrafast random bit generation with a chip-scale laser," Science **371**, 948 (2021).
37. C.-G. Ma, J.-L. Xiao, Z.-X. Xiao, Y.-D. Yang, and Y.-Z. Huang, "Chaotic microlasers caused by internal mode interaction for random number generation," Light Sci. Appl. **11**, 187 (2022).
38. J.-C. Li, J.-L. Xiao, Y.-D. Yang, and Y.-Z. Huang, "Random bit generation based on self-chaotic microlasers with enhanced chaotic bandwidth," arXiv: 2301.00111 (2022).
39. F. Y. Lin and J. M. Liu, "Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback," Opt. Commun. **221**, 173 (2003).
40. Y.-Z. Hao, C.-G. Ma, Z.-Z. Shen, J.-C. Li, J.-L. Xiao, Y.-D. Yang, and Y.-Z. Huang, "Comparison of single- and dual-mode lasing states of a hybrid-cavity laser under optical feedback," Opt. Lett. **46**, 2115 (2021).
41. C. Ma, J. Wu, J. Xiao, Y. Huang, Y. Li, Y. Yang, and Y. Huang, "Wideband chaos generation based on a dual-mode microsquare laser with optical feedback," Chin. Opt. Lett. **19**, 111401 (2021).
42. Y.-L. Li, C.-G. Ma, J.-L. Xiao, T. Wang, J.-L. Wu, Y.-D. Yang, and Y.-Z. Huang, "Wideband chaotic tri-mode microlasers with optical feedback," Opt. Express **30**, 2122 (2022).
43. A. Wang, L. Wang, P. Li, and Y. Wang, "Minimal-post-processing 320-Gbps true random bit generation using physical white chaos," Opt. Express **25**, 3153 (2017).
44. V. N. Chizhevsky, "Symmetrization of single-sided or nonsymmetrical distributions: the way to enhance a generation rate of random bits from a physical source of randomness," Phys. Rev. E **82**, 050101 (2010).
45. https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software.