Real-time online photonic random number generation

Li, Pu; Zhang, Jianguo; Sang, Luxiao; Liu, Xianglian; Guo, Yanqiang; Guo, Xiaomin; Wang, Anbang; Shore, K. Alan; Wang, Yuncai

Optics Letters

DOI:
10.1364/OL.42.002699

Published: 15/07/2017

Peer reviewed version

Real-time On-line Photonic Random Number Generation

PU LI,[1,2,3] JIANGUO ZHANG,[1,2] LUXIAO SANG,[1,2] XIANGLIAN LIU,[1,2] YANQIANG GUO,[1,2] XIAOMIN GUO,[1,2] ANBANG WANG,[1,2,*] K. ALAN SHORE,[3] YUNCAI WANG [1,2]

[1] *Key Lab. of Advanced Transducers & Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan 030024, China*
[2] *Institute of Optoelectronic Engineering, College of Physics & Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China*
[3] *School of Electronic Engineering, Bangor University, Wales LL57 1UT, U.K.*
**Corresponding author: wanganbang@tyut.edu.cn*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

We present a real-time scheme for ultrafast random number extraction from a broadband photonic entropy source. Ultralow jitter mode-locked pulses are used to sample the stochastic intensity fluctuations of the entropy source in the optical domain. A discrete self-delay comparison technology is exploited to quantize the sampled pulses into continuous random number streams directly. This scheme is bias-free and both eliminates the electronic jitter bottleneck confronted by currently available physical random number generators and has no need for threshold-tuning and post-processing. To demonstrate its feasibility, we perform a proof of principle experiment using an optically injected chaotic laser diode. Random number streams at up to 7 Gb/s with verified randomness were thereby successfully extracted in real time. With the provision of a photonic entropy source with sufficient bandwidth, the present approach is expected to provide random number generation rates of several tens of Gb/s. © 2017 Optical Society of America

OCIS codes: *(190.3100) Instabilities and chaos; (140.5960) Semiconductor lasers; (140.1540) Chaos; (060.4785) Optical security and encryption.*

http://dx.doi.org/10.1364/OL.99.099999

In order to achieve perfectly secure communications, use should be made of the well-known 'one-time-pad' cipher. According to this cipher, random numbers (RNs) used as cryptographic keys must have at least the same length as the encrypted messages and never be reused; distribution of such keys must also be made without disclosure to unauthorised users. With great improvements in secure key distribution [1-2], the main bottleneck impeding the implementation of this perfect security in current large-capacity communications is the need to generate real-time and ultrafast RNs.

Since the pioneering work by Uchida et al. in 2008 [3], utilizing broadband photonic entropy sources to generate ultrafast physical RNs has been viewed as a promising solution to this problem [4-5]. A considerable number of schemes have been proposed to extract RNs from amplified spontaneous emission [6-7], laser phase noise [8-9], and laser chaos [10-21]. Most such schemes require offline processing the stored chaotic time series and so do not function in real time.

To a great extent, the reason why these schemes are so difficult to be put into practice lies in their use of essentially similar methodology: (i) harvesting raw random numbers by electrically sampling the continuous-time random signal via 1-bit or multi-bit ADCs triggered by an external RF clock; (ii) post-processing the raw random numbers to eliminate their residual correlation and bias. Unfortunately, just the aperture jitter from the RF clock commonly limits the actual operation response of electrical ADCs to a few GHz [22]. Also, the electronic jitter in the harvesting mechanism greatly deteriorates the undesirable residual correlation and bias stemming from the entropy sources. Both imperfections in the entropy source and the harvesting mechanism cause the further necessity of the post-processing within the available schemes. The introduction of digital post-processes not only exacerbates the technical hurdles such as the synchronization difficulty, but sacrifices timeliness of response due to the excess computation time.

Utilizing parallel techniques can help reduce the pressures arising from the use of electronic components [23-25], but not solve the aforementioned issues. A 12.8 Gb/s RN throughput was obtained by implementing more than one hundred 100 Mb/s uncoupled Boolean chaos networks in parallel on a field programmable gate array (FPGA) in [23]. In [24-25], the throughput of 4 and 21.1 Gb/s were obtained by retaining several

significant bits of the full 12 bits as the multiple parallel outputs through a sophisticated FPGA, but the real-time rates in each output channel are still limited to 1 and 3.6 Gb/s, respectively.

Recently, we demonstrated that using optical sampling could overcome the electronic jitter bottleneck [26], but the second issue still exists: the scheme in this work also has to do offline single-end threshold comparison and XOR post-process to the stored chaotic pulse train using a sophisticated oscilloscope for final random numbers with verified randomness. Moreover, two additional requirements further limit its performance: (i) The threshold level need be continuously and carefully tuned to achieve the unbiased random numbers; (ii) The optical sampling period must be not the integer multiple of the trip time of the external feedback cavity to suppress the weak periodicity of the optical feedback chaotic laser diode (LD).

Here, we present a photonic scheme for real-time extraction of ultrafast physical RNs. Through all-optically sampling the broadband entropy signal using ultralow jitter mode-locked pulses, this scheme exploits a discrete self-delay comparison technology to continuously quantize the sampled stochastic pulses into high-quality RNs. With no requirement for post-processing and threshold-tuning, this method both overcomes the technical impediments induced by the electronic jitter and is bias-free from the imperfections in the photonic entropy sources and environmental fluctuations.

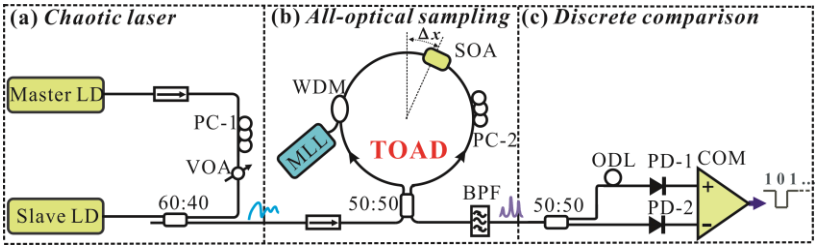

FIG. 1. Schematic of the proof of principle experiment. LD, laser diode; PC-1, PC-2, polarization controllers; VOA, variable optical attenuators; 60:40, 50:50, 60:40 and 50:50 optical couplers; MLL, mode-locked laser; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; BPF, optical band-pass filter; ODL, optical delay line; PD-1, PD-2, photodetectors; COM, comparator.

The feasibility of the proposed method is confirmed by a proof of principle experiment using an optically injected chaotic LD. As depicted in Fig. 1, the experimental setup contains three elements: (a) chaotic laser, (b) all-optical sampling and (c) discrete self-delay comparison. The optically injected chaotic laser is a master-slave configuration constructed by two DFB LDs, which are biased at the same current of 37.4 mA, but stabilized at different wavelengths of 1553.72 nm and 1553.76 nm, forming a 5 GHz frequency detuning. Setting the injection strength from the master to slave LD at 3.6 % with a variable attenuator (VOA), we can obtain the chaotic output at the 60:40 optical coupler.

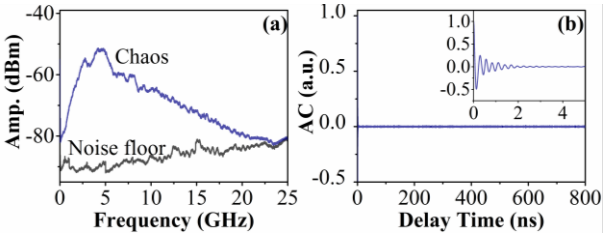

FIG. 2. Characteristics of the chaotic laser. (a) RF spectrum of the chaotic laser and (b) its autocorrelation (AC) function. The inset in Fig. 2(b) is its partial enlargement from 0 to 5 ns.

Figure 2 shows the measured RF spectrum and autocorrelation (AC) function of the chaotic signal, recorded by a 26.5 GHz RF spectrum analyzer (Agilent N9020A, 3 MHz RBW, 3 KHz VBW) and a 36 GHz oscilloscope (Lecroy LabMaster10-36Zi, 80 GSa/s Sampling Rate) via a 45 GHz photodetector (PD, U2T XPDV2120RA), respectively. It is clear that the chaos has a larger signal level than the noise floor and a bandwidth about 7.4 GHz. More importantly, it should be noted from the associated AC function with a delta-profile that the chaotic signal has no redundant correlation, unlike the optical feedback chaotic LD. Both features basically guarantee the generation of fast and high-quality RNs.

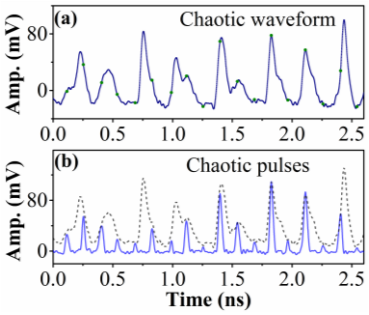

FIG. 3. All-optical sampling characteristics. (a) Continuous-time chaotic waveform to be sampled and (b) Discrete-time chaotic pulses after the all-optical sampling unit.

The all-optical sampling to the chaotic laser is executed using a terahertz optical asymmetric demultiplexer (TOAD) constructed by placing a nonlinear semiconductor optical amplifier (SOA) asymmetrically within a fiber loop mirror, as shown in Fig. 1(b). Having been fed into the TOAD via a 50:50 optical coupler, the chaotic light is divided into two equal parts in the clockwise (CW) and counterclockwise (CCW) direction. Then, a clock pulse train from the mode-locked laser (MLL) enters the TOAD via a WDM coupler (WDM), which periodically switches the TOAD gate so that the chaotic light will be sampled at the clocking rate. The sampled chaotic pulses are finally separated by a band-pass filter (BPF) near the output port of TOAD.

In the experiment, the SOA (Kamelian, SOA-NL-L1-C-FA) with a gain recovery time of 25 ps and a small-signal gain of 26 dB is biased at 300 mA and stabilized at a peak gain wavelength of 1550 nm. The clocking rate and wavelength of the MLL (Pritel, UOC-05-14G-E) are set at 7 GHz and 1551 nm respectively; the timing jitter is less than 50 fs. The BPF works at a center wavelength of 1553.8 nm with a 3-dB bandwidth of 0.2 nm, corresponding to that of the sampled output, so the sampled output can be separated from the clock and ASE noise. Figure 3 is the recorded chaotic temporal waveforms before and after the all-optical sampling procedure. The sampling window is set to 36 ps. Due to the ultralow jitter scaling from RF to optical clocks, a high-fidelity sampling result can be observed by comparing Fig. 3(a) with Fig. 3(b) that the peaks of the sampled chaotic pulses perfectly matches the analog chaotic envelope.

Finally, a discrete self-delay comparison is used to digitize the sampled chaotic pulse train to a RN stream and thereby efficiently avoid any bias. As shown in Fig. 1(c), the chaotic pulse train is first equally split into two paths with a relative time delay by the other 50: 50 optical coupler (50:50), and then enters into a differential latched comparator (COM, Hittite HMC675LP3E, 10GHz equivalent input bandwidth) via two identical 45 GHz photodetectors (PD-1 and PD-2), respectively. The digital RN stream is obtained at the output port of the COM: the output is a "0" level when the chaotic pulse at the "+" input port of the COM is larger than the self-delayed one at the "-"input port, and "1" otherwise. Fig. 4(a) shows the measured waveform of the final 7 Gb/s RN stream. The calculated bias of the generated RNs with different sizes m=1, 2, ... , 16 Mbit is shown in Fig. 4(b), while Fig. 4(c) is the normalized AC function of the RN stream where m= 1 Mbit. Both of the bias and AC function are estimated using the normal distribution estimation $N(0, \sigma^2)$. It can be seen that both the bias and AC coefficient always are below the associated three-standard-deviation σ [note: $3\sigma_{bias}=3m^{-1/2}/2$ and $3\sigma_{AC}=3m^{-1/2}$]. That indicates the RNs can be statistically viewed to be unbiased and independent. It is noted that polarization maintaining fibers are used for all the optical fiber components to ensure the stability of the comparison process.

More stringent randomness verification is performed by the statistical test suite of the NIST SP800-22 [27], which is widely accepted to be the benchmark in secure communications. The tests contain 15 items shown along the horizontal axis in Fig. 5. All the tests are made using 1000 samples of 1 million bits with a significance level α=0.01. It is noted that the RNs are obtained by coding the real-time random waveform in the way shown in Fig. 4(a). In each test, a p-value is calculated. The passing criteria include two aspects: (i) the proportion of the tested RNs satisfying condition for the p-value larger than α should be in the confidence interval of 99% ± 0.94392%; (ii) the P-value, the uniformity of the p-values, should be larger than the failure level of 0.0001. From Fig. 5, it can be confirmed the 7 Gb/s RNs can successfully pass all the NIST tests.

The core in the discrete self-delay comparison to guarantee that the extracted RNs are bias-free is the selection of the relative time delay, controlled by an optical delay line (ODL). Two requirements must be satisfied: (i) The delay must be a high-order integer multiple of the clock period; (ii) The AC coefficient of the chaotic pulses at the delay should be close to zero, which indicates a statistically insignificant correlation. Based on extensive experiments, we get an empirical criterion for the AC coefficient, which should be in the range of ±0.007. In the experiment, we set the delay be 200 μs where the AC coefficient is nearly zero as shown in the inset of Fig. 6(a), which is the AC curve of the sampled chaotic pulse train $A[n]$ with a size of 1.6 million data. It can be shown mathematically that when two independent signals obey the same distribution, their differential signal will have a highly symmetric distribution with a mean value of 0. This is supported by comparing the normalized histogram between $A[n]$ and the difference of $A[n]$ and its delay $A[n+n_\tau]$, as respectively shown in Figs. 6(b) and 6(c). After calculation, an 0/1 bias of about 0.0053% is obtained for the difference $A[n]$ - $A[n+n_\tau]$.

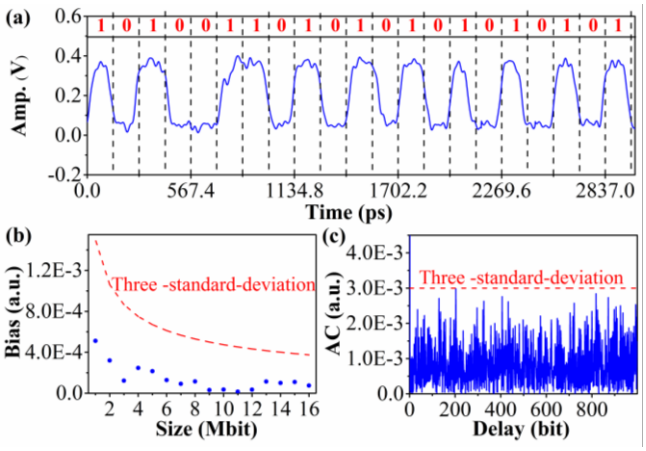

FIG. 4. (a) Temporal waveform of the 7 Gb/s RN stream, (b) Bias versus the size m=1, ..., 16 Mbit of the RN stream, and (c) Autocorrelation (AC) curve of the RN stream with a size of m=1 Mbit. It is noted that the coded RNs are depicted in the strip above the signal trace in Fig. 4(a).

We discuss the physical limit in the real-time rate in the current experiment system. In our method, the RN rate is determined by the clocking rate of the MLL at the TOAD sampling gate. The gain recovery time of the nonlinear SOA is below 25 ps, so the response rate of our system can be tuned at least to 40 Gb/s. However, due to the limited 7.4 GHz bandwidth of the optically injected chaotic laser in our proof of principle experiment, the maximum generation rate with verified randomness is just 7 Gb/s. Higher rates of RNs may be obtained by using bandwidth-enhanced chaotic entropy sources such as cascaded semiconductor lasers [19] or fiber ring resonators [28-29]. The current system reported here may be seen to be rather complex. In particular, it is apparent that two DFB LDs, a VOA and a PC are involved in generating the laser chaos. Significant simplification of this aspect can be achieved by the use of photonic integration technology which has already been utilized for laser chaos sources [30-31].

In conclusion, a novel photonic extraction approach for real-time and ultrafast physical RNs has been demonstrated. The scheme obviates the need for post-processes, solves the electronic jitter bottleneck and is free from bias due to the imperfections in the photonic entropy source. Continuous RN streams with a rate up to 7 Gb/s was successfully obtained in the proof of principle experiment. Higher real-time rates of order 40 Gb/s is feasible by using chaotic lasers with enhanced bandwidth.

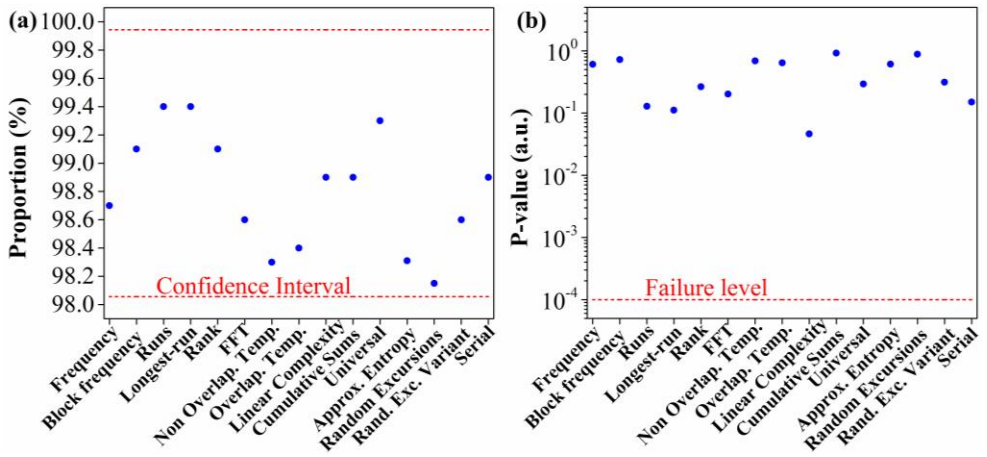

FIG. 5. Typical results of the NIST statistical tests. (a) Proportion of the tested RNs, which should be in the confidence interval of 99% ± 0.94392%. (b) P-value, which should be larger than the failure level of 0.0001.

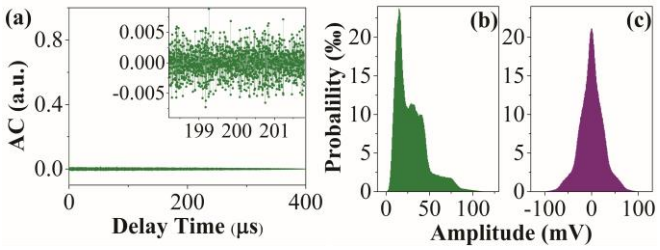

FIG. 6. (a) Autocorrelation (AC) curve and (b) Normalized histogram of the chaotic pulses $A[n]$, and (c) Normalized distribution of the difference between $A[n]$ and its delay $A[n+n_\tau]$. The inset in Fig. 6(a) is its partial enlargement from 199 to 201 μs.

Funding. National Natural Science Foundation of China (NSFC) (61505137, 51404165, 61405138, 61475111, 61527819 and 61505136); Natural Science Foundation of Shanxi (2015021088); Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (2015122); Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi (OIT).

Acknowledgment. We thank the reviewers for their valuable suggestions.

References

1. H. K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
2. K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, Phys. Rev. Lett. **108**, 070602 (2012).
3. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat. Photonics **2**, 728 (2008).
4. T. E. Murphy and R. Roy, Nat. Photonics **2**, 714 (2008).
5. M. Sciamanna and K. A. Shore, Nat. Photonics **9**,151 (2015).
6. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).
7. A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, J. Lightwave Technol. **30**, 1329–1334 (2012).
8. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
9. J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, Opt. Express **24**, 27475 (2016).
10. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
11. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photonics **4**, 58 (2010).
12. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, IEEE J. Quantum Electron. **49**, 910 (2013).
13. A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, Opt. Express **21**, 20452 (2013).
14. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, Opt. Express **20**, 28603 (2012).
15. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express 18, 18763 (2010).
16. X. Z. Li and S. C. Chan, Opt. Lett. **37**, 2163 (2012).
17. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, Opt. Express **22**, 17271 (2014).
18. N. Q. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, Opt. Express **22**, 6634 (2014).
19. R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, Opt. Express **23**, 1470 (2015).
20. T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, Opt. Lett. **41**, 388 (2016).
21. X. Tang, Z.M. Wu, J.G. Wu, T. Deng, J.J. Chen, L. Fan, Z. Q. Zhong, and G.Q. Xia, Opt. Express **23**, 33130 (2015)
22. R. Walden, in *Wiley Encyclopedia of Computer Science and Engineering* (Wiley, 2008), p. 126.
23. D. P. Rosin, D. Rontani, and D. J. Gauthier, Phys. Rev. E **87**, 040902 (2013).
24. S. Shinohara, K. Arai, P. Davis, S.Sunada, and T. Harayama, Opt. Express **25**, 6461 (2017).
25. K. Ugajin, Y. Terashima, K. Iwakawa, A. Uchida, T. Harayama, K.Yoshimura, and M. Inubushi, Opt. Express **25**, 6511 (2017).
26. P. Li, Y. Y. Sun, X. L. Liu, X. G. Yi, J. G. Zhang, X. M. Guo, Y. Q. Guo, and Y. C. Wang, Opt. Lett. **41**, 3347(2016).
27. http://csrc.nist.gov/groups/ST/toolkit/rng/index.html
28. A. Wang, Y. Wang, Y. Yang, M. Zhang, H. Xu, and B. Wang, Appl. Phys. Lett. **102**, 031112 (2013).
29. Y. Hong, X. Chen, P. S. Spencer, and K. A. Shore, IEEE J. Quantum Electron. **51**, 1200106 (2015).
30. A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, Phys. Rev. Lett. **100**, 194101 (2009).

31. J. G.Wu, L.. J. Zhao, Z. M. Wu, D. Lu, X. Tang, Z. Q. Zhong, and G. Q. Xia, Opt. Express **21**, 23358 (2013).

Full References

1. H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604(2014).
2. K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," Phys. Rev. Lett. **108**(7), 070602 (2012).
3. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**(12), 728–732 (2008).
4. T. E. Murphy and R. Roy, "Chaotic lasers: The world's fastest dice," Nat. Photonics **2**(12), 714 - 715 (2008).
5. M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," Nat. Photonics **9**(3),151-162 (2015).
6. 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**(23), 23584–23597 (2010).
7. 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. Lightwave Technol. **30**(9), 1329–1334 (2012).
8. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**(3), 312–314 (2010).
9. J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation," Opt. Express **24**(24), 27475–27481 (2016).
10. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**(2), 024102 (2009).
11. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).
12. 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. **49**(11), 910–918 (2013).
13. A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, "4.5 Gbps high-speed real-time physical random bit generator" Opt. Express **21**(17), 20452-20462(2013).
14. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, "Fast random bits generation based on a single chaotic semiconductor ring laser," Opt. Express **20**(27), 28603–28613 (2012).
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. Express **18**(18), 18763–18768 (2010).
16. X. Z. Li and S. C. Chan, "Random bit generation using an optically injected semiconductor laser in chaos with oversampling," Opt. Lett. **37**(11), 2163–2165 (2012).
17. M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," Opt. Express **22**(14), 17271-17280(2014).
18. N. Q. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan," Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," Opt. Express **22**(6), 6634-6646 (2014).
19. 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**(2), 1470-1490(2015).
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**(2), 388–391 (2016).
21. 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**(26), 33130-33141 (2015)
22. R. Walden, "Analog-to-digital conversion in the early twenty-first century," in Wiley Encyclopedia of Computer Science and Engineering (Wiley, 2008), pp. 126–138.
23. D. P. Rosin, D. Rontani, and D. J. Gauthier, "Ultrafast physical generation of random numbers using hybrid Boolean networks," Phys. Rev. E **87**(4), 040902 (2013).
24. S. Shinohara, K. Arai, P. Davis, S.Sunada, and T. Harayama, "Chaotic laser based physical random bit streaming system with a computer application interface," Opt. Express **25**(6), 6461-6474 (2017).
25. 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. Express **25**(6), 6511-6523 (2017).
26. P. Li, Y. Y. Sun, X. L. Liu, X. G. Yi, J. G. Zhang, X. M. Guo, Y. Q. Guo, and Y. C. Wang, "Fully photonics-based physical random bit generator," Opt. Lett. **41**(14), 3347-3350(2016).
27. http://csrc.nist.gov/groups/ST/toolkit/rng/index.html
28. A. Wang, Y. Wang, Y. Yang, M. Zhang, H. Xu, and B. Wang, "Generation of flat-spectrum wideband chaos by fiber ring resonator," Appl. Phys. Lett. **102**(3), 031112 (2013).
29. Y. Hong, X. Chen, P. S. Spencer, and K. A. Shore, "Enhanced Flat Broadband Optical Chaos Using Low-Cost VCSEL and Fiber Ring Resonator," IEEE J. Quantum Electron. **51**(3), 1200106 (2015).
30. A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," Phys. Rev. Lett. **100**(19), 194101 (2009).
31. J. G.Wu, L.. J. Zhao, Z. M. Wu, D. Lu, X. Tang, Z. Q. Zhong, and G. Q. Xia, "Direct generation of broadband chaos by a monolithic integrated semiconductor laser chip," Opt. Express **21**(20), 23358–23364 (2013).