Optics EXPRESS

Minimal-post-processing 320-Gbps true random bit generation using physical white chaos

ANBANG WANG,[1,2,*] LONGSHENG WANG,[1,2] PU LI,[1,2] AND YUNCAI WANG[1,2]

[1]*Key Lab of Advanced Transducers and Intelligent Control System, Ministry of Education & Shanxi Province, Taiyuan 030024, China*
[2]*College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China*
**wanganbang@tyut.edu.cn*

Abstract: Chaotic external-cavity semiconductor laser (ECL) is a promising entropy source for generation of high-speed physical random bits or digital keys. The rate and randomness is unfortunately limited by laser relaxation oscillation and external-cavity resonance, and is usually improved by complicated post processing. Here, we propose using a physical broadband white chaos generated by optical heterodyning of two ECLs as entropy source to construct high-speed random bit generation (RBG) with minimal post processing. The optical heterodyne chaos not only has a white spectrum without signature of relaxation oscillation and external-cavity resonance but also has a symmetric amplitude distribution. Thus, after quantization with a multi-bit analog-digital-convertor (ADC), random bits can be obtained by extracting several least significant bits (LSBs) without any other processing. In experiments, a white chaos with a 3-dB bandwidth of 16.7 GHz is generated. Its entropy rate is estimated as 16 Gbps by single-bit quantization which means a spectrum efficiency of 96%. With quantization using an 8-bit ADC, 320-Gbps physical RBG is achieved by directly extracting 4 LSBs at 80-GHz sampling rate.

OCIS codes: (140.1540) Chaos; (060.2840) Heterodyne; (140.5960) Semiconductor lasers; (190.7110) Ultrafast nonlinear optics; (060.4785) Optical security and encryption.

References and links

1. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).
2. D. R. Stinson, *Cryptography*: *Theory and Practice* (CRC Press, 1995).
3. I. Kanter, M. Butkovski, Y. Peleg, M. Zigzag, Y. Aviad, I. Reidler, M. Rosenbluh, and W. Kinzel, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," Opt. Express **18**(17), 18292–18302 (2010).
4. 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).
5. T. E. Murphy and R. Roy, "Chaotic lasers: The world's fastest dice," Nat. Photonics **2**(12), 714–715 (2008).
6. M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," Nat. Photonics **9**(3), 151–162 (2015).
7. 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).
8. Y. H. Hong, P. S. Spencer, and K. A. Shore, "Enhancement of chaotic signal bandwidth in vertical-cavity surface-emitting lasers with optical injection," J. Opt. Soc. Am. B **29**(3), 415–419 (2012).
9. A. B. Wang, Y. C. Wang, Y. B. Yang, M. J. Zhang, H. Xu, and B. J. Wang, "Generation of flat-spectrum wideband chaos by fiber ring resonator," Appl. Phys. Lett. **102**(3), 031112 (2013).
10. 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).
11. 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).
12. 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).
13. 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. **40**(17), 3970–3973 (2015).

#285586 https://doi.org/10.1364/OE.25.003153
Journal © 2017 Received 27 Jan 2017; accepted 1 Feb 2017; published 6 Feb 2017

14. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, “An optical ultrafast random bit generator,” Nat. Photonics **4**(1), 58–61 (2010).
15. N. 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).
16. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, “Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers,” Opt. Express **18**(6), 5512–5524 (2010).
17. Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Araiet, K. Yoshimura, and P. Davis, “Fast Random Number Generation With Bandwidth-Enhanced Chaotic Semiconductor Lasers at 8×50 Gb/s,” IEEE Photonics Technol. Lett. **24**(12), 1042–1044 (2012).
18. 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).
19. X. Z. Li and S. C. Chan, “Heterodyne random bit generation using an optically injected semiconductor laser in chaos,” IEEE J. Quantum Electron. **49**(10), 829–838 (2013).
20. 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).
21. D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, “Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback,” Opt. Lett. **32**(20), 2960–2962 (2007).
22. S. S. Li, Q. Liu, and S. C. Chan, “Distributed feedbacks for time-delay signature suppression of chaos generated from a semiconductor laser,” IEEE Photon. J. **4**(5), 1930–1935 (2012).
23. 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**(7), 8701–8710 (2013).
24. L. Hong, Y. H. Hong, and K. Alan Shore, “Experimental study of time-delay signatures in vertical-cavity surface-emitting lasers subject to double-cavity polarization-rotated optical feedback,” J. Lightwave Technol. **32**(9), 1829–1836 (2014).
25. N. Oliver, M. Soriano, D. 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).
26. C. R. 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).
27. A. B. Wang, B. J. Wang, L. Li, Y. C. Wang, and K. Alan Shore, “Optical heterodyne generation of high-dimensional and broadband white chaos,” IEEE J. Sel. Top. Quantum Electron. **21**(6), 531–540 (2015).
28. J. P. Eckmann and D. Ruelle, “Fundamental limitations for estimating dimensions and Lyapunov exponents in dynamical systems,” Physica D **56**(2), 185–187 (1992).
29. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dary, and S. Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800–22, Revision 1a (2010).
30. X. Fang, B. Wetzel, J. M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, “Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources,” IEEE Trans. Circuits Syst. I **61**(3), 888–901 (2014).

1. Introduction

Fast physical random bit generation (RBG), used to supply digital key, is of vital importance to information security of current high-speed optical communication [1–4]. In recent years, physical RBG based on chaotic external-cavity semiconductor lasers (ECLs) has attracted intensive attention because the generation speed can readily exceed one gigabit per second (Gbps) [5,6]. The first experimental demonstration achieved 1.7-Gbps random bit sequence by single-bit extraction, which uses a 1-bit analog-to-digital converter (ADC) to converts a sampling point of chaotic light into a digital bit 0 or 1 [7]. Recently, the entropy rate has been increased by enhancing the bandwidth of laser chaos with additional optical injection [8,9], for instance, 20-Gbps RBG was achieved using three cascaded semiconductor lasers [10]. More interestingly, the rate of RBG can be greatly improved to hundreds of Gbps and even over Tbps by using multi-bit extraction method, in which each sampling point is converted to several digital bits by using a multi-bit ADC [10–20].

In the multi-bit extraction, post processing is required to improve randomness of generated bits. Otherwise, only binary output from a few least significant bits (LSBs) of ADC can be selected as random bits which can pass randomness tests, due to ECL’s randomness defects including sharp spectrum, asymmetrical distribution, and time-delay signature. Many post-processing methods have been developed, which can mainly be classified into three types: derivative [11–15], time-shift XOR [10,16–19], and over-resolution extraction

[14,15,20]. However, the post-processing methods become more complicated for generation rate higher than one hundred Gbps. For example, demonstrated by Kanter *et al*., first-order derivative post processing obtained 12.5-Gbps (5 LSBs retained × 2.5 GHz sampling rate) random bits from a chaotic ECL [11]; by contrast, achieving 300 Gbps (15 LSBs × 20 GHz) required 16th-order derivative [14]. Note that, in the latter work the number of LSBs retained is larger than the 8-bit resolution of ADC used. This actually is another post-processing method called over-resolution extraction which involves a processing of increasing the resolution of sampling values by introducing ADC-noise-related computational redundancy through derivative or numeric type conversion [15,20]. For XOR processing, as reported by Uchida *et al*, a generation rate of 400 Gbps (8 LSBs × 50 GHz) was achieved using a bandwidth-enhanced chaos with bit-order reversal time-shift XOR [17], whereas only 75 Gbps (6 LSBs × 12.5 GHz) was obtained without bit-order reversal [16]. These complicated post-processing methods are usually operated offline and time consuming, and thus cannot support real-time generation of random bits. In addition, post processing like over-resolution extraction relying on computational redundancy even can result in pseudo randomness [15].

Therefore, it is interesting to construct a high-speed multi-bit true RBG with minimal post processing which does not include any other post processing except for LSBs retaining. The solution is finding a way to improve randomness defects of laser chaos mentioned above. Recent attention is focused on the suppression of time-delay signature [13,21–24]. Oliver *et al*. utilized polarization-rotated feedback to suppress the time-delay signature, and then generated 160-Gbps random bit sequence by directly selecting 4 LSBs at a sampling rate of 40 GHz [25]. It should be remarked that only a few small regions of laser bias current and feedback strength can successfully generate random bits. The reason is that in most cases laser chaos has a sharp spectrum and an asymmetrical amplitude distribution [25]. A more obvious way is to rely on chaotic sources that are not generated by external-cavity feedback like optical injection [18] or even on entropy sources that are not related to laser chaos such as amplified spontaneous emission [26]. Unfortunately, post processing is still required. This is because the optical injection-induced laser chaos remains having sharp spectrum and asymmetric amplitude distribution, and the amplified spontaneous emission still has asymmetric amplitude distribution due to optical filtering. Consequently, finding a wideband entropy source without all of above defects is the key to realize high-speed multi-bit RBG with minimal post processing.

Our previous work found that optical heterodyning of two chaotic ECLs can readily obtain a wideband chaos referred to as white chaos, which not only has no time-delay signature but also has a flat spectrum and a symmetric distribution [27]. In this paper, taking this optical heterodyne white chaos as physical entropy source, we experimentally demonstrate fast true RBG with minimal post processing. In our experiments, a white chaos with 16.7-GHz bandwidth is generated and used, of which the entropy rate is estimated as 16 Gbps by single-bit extraction. After quantization using an 8-bit ADC, 320-Gbps physical random bits are achieved by directly extracting 4 LSBs at 80-GHz sampling rate.

2. Experimental setup

The experimental setup of RBG using optical heterodyne white chaos is presented in Fig. 1. It includes two parts: generation and quantization of white chaos. For generation of white chaos, as shown in the left box, two external-cavity lasers are constructed, each of which consists of a distributed feedback semiconductor laser (DFB$_{1,2}$) subject to optical feedback from a fiber mirror (M$_{1,2}$). Note that the laser facet and the mirror comprise a feedback external cavity. In the feedback cavity, a polarization controller (PC$_{1,2}$) is used to match the polarization state of feedback light to that of the laser, and a variable attenuator (VA$_{1,2}$) is utilized to adjust the feedback strength to change the dynamic state of the laser. After optical isolators (OI$_{1,2}$), the outputs of two ECLs are mixed through a 3-dB fiber coupler, and then the optical heterodyne signal is detected by a balanced photo-detector. The heterodyne signal is expressed as

$2(I_1I_2)^{1/2}\sin(2\pi\Delta\nu t + \varphi_2\text{-}\varphi_1)$, where $I_{1,2}$ and $\varphi_{1,2}$ are the intensity and phase of lasers $\mathrm{DFB}_{1,2}$, and $\Delta\nu$ is the optical frequency difference of two lasers. As plotted in the right box, the optical heterodyne signal is inputted to and quantized by an 8-bit ADC: each sampling point is converted into 8-bit binary digits. The random bits are generated by extracting binary digits of several LSBs and discarding the other most significant bits (MSBs).

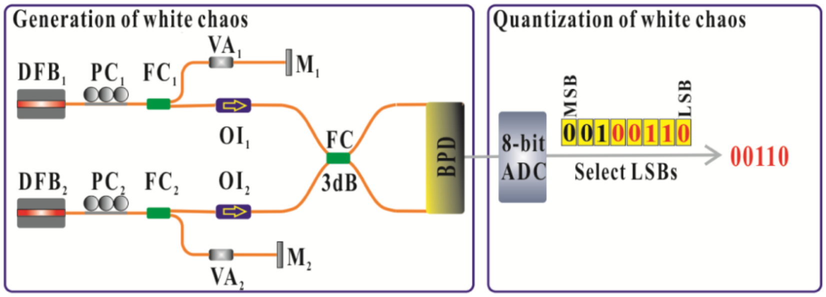

Fig. 1. Experimental setup. $\mathrm{DFB}_{1,2}$: distributed feedback semiconductor laser; $\mathrm{PC}_{1,2}$: polarization controller; $\mathrm{FC}_{1,2}$, FC: fiber coupler; $\mathrm{VA}_{1,2}$: variable attenuator; $\mathrm{OI}_{1,2}$: optical isolator; $\mathrm{M}_{1,2}$: fiber mirror; BPD: balanced photodetector; ADC: analog-to-digital converter; MSB: most significant bit; LSB: least significant bit.

In our experiments, the lasers DFB_1 and DFB_2 (Eblana, EP1550-DM-B05-FM) have threshold currents of 13.68 mA and 13.88 mA respectively, and both operate at a bias current of 34.0 mA which are controlled by laser drivers (ILX Lightwave, LDX-3412). The central wavelengths of DFB_1 and DFB_2 are slightly tuned by temperature controllers (ILX Lightwave, LDT-5412) to adjust the frequency difference $\Delta\nu$. The balanced photodetector ($\mathrm{u^2t}$, BPDV2120R) has a bandwidth of 45GHz. The optical spectra of lasers are measured by an optical spectrum analyzer with a resolution of 0.02nm (YOKOGAWA, AQ6370C). The lasers' intensity output and the heterodyne signal are measured by a radio-frequency spectrum analyzer (Agilent, N9010A, 26.5-GHz bandwidth) and a high-speed real-time oscilloscope (LeCroy, LABMASTER10ZI, 36-GHz bandwidth, 80 GS/s, 8-bit vertical resolution).

3. Experimental results

3.1 Generation of white chaos by optical heterodyning

The properties of the optical heterodyne signal for different parameters have been investigated in our previous work [27]. Here, we outline the conditions of generation of white chaos. First, the two ECLs should have fast phase dynamics which is not dominated by laser relaxation oscillation, so that the heterodyne converting phase into intensity can generate a flat wideband spectrum by controlling the frequency difference. Second, the two feedback delays, i.e. the round-trip time in external cavities, should be incommensurate in principle, so that the external-cavity modes of the two lasers have incommensurate mode frequency intervals. Thus, the heterodyne leads to non-resonance beatings and then totally eliminates the time-delay signatures. It is worth noting that, due to that the number of external-cavity modes is actually finite, the delay condition can be eased as $q\tau_1 = p\tau_2$ with large enough integers p and q.

In this experiment, the feedback strength defined as the power ratio of the feedback light to the laser output is adjusted to be –9.3 dB for ECL_1 and –10.6 dB for ECL_2. The two feedback delays are τ_1 = 93.6ns and τ_2 = 93.1ns. The center wavelengths of DFB_1 and DFB_2 are 1550.51nm and 1550.40nm, respectively, which are red shifted by 0.06nm and 0.04nm compared to the static-state wavelengths due to optical feedback. With these parameters, we experimentally obtain a white chaos by optical heterodyning. Figure 2 shows the characteristics of the white chaos, including radio-frequency spectrum, time-delay signature, temporal waveform and amplitude probability distribution. For comparison, the ECL's intensity chaos is also presented. Due to similarity, we only show the output of ECL_1 in the text for the sake of simplicity.

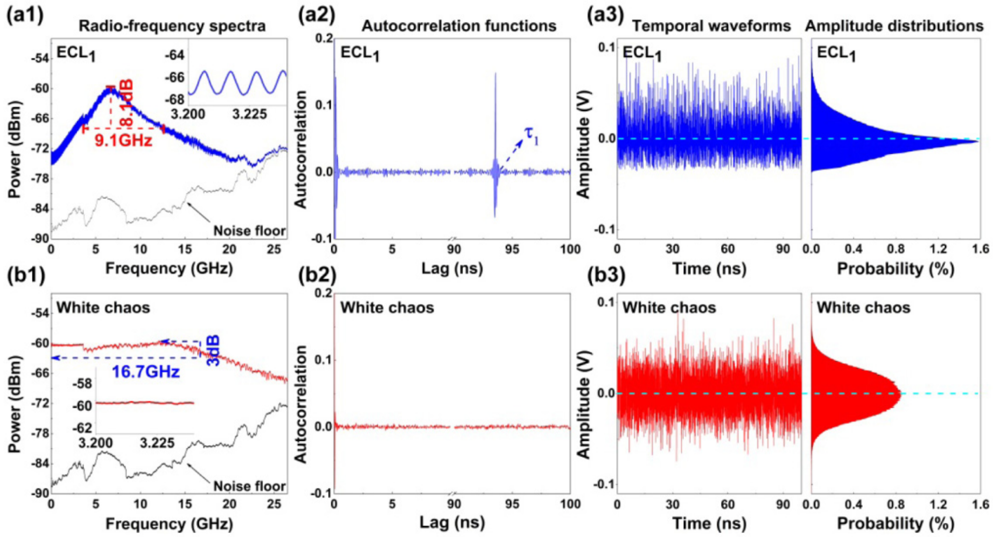

Fig. 2. Comparison of characteristics of experimental white chaos and intensity chaos of ECL_1: (a1)-(a3) radio-frequency spectrum, autocorrelation trace, and temporal waveform and amplitude distribution of ECL_1, and (b1)-(b3) those of the white chaos.

Figures 2(a1) and 2(b1) plot the radio-frequency spectra of the intensity chaos of ECL_1 and the heterodyne white chaos, respectively. For ECL_1 shown in Fig. 2(a1), a peak approximately at the relaxation frequency can be clearly observed. This peak is much higher than the lowest spectral component and dominates the whole spectrum. These defects greatly restrict the ECL_1 spectrum's bandwidth and flatness. Its effective bandwidth is calculated as 9.1 GHz and the spectrum flatness is 8.1 dB. In addition, as depicted by the inset, the spectrum has an obvious periodic modulation, of which the period corresponds to the reciprocal of feedback delay time (τ_1). The periodic modulation is actually the time-delay signature which is harmful to randomness of laser chaos. By contrast, shown in Fig. 2(b1), the heterodyne chaos has a white-noise-like spectrum free of dominant peaks and periodic modulation, which is why it is called white chaos. The spectrum is wider and flatter than that of the laser chaos. The effective bandwidth increases to 16.7 GHz and the flatness reduces to 3 dB.

The autocorrelation traces of the intensity chaos of ECL_1 and the white chaos are shown in Figs. 2(a2) and 2(b2), respectively, in order to examine the time-delay signature. It is quite apparent from Fig. 2(a2) that the ECL_1 establishes a correlation peak at the feedback delay (τ_1). Such time-delay signature leads to correlation in the extracted random bits and thus results in deterioration of randomness. By contrast, as shown in Fig. 2(b2), the correlation trace of the white chaos has no peaks at delays τ_1 and τ_2, indicating the elimination of time-delay signature. The elimination of time-delay signature not only improves the randomness of chaos but also enables a continuously tunable rate of RBG [13].

The last characteristic we explore is the amplitude probability distribution. Figure 2(a3) lists the temporal waveform and the corresponding amplitude probability of ECL_1 output, and Fig. 2(b3) plots those of the white chaos. Comparison clearly tells that the white chaos oscillates more symmetrically with respect to its mean value of zero volt. Quantitatively, the white chaos has a skewness of 0.072 which is significantly less than the skewness of ECL_1 which is 0.941. The more symmetrical amplitude distribution of chaos means equilibrium of probability of bits 0 and 1 in RBG [11,14].

3.2 Estimation of entropy rate

Entropy rate is the fundamental rate of RBG determined by the physical characteristics of entropy source. It can be estimated with largest Lyapunov exponent. But this value is difficult to be calculated for experimental white chaos because of requiring a huge data set [28]. Here, we adopted a more efficient estimation method mentioned in Ref [10], in which the entropy rate is estimated as the maximum rate of the RBG using single-bit extraction. To estimate the entropy rates of white chaos as well as laser chaos, we extract random bits using single-bit extraction at different sampling rates and examine the corresponding randomness through the National Institute of Standards and Technology (NIST) test suite [29].

The single-bit extraction process is implemented as follows. The electronic analog signal from the photodetector is quantized to a raw binary sequence by a 1-bit ADC with a comparing threshold which is the median of amplitude distribution. Then, the final random bit sequence is achieved by executing logical XOR between the raw sequence and its duplicate with a 3.7-ns delay. Note that the delay time for XOR operation should not equal the integer multiple of feedback delay in order to avoid correlation.

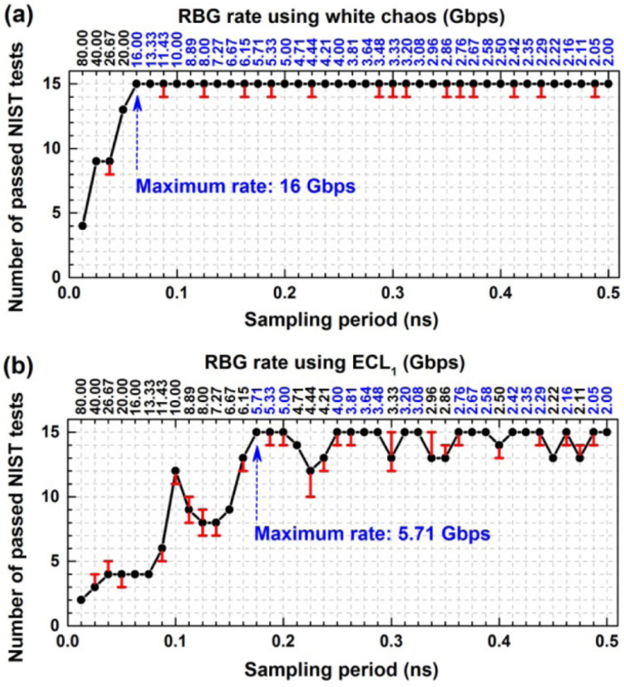

Fig. 3. Number of passed NIST tests as a function of the sampling period for random bits generated from (a) heterodyne white chaos and (b) ECL$_1$. The tests for each generation rate are examined five times, and the median of the numbers of passed terms is denoted as black dots, and the maximum and minimum numbers of passed terms are indicated with red bars. The random bit sequence is treated as passing the NIST tests when the median equals 15.

Figure 3(a) shows the NIST test results at different extracting rates for the white chaos, and Fig. 3(b) shows that for the laser chaos for comparison. The NIST test suite consists of 15 statistical terms which are accomplished by using 1000 samples of 1-Mbit sequence with a significance level of 0.01 [29]. The ordinate is the number of passed terms. The lower horizontal axis represents the sampling period, and the corresponding generation rate is labeled on the upper horizontal axis. At each sampling rate, we test five times in order to reduce errors. The median of the numbers of passed terms is plotted as black dots, and the maximum and minimum numbers of passed terms are indicated with red bars. If the median equals 15, the random bit sequence is treated as passing the NIST tests. Shown in Fig. 3(a), the maximum random bit generation rate, i.e., the entropy rate of the white chaos reaches 16 Gbps. By contrast, the entropy rate of the laser chaos of ECL_1 is estimated as 5.71 Gbps, as shown in Fig. 3(b). The reason is that the white chaos has a larger effective bandwidth and a smaller spectral flatness. It is worth noting that benefiting from the flat spectrum the white chaos has a higher bandwidth-utilization efficiency reaching about 96%, while the level is only 63% for the laser chaos of the ECL_1.

In addition, it can also be found that the random bits extracted from the white chaos with rates below 16 Gbps pass all the tests. This means a continuously tunable rate of RBG. This merit is brought by the elimination of time-delay signature. By comparison, RBG taking laser intensity chaos as entropy source cannot tune the generation rate continuously.

3.3 Minimal-post-processing 320-Gbps physical RBG

In this section, we experimentally demonstrate random bit generation from the heterodyne white chaos by using multi-bit extraction without any other post processing. In experiments, an 8-bit ADC in the real-time oscilloscope is used to quantize the analog chaotic signal. Each sampling point is converted into 8 binary bits, and N ($N \leq 8$) least significant bits of them are retained as output of random bits. The generation rate is thus equal to N times sampling frequency.

We first analyze the possible maximum sampling frequency for the multi-bit extraction by calculating spectra of temporal waveforms which are recovered by digital-analog conversion with N-LSB binary digits. Figures 4(a1)-4(a3) show the spectra of the recovered heterodyne white chaos with different numbers of LSBs, i.e. $N = 6, 5, 4$, respectively. The corresponding results for ECL_1 are listed in Figs. 4(b1)-4(b3). As shown in Fig. 4(a1), when we select 6 LSBs, the 3-dB bandwidth of the recovered heterodyne white chaos is increased to 26 GHz, which is about 10 GHz larger than the original bandwidth shown in Fig. 2(b1). By comparing with Fig. 4(a2), one can find that the bandwidth further increases as N decreases, which is caused by the nonlinear frequency mixing during selecting LSBs [13,30]. This bandwidth-enhancement effect also appears on the laser intensity chaos, as plotted in Figs. 4(b1)-4(b3). It is thus concluded that the operation of retaining LSBs enables a high sampling frequency for RBG because of the bandwidth-enhancement effect. In addition, it is worth emphasizing that the recovered heterodyne white chaos still has advantage in bandwidth over the laser intensity chaos. The bandwidth difference even becomes greater. For example, as depicted in Fig. 4(b2), when 5 LSBs are retained, the bandwidth of recovered laser chaos is about 13 GHz. By comparison, shown in Fig. 4(a2), the bandwidth of the recovered heterodyne white chaos exceeds 40 GHz, which is the Nyquist bandwidth of the real-time oscilloscope used. This means that a sampling frequency of 40 GHz for RBG is allowed by signal bandwidth when we extract 5 LSBs from the heterodyne white chaos. A higher sampling frequency is possible if we retain 4 LSBs because the bandwidth increases as the number of LSBs decreases.

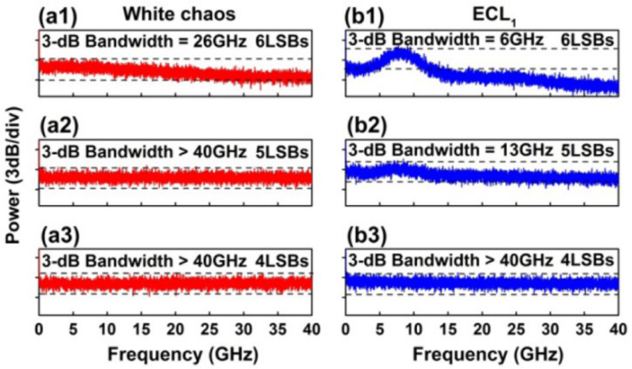

Fig. 4. Radio-frequency spectra of (a1)-(a3) the quantized heterodyne white chaos and (b1)-(b3) the quantized ECL_1 chaos recovered with 6 LSBs, 5 LSBs, and 4 LSBs, respectively.

Then, we evaluate the randomness of the binary sequence obtained by retaining N LSBs. The randomness is generally represented by correlation and probability distribution. Figures 5(a)-5(c) plot the autocorrelation traces of the decimal sequences separately converted with 5 LSBs, 4 LSBs and 3 LSBs, respectively. As indicated by the blue (black) traces in Fig. 5, the extracted binary sequence from laser chaos inherits the time-delay signature or correlation as $N > 3$. We note that further decreasing the number of LSBs retained can suppress the time-delay signature because more features of chaotic dynamics are lost, but resultantly the rate of RBG will be greatly reduced. By contrast, shown in the red (gray) autocorrelation traces, the quantized output from the heterodyne white chaos has no correlation peak for any value of N thanks to the elimination of time-delay signatures by the optical heterodyning.

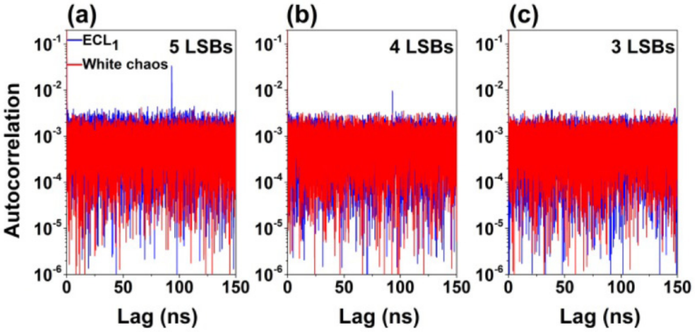

Fig. 5. Autocorrelation traces of the decimal sequences separately converted from the binary series of (a) 5 LSBs, (b) 4 LSBs and (c) 3 LSBs, respectively. Red (gray): heterodyne white chaos; blue (black): ECL_1 chaos.

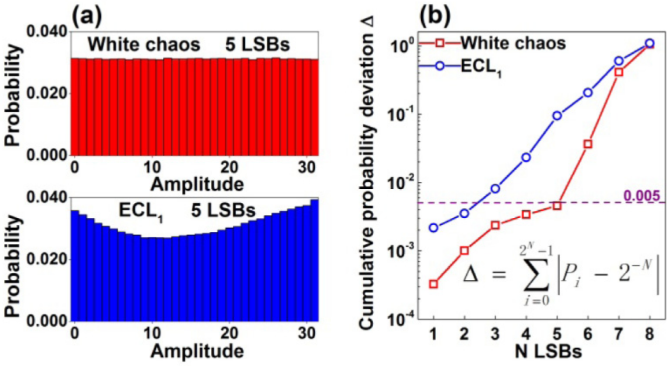

Fig. 6. (a) Amplitude probability distribution of 5-LSB sequence extracted from the 8-bit quantized heterodyne white chaos (upper) and ECL$_1$ intensity chaos (lower); (b) Cumulative probability deviation to uniform distribution $\Delta = \sum_{i=0}^{2^N-1} | P_i - 2^{-N} |$, where N is the number of LSBs retained, P_i is the probability of an N-bit binary number corresponding to a decimal integer i between 0 and 2^N–1. The amplitude distribution is calculated from 1 M data points.

Figure 6(a) demonstrates the amplitude probability distributions of quantization sequences obtained with 5-LSB extraction. The upper and the lower are results of the heterodyne white chaos and the laser intensity chaos, respectively. Note that the decimal integers in the horizontal coordinate denote the corresponding 5-bit binary numbers, for example, 0 representing 00000 and 31 representing 11111. It is clearly shown that the probability distribution for the heterodyne white chaos is much more uniform than that for the laser chaos of ECL$_1$. The more uniform the distribution is, the closer the numbers of ones and zeros in generated random bits will be. This means better randomness. To quantitatively evaluate the uniformity, a definition of cumulative probability deviation $\Delta = \sum_{i=0}^{2^N-1} | P_i - 2^{-N} |$ is adopted, where P_i is the probability of an N-bit binary number corresponding to a decimal integer i between 0 and 2^N–1. For a uniform distribution, $P_i = 2^{-N}$ and then $\Delta = 0$. This means that a smaller cumulative probability deviation indicates a distribution closer to uniform distribution. According to the definition, the cumulative probability deviation of the quantization sequences obtained with 5-LSB extraction from the heterodyne white chaos is 0.0046, greatly lower than that of ECL$_1$ which is 0.0950. Figure 6(b) further depicts the cumulative probability deviation as a function of the number of LSBs retained. As shown in squares, for the heterodyne white chaos the probability deviation is lower than 0.005 as $N < 6$. This means that these probability distributions for binary sequences extracted with 5 LSBs or less LSBs have a uniform profile similar to the upper one in Fig. 6(a). By contrast, for the laser chaos plotted in circles in Fig. 6(b), the cumulative probability deviation is below 0.005 only for $N < 3$, and then quickly increases with increase of N. The above analysis of probability distribution indicates that compared to the laser intensity chaos, the heterodyne white chaos enables more LSBs directly as output of RBG without any post processing.

Having explored the characteristics of the quantized heterodyne white chaos, attention is now turned to extracting random bits. The random bits are generated by directly extracting LSBs from the heterodyne white chaos as well as the intensity chaos of ECL$_1$ separately at the sampling rates of 40 GS/s and 80 GS/s. Figure 7 shows the number of passed NIST terms as a function of the number of LSBs retained. As shown in Fig. 7(a1), for 40-GS/s sampling rate, random bits extracted by retaining up to 5 LSBs from the heterodyne white chaos can pass all the NIST test terms. By contrast, for ECL$_1$ chaos shown in Fig. 7(b1) random bits only extracted from LSB or 2 LSBs can pass all the NIST tests. It should be mentioned that for 3-

LSB and 4-LSB extraction from the laser intensity chaos the failed NIST terms are “Runs” and “Block-frequency”, meaning that the reason is the non-uniform amplitude distribution. Further increasing the number of the extracted LSBs, the NIST term “Approximate-entropy” also fails to pass. This is caused by the reduced bandwidth as shown in Figs. 4(b1) and 4(b2). Benefiting from improvement in bandwidth and distribution, the heterodyne white chaos can be directly converted into random bits with 5-LSB extraction at a sampling rate of 40 GS/s, and then 200-Gbps RBG without post processing is obtained, of which the detail NIST results are listed in Table 1.

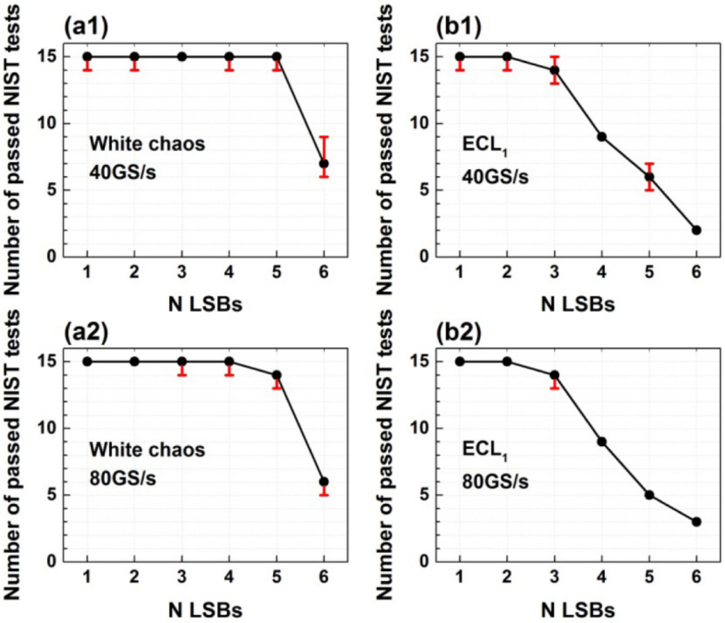

Fig. 7. Number of passed NIST tests as a function of the extracted LSBs for (a1), (a2) heterodyne white chaos and (b1), (b2) ECL$_1$ under different sampling rates of 40 GS/s and 80 GS/s.

As shown in Fig. 7(a2), further increasing the sampling rate to 80 GS/s, random bits obtained with 5-LSB extraction from the heterodyne white chaos cannot pass the NIST tests, but 4-LSB-extraction random bits still can. The reason can be deduced from autocorrelation traces. For 5-LSB extraction, as indicated by in the red (gray) points in Fig. 8(a), two neighboring points have a correlation value of 0.01, which means that the sampling rate is higher than signal bandwidth. For 4-LSB extraction the correlation between neighboring points is down to the level of background noise shown in Fig. 8(b). Therefore, 4-LSB extraction at 80 GS/s can achieve random bits passing the NIST tests, of which the test results are shown in the right column in Table 1. Thus, the maximum generation rate reaches 320 Gbps. By contrast, the laser intensity chaos of ECL$_1$ enables only 2 LSBs at most to be selected directly as random bits at 80-GS/s sampling rate, according to Fig. 7(b2).

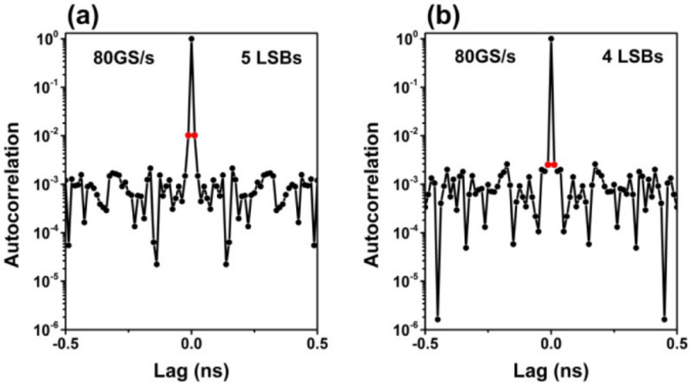

Fig. 8. Autocorrelation traces of the decimal sequences recovered from the binary series of heterodyne white chaos with (a) 5 LSBs and (b) 4 LSBs at a sampling rate of 80 GS/s.

Table 1. Results of NIST test for 200-Gbps (5 LSBs × 40 GS/s) and 320-Gbps (4 LSBs × 80 GS/s) random bit sequences extracted from the heterodyne white chaos. Using 1000 samples of 1 Mbit data and significance level α = 0.01, for "Success", the p-value should be larger than 0.0001 and the proportion should be in the range of 0.99 ± 0.0094392. For tests which produce multiple p-values and proportions, the worst case is shown.

	200-Gbps RBG		320-Gbps RBG		
Statistical test	P-value	Proportion	P-value	Proportion	Results
Frequency	0.856359	0.9870	0.159910	0.9900	Success
Block Frequency	0.429923	0.9950	0.476911	0.9940	Success
Cumulative Sums	0.709558	0.9880	0.192724	0.9930	Success
Runs	0.078567	0.9870	0.088762	0.9900	Success
Longest Run	0.246750	0.9860	0.492436	0.9930	Success
Rank	0.614226	0.9900	0.689019	0.9940	Success
FFT	0.378705	0.9890	0.204439	0.9950	Success
Non Overlapping Template	0.005847	0.9890	0.002993	0.9880	Success
Overlapping Template	0.457825	0.9900	0.360287	0.9850	Success
Universal	0.299736	0.9870	0.773405	0.9900	Success
Approximate Entropy	0.454053	0.9850	0.077131	0.9850	Success
Random Excursions	0.002737	0.9916	0.216096	0.9852	Success
Random Excursions Variant	0.091403	0.9882	0.001174	0.9934	Success
Serial	0.277082	0.9900	0.450297	0.9860	Success
Linear Complexity	0.837781	0.9900	0.680755	0.9870	Success

4. Discussion and conclusion

In experiments, the white chaos can be generated as long as the parameter conditions listed in section 3.1 are satisfied, among which appropriate optical frequency difference and incommensurate external-cavity feedback delays are most fundamental. These conditions can be easily obtained by adjusting corresponding hardwares such as laser driver, temperature controller, variable attenuator and fiber length of external cavity in the generation system, which is expected to be further miniaturized with current monolithically integrated technology. More importantly, the white chaos generated with this system enables minimizing post processing in the multi-bit RBG. This is a step forward for realizing high-speed real-time RBG, which is now under our investigation with single-bit extraction.

In conclusion, a scheme of fast true RBG with minimal post processing based on physical white chaos is experimentally demonstrated. The white chaos has wide flat-spectrum, symmetric amplitude distribution, and no time-delay signature compared with laser chaos generated by external-cavity feedback. Benefitting from these merits, 320-Gbps RBG using LSB extraction without any other post processing is achieved. It is believed that this scheme paves the way for realization of real-time high-speed random bit generation and boosts its applications in the fields of information security.

Acknowledgment

This work was supported in part by National Nature Science Foundation of China (NSFC) under grants 61475111, 61671316, 61227016, in part by Natural Science Foundation for Excellent Young Scientists of Shanxi (2015021004); in part by Program for the Innovative Talents of Higher Learning Institutions of Shanxi; and in part by International Science and Technology Cooperation Program of China and Shanxi (2014DFA50870, 201603D421008).