Random bit generation using an optically injected semiconductor laser in chaos with oversampling

Xiao-Zhou Li and Sze-Chun Chan*

Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
**Corresponding author: scchan@cityu.edu.hk*

Received February 21, 2012; revised April 12, 2012; accepted April 20, 2012;
posted April 23, 2012 (Doc. ID 163393); published June 1, 2012

Random bit generation is experimentally demonstrated using a semiconductor laser driven into chaos by optical injection. The laser is not subject to any feedback so that the chaotic waveform possesses very little autocorrelation. Random bit generation is achieved at a sampling rate of 10 GHz even when only a fractional bandwidth of 1.5 GHz within a much broader chaotic bandwidth is digitized. By retaining only 3 least significant bits per sample, an output bit rate of 30 Gbps is attained. The approach requires no complicated postprocessing and has no stringent requirement on the electronics bandwidth. © 2012 Optical Society of America

OCIS codes: 140.5960, 140.1540, 140.3520, 190.3100.

Random bit generation requires each output bit to be associated with an unbiased probability for 0 and 1, independent of the rest of the bits. Applications of random bit generators include stochastic modeling, encryption, and secure communication, where a fast generation speed often has positive impact on the performances. The broad bandwidths offered by photonic devices have recently been utilized for high-speed random bit generation [1,2]. For instance, random bit generation using quantum randomness in a pulsed laser was demonstrated [3]. Randomness of spontaneous emissions from incoherent light sources was also utilized [4,5]. Pioneered by Uchida *et al.*, chaotic dynamics of semiconductor lasers continue to be important for fast random bit generation [1]. In their work, chaotic intensities were emitted from two lasers subject to optical feedback. Upon detection by photodetectors, chaotic waveforms with electronic bandwidths of about 3 GHz were obtained. The waveforms were digitized at a sampling rate of 1.7 GHz by analog-to-digital converters (ADCs) of 1-bit resolution. The digitized signals were merged using exclusive-or (XOR) so the resultant output bit rate was 1.7 Gbps. Progress was made by further optically injecting the chaotic waveforms into another laser, which enhanced the bandwidths to attain increment of the output bit rates [6]. Simulations on all-optical generation were also conducted [7,8]. Additionally, by incorporating high-resolution ADCs, more than 1 bit can be generated in each sampling period so that the effective output bit rate can be significantly increased. Kanter *et al.* demonstrated generation of 15 random bits per sampling period [2]. With an electronic detection bandwidth of 12 GHz and a sampling rate of 20 GHz, an effective output rate of 300 Gbps was achieved after much postprocessing. High-order derivatives were computed to enhance small fluctuations of the digitized signals in order to pass the randomness tests. Simplifications by discarding the most significant bits (MSBs) and retaining the least significant bits (LSBs) were also reported [9].

Two features are common to the above approaches. First, the chaotic waveforms were always generated by optical feedback into the lasers, even if the waveforms were further broadened by optical injection into or from another laser. This often leads to residual autocorrelation at the feedback round-trip time, which should be set incommensurate with the sampling period through careful design [10,11]. Second, the chaotic waveforms were always undersampled in which two times their electronic bandwidths exceeded the respective sampling rates. Undersampling violates the Nyquist criterion to cause aliasing and flattening of the spectrum for random bit generation. However, the chaotic waveforms, photodetectors, and front ends of the ADCs must have sufficiently large bandwidths in order to support high sampling rates.

In this Letter, we experimentally demonstrate random bit generation using an optically injected laser and oversampling. A chaotic waveform is generated by the injected semiconductor laser. The waveform is digitized by an 8-bit ADC with a low front-end bandwidth of only 1.5 GHz, but is oversampled at a sampling rate of 10 GHz. By retaining only the 3 LSBs and performing XOR on consecutive samples, random bits are generated at an output bit rate of 30 Gbps. Since the laser is not subject to any feedback, there is no round-trip time for the sampling period to avoid. The use of oversampling also relaxes the requirements on the front-end bandwidth of the ADC. The output bits are shown to pass the standard test suite for random numbers from the National Institute of Standards and Technology (NIST).

Figure 1 shows our experimental setup for random bit generation. The master and slave lasers are both

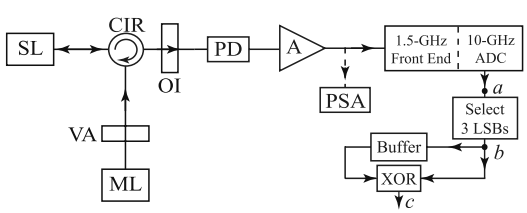

Fig. 1. Schematic of the experimental setup. ML, master laser; SL, slave laser; VA, variable attenuator; CIR, circulator; OI, optical isolator; PD, photodetector; A, amplifier; PSA, power spectrum analyzer.

single-mode distributed-feedback lasers (Mitsubishi ML920T43S-01) emitting at about 1.55 μm. The slave laser is biased above threshold at 40 mA and is temperature stabilized at 26.50 °C. It emits about 10 mW with a relaxation resonance frequency of about 11 GHz. The master laser is biased at 128.5 mA and is also temperature stabilized. Its continuous-wave emission passes through a variable attenuator, a free-space circulator, and impinges on the slave laser facet with about 0.3 mW. The optical frequency detuning of the master laser from the slave laser is about 12.5 GHz. Such optical injection drives the slave laser into chaotic oscillation [12,13]. Chaotic oscillations are capable of amplifying the effects of intrinsic laser noise [14]. The emission from the slave laser then passes the circulator and an isolator so that about 0.5 mW enters a photodetector (Newport AD-10ir) for optical-to-electrical conversion. The electrical chaotic waveform is then amplified by 40 dB using a microwave amplifier. For digitization, the electrical chaotic waveform is monitored by an 8-bit ADC in an oscilloscope (Agilent 90254A) for subsequent processing in a computer. The front-end bandwidth of the ADC is only 1.5 GHz, but the sampling rate is set at 10 GHz. To ensure randomness, only the 3 LSBs are retained for each sample. The bits of each sample are then compared by an XOR to the respective bits of the previous sample, which are stored in a buffer. The buffer is equivalent to a delay of one sampling period. So the output from the XOR is a bit stream at 30 Gbps.

The chaotic waveform is first characterized by connecting the output of the amplifier in Fig. 1 to a power spectrum analyzer (Agilent N9010A) instead of the ADC. The red curve in Fig. 2(a) shows the power spectrum of the chaotic waveform. The signal bandwidth is about 10.27 GHz according to the convention of 80% containment of total power [15]. The gray curve in Fig. 2(a) shows the noise spectrum measured when the master laser is turned off and the slave laser is free-running. It is clear that the chaos spectrum is stronger than and different from the noise spectrum. The corresponding autocorrelation trace of the chaotic waveform is shown in Fig. 2(b). The autocorrelation quickly diminishes as the delay time increases from zero. Its magnitude is lower than 0.02 when the delay is longer than 2 ns. By contrast, chaotic lasers under optical feedback are often associated with stronger autocorrelation peaks at multiples of the feedback round-trip time, which cause restrictions on the sampling frequency [10,16]. Therefore, the absence of any feedback round-trip time is a unique advantage of optical injection over optical feedback.

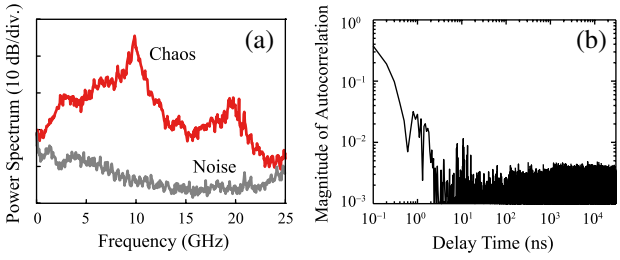

Fig. 2. (Color online) Measurements at the output of the amplifier. (a) Power spectrum of chaos (red) and noise (gray). (b) Magnitude of autocorrelation of chaos.

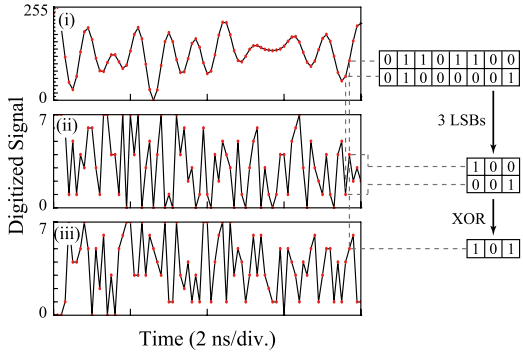

Fig. 3. (Color online) Digitized signals obtained at (i) position a, (ii) position b, and (iii) position c of the experimental setup.

The chaotic waveform after the amplifier is input to the ADC in Fig. 1. The peak-to-peak amplitude of the input waveform is about 0.2 V. The digitized signal obtained at position a immediately after the ADC in Fig. 1 is shown in Fig. 3(i). Each sampled data point is digitized into 8 bits corresponding to 256 digitization levels, as the corresponding inset shows. The front-end of the ADC has a low-pass cutoff frequency of only 1.5 GHz, but the ADC performs oversampling at a sampling frequency of 10 GHz. This resulted in the rather smooth digitized signal, which cannot be directly used as random bits. However, Fig. 3(ii) shows a very irregular signal at position b of Fig. 1. It is because the 5 MSBs of each data point are discarded and only the 3 LSBs are selected. Selecting the LSBs is equivalent to a modulo operation, or a folding action, that scrambles the data points [17]. The final output at position c of Fig. 1 is then obtained by comparing consecutive data points through bitwise XOR operations, as shown in Fig. 3(iii). The XOR operations effectively reduce any small statistical bias of the bits [10]. Overall, the output bits are generated at a rate of 30 Gbps. They are verified to be random through passing the NIST Special Publication 800-22 statistical

Table 1. Results of the NIST Special Publication 800-22 Statistical Tests for Random Bits

Statistical Test	*P*-value	Proportion	Result
Frequency	0.919131	0.9890	Success
Block-frequency	0.735908	0.9930	Success
Cumulative-sums	0.298282	0.9870	Success
Runs	0.643366	0.9900	Success
Longest-run	0.112047	0.9920	Success
Rank	0.030399	0.9910	Success
FFT	0.002058	0.9910	Success
Nonperiodic-templates	0.007639	0.9820	Success
Overlapping-templates	0.454053	0.9920	Success
Universal	0.052275	0.9940	Success
Approximate-entropy	0.518106	0.9890	Success
Random-excursions	0.299251	0.9842	Success
Random-excursions-variant	0.068219	0.9826	Success
Serial	0.429923	0.9830	Success
Linear-complexity	0.618385	0.9890	Success
Total			15

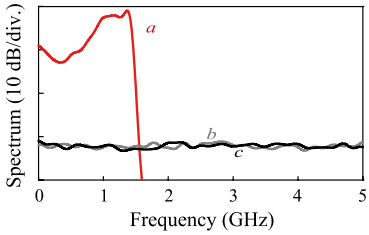

Fig. 4. (Color online) Spectra of the digitized signals obtained at position a (red), position b (gray), and position c (black) of the experimental setup.

tests, which are standard tests for randomness. A total of 1000 sequences, each of size 1 Mbit, are collected for testing. At significance level $\alpha = 0.01$, the success proportion should be in the range of 0.99 ± 0.0094392. The composite P-value should be larger than 0.0001 to ensure uniformity. The testing results are summarized in Table 1, where the worst case is shown for tests producing multiple P-values and proportions. Besides, when the master laser is switched off, noise from the free-running slave laser and the electronics is responsible for generating the output bits. Because the corresponding noise spectrum in Fig. 2(a) is very weak, the output bits are found to fail the randomness tests even if 7 MSBs are discarded in retaining only 1 LSB. This shows that the chaotic waveforms are essential to random bit generation in the experiment.

Random bits can be generated from the oversampled signal because the signal bandwidth is significantly broadened when the MSBs are discarded. Figure 4 shows the spectra of the digitized signals at positions a, b, and c of the setup in Fig. 1, which are Fourier transforms of the digitized signals in Figs. 3(i), 3(ii), and 3(iii), respectively. The full frequency-span of 5 GHz at half the sampling frequency is presented. The red curve shows the signal at position a. Limited by the front-end bandwidth of the ADC, the signal drops quickly at 1.5 GHz and is thus not suitable for random bit generation. However, the gray curve obtained at position b shows a much broadened and nearly white spectrum. This is because the MSBs are discarded in selecting the LSBs, which is a very nonlinear operation that causes significant frequency mixing. Experimentations show that at least 5 MSBs have to be discarded in order to ensure sufficient frequency mixing for passing the randomness tests. The final output at position c has a featureless white spectrum as shown by the black curve, which is an essential indicator that the output bits are random.

In summary, random bit generation is demonstrated using a chaotic laser driven by optical injection alone. Because of the absence of optical feedback, the autocorrelation of the chaotic waveform is free from any problematic side peaks. Also, in spite of oversampling, random bit generation is enabled by selecting only the LSBs to effectively broaden the spectrum during postprocessing. This relaxes the electronic bandwidth requirements of the ADC front end. Utilizing only 1.5 GHz of a much broader chaos spectrum, random bit generation at 30 Gbps is successfully demonstrated.

The work described in this paper was fully supported by a grant from the Research Grants Council of Hong Kong, China (Project No. CityU 111210).

References

1. 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. Photon. **2**, 728 (2008).
2. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nat. Photon. **4**, 58 (2010).
3. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
4. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).
5. X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Opt. Lett. **36**, 1020 (2011).
6. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, Opt. Express **18**, 5512 (2010).
7. P. Li, Y. C. Wang, and J. Z. Zhang, Opt. Express **18**, 20360 (2010).
8. P. Li, Y. C. Wang, A. B. Wang, L. Z. Yang, M. J. Zhang, and J. Z. Zhang, Opt. Express **20**, 4297 (2012).
9. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Opt. Express **18**, 18763 (2010).
10. K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, IEEE J. Quantum Electron. **45**, 1367 (2009).
11. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, Opt. Lett. **36**, 4632 (2011).
12. S. C. Chan, IEEE J. Quantum Electron. **46**, 421 (2010).
13. X. Fu, S. C. Chan, Q. Liu, and K. Y. Y. Wong, Appl. Opt. **50**, E92 (2011).
14. T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, Phys. Rev. E **85**, 016211 (2012).
15. F. Y. Lin and J. M. Liu, Opt. Commun. **221**, 173 (2003).
16. J. G. Wu, G. Q. Xia, X. Tang, X. D. Lin, T. Deng, L. Fan, and Z. M. Wu, Opt. Express **18**, 6661 (2010).
17. K. W. Tang, H. S. Kwok, W. K. S. Tang, and K. F. Man, Int. J. Bifurc. Chaos **18**, 851 (2008).