4.5 Gbps high-speed real-time physical random bit generator

Anbang Wang, Pu Li, Jianguo Zhang, Jianzhong Zhang, Lei Li and Yuncai Wang*

Key Laboratory of Advanced Transducers & Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan 030024, China

Institute of Optoelectronic Engineering, College of Physics & Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China

**wangyc@tyut.edu.cn*

Abstract: We report a prototype of high-speed real-time physical random bit generator based on a chaotic laser. The chaotic laser consists of a semiconductor laser with optical feedback in fiber external cavity configuration. The chaotic laser intensity signal is quantized into binary stream by differential comparison which makes the amplitude distribution symmetric with respect to zero mean value. An exclusive-OR gate operation between two raw binary streams from the chaotic signal and its delayed signal is used to overcome the influences of the weak periodicity induced by the external cavity resonance inherent in the chaotic laser. After exclusive-OR operation, the prototype can generate a single fast random bit stream in real time without any off-line processing procedures. Its bit rate can be handily and continuously tuned up to 4.5 Gbps by a trigger clock. Experiment results demonstrate that our generator possesses high-quality randomness with verified by the three-standard-deviation criterion and industry-benchmark statistical tests.

OCIS codes: (140.1540) Chaos; (190.3100) Instabilities and chaos; (140.5960) Semiconductor lasers; (060.4510) Optical communications.

References and links

1. S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer-Verlag, 2007).
2. N. Metropolis and S. Ulam, "The Monte Carlo method," J. Am. Stat. Assoc. **44**(247), 335–341 (1949).
3. D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995).
4. R. G. Gallager, *Principles of Digital Communication* (Cambridge University Press, 2008).
5. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).
6. C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circ. Syst. I Fundam. Theory Appl. **47**(5), 615–621 (2000).
7. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC," IEEE Trans. Comput. **52**(4), 403–409 (2003).
8. R. S. Maddocks, S. Matthews, E. W. Walker, and C. H. Vincent, "A compact and accurate generator for truly random binary digits," J. Phys. E **5**(6), 542–544 (1972).
9. T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators–Part II: practical realization," IEEE Trans. Circ. Syst. I Fundam. Theory Appl. **48**(3), 382–385 (2001).
10. M. A. Wayne and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express **18**(9), 9351–9357 (2010).
11. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**(12), 13029–13037 (2010).
12. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. Lett. **34**(12), 1876–1878 (2009).
13. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Appl. Phys. Lett. **98**(17), 171105 (2011).
14. 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).
15. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

16. 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).
17. 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).
18. P. Li, Y. C. Wang, and J. Z. Zhang, "All-optical fast random number generator," Opt. Express **18**(19), 20360–20369 (2010).
19. N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation," Opt. Lett. **36**(23), 4632–4634 (2011).
20. 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).
21. Y. Y. Zhang, J. Z. Zhang, M. J. Zhang, and Y. C. Wang, "2.87-Gb/s random bit generation based on bandwidth-enhanced chaotic laser," Chin. Opt. Lett. **9**, 031404 (2011).
22. P. Li, Y. C. Wang, A. B. Wang, L. Z. Yang, M. J. Zhang, and J. Z. Zhang, "Direct generation of all-optical random numbers from optical pulse amplitude chaos," Opt. Express **20**(4), 4297–4308 (2012).
23. 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).
24. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **81**(5), 051137 (2010).
25. X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," Opt. Lett. **36**(6), 1020–1022 (2011).
26. 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).
27. 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).
28. W. Wei, G. Xie, A. Dang, and H. Guo, "High-speed and bias-free optical random number generator," IEEE EEE Photon. Technol. Lett. **24**(6), 437–439 (2012).
29. Y. Liu, M. Y. Zhu, B. Luo, J. W. Zhang, and H. Guo, "Implementation of 1.6 Tb s^{-1} truly random number generation based on a super-luminescent emitting diode," Laser Phys. Lett. **10**(4), 045001 (2013).
30. 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**(10), 711–715 (2010).
31. T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett. **98**(23), 231103 (2011).
32. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**(21), 20665–20672 (2011).
33. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A **81**(6), 063814 (2010).
34. 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 the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications", http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
35. S. Lepri, G. Giacomelli, A. Politi, and F. T. Arecchi, "High-dimensional chaos in delayed dynamical systems," Physica D **70**(3), 235–249 (1994).
36. 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).
37. Y. Wu, Y. C. Wang, P. Li, A. B. Wang, and M. J. Zhang, "Can fixed time delay signature be concealed in chaotic semiconductor laser with optical feedback?" IEEE J. Quantum Electron. **48**(11), 1371–1379 (2012).
38. J. Zhang, Y. Wang, M. Liu, L. Xue, P. Li, A. Wang, and M. Zhang, "A robust random number generator based on differential comparison of chaotic laser signals," Opt. Express **20**(7), 7496–7506 (2012).
39. J. Zhang, Y. Wang, L. Xue, J. Hou, B. Zhang, A. Wang, and M. Zhang, "Delay line length selection in generating fast random numbers with a chaotic laser," Appl. Opt. **51**(11), 1709–1714 (2012).
40. T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," Opt. Express **17**(11), 9053–9061 (2009).
41. S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Chaos laser chips with delayed optical feedback using a passive ring waveguide," Opt. Express **19**(7), 5713–5724 (2011).
42. 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 (2008).

1. Introduction

Random bit or number generators are key ingredients in a large number of fields such as scientific computations [1], stochastic experiments [2], cryptography [3] and communications [4]. In particular, the security of communication and cryptography vitally depends on the quality and quantities of random ciphers (*i.e.*, random bits or numbers).

Perfect encryption should resort to the provably unbreakable system found by Shannon, 'one time pad', where the plain text is encrypted by modular addition to a stream of non-

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

deterministic random ciphers that is used only once and not shorter than the plain-text [5]. However, this idea of 'one time pad' has not been widely used in practice. One of the main technical impediments is the difficulty of real-time high-quality random cipher generation whose rate must not be lower than the current high communication rate.

Pseudo-random bit generators based on classical computer algorithms have the ability to produce fast random bits, but they are fully deterministic or periodic and thus not appropriate for secure applications. In contrast to pseudo-random bit generators, physical random bit generators can offer non-determined random bits and ensure the confidentiality, because they commonly operates by measuring unpredictable physical processes such as thermal noise from a resistors [6], frequency jitter of an oscillator [7], elapsed time between emission of particles during radioactive decay [8], electrical chaos in nonlinear circuits [9] and photon-events in attenuated light [10–13]. However, these conventional physical random bit generators have been limited in bandwidth to very slow rates at Mbps and do not satisfy completely the requirements of unconditional secure modern communications with data rates at Gbps.

In recent years, intensive effort has been devoted to develop fast physical random bit generators so as to replace high-speed pseudo-random bit generators. Optical chaos [14–22], laser phase noise [23, 24], amplified spontaneous emission [25–29] and quantum vacuum states [30–33] have been widely employed as broadband entropy sources for Gbps or even faster non-determined random bit generation. However, to our knowledge, most of these studies except for that reported in Refs [14], [21]. and [31] are demonstrated in theory through offline computer processing for experimental waveform data of physical entropy sources. Strictly speaking, they do not generate continuous random bit stream with verified randomness in real time, whereas real-time output is necessary in practical applications for a random bit generator.

In the meantime, even for these few systems of real-time fast physical random bit generation, the stable output of a high-quality random bit stream in a long time is actually not an easy task. Specifically, Uchida *et al.* in 2008 experimentally realized the generation of 1.7 Gbps continuous random bit stream by digitizing the output of two chaotic semiconductor lasers with 1-bit ADCs, but such a system requires a constant average laser intensity and a carefully tuned bit decision voltage that are difficult to stay for long [14]. In 2011, our group generated 2.87 Gbps random bit sequence in real time by using a bandwidth-enhanced chaotic laser from an optical feedback laser diode with optical injection, whereas we also suffer from the similar problems [21]. Later, Symul *et al.* demonstrate 2 Gbps real-time random bit generation using vacuum fluctuations, but their scheme is inconvenient from the viewpoint of practical applications because of the inevitable use of optical spatial components for vacuum state detection [31]. Therefore, there is a great necessity to achieve practical high-speed physical random bit generators for actual needs.

In this paper, we report a prototype of integrated physical random bit generator. Our system utilizes optical fiber components to construct a chaotic laser as the broadband physical entropy source so that it is relatively robust to environmental fluctuations. Utilizing differential comparison and quantization technique, we avoid the strict threshold voltage adjustment as in Refs [14]. and [21] to generate good binary sequences. Finally, our generator can output high-speed and real-time continuous random bit stream with no need of any off-line processing, after an exclusive-OR operation between the two binary sequences. The bit rate of our generator is controlled by a trigger clock and can be continuously tuned up to 4.8 Gbps. The generated random bit streams with this generator are bias-free and mutually independent according to the criteria of three-standard-deviation and can pass successfully industry-standard benchmark tests for randomness provided by the National Institute of Standard Technology (NIST) [34].

2. Experimental Setup

The schematic layout of the prototype of physical random bit generator based on chaotic laser is shown in Fig. 1(a), which includes two main parts: a chaotic laser as physical entropy

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

source and an electronic circuit for quantization. Correspondingly, Figs. 1(b) and 1(c) are the associated external and internal photographs of this prototype whose overall size is 30 cm × 26 cm × 12 cm. Specific operation procedures of our system are as below.

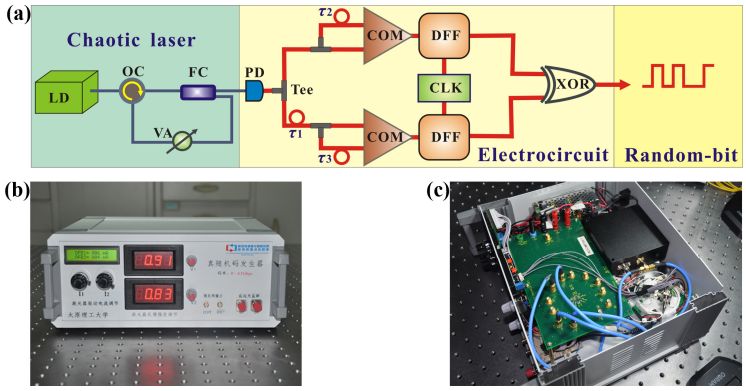

Fig. 1. Device structure. (a) Schematic block diagram of the prototype of physical random bit generator based on optical chaos. LD, a distributed feedback laser diode; OC, an optical circulator; VA, a variable optical attenuator; FC, a fiber coupler; PD, a photo-detector; Tee, Tee connector; COM, a 1-bit comparator; DFF, a D-type flip-flop; CLK, a trigger clock; XOR, an exclusive-OR gate. (b) External photograph and (c) internal photograph of the prototype with a overall size of 30 cm × 26 cm × 12 cm.

The chaotic laser consists of a distributed feedback laser diode (LD, WTD LDM5S752) subject to external optical feedback with a ðber ring cavity, biased at 1.6 times threshold current and stabilized at 1554 nm by a temperature controller. Polarization-maintaining fibers are used for all the optical fiber components. The LD connects to an 80:20 optical fiber coupler (FC) whose principal output passes through a variable optical attenuator (VA) onto a optical circulator (OC), forming the fiber feedback cavity with a time delay on 74 ns and a feedback strength of 40%. Such an optical feedback drives the LD into high-frequency chaotic oscillation, whose characteristics will get detailed analyses in the next section.

The output of chaotic laser is converted and amplified into an electrical stochastic signal through a 12 GHz photodetector (PD, NEW FOCUS Model1554-B) coupled with a direct-current blocking capacitor, which then is split into two beams through a following Tee connector (Tee). After a time lag of τ_1 between the two beams shown in Fig. 1(a), each of them is differentially coupled into a comparator with a 5 GHz equivalent bandwidth (COM, ADCMP567) so that two binary streams are obtained through comparing these associated differential inputs of their respective comparators. Here, note that there are also other time lags between the two differential inputs in each COM [*i.e.*, τ_2 and τ_3 shown in Fig. 1(a)]. After that, two D-type flip-flop with a 6 GHz maximum frequency (DFF, MC10EP52) triggered by the same clock (CLK) are applied to each binary stream so as to generate two raw random bit steams with a determined bit rate, respectively.

Finally, the two raw random bit streams extracted from the chaotic signal and its delay signal with a time lag τ_1 between them undergo a logical exclusive-OR gate (XOR, MC10EP08) so that a real-time continuous high-quality random bit stream with good randomness can be obtain at the output of XOR gate, which will be observed and recorded by an oscilloscope in our experiment.

3. Experimental results

3.1 Chaotic laser characteristics

Figures 2(a) and 2(b) show the measured power spectral density (PSD) and temporal waveform of the chaotic laser operating in the conditions mentioned in section 2. In our measurements, the 12-GHz PD mentioned above, a RF spectrum analyzer with a cutoff frequency of 26.5-GHz (Agilent N9020A, 1 MHz RBW, 3 KHz VBW, 10 ms Sweep time,)

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

and a real time oscilloscope with 6-GHz bandwidth (LeCroy SDA806Zi-A) are used. In addition, the measured PSD here is a result with average times of 100 and thus it is slim and smooth. According to the bandwidth definition of the span between zero and the frequency where 80% of the energy is contained, the bandwidth of the chaotic laser is calculated as about 7 GHz, which guarantees high-speed random bit generation at rates up to Gbps.

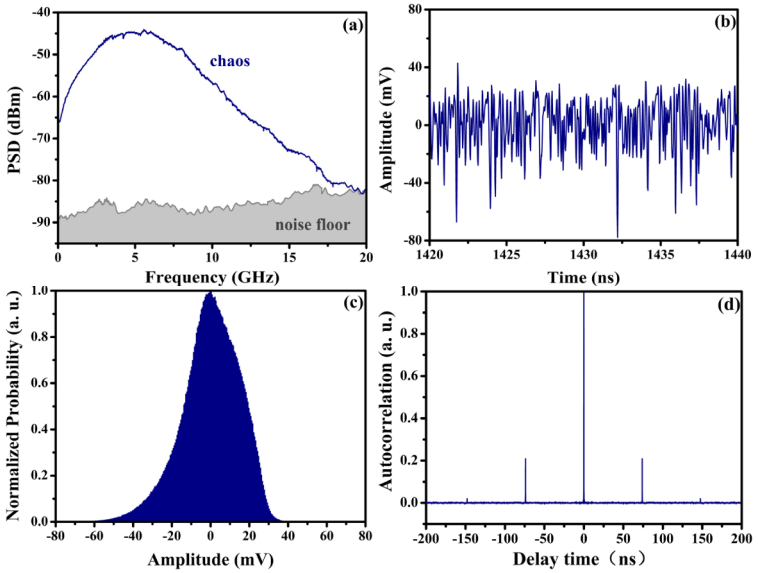

Fig. 2. Characteristics of chaotic laser. (a) Measured power spectral density (PSD) and (b) temporal waveform of the chaotic laser; (c) probability density function (histogram) and (d) autocorrelation function of the temporal waveforms of the chaotic laser.

At the same time, one must note that the chaotic laser with optical feedback has also two inherent shortcomings unfavorable for high-quality random bit generation. The first one is the asymmetric amplitude distribution, which is a typical feature for chaotic systems [35, 36]. Figure 2(c) is the probability density function (histogram) of our chaotic waveforms for a 50 μs data steam, where negative values appear more frequently than positive values. It is difficult for such an asymmetric histogram to perform an equipartition and also difficult to achieve a stationary distribution in short time. Consequently, bias is introduced unavoidably when the chaotic laser is directly converted to a binary sequence by comparing with a constant threshold voltage. This is the main reason that the previous real-time methods for random bit generation need a careful adjustment of decision voltage and they are hard to work smoothly in a long time. The other one is the weak periodicity associated with optical feedback cavity. It can be characterized clearly through the autocorrelation function of the time series. Shown in Fig. 2(d), there is a peak with a correlation coefficient about 0.2 at the location of a delay time 74 ns which corresponds to the round trip time in the external feedback cavity. This kind of weak periodicity cannot be completely eliminated by simply varying the cavity length or feedback strength [37]. These two problems will be dealt with using differential comparison and self-delay XOR techniques in our system, which will be introduced in the second part of this section.

3.2 Random bit generation with differential comparison method

As mentioned above, the conventional quantization to chaotic signal through directly comparing with a threshold needs an accurately decision voltage. This induces the difficulty of longtime stable operation and has a highly adverse effect on practical applications because of the asymmetric amplitude distribution and the threshold voltage drift. To solve this problem, the differential comparison technique is used in our generator. As shown in Fig.

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

1(a), the practical differential comparison operation of our comparators (i.e. COM in Fig. 1) is realized as follows: the chaotic signal $V(t)$ and its delayed signal $V(t-\tau)$ are connected to the differential logic input ports of a COM so that a high level (i.e. logical '1') is obtained when $V(t)$-$V(t-\tau) > 0$ and otherwise a low level (i.e. logical '0') is produced. In other words, the varying physical quantity $V(t-\tau)$ would be regarded as a real threshold voltage when $V(t)$ is treated as the quantized stochastic signal. In principle or theory, this differential comparison process is equivalent to produce a binary sequence via a COM by comparing chaotic signal difference $V(t)$-$V(t-\tau)$ with a equivalent threshold voltage of 0 mV. Note that in this comparison process there is no a real threshold needing to be tuned carefully. Herein, the time lag τ corresponds to the mark of τ_2 or τ_3 shown in Fig. 1(a), and appropriate selection of the lag is the key whether the differential comparison succeeds.

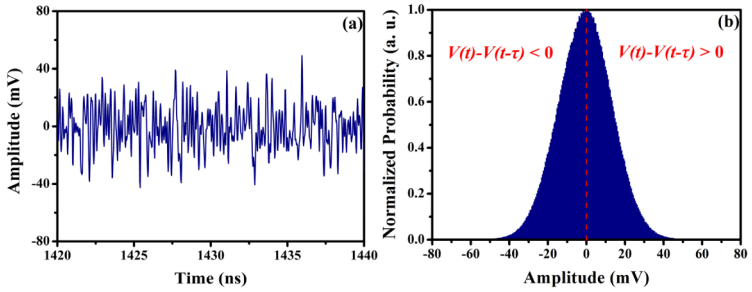

Fig. 3. Characteristics of the calculated temporal waveform $V(t)$-$V(t-\tau)$ through doing subtraction between the measured chaotic signal $V(t)$ and its delayed signal $V(t-\tau)$. (a) Time series and (b) its associated statistical histogram. The Pearson's median skewness coefficient of the histogram is –0.001.

In our system, both τ_2 and τ_3 are set as 2.5 ns through a 0.5 m electrical delay line. At this time, the correlation coefficient between the two differential input signals (*i.e.* $V(t)$ and $V(t-\tau)$) can be calculated to be 0.0003 from Fig. 2(d). Under this condition, they can be considered to be nearly independent with each other and their difference will have a provable highly symmetric amplitude distribution with a determined mean or media value equal to 0 mV [38]. To demonstrate this, we experimentally recorded a chaotic signal $V(t)$ and its delayed signal $V(t-\tau)$ and then calculated their difference. Figures 3(a) and 3(b) display the time series and statistical histogram of the difference between the two chaotic signals, respectively. The statistical histogram has a symmetric profile around 0 with a Pearson's median skewness coefficient of –0.001. This indicates that the differential comparison can yield balanced logical "0" and "1" bits, although the measured chaotic signals unavoidably have a asymmetric amplitude distribution and mean voltage drift mainly induced by thermal or mechanical fluctuations. Thus, our system can avoid the difficulty in decision voltage predetermination and careful tuning to generate a binary signal with a COM. Further, an unbiased binary digital signal with a certain bit rate can be generated after a DFF samples the COM output at the rising edge of CLK, whose rate is determined by the frequency of the CLK frequency.

Certainly, the generated binary sequences only after these procedures above cannot be used directly as random bits due to its inherited weak periodicity from the chaotic laser. So a self-delay logical XOR operation in our system is executed between the two binary sequences from the chaotic signal and its delayed signal with a proper time lag of τ_1 to overcome this limitation, as illustrated in the part of electrical circuit [Fig. 1(a)]. According to the theoretically and experimentally demonstrated criterion about the delay time selection [39], the weak periodicity can be eliminated completely as long as the corresponding autocorrelation coefficient of chaotic signal at τ_1 is less than 0.007. In our prototype generator, the time lag τ_1 is set as 5 ns, around which the correlation coefficient is about 0.001 [Fig. 2(d)].

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

Figures 4(a) and 4(b) are the photographs of the final continuous random bit steam output from the XOR gate and the associated eye diagram, measured with the CLK frequency set to 4.5 GHz and recorded by the real time oscilloscope with a 6 GHz bandwidth and 40 GS/s sample rate. Obviously, the random bit signal is in a non-return-to-zero (NRZ) format and has a bit rate of 4.5 Gbps determined by the CLK frequency. Its eye diagram is opened well, that indicates a good performance.

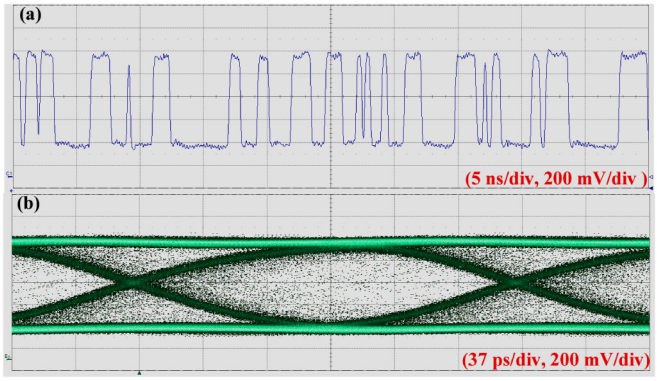

Fig. 4. Photographs of the generated random bit stream after a XOR operation recorded by a real time oscilloscope (LeCroy SDA806Zi-A) when the CLK frequency is set to 4.5 GHz. (a) Temporal waveforms, where these units in vertical and horizontal axes are 200 mV/div and 5 ns/ div, respectively; (b) Eye diagram, where these units in vertical and horizontal axes are 200 mV/div and 37 ps/ div, respectively.

3.3 Randomness verification and stability analysis

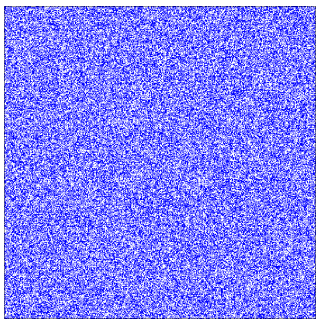

Fig. 5. Bitmap image constructed from 500 × 500 bits of the generated random bit stream with a 4.5 Gbps bit rate. Here, blue and white dots denote logical bits '1' and '0', respectively.

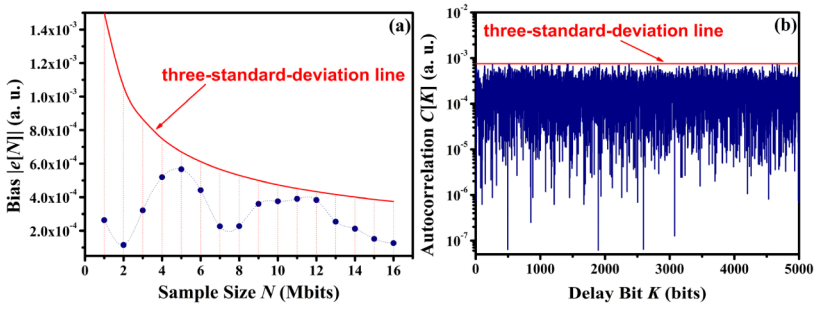

Fig. 6. (a) Bias $|e[N]|$ versus the sample size of the generated 4.5 Gbps random bit sequence; The red line in (a) is its three-standard-deviation line, $3\sigma_e = (3N^{1/2})/2$ where $N = 1, 2, 3, \ldots, 16$ Mbits. (b) Autocorrelation coefficient $C[K]$ as a function of the delay bit K for a 16×10^6 bit

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

stream with a 4.5 Gbps bit rate versus 4.5 Gbps random bit sequence after the XOR operation, respectively; The red lines in (b) is corresponding three-standard-deviation line, $3\sigma_c = 3N^{1/2}$ where N = 16 Mbits.

In this section, we consider the statistical property of the finally acquired random bit streams above. Here, we point out that a high level in the random bit streams is encoded into a logical '1' and otherwise a logical '0' is coded in our analyses.

A true random bit sequence should be bias-free and mutually independent. A qualitative verification of statistical randomness can be characterized by constructing 500 × 500 bits of the generated random bit stream into a bitmap image [Fig. 5], where we can see clearly the bitmap image exhibits no apparent pattern or bias. Further, we give a quantitative demonstration by calculating the bias $|e[N]|$ of the random bit stream (expressed as a[n]) as the sample size N and the normalized autocorrelation coefficient $C[k]$ of a[n] as a function of the delay bit k, respectively. $|e[N]|$ and $C[k]$ are defined as below:

$$|e[N]| = \left| \langle a[n] \rangle - \frac{1}{2} \right|, \tag{1}$$

$$C[k] = \frac{\langle a[n]a[n+k] \rangle - \langle a[n] \rangle^2}{\left(\langle a^2[n] \rangle - \langle a[n] \rangle^2 \right)}, \tag{2}$$

where, <·> represents the statistically evaluated proportion of '1' in the random bit stream. Figure 6(a) depicts the calculated $|e[N]|$ versus different N from 1M bits to 16M bits, while $C[k]$ versus k for a[n] with N = 16M bits is shown in Fig. 6(b). For a finite length of ideal independent random bit sequence, a Gaussian distribution estimation ¥ (0, σ^2) is widely used to evaluate its randomness, where the standard deviation σ equals to $(N^{1/2})/2$ for the estimate of $e[N]$ but is equivalent to $N^{1/2}$ for the estimate of $C[k]$ [15, 25, 26, 28, 29]. When these two estimates of $e[N]$ and $C[k]$ keeps below their own three-standard-deviations written as $3\sigma_e$ and $3\sigma_c$, the evaluated random bit sequence can be considered to be statistically unbiased and independent. It can be clearly conðrmed from Fig. 6 that our generated 4.5 Gbps random bit sequence obeys these three-standard-deviation criteria.

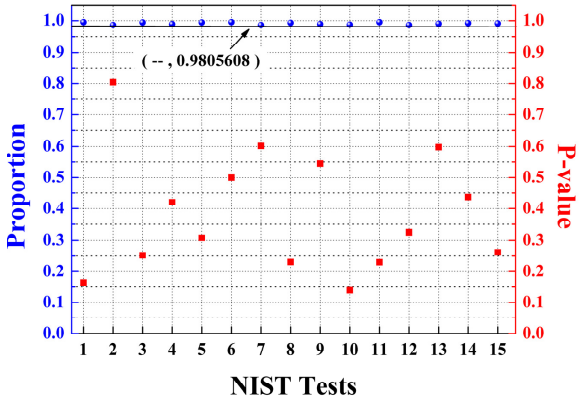

Fig. 7. Typical results of NIST statistical tests. Using 1000 samples of 1 Mb data and significance level β = 0.01, for "Success", the P-value (uniformity of p-values) should be larger than 0.0001 and the proportion should be greater than 0.9805608.

To better qualify the statistical randomness of our generator, we use the more stringent industry-standard statistical test suites provided by the National Institute of Standards and Technology (NIST) [34]. The NIST test suite contains 15 types of statistical tests and each test is based on a calculated statistical p-value, a function of the data being tested. The passing criterion is determined by the length of the tested bit sequence N and the significant level β. In

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

our tests, $N = 1000$ samples of 1 Mb data are applied and α is chosen to be 0.01. In this case, when the proportion of the sequences satisfying p-value > β is in the range of $(1-\beta) \pm \{3 \times [(1-\beta)\ \beta/n]^{1/2}\} = 0.99 \pm 0.0094392$ and the uniformity of the p-values (i.e. the P-value) is larger than 0.0001, the sequences are considered to be random. Figure 7 is a typical result of NIST tests, where the left and right diagram shows the passed proportion and P-value of each tests, respectively. The numbers from 1 to 15 on the horizontal axis represent 15 different statistical tests in NIST test suite, which are named as 'Frequency', 'Block frequency', 'Cumulative sums', 'Runs', 'Longest-run', 'Rank', 'FFT', 'Non-periodic templates', 'Overlapping templates', 'Universal', 'Approximate entropy', 'Random excursions', 'Random excursions variant', 'Serial' and 'Linear Complexity', respectively.

Finally, the stability of our generator is analyzed through monitoring the frequency of '0' bits, which is a good real-time indicator of the randomness of the bit sequence [40]. In the experiment, we recorded a 1 Mb random bit sequence every two minutes to measure its frequency. According to the NIST tests, only a deviation value of 0.13% in the frequency is allowed in this condition. Figure 8 is a typical frequency of '0' bits for the 4.5 Gbps physical random bit generator as a function of time, where the dash lines show the range 50.00 ± 0.13%. This demonstrates that our system can operate stably at least 24 hours.

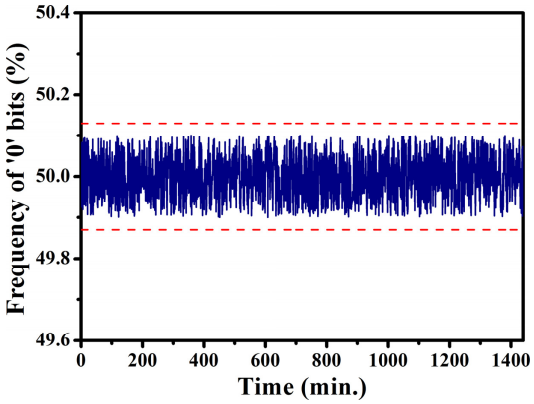

Fig. 8. Measured frequency of '0' bits for the 4.5 Gbps physical random bit generator. Note that the dash lines show the range 50.00 ± 0.13%.

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

4. Discussions and conclusions

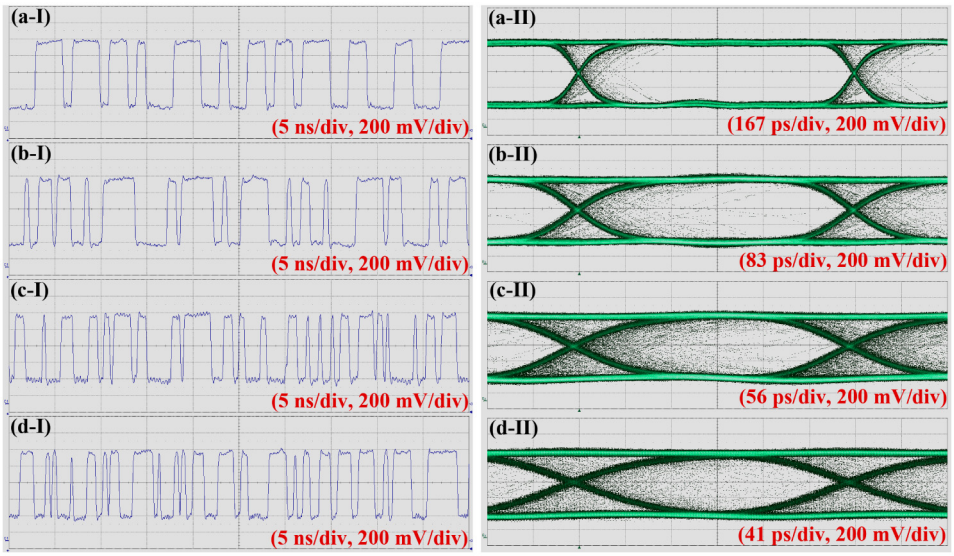

Fig. 9. Photographs of the temporal waveforms (left column, -I) and associated eye diagrams (right column, -II) of the generated random bit streams at different rates of 1 Gbps, 2 Gbps, 3 Gbps and 4 Gbps, which are also measured and recorded with the 6 GHz bandwidth real time oscilloscope(LeCroy SDA806Zi-A). (a) 1 Gbps, (b) 2Gbps, (c) 3 Gbps and (d) 4 Gbps.

One critical factor for many applications of a random generator is the bit rate. The rate in our generator is primarily determined by the frequency of the external trigger clock [CLK shown in Fig. 1(a)]. Through adjusting the repetition frequency of the clock, we can tune the bit rate continuously from 0 to 4.5 Gbps. Figure 9 shows several typical random steam waveforms at different bit rates from our generator and associated measured eye diagrams, where the clock frequency is set to (a) 1 GHz, (b) 2 GHz, (c) 3 GHz and (d) 4 GHz, respectively. This merit of tunability is very useful to efficiently realize absolutely secure communications, because the data rate diversity in the communication networks needs a cipher stream with matched rates to encrypt plaintexts. Herein, we point out that the highest bit rate of our generator can reach 4.5 Gbps, which is mainly limited by the bandwidth of the applied electrical comparator (COM, ADCMP567, 5 GHz equivalent bandwidth). This generation rate of 4.5Gbps has a great practical significance, although it is not very fast. For example, it is sufficient for one-time pad encryption in the widely used Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) with a typical data rate below than 2.5 Gbps. Much higher generation rate can be obtained with the use of faster components and broader bandwidth optical chaos.

Another considered factor for a random generator in practice is its size. The trend in the modern communication systems is towards integration and miniaturization. Regrettably, our current real-time implementation has a overall size of 30 × 26 × 12 cm^3. The occurrence of such a large size is because all of the components in our prototype is discrete and connected via optical fibers or electrical cables. In fact, these components including the chaotic laser, electrical comparators and flip-flops have great potential to be integrated, which will help to highly reduce the overall size. For instance, S. Sunada *et al.* [41] and A. Argyris *et al.* [42] demonstrated that the chaotic laser, the most difficult part to be diminished in size, can be integrated into a chip within a few mm scale by using the photonic integrated circuits. The miniaturization of the proposed prototype into a chip will be one of our future works.

In summary, a prototype of high-speed real-time physical random bit generator based on a chaotic semiconductor laser is achieved and demonstrated to work efficiently. There are two significant merits of our system favorable for practical applications. First, it can output stably

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013

continuous random bit stream in real time, with no need of any off-line processing. Second, its bit generation rate can be continuously tuned up to 4.5 Gbps through handily varying the repetition rate of the external trigger clock. Our system can provide a random bit source for secure communication and cryptography.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant Nos. 60927007, 60908014, 61001114, 61227016, and 61205142), by Shanxi Scholarship Council of China, and by the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi, China (OIT).

#191114 - $15.00 USD Received 23 May 2013; revised 16 Jul 2013; accepted 5 Aug 2013; published 23 Aug 2013