Delay line length selection in generating fast random numbers with a chaotic laser

Jianzhong Zhang, Yuncai Wang,* Lugang Xue, Jiayin Hou, Beibei Zhang, Anbang Wang, and Mingjiang Zhang

Institute of Optoelectronic Engineering, College of Physics & Optoelectronics, Taiyuan University of Technology, 79 West Yingze Street, Taiyuan, Shanxi, 030024, China

*Corresponding author: wangyc@tyut.edu.cn

Received 10 October 2011; revised 5 January 2012; accepted 6 January 2012; posted 6 January 2012 (Doc. ID 156207); published 5 April 2012

The chaotic light signals generated by an external cavity semiconductor laser have been experimentally demonstrated to extract fast random numbers. However, the photon round-trip time in the external cavity can cause the occurrence of the periodicity in random sequences. To overcome it, the exclusive-or operation on corresponding random bits in samples of the chaotic signal and its time-delay signal from a chaotic laser is required. In this scheme, the proper selection of delay length is a key issue. By doing a large number of experiments and theoretically analyzing the interplay between the Runs test and the threshold value of the autocorrelation function, we find when the corresponding delay time of autocorrelation trace with the correlation coefficient of less than 0.007 is considered as the delay time between the chaotic signal and its time-delay signal, streams of random numbers can be generated with verified randomness.

OCIS codes: 140.1540, 190.3100, 140.5960, 060.4510.

1. Introduction

Random number generators (RNGs) have extensive applications in secure communications. For example, random numbers are used as encryption keys and digital signature codes to ensure confidentiality and integrity of the information. There are two categories of RNGs: deterministic pseudorandom number generators (PRNGs) and nondeterministic physical random number generators. Pseudorandom numbers are generated by calculating a deterministic algorithm. Since the result of the algorithm is always determined by the initial seed, the requirement of complete unpredictability is unrealistic, no matter how random the generated sequence is. Distinct from PRNGs, physical random number generators are based on the nondeterministic physical processes, such as radioactive decay [1], atmospheric noise [2], electric noise in circuits [3], frequency jitter of electric oscillator [4], chaotic circuits [5,6], and those based on laser (photon) emission [7–9], which can ensure the inability of pre-estimation on random numbers. However, limited by the mechanism of extracting bit sequences, the rates of such generators have been only several tens of megahertz per second, which is far slower than the data rates of fiber communications.

Chaotic laser signals have been considered as physical entropy source of extracting high-speed random numbers due to their broad bandwidth. Recently, random numbers at rates up to several gigabits per second, and even higher utilizing chaotic lasers have been generated [10–17]. In general, the chaotic light can be achieved by semiconductor lasers through optical injection [18], optical feedback [19], and optoelectronic feedback [20]. Compared with other systems, the laser system with optical feedback can be more easily integrated because of its simple structure [21]. Nevertheless, chaotic signals from semiconductor lasers with optical feedback are characteristic of the periodicity corresponding to the photon round-trip time in the external cavity. The periodicity can seriously influence the randomness

1559-128X/12/111709-06$15.00/0

of the generated random numbers. Thus, to overcome it, the two methods are taken into consideration. One, in terms of chaotic sources, is that a new generation scheme concerning chaotic light is developed to eliminate the feedback-induced periodicity. For example, we proposed and numerically demonstrated that the feedback-induced periodicity signature was suppressed by randomly modulating feedback phase in an external cavity semiconductor laser [22]. Amplitude modulation was also introduced to overcome the quasi periodicity of chaotic signal and especially for the application of physical RNG to public channel tasks [23]. In addition, a photonic integrated chaotic laser with short feedback delay was employed to suppress the existence of external cavity modes [14,17]. The other is that the postprocessing is adopted to improve the randomness. In the case of the latter, there exist two typical techniques. For one thing, the exclusive-or (XOR) operation on two random sequences exacted from two uncorrelated chaotic laser sources was carried out to yield high-quality random numbers [10,16]. For another, the XOR operation on corresponding random bits in samples of the chaotic signal and its time-delay signal from a single chaotic laser was executed [13]. Considering the simplicity and the cost, the latter outweighs the former. However, in this scheme, how to select a suitable delay length is a key issue to ensure high-quality random bit sequence generation.

In this paper, we experimentally summarize a criterion about the selection of the proper delay length. The corresponding delay time of autocorrelation trace with the correlation coefficient of less than 0.007 is selected as the delay time between the chaotic signal and its time-delay signal. This criterion can be theoretically interpreted using the relationship between the correlation coefficient and the total number of the runs in random number sequence. With this criterion, a random number sequence at rates of 1.44 Gbit/s is generated in real time.

2. Experimental Setup

Figure 1 shows the experimental setup of random number generation using a chaotic laser. A distributed-feedback (DFB) laser diode subject to external optical feedback is referred to as the chaotic light source. The amount and polarization state of the feedback light are adjusted by a variable optical attenuator (VOA) and a polarization controller (PC), respectively. The laser output is divided into two beams by a fiber coupler (40:60 coupling ratio), one of which is made as the output of chaotic light source and the other of which is reflected into the laser by a fiber mirror (FM), inducing high-frequency chaotic oscillations of the optical intensity. An optical isolator (OI) is used to prevent unwanted optical feedback into the DFB laser diode. The chaotic laser output is divided into two beams by a 50:50 fiber coupler, again. One beam is detected and converted to the electrical signal by an amplified photodetector (PD1, Thorlabs, PDA8GS, 9 GHz bandwidth). The other beam is through an extra tunable optical delay line (TODL) detected and converted to the electrical signal by PD2 with the same parameter as PD1. The converted electrical signal is coupled to a 1 bit analog-to-digital converter (ADC) consisting of a comparator (ADCMP567) and a D flip-flop (MC10EP52). The binary signal is obtained by comparing with the threshold voltage and then sampled at the rising edge of clock (AD9516-1) to reshape the code width. Finally, to eliminate the periodicity in random sequence due to the photo round-trip time in the external cavity, the XOR operation on corresponding random bits in samples of the chaotic signal and its time-delay signal from a same chaotic laser is done. Thus, the high-speed physical random sequences can be generated in real time. The temporal waveforms of the chaotic signal and random sequence are observed and recorded by a digital oscilloscope (Tektronix, DSA70404B, 4 GHz bandwidth, 25 GS/s). The corresponding radio-frequency (RF) spectrum of the chaotic signal is measured by a spectrum analyzer (Agilent, E4407B, 26.5 GHz bandwidth). However, in the following section, in order to analyze the selection of the delay line length conveniently and in detail, we use the off-line processing. The oscilloscope acquires a digital chaotic time series by 8-bit analog-to-digital sampling of the amplitude at sampling rate of 25 GS/s. The offline processing corresponding to the 1 bit ADC and XOR operation is implemented in three steps as follows:

(1) Each of the 8 bit samples acquired by the oscilloscope is compared with a special 8 bit threshold value to obtain a single bit per sample.

(2) Every 25th bit is extracted, corresponding to the specified clock rate of 1.0 GHz.

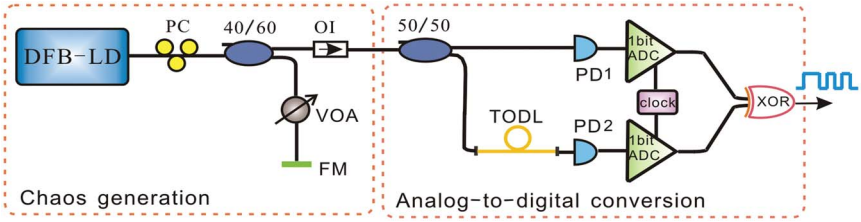

Fig. 1. (Color online) Experimental setup of random number generation using a chaotic laser. PC, polarization controller; OI, optical isolator; PD, photodetector; TODL, tunable optical delay line; VOA, variable optical attenuator; FM, fiber mirror; 1 bit ADC, 1 bit analog-to-digital converter consisting of a comparator and a D flip-flop; XOR, exclusive-OR.

(3) The bit sequences extracted from the chaotic signal and its delayed signal are combined using bitwise XOR operation.

3. Delay Line Length Determination

In the experiment, we adjust the injection current, the length of the external cavity, and the external feedback strength to put the laser in a regime of high-bandwidth chaos. The semiconductor laser is biased at 1.8 times its threshold current (21 mA). The fiber length between the semiconductor laser and the fiber reflector is about 8.4 m, corresponding to the feedback delay time (round trip) of 84 ns. The feedback strength is 80% of laser output power. Under these conditions, chaotic laser signal, the bandwidth of which is about 7.5 GHz, is obtained, and the length of each data frame recorded by the oscilloscope is 5 megasamples (The sampling rate is fixed at 5 GS/s). The corresponding RF spectrum of chaotic laser output is shown in Fig. 2. Here, we adopt the bandwidth definition of chaotic waveform as the span between the zero and the frequency where 80% of the energy is contained within it. For more details, see [24]. The broad chaos bandwidth enables us to generate high-speed random number sequences. However, by enlarging the small part of the RF spectrum over 2.5–2.6 GHz, as shown in the inset of Fig. 2, we can see that the peak interval is constant at 12 MHz, and it corresponds to the inverse of the round-trip time of the feedback light in the external cavity. The occurrence of the feedback delay induced periodicity can decrease the randomness of the random bit sequence.

To suppress the periodicity, the XOR operation on corresponding random bits in samples of the chaotic signal from a single chaotic laser and its time-delay signal is required. How to select a proper delay line length is a key issue to ensure the low correlation of two XORed random sequences. The delay line length between the chaotic signal and its time-delay signal corresponds to x-coordinate of autocorrelation trace of the chaotic signal, i.e., the delay time of Fig. 3. So the correlation between the chaotic signal and its time-delay signal can be assessed by the correlation coefficient of autocorrelation trace of the chaotic signal. From Fig. 3, we can see that the secondary peak of the autocorrelation trace appears at 84 ns, corresponding to the external cavity round-trip time, also showing the periodicity induced by the external cavity.

Here, the delay line length is gradually changed to eventually generate binary bit sequences with different randomness. The randomness of generated digital bit sequences is tested using the standard statistical test (NIST Special Publication 800–22) suite for random number generators provided by the National Institute of Standard Technology (NIST) [25]. The NIST SP 800–22 test consists of 15 statistical tests. When the delay line length is gradually adjusted from 0 m to 10 m, a large number of random sequences extracted from the chaotic laser with different chaotic states tested. The different chaotic states are obtained by changing the external cavity length, bias current, and feedback strength of the external cavity semiconductor laser. Therefore, as far as each delay line length is concerned, approximately 10,000 series of random sequences are generated by changing the above three parameters. The sufficient data for the statistical test of randomness can be ensured. The relationship between the autocorrelation coefficient and randomness tests is further investigated. Figure 4 shows the summary of the number of passed tests for NIST SP 800–22 at different chaotic autocorrelation coefficient, which corresponds to the certain delay line length. All 15 tests are passed when the correlation coefficient is located between −0.007 and 0.007. Furthermore, the proportion of all 15 passed tests is 1.0 for nearly 10,000 random sequences. However, the number of passed tests keeps decreasing when the absolute value of the correlation coefficient continued to increase over 0.007, as shown in Fig. 5. When the absolute value of the

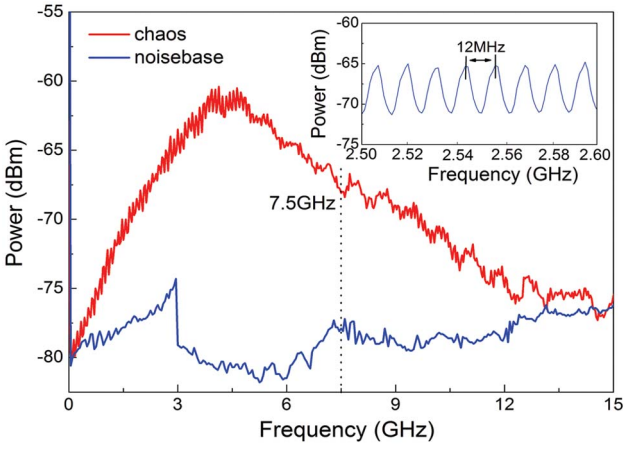

Fig. 2. (Color online) RF spectrum of chaotic laser output. The inset shows the enlargement of the small part of the chaotic RF spectrum over 2.5–2.6 GHz.

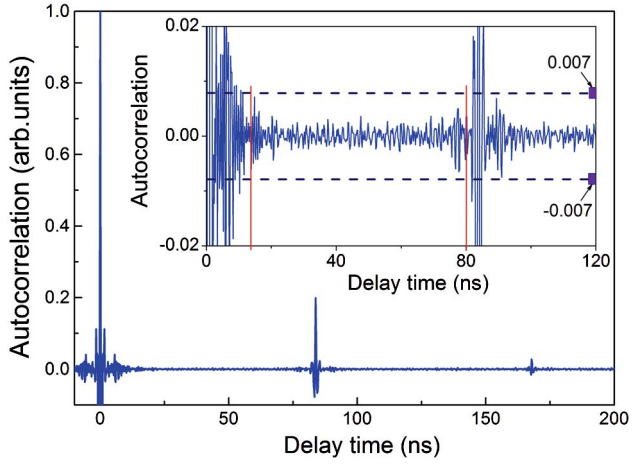

Fig. 3. (Color online) Autocorrelation function of the chaotic laser signal. The y-coordinate represents the correlation coefficient. The inset shows the enlargement of the short-time autocorrelation from 0 and 120 ns.

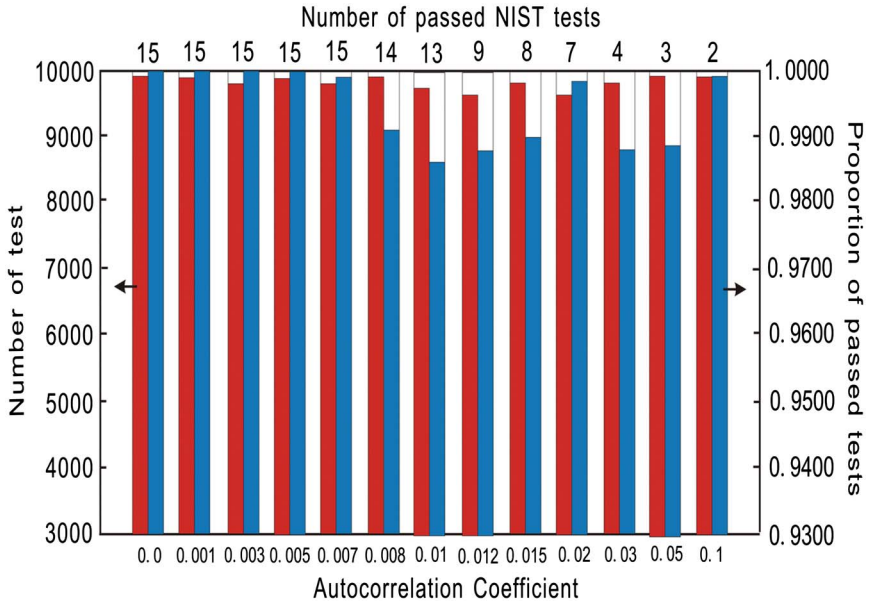

Fig. 4. (Color online) Summary of the number of passed tests for NIST SP 800–22 at different chaotic autocorrelation coefficients, which corresponds to the delay line length.

autocorrelation coefficient is increased to 0.1, the number of passed tests is degraded to 2. Hence, according to the correlation coefficient distribution from the autocorrelation trace of the chaotic signal, we can judge how long a delay line is, which helps to generate high-quality random number sequence. As the example shown in the inset of Fig. 3, when the length of delay line is set from 1.5 to 8 m (the delay time is from 15 to 80 ns correspondingly), all the correlation coefficients are less than 0.007, so this can be a proper range to choose a delay line length.

From the above analysis, we demonstrate that when the correlation coefficient of chaotic signal is larger than 0.007, all 15 tests in NIST SP 800–22 are not passed. Moreover, we notice that under normal circumstances, the runs test is firstly failed. As the correlation coefficient increases, more tests can be failed. We also find that the runs test is always one of the failed tests. To give more insight into the dependence of the runs test on the correlation coefficient, we focus on the runs test. This test mainly

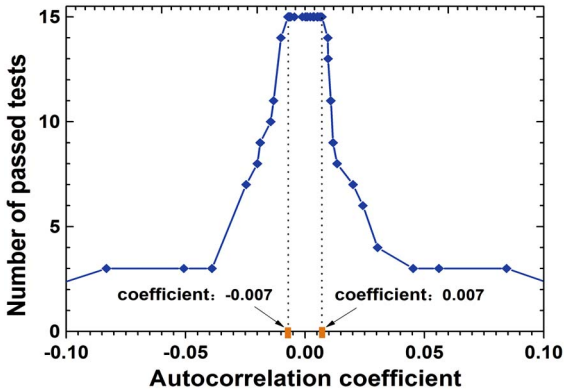

Fig. 5. (Color online) Number of passed tests for NIST SP 800–22 at different chaotic autocorrelation coefficients, which corresponds to the delay line length.

examines the total number of runs in the sequence, and determines whether the oscillation between such zeros and ones is too fast or too low. A run is an uninterrupted sequence of identical bits. The total number of runs across all the bits including the total number of zero runs and the total number of one runs is calculated as follows:

$$V_n(\text{obs}) = \sum_{k=1}^{n-1} r(k) + 1, \tag{1}$$

$$r(k) = \begin{cases} 0, & \varepsilon_k = \varepsilon_{k+1} \\ 0, & \varepsilon_k \neq \varepsilon_{k+1} \end{cases}, \tag{2}$$

where ε is the sequence of bits being tested ($\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$; $\varepsilon_k = 0$ or 1) and n is the length of the bit string. The zeros and ones of the input sequence (ε) are converted to values of -1 and $+1$ to create the sequence $\xi = \xi_1, \xi_2, ..., \xi_n$, where $\xi_k = 2\varepsilon_k - 1$. The normalized correlation coefficient of the sequence (ξ) at lag 1 bit is computed in the following way:

$$\rho = \frac{1}{n} \sum_{k=1}^{n-1} \xi_k \xi_{k+1} \tag{3}$$

Note that for the sequence (ε), if $\varepsilon_k = \varepsilon_{k+1}$, $r(k) = 0$, otherwise, $r(k) = 1$; for the converted sequence (ξ), if ξ_k and ξ_{k+1} have the same sign, the value of $\xi_k \cdot \xi_{k+1}$ is 1, otherwise, the value is -1. Thus, the corresponding equation is obtained as

$$\xi_k \xi_{k+1} = -2r(k) + 1 \tag{4}$$

According to Eq. (1) and Eq. (4), we find that the relation between the correlation coefficient and the total number of runs can be expressed as

$$\rho = 1 + \frac{1}{n} - \frac{2}{n} V_n(\text{obs}), \tag{5}$$

In the runs test, the test statistic $V_n(\text{obs})$ is used to calculate a P-value according to Eq. (6) in order to assess a confidence level of that a sequence would be random:

$$P - \text{value} = \text{erfc}\left[\frac{|V_n(\text{obs}) - 2n\delta(1-\delta)|}{2\sqrt{2n}\delta(1-\delta)}\right], \tag{6}$$

where δ is the proportion of ones in the input sequence (ε) and is 0.5 for a completely random binary sequence. For the decision rule of the runs test, if the computed P-value is larger than 0.01, then conclude that the sequence is random. Thus, according to Eq. (5) and Eq. (6), we obtain that if the generated random sequence can pass the runs test, the correlation coefficient should be less than 0.003. Actually, the autocorrelation trace of the chaotic signal has almost same distribution as the autocorrelation trace of the corresponding extracted random bit sequence. Therefore, the correlation coefficient of the chaotic signal is required to be less than 0.003 for the passage of the runs test. However, in the above experimental analysis, the correlation coefficient should be less than 0.007. This is because a random bit stream is finally obtained by XOR operation on corresponding random bits in samples of the chaotic signal and its time-delay signal. The XOR operation can improve the distribution of the runs in random sequence to some extent. Thus, the range of the theoretically calculated correlation coefficient may be expanded to less than 0.007, as is shown by a large number of experiments.

4. Random Number Generation

Making use of the above-obtained criterion, an example of random bit generation at 1 Gbit/s is given using the chaotic waveforms recorded. The fiber delay line length is set to 4 m, and the corresponding correlation coefficient is 0.003 less than 0.007. Two beams of chaotic light are converted to binary bit signal (0 and 1) at clock rate of 1 GHz by two comparators with the set threshold values. Then the two binary signals are combined by a logical XOR operation to generate a 1 Gbit/s random number sequence, as shown in Fig. 6. The sequences pass NIST SP 800–22 tests, and typical results are shown in Table 1.

In addition, with this criterion, a real-time output example of random bit sequence is given under the

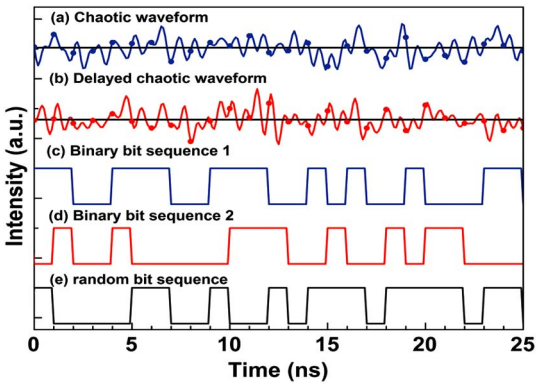

Fig. 6. (Color online) Extraction of random number sequence from chaotic signals. (a) Time series of the chaotic waveforms; (b) time series of the time-delay signal; (c) and (d) the extracted binary bit signals; (e) output random number sequence after XOR operation.

Table 1. Results of NIST SP 800–22 Statistical Tests. For "Success" Using 1000 Samples of 1-Mbit Data and Significance Level $\alpha = 0.01$, the *P*-value (Uniformity of *P*-values) Should Be Larger Than 0.0001 and the Proportion Should Be within the Range of 0.99 ± 0.0094392. For the Tests that Produce Multiple *P*-values and Proportions, the Worst Case Is Shown

Statistical test	*P*-value	Proportion	Result
Frequency	0.691219	0.997	success
Block frequency	0.811212	0.992	success
Cumulative sums	0.381563	0.994	success
Runs	0.977532	0.995	success
FFT	0.542236	0.996	success
Longest-run	0.145537	0.986	success
Rank	0.689524	0.991	success
Nonperiodic templates	0.289674	0.995	success
Overlapping templates	0.767545	0.994	success
Universal	0.654563	0.989	success
Approximate	0.377568	0.997	success
Random excursions	0.426468	0.993	success
Random excursions variant	0.125687	0.995	success
Serial	0.648254	0.994	success
Linear complexity	0.467452	0.993	success

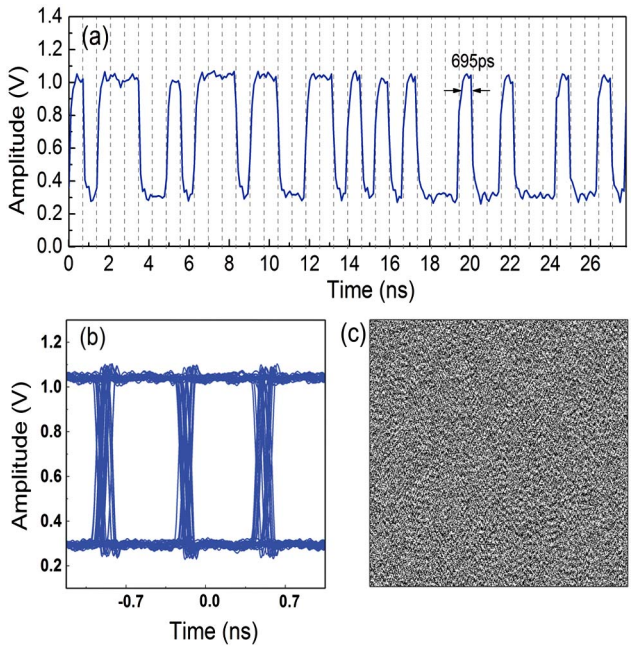

Fig. 7. (Color online) Real-time output random bit sequence from RNG experimental system. (a) The temporal waveform of the random sequence at 1.44 Gbit/s after the XOR operation. (b) An eye diagram of the random sequence. (c) A random dot diagram of the random sequence. Random bit patterns with 500×500 bits are shown in a two-dimensional plane. Bits "1" and "0" are converted to white and black dots, respectively, and placed from left to right (and from top to bottom).

same experimental conditions as the above offline processing. The generation rate is 1.44 Gbit/s, corresponding to a clock frequency of 1.44 GHz generated by AD9516-1 clock module. Figure 7(a) shows the temporal waveform of the random bit sequence at 1.44 Gbit/s after the XOR operation. The output sequence is in a non-return-to-zero code format, in which the minimum code width is 695 ps and the peak-to-peak voltage value is about 0.7 V. Figure 7(b) depicts an eye diagram of the generated random bit sequence. The measured eye diagram is obviously opening. Figure 7(c) illustrates a random dot diagram with 500 × 500 bits in a two-dimensional plane. Bits "1" and "0" are converted to white and black dots, respectively, and placed from left to right (and from top to bottom). It can be seen that there are no obvious patterns, as we would expect that the ratio of 1 and 0 is roughly equal. To further evaluate the statistical properties of random bit sequences, we use NIST SP 800–22 tests. The tests are carried out using 1000 samples of 1 Mbit data for NIST tests. The sequences pass all the NIST tests.

5. Conclusions

In conclusion, to overcome the external cavity induced periodicity in random sequence, the XOR operation on corresponding random bits in samples of the chaotic signal and its time-delay signal from a chaotic laser is executed. In this scheme, the proper selection of delay length is a key issue to generate a high-quality random bit sequence. A large number of experiments show that the selection of a proper delay length depends on the correlation coefficient of autocorrelation trace of the chaotic signal. The experimental results demonstrate that when the correlation coefficient is less than 0.007 and the corresponding delay time of autocorrelation trace is considered as the delay time between the chaotic signal and its time-delay signal, the random bit sequence can be generated with verified randomness. A theoretical interpretation can be provided by analyzing the relationship between the correlation coefficient and the total number of the runs in the generated random sequence. Under the guidance of the above results, a random bit stream at rates of 1.44 Gbit/s is generated in real time.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 60927007 and 61001114) and Shanxi Province Science Foundation for Youths (Grant No. 2010021003-4).

References

1. J. Walker, "HotBits: random numbers from radioactive decay," http://www.fourmilab.ch/.
2. M. Haahr, "Random.org: true random number service," http://www.random.org/.
3. C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I **47**, 615–621 (2000).
4. B. Jun and P. Kocher, "The Intel random number generator," white paper prepared for Intel Corporation (1999).
5. T. Stojanovski and L. Kocarev, "Chaos-based random number generators—part I: analysis," IEEE Trans. Circuits Syst. I **48**, 281–288 (2001).
6. T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators-part II: Practical realization," IEEE Trans. Circuits Syst. I **48**, 382–385 (2001).
7. H. Q. Ma, Y. J. Xie, and L. A. Wu, "Random number generation based on the time of arrival of single photons," Appl. Opt. **44**, 7760–7763 (2005).
8. O. Kwon, Y. W. Cho, and Y. H. Kim, "Quantum random number generator using photon-number path entanglement," Appl. Opt. **48**, 1774–1778 (2009).
9. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**, 13029–13037 (2010).
10. 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. Photon. **2**, 728–732 (2008).
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**, 024102 (2009).
12. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photon. **4**, 58–61 (2010).
13. 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**, 5512–5524 (2010).
14. 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**, 18763–18768 (2010).
15. P. Li, Y. C. Wang, and J. Z. Zhang, "All-optical fast random number generator," Opt. Express **18**, 20360–20369 (2010).
16. 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).
17. T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," Phys. Rev. A **83**, 031803 (2011).
18. S. K. Hwang and J. M. Liu, "Dynamical characteristics of an optically injected semiconductor laser," Opt. Commun. **183**, 195–205 (2003).
19. Y. C. Wang, L. Q. Kong, A. B. Wang, and L. L. Fan, "Coherence length tunable semiconductor laser with optical feedback," Appl. Opt. **48**, 969–973 (2009).
20. S. Tang and J. M. Liu, "Chaotic pulsing and quasi-periodic route to chaos in a semiconductor laser with delayed opto-electronic feedback," IEEE J. Quantum Electron. **37**, 329–336 (2001).
21. A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," Phys. Rev. Lett. **100**, 194101 (2008).
22. J. Z. Zhang, A. B. Wang, M. J. Zhang, X. C. Li, and Y. C. Wang, "Elimination of time-delay signature in an external cavity semiconductor laser by randomly modulating feedback phase," Acta Phys. Sin. **60**, 094207 (2011).
23. I. Kanter, M. Butkovski, Y. Peteg, 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**, 18292–18302 (2010).
24. A. B. Wang, Y. C. Wang, and H. C. He, "Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback," IEEE Photon. Technol. Lett. **20**, 1633–1635 (2008).
25. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Spec. Publ. 800–22, rev. 1 (2008).