Chaotic-laser-based true random sequence generation for spread-spectrum communications

Zhaoxia Zhang (张朝霞)[1,2*], Junjie Zhou (周俊杰)[1], Dongze Zhang (张东泽)[1], Zheng Fu (傅 正)[1], and Jianzhong Zhang (张建忠)[1]

([1] *College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan* 030024, *China*
[2] *State Key Laboratory of Millimeter Waves, Southeast University, Nanjing* 210096, *China*)

[*] *Corresponding author: zhangzhaoxia@tyut.edu.cn*

Received May 17, 2012; accepted July 16, 2012

Abstract We propose a scheme for spread-spectrum communications using true random sequences generated by chaotic semiconductor lasers as spreading codes. These sequences can eliminate the inherent periodicity of pseudorandom sequences, enlarge the capacity of spread-spectrum codes, improve communication security, and increase the number of users of the system. When a true random sequence with an appropriate length is used as the spread-spectrum code and the information speed is maintained constant, the system acquires a greater spread-spectrum gain and a lower bit-error ratio (BER) than the traditional spread-spectrum system. The communication security is also enhanced. The BER smoothly increases with the number of users, which indicates the good multiple-access capability of the system.

OCIS codes 060.4510; 060.4785; 060.2605; 140.3490

doi: 10.3788/CJL201239.1005006

1 Introduction

The direct sequence spread spectrum (DSSS) is one of several approaches to spread-spectrum modulation for digital signal transmission over airwaves. In the DSSS, the stream of information to be transmitted is multiplied by a higher-data-rate bit sequence (also known as a random sequence) to accomplish the spreading operation. The signal in the receiver is multiplied by the same random sequence to accomplish the despreading operation. The random sequence helps the signal resist interference and enables the original information to be recovered in the receiver.

In a spread-spectrum communication system, the spread spectrum is widely realized by substituting high speed random codes for a 1-bit source stream, which helps improve the anti-interference ability of the system. In traditional DSSS communications, once the spread-spectrum sequence is generated, it becomes constant during the process of communication and induces the code periodicity. Hackers can easily use this periodicity to obtain the spread-spectrum codes. The codes should be changed to enhance the anti-interference ability and the safety of spread-spectrum systems. In 2005, Wang *et al*.[1] proposed a scheme to generate chaotic binary codes using a chain of coupled chaotic maps, and demonstrated that the codes could be applied to baseband spread-spectrum communications. Theoretically, the above chaotic code period is infinitely long. However, the period is practically limited by the word length of the microprocessor and can be deciphered[2]. True random sequences can meet these requirements for spread-spectrum communication security. Compared with pseudorandom numbers as spreading codes, true random sequences are characterized by aperiodicity, unpredictability, non-replicability, and difficult decipherability.

Various methods are used to generate true random numbers. Traditional random-number generators (RNGs) are based on the thermal noise of circuits or resistances[3,4], oscillation frequency of oscillation circuit[5], randomness of quantum mechanics fundamental quantity[6], and circuit chaos[7]. However, the rates of these approaches are limited by their low bandwidths. Typically, the bandwidths of electric chaos are below 1 GHz and can only reach a rate less than 200 Mb/s[7]. Another kind of novel RNG is based on chaotic lasers. The wide bandwidth of a chaotic laser is sufficient to reach the upper-limit bandwidth of electronic data processing. In 2007, our group proposed a fast true RNG utilizing a wideband chaos light that was realized by an optical feedback semiconductor laser[8]. In 2008, Uchida *et al*.[9,10] experimentally obtained for the first time a 1.7-Gb/s RNG using chaotic lasers. In the same year, we enhanced the bandwidth of an optical feedback semiconductor laser to several tens of gigahertzs using continuous-wave (CW) optical

injection[11]. This achievement indicates that true random numbers with high rates can be accomplished. In 2010, we then demonstrated an all-optical scheme of a RNG that performed all signal processing in the optical domain, and could generate 10-Gb/s random numbers[12].

From the analysis above, we know that the rate of a true RNG has widely reached the order of magnitude of gigabits per second. The synchronization technique of the true random numbers has also been realized[13]. Thus, adopting true random numbers as spread-spectrum sequences in spread-spectrum communications is feasible.

In this paper, we propose a spread-spectrum scheme using the true random numbers produced by chaotic semiconductor lasers as spread-spectrum codes to implement safe and highly efficient spread-spectrum communications. We demonstrate the feasibility and practicability of the scheme using Matlab software.

2 Scheme of true random sequence for spread spectrum

The schematic of spread-spectrum communications is shown in Fig. 1. The transmitter converts the input message into a digital signal through an information source encoder. Then, the digital signal after the spread spectrum is radio-frequency (RF) modulated and transmitted via antennas. Compared with the traditional spread-spectrum communication system, we utilize the true random sequences above for random sequences. In the receiver, the original input message can be recovered through opposite operations.

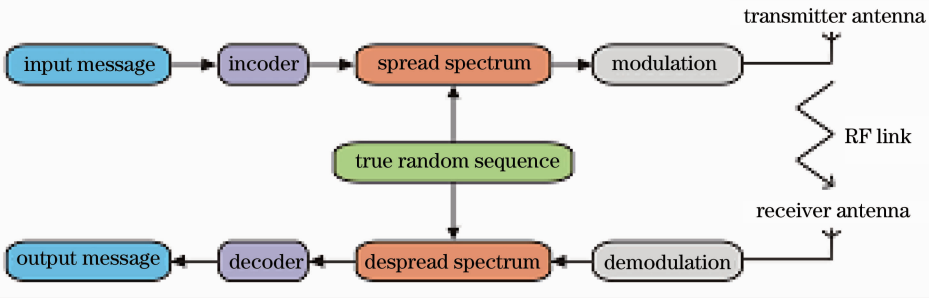

Fig. 1 Schematic of spread-spectrum communications using a true random sequence.

We utilize Simulink to build the simulation model of a DSSS communication system, as shown in Fig. 2. The binary random signal source is multiplied by the input true random sequences after polarity-reversal, which can realize spread-spectrum communications. The signal subsequently passes through the additional white Gaussian noise channel. In the receiver, the signal is multiplied by the true random sequences to complete the process of despreading. Afterwards, the signal becomes binary random sequences via polarity reversal. During the simulation, we use a bit-error analyzer to compare the transmitted binary random codes with the despreaded random codes to calculate the bit-error ratio (BER).

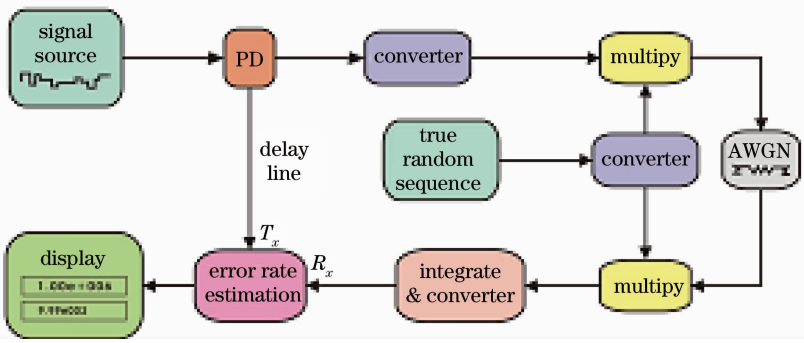

Fig. 2 Simulation model of a DSSS communication system.

3 Experimental results

3.1 Experimental setup

The schematic of the generation of the true random sequence based on chaotic lasers is shown in Fig. 3.

Two semiconductor lasers are used for the chaotic intensity oscillations in the scheme. The output intensity of each laser is converted to an alternating current (AC) electrical signal using photodetectors (PDs). After amplification, the AC electrical signal is converted into a binary signal using two comparators

(Comp). The binary signal is then converted into the random number and its code rate is controlled by the clock. The binary bit signals obtained from the lasers are combined by a logical exclusive-OR (XOR) operation to generate a single random-bit sequence. The subsequent process, i. e., XOR, improves the randomness of the random sequence. The experimental setup of chaotic laser signals using distributed-feedback semiconductor lasers is described elsewhere[14].

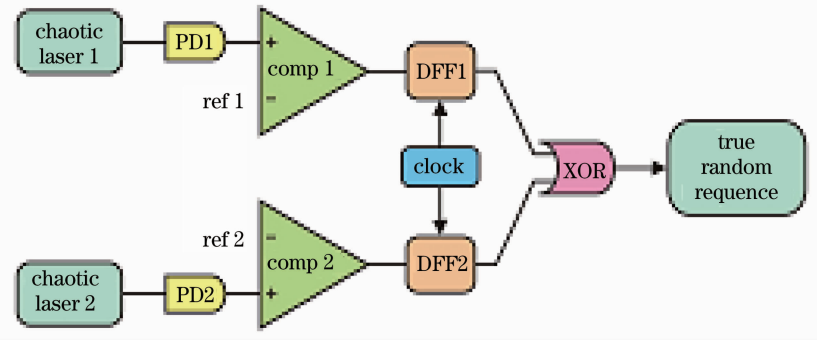

Fig. 3 Experimental setup of the true random sequence.

3.2 Characteristics of true random sequences

We generate many random sequences using the chaotic lasers, as shown in Fig. 3. The length of the random sequence is selected according to our need. For example, we can select the first 2000 bits for the first random sequence, the following 2000 bits for the second sequence, and so on. The first random sequence is one of the true random sequences (expressed as x_1), and the second random sequence (expressed as x_2) is another true random sequence generated by the chaotic lasers.

First, we analyze the self-similarity of the true random sequences. The similarity between two random sequences can be expressed by the autocorrelation function $R_{ac}(m)$ and the cross-correlation function $R_{cc}(m)$, which are expressed as

$$R_{ac}(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \overline{x})(x_{i+m} - \overline{x}), \quad (1)$$

$$R_{cc}(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_{1i} - \overline{x})[x_{2(i+m)} - \overline{x}], \quad (2)$$

where m is the delay bit of the random sequence, x_i is the ith bit value of the random sequence, x_{i+m} is the $(i+m)$th bit value of the random sequence, $\overline{x}$ is the mean value of the random sequence, x_{1i} is the ith bit value of the first random sequence of x_1, and $x_{2(i+m)}$ is the $(i+m)$th bit value of the second random sequence of x_2. The autocorrelation and cross-correlation coefficients are the normalization of the autocorrelation and cross-correlation functions, respectively. Ideally, the value of the autocorrelation and cross-correlation functions of the true random number sequence is δ function and 0, respectively.

Fig. 4(a) illustrates the autocorrelation function of a traditional m sequence, and shows that the m sequence has a strong periodicity. In comparison, the autocorrelation of the random sequences generated by the chaotic lasers is shown in Fig. 4(b), which demonstrates a shape similar to a δ function. This result indicates that the true random numbers are much better than the m sequences.

Fig. 4(c) and (d) are the cross-correlation functions of the m sequences and true random numbers, respectively. These functions illustrate a sharp pulse spiking in the cross-correlation function of m sequences, whereas the true random numbers have a relatively better cross-correlation function. True random numbers are better than m sequences as spread-spectrum codes.

Then, we consider the effect of random sequences on the capacity of a communication system. The capacity of a traditional DS-CDMA communication system is determined by the available spread-spectrum numbers. For example, if the spreading factor N is 1023, the available number of m sequence is only 60, which limits the capacity of the system. In contrast, using the true random numbers as spread-spectrum codes can significantly enhance the capacity of the system. True random sequences generated by chaotic semiconductor lasers are sequences whose codes are random and independent of one another. The high linear complexity in such sequences enhances the anti-decryption and anti-interference performances of the system.

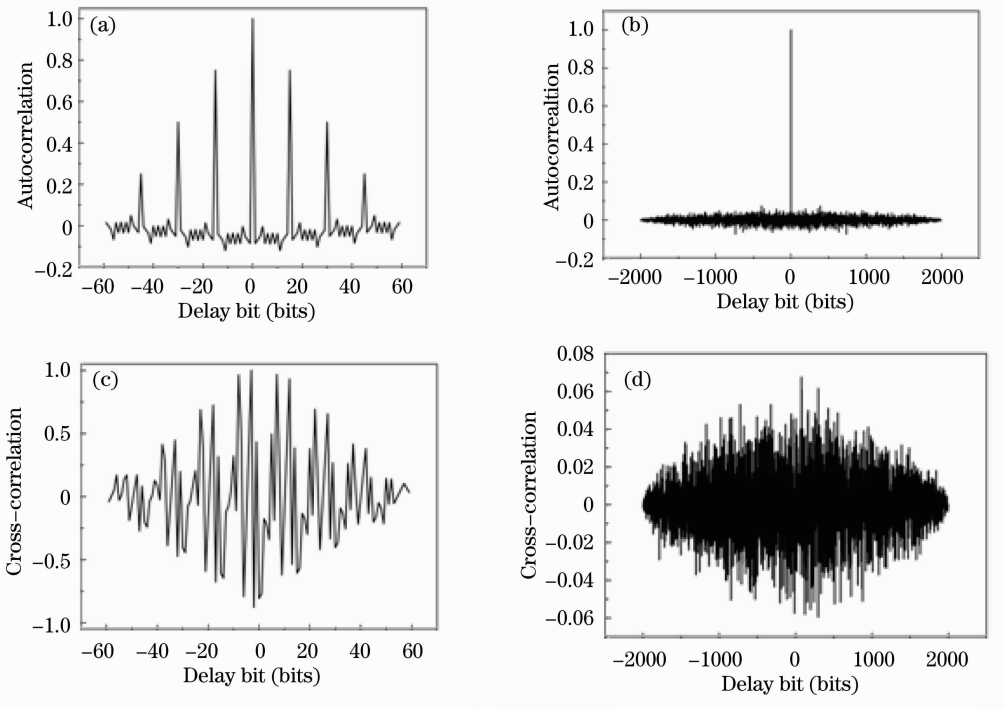

Fig. 4 Autocorrelation and cross-correlation of m sequences and generated random sequences. (a) Autocorrelation of the m sequence whose period is 15; (b) autocorrelation of the generated random sequence; (c) cross-correlation of the m sequence whose period is 15; (d) cross-correlation of the generated random sequence.

3.3 Realization of spread-spectrum communications

Fig. 5 shows the relationship among the information rate, spread-spectrum gain, and BER. As shown in Fig. 5, when the information rate is constant, the spread-spectrum gain increases with decreased BER. When the signal-to-noise ratio (SNR) is -20 dB, increasing the spread-spectrum gain can effectively reduce the BER of the system. Fig. 5 also shows that when the information rate is 2 MHz, the spread-spectrum gain is 0 dB and the BER of the system is 0.4623. If the information rate is 2 MHz and the spread-spectrum gain is 10 dB, the BER of the system is 0.3765. If the spread-spectrum gain is 20 dB, the BER of the system is 0.1567. Hence, the influence of the information rate on the BER is very small because the channel bandwidth is correspondingly enhanced with increased information rate. Therefore, we can reduce the BER by increasing the spread-spectrum gain in a practical communication system. At the same time, our system assigns a section of the random sequence to represent "1" and the other different section of the random sequence to represent "0". This processing method doubles the noise margin of a communication system compared with the orthogonal code.

Alternatively, we want to stress the anti-interference of the system. Two main interferences are found in a spread-spectrum communication system,

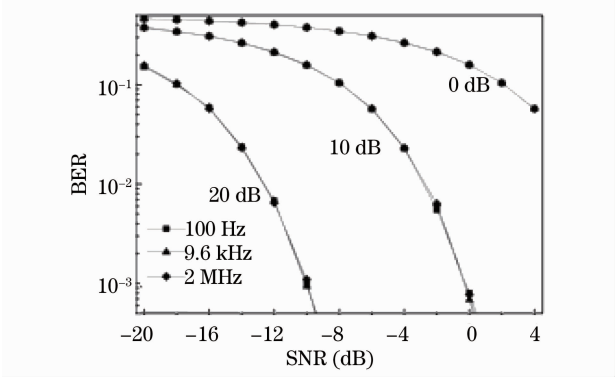

Fig. 5 Relationship of the BER and spread-spectrum gain with the SNR.

namely, multi-path and multi-user interferences. Multi-path interference is associated with the autocorrelation of spread-spectrum codes, whereas multi-user interference is mainly related to the cross-correlation of spread-spectrum codes. Therefore, we choose the orthogonal spread-spectrum codes to minimize the relevance between codes. We also find that the autocorrelation and cross-correlation of the true random sequence decrease with increased length of the random sequence length. Therefore, if the spread-spectrum codes have an appropriate length, the interference of the system is reduced.

Performance against multi-path and multi-user interferences can be characterized by the mean-square

values of the autocorrelation side lobe $[\delta_{ac}^2(m)]$ and of the cross-correlation $[\delta_{cc}^2(m)]$, respectively:

$$\delta_{ac}^2(m) = \frac{1}{M}\sum_{m=1}^{M}[R_{ac}(m)]^2, \tag{3}$$

$$\delta_{cc}^2(m) = \frac{1}{2M+1}\sum_{m=-M}^{M}[R_{cc}(m)]^2, \tag{4}$$

where $R_{ac}(m)$ and $R_{cc}(m)$ are the values of the autocorrelation and cross-correlation of the m bit of the generated sequence, respectively.

Fig. 6 is the curve of the mean-square value of our random sequence. The mean-square values of the autocorrelation side lobe and cross-correlation decrease with increased random-sequence length. When the random-sequence length increases to 2000, the mean-square values of the autocorrelation side lobe and cross-correlation are less than 0.6×10^{-3}. In the following simulation, we choose 2000 to 5000 bit random sequences as spread-spectrum codes.

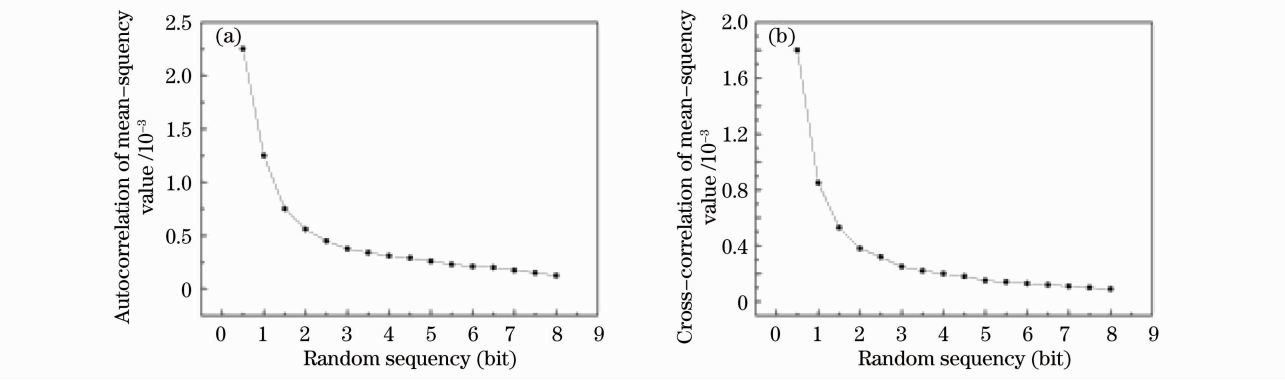

Fig. 6 Mean-square values of the autocorrelation and cross-correlation of the random sequence.

The simulation results of the error probabilities for the true random sequence and m sequence are shown in Fig. 7. When the users are the same, the BER of the true random sequence is lower than that of the m sequence. This result demonstrates that the communication system can hold more users if true random sequences are used for spreading-spectrum codes. Therefore, the performance of the proposed system is enhanced.

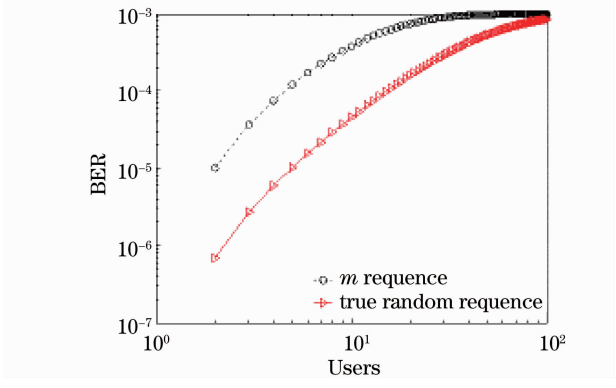

Fig. 7 Comparison of the error probabilities of a system using the true random sequence and m sequence for a sequence length of 63 and for different numbers of users (channel SNR is 25 dB).

4 Discussions

The pseudorandom sequences in the traditional spread-spectrum system have inherent periodicity, which limits the capacity of the system and threatens the system safety. Pseudorandom sequences usually generated by n-level m sequence shifts registered with the longest period of 2^n-1 are commonly adopted as spread-spectrum codes. Theoretical studies have proven that this kind of spread-spectrum communications based on pseudorandom sequences can be easily deciphered because the m sequence can be determined when the $2n$ bit of the m sequence is cracked[15].

In our scheme, pseudorandom sequences are substituted with true random sequences generated by chaotic lasers to circumvent the aforementioned problem. The true random sequences can eliminate the inherent periodicity of pseudorandom sequences, thereby improving the communication security and increase the number of users of the system. True random sequences are characterized by unpredictability, non-replicability, and difficult decipherability.

5 Conclusion

We propose a spread-spectrum communication scheme utilizing true random numbers generated by chaotic semiconductor lasers as spread-spectrum sequences. We simulate the direct spread-spectrum system using the Simulink software. The simulation results demonstrate the feasibility of using the true random numbers generated by the chaotic semiconductor lasers as spread-spectrum codes. Compared with the traditional spread-spectrum communication system, the proposed scheme can be easily established, has higher capacity, and is aperiodic, which enhances the system security.

This work was supported by the Special Funds of the National Natural Science Foundation of China (No. 61108027), the National Natural Science Foundation of China (No. 60927007), and the Open Subject of the State Key Laboratory of Millimeter Waves (No. K201108).

References

1 X. Wang, M. Zhan, X. Gong *et al*.. Spread-spectrum communication using binary spatiotemporal chaotic codes [J]. *Phys. Lett. A*, 2005, **334**(1): 30～36

2 Yu Zhengbiao, Feng Jiuchao. A method for generating chaotic spread-spectrum sequences and their optimized selection algorithm [J]. *Acta Physica Sinica*, 2008, **57**(3): 1409～1415
余振标，冯久超. 一种混沌扩频序列的产生方法及其优选算法 [J]. 物理学报, 2008, **57**(3): 1409～1415

3 C. S. Petrie, J. A. Connelly. A noise-based IC random number generator for applications in cryptography [J]. *IEEE Trans. Circuits Syst. I*, 2000, **47**(5): 615～621

4 Deke Yan, Yongsheng Gou, Zhiyuan Song *et al*.. Study on the circuit producing high-speed pulse with high peak current [J]. *Chin. Opt. Lett.*, 2011, **9**(s1): s10307

5 M. Bucci, L. Germani, R. Luzzi *et al*.. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC [J]. *IEEE Trans. Computers*, 2003, **52**(4): 403～409

6 Liao Jing, Liang Chuang, Wei Yajun *et al*.. True random number generator based on a photon beamsplitter [J]. *Acta Physica Sinica*, 2001, **50**(3): 467～472
廖　静，梁　创，魏亚军 等. 基于光量子的真随机源 [J]. 物理学报, 2001, **50**(3): 467～472

7 Huang Zhun, Zhou Tao, Bai Qiangguo *et al*.. A truly random source circuit based on chaotic dynamical system [J]. *Chin. J. Semiconductors*, 2004, **25**(3): 333～339
黄　谆，周　涛，白国强 等. 一种基于混沌的真随机源电路 [J]. 半导体学报, 2004, **25**(3): 333～339

8 Wang Yuncai, Tang Junhua, Han Guohua *et al*.. A true random generator and method generated true random codes based on chaotic lasers [P]. ZL200710062140.1
王云才，汤君华，韩国华 等. 一种基于混沌激光的真随机码发生器及其产生随机码的方法 [P]. ZL200710062140.1

9 A. Uchida, K. Amano, M. Inoue *et al*.. Fast physical random bit generation with chaotic semiconductor lasers [J]. *Nature Photon.*, 2008, **2**(12): 728～732

10 K. Hirano, K. Amano, A. Uchida *et al*.. Characteristics of fast physical random bit generation using chaotic semiconductor Lasers [J]. *IEEE J. Quantum Electron.*, 2009, **45**(11): 1367～1379

11 A. Wang, Y. Wang, H. He. Enhancing the bandwidth of the optical chaotic signal generated by semiconductor laser with optical feedback [J]. *IEEE Photon. Technol. Lett.*, 2008, **20**(19): 1633～1635

12 P. Li, Y. Wang, J. Zhang. All-optical fast random number generator [J]. *Opt. Express*, 2010, **18**(19): 20360～20369

13 I. Kanter, M. Butkovski, Y. Peleg *et al*.. Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography [J]. *Opt. Express*, 2010, **18**(17): 18292～18302

14 J. Zhang, Y. Wang, M. Liu *et al*.. A robust random number generator based on differential comparison of chaotic laser signals [J]. *Opt. Express*, 2012, **20**(7): 7496～7506

15 K. Kurosawa, F. Sato, T. Sakata *et al*.. A relationship between linear complexity and k-error linear complexity [J]. *IEEE Trans. Inform. Theory*, 2000, **46**(2): 694～698

栏目编辑：张　雁