Optik xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Influence of statistical distribution properties on ultrafast random-number generation using chaotic semiconductor lasers

Nianqiang Li*, Wei Pan, Shuiying Xiang, Lianshan Yan, Bin Luo, Xihua Zou

Center for Information Photonics and Communications, Southwest Jiaotong University, Chengdu 610031, China

ARTICLE INFO

Article history:
Received 11 July 2013
Accepted 4 January 2014
Available online xxx

Keywords:
Random-number generation
Semiconductor laser
Statistical intensity distribution
Chaos

ABSTRACT

We study the influence of statistical distribution properties on ultrafast random-number generators (RNGs) using chaotic laser system consisting of a semiconductor laser subject to dual-chaotic optical injections. Two completely different distributions are considered in this paper: one is a long-tailed distribution, and the other is a well-fitted Gaussian distribution. The numerical results show that, using minimum post-processing, symmetric distribution allows for the extraction of 4 least significant bits (LSBs) per sample; while for the asymmetric distribution the produced sequence based on the last LSB still exhibits certain bias. In other words, the important role of symmetric distribution in fast generation of random bits using multi-bit extraction scheme is demonstrated in numerical simulations.

1. Introduction

Random numbers play an important role in a wide range of areas, such as Monte Carlo simulations, stochastic modeling and secure communications. Generally speaking, two traditional ways are widely employed to generate random-bit steam. A common method is based on fast seeds and generation algorithms [1]. They produce pseudorandom numbers due to the deterministic features of their generation processes. An alternative approach used for random-number generation takes advantage of nondeterministic and stochastic physical phenomena, such as frequency jitter in oscillators [2,3], photon noise [4,5], and thermal noise [6]. This type of generators can produce truly random numbers, however, the effective rates are much slower than the pseudorandom numbers. More recently, random-number generators (RNGs) based on chaotic behaviors of semiconductor lasers with time-delayed optical feedback have been proposed to generate physical random bits [7–13]. This type of generators exhibit many fascinating merits, including ultrahigh-speed bit generation rate and ease of implementation.

In the literature, there are a few works aiming at creating efficient RNGs based on the use of chaotic dynamics in laser-based systems, including single laser [8], two independent lasers [7,14], and coupled lasers [15,16]. These physical RNGs have been well exploited in the experiments. We note that in these experiments the statistical distribution of the intensity fluctuations of chaotic lasers usually appears roughly Gaussian, but slightly skewed [8,17,18]. That is, the histogram already shows a symmetric distribution around zero to some extent. Therefore, it is not surprising that the degree of symmetry of the statistical intensity distribution can be efficiently improved by using intensity derivate or difference technique [8]. As a consequence, for multi-bit extraction scheme the substantial increase in the speed at which the random bit stream can be generated has been achieved. However, despite this large body of experimental works, the theoretical demonstration of fast generation of random bits based on chaotic lasers modeled by the well-known Lang–Kobayashi (LK) equations remains scarce [12,19]. In addition, it is still unclear whether the influence of statistical distribution properties on ultrafast random-number generation using chaotic semiconductor lasers can be effectively demonstrated in numerical simulations. Especially in simulating the LK equations, the raw distribution is highly asymmetric and exhibits exponential decay on the high-intensity side.

In this study, we consider two completely different cases of statistical intensity distributions. One is the long-tailed distribution, and the other is the well-fitted Gaussian distribution. The chaotic entropy source and the used post-processing are assumed to be the same for the two cases. Furthermore, we also note that the fast generation of random bits should be completely free from the influence of chaos complexity, the bandwidth and its flatness, and the periodicity due to the time-delay signature. To this end, we employ a semiconductor laser subject to dual-chaotic optical injections for chaos generation, as described in [20,21]. Under proper conditions, such a configuration can output a wideband

* Corresponding author. Tel.: +86 13438884668.
E-mail address: wan_103301@163.com (N. Li).

http://dx.doi.org/10.1016/j.ijleo.2014.01.052
0030-4026/

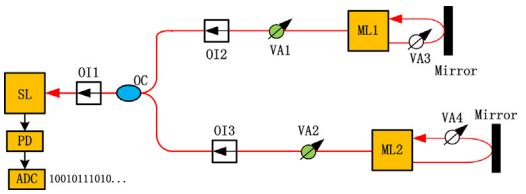

Fig. 1. Schematic diagram of the semiconductor laser subject to dual-chaotic optical injections. ML1 and ML2: two master lasers; SL: slave laser; VA: variable attenuator; OC: optical coupler; OI: optical isolator; PD: photodetector; ADC: analog to digital converter (color online).

unpredictability-enhanced chaotic signal; in the meantime, the time-delay signatures are highly suppressed and even completely eliminated. (While the time-delay concealment is important for encryption [20,22], this may not be of direct importance for RNG. Nevertheless, we hope that the enhanced dynamical complexity leads to both time-delay concealment and enhanced RNG.) This means that we are able to focus solely on the importance of the symmetry of the statistical distribution for RNG in the LK model, since other important features mentioned above are assured with this dedicated configuration.

2. Model and results

The configuration is illustrated in Fig. 1. The details of our implementation of the system are presented in [20]. Here, a brief summary is presented. Two master lasers (MLs) operate in the chaotic regimes due to optical feedback; a slave laser (SL) can output a chaotic waveform because of the chaotic injections from the two MLs (ML1 and ML2); the chaotic output of SL is employed as the source of physical entropy. The equations for the slowly varying complex amplitude E and the carrier number N obey [20,21]

$$\dot{E}_j = \frac{1}{2}(1+i\alpha)\left[G(t)-\frac{1}{\tau_p}\right]E_j(t)+\sqrt{2\beta_{sp}N_j}\xi_j + k_{mj}E_j(t-\tau_{mj})\exp(-i2\pi f_{mj}\tau_{mj}), \quad (1)$$

$$\dot{E}_s = \frac{(1+i\alpha)}{2}\left[G_s(t)-\frac{1}{\tau_p}\right]E_s(t)+\sqrt{2\beta_{sp}N_s}\xi_s + \eta_1 E_{m1}(t-\tau_c)\exp(-i2\pi f_{m1}\tau_c+i2\pi\Delta f_1 t) + \eta_2 E_{m2}(t-\tau_c)\exp(-i2\pi f_{m2}\tau_c+i2\pi\Delta f_2 t), \quad (2)$$

$$\dot{N}_{j,s} = \frac{I_{j,s}}{q}-\frac{N_{j,s}(t)}{\tau_e}-G_{j,s}(t)|E_{j,s}(t)|^2, \quad (3)$$

$$G_{j,s}(t) = \frac{g(N_{j,s}-N_0)}{1+\varepsilon|E_{j,s}(t)|^2}, \quad (4)$$

where subscript $j = 1, 2$ represents two master lasers, ML1 and ML2, respectively, s stands for SL. For simplicity, the three lasers have identical device parameters and optical frequencies, and their definitions and values can be found in [20]; the lasers are pumped at 1.50 times their threshold. We consider the following values for the feedback and injection parameters: $K_{m1} = 30\,\text{ns}^{-1}$ and $\tau_{m1} = 2$ ns (feedback strength and time delay for ML1), $K_{m2} = 30\,\text{ns}^{-1}$ and $\tau_{m2} = 3$ ns (ML2), $\eta_1 = 30\,\text{ns}^{-1}$ (injection strength, from ML1 to SL) and $\eta_2 = 30\,\text{ns}^{-1}$ (injection strength, from ML2 to SL). To guarantee the non-determinism of the physical RNGs, the spontaneous emission noise has been taken into account by choosing the spontaneous emission factor to be $\beta_{sp} = 1 \times 10^3$.

Fig. 2 displays the autocorrelations (left column) and RF spectra (right column) of the three lasers. With our parameters, the

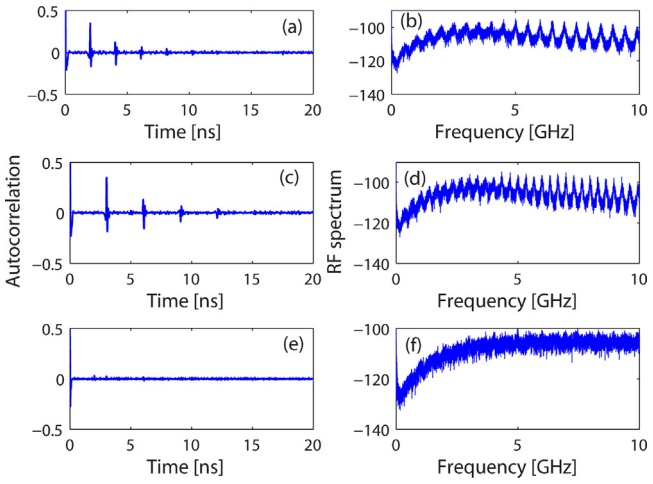

Fig. 2. Calculated autocorrelation of the intensity time series (left column) and RF spectra (right column) for ML1 (a and b), ML2 (c and d) and SL (e and f). The feedback and injection parameters are specified in the text (color online).

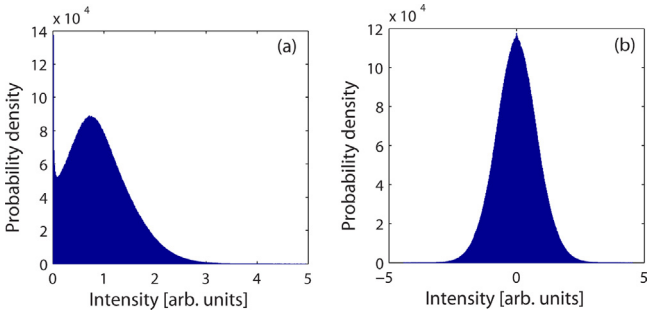

Fig. 3. Statistical distributions of the raw time series (a) and differential time series (b) (color online).

two MLs show obvious time-delay signatures that can be retrieved from the peaks of the autocorrelation curves (Fig. 2(a) and (c)) and from the periodicities of the external cavity modes (ECMs) in RF spectra (Fig. 2(b) and (d)). In contrast, the SL can generate a chaotic signal with the time delays well concealed (Fig. 2(e)). We attribute the concealment of the relevant time delays to the interaction between the two injection fields and the SL field, while neither injection field dominates the nonlinear dynamics of SL (see details in [20]). In addition, a broad and flat spectrum, without periodicities, is achieved in the SL. This result is confirmed by the RF power spectrum shown in Fig. 2(f).

We begin our analysis by preparing two completely different statistical distributions from the same source of physical entropy. As shown in Fig. 2, the laser intensity output of SL can be regarded as the optimum chaotic entropy source, where the sampling rate is 10 GS/s. (Here the sampling rate should be carefully chosen so as to avoid the occurrence of many repeated and correlated values.) The histogram of the raw time series is shown in Fig. 3(a), which exhibits an extremely asymmetric distribution. To our knowledge, differential comparison is a commonly employed technique to improve the intensity statistics of the laser dynamics [23–25]. To be precise, let $X1$, $X2$ be independent, identically distributed random variables, in the sense that the difference $Y = X1 - X2$ has a symmetric distribution. For the differential time series, the selection of time delay is flexible (but it should be larger than the decorrelation time), since there are no pronounced time-delay signatures in the autocorrelation (Fig. 2(e)). Here we see a highly Gaussian distribution for the differential time series as shown in Fig. 3(b). In order to confirm the degree of symmetry of the two distributions, we calculate

Please cite this article in press as: N. Li, et al., Influence of statistical distribution properties on ultrafast random-number generation using chaotic semiconductor lasers, Optik - Int. J. Light Electron Opt. (2014), http://dx.doi.org/10.1016/j.ijleo.2014.01.052

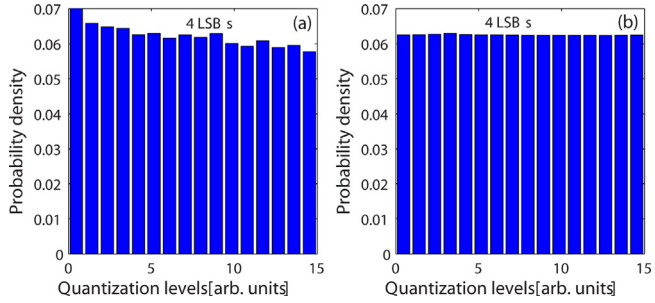

Fig. 4. Statistical distributions of the retained 4 LSB bit sequence obtained from the raw signal (a) and differential signal (b) (color online).

their coefficients of skewness $S = \mu_3/\sigma^3$, where μ_3 and σ are the third central moment and the standard deviation, respectively [25]: i.e., $S_1 \approx 0.82$ for the raw time series and $S_2 \approx 3.7 \times 10^{-3}$ for the differential time series. This means that two completely different distributions are achieved in our simulations with the same entropy source.

Next, we used a multi-bit scheme for random-number generation to evaluate the important role of the symmetric distribution [17]. In this scheme, the sampled chaotic time series is guided to an 8-bit analogy to digital converter (ADC), either based on a hardware or software implementation. From each 8-bit digitized output, lower bits than 8-bit are extracted and interleaved to generate a random-bit sequence. One monitors the statistical distribution of the retained least significant bits (LSBs) by gradually discarding the most significant bit (MSB) until the resulting histogram is well described by the uniform distribution. Therefore, only several LSBs of the 8-bit analog-to-digital (A/D) converted signal are extracted in order to pass the National Institute of Standard Technology (NIST) tests [13]. For the raw time series, it is difficult to enhance uniformity by discarding the MSBs due to its long-tailed distribution. In this case, we cannot obtain uniform distribution even if only the last LSB is retained. On the contrary, for the differential time series the Gaussian distribution guarantees that the distribution of the retained 4 LSBs or fewer is asymptotically ideally uniform.

In Fig. 4 the statistical distributions of the multi-bit data when including 4 LSBs, for the raw (Fig. 4(a)) and differential (Fig. 4(b)) time series, are presented. As can be seen from the figure, for the case of raw signal, the density of some values is higher than others, and the resulting sequence will lead to considerable bias. This means that additional post-processing, e.g., exclusive-OR (XOR) operation, should be carried out to improve the randomness. By contrast, for the case of the differential signal, the 4 LSBs pattern follows a completely uniform distribution. This means that there is no necessary to use additional post-processing procedures. Note that the produced sequence of random bits in this case is free from any significant bias and correlations, which can be evaluated by performing the statistic bias and autocorrelation coefficients.

Let us further employ the NIST benchmark (NIST Special Publication 800-22) to demonstrate randomness of the generated bit sequences by retaining 4 LSBs from the differential time series [26]. To make sure a meaningful NIST test, the required sequence length should exceed 10^8 bits. In our simulations, 2×10^8 bit data (200 frames of 1 M bit sequences) and the significance level $\beta = 0.01$ are used.

The typical results for the bit sequences generated at a sample rate of 10 GS/s are shown in Table 1. Note that for successful NIST tests, the composite P-value (uniformity of p-values) of each test should exceed 10^{-4}, and there may be no more than 7 failures out of 200 trials. (The random excursions and random excursions variant tests may have no more than 5 failures out of 124 trials). As seen in Table 1, all the tests are passed. These results correspond to random-bit generation rate at 40 Gb/s = 4 bit × 10 GS/s.

Table 1
Results of NIST SP 800-22 statistical tests for a set of 200 sequences generated using 4 LSBs from the differential signal. For tests which produce multiple P-values and proportions, the worst case is shown.

Statistical test	P-value	Proportion	Result
Frequency	0.236810	196/200	Success
Block frequency	0.428095	198/200	Success
Cumulative sums	0.262249	197/200	Success
Runs	0.816537	197/200	Success
Longest run	0.574903	199/200	Success
Rank	0.446556	198/200	Success
FFT	0.941144	199/200	Success
Nonoverlapping template	0.013102	196/200	Success
Overlapping template	0.834308	198/200	Success
Universal	0.334538	197/200	Success
Approximate entropy	0.544254	199/200	Success
Random excursions	0.043745	123/124	Success
Random excursions variant	0.057146	122/124	Success
Serial	0.514124	198/200	Success
Linear complexity	0.616305	200/200	Success

Our results may provide a significant insight for the role of symmetric statistical distributions in random-bit generation. One can see that, under the same circumstances, for the differential time series, 4 LSBs are retained to pass the randomness tests, whereas for the raw time series, even the last LSB still shows considerable bias. In this sense, the importance of the symmetry of the statistical distribution can be embodied by the RNG capacity, which comes from the qualitative difference in the two histograms, i.e., a long-tailed distribution and a well-fitted Gaussian distribution. Therefore the statistical properties of the chaotic source are very important for generating random-bit sequences at high rates. In other words, the significant influence of statistical distribution properties on ultrafast random-number generation based on LK equations is demonstrated.

We also remark that this work primarily aims at demonstrating the importance of symmetrical statistical distributions in fast generation of random bits based on LK equations. In fact, the configuration composed of a semiconductor laser subject to dual-chaotic optical injections may be not a potential candidate for a practical and efficient RNG due to the system complexity. Nevertheless, the use of a single semiconductor laser with time-delayed feedback already meets the demand of ultrafast random-bit generation by employing high-order derivates [27].

3. Conclusions

The influence of statistical distribution properties on ultrafast RNGs using chaotic semiconductor lasers is studied numerically. A semiconductor laser subject to dual-chaotic optical injections is used to generate wideband unpredictability-enhanced chaotic time series. The results for two extremely different distributions, i.e., a long-tailed distribution and a well-fitted Gaussian distribution, are compared. We demonstrate that the symmetric distribution allows us to retain 4 LSBs per symbol to generate random bits with verified randomness. On the contrary, without XOR operation, the sequence based on the asymmetric distribution always shows bias even if only the last LSB is retained. In this respect, the symmetric statistical distributions of the intensity time series are beneficial for ultrafast RNG, since the retained bits from a single variable are determined to some extent by the degree of symmetry of the statistical distributions. Our findings are promising for analyzing the performance of random-number generation based on the well-known LK model.

Please cite this article in press as: N. Li, et al., Influence of statistical distribution properties on ultrafast random-number generation using chaotic semiconductor lasers, Optik - Int. J. Light Electron Opt. (2014), http://dx.doi.org/10.1016/j.ijleo.2014.01.052

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (60976039, 61274042), the Basic Research Foundation of Sichuan Province (2011JY0030), and the funds for the Excellent Ph.D. Dissertation of the Southwest Jiaotong University (2011).

References

[1] D. Knuth, The Art of Computer Programming Seminumerical Algorithms, vol. 2, 3rd ed., Addison-Wesley Professional, Boston, MA, 1996.
[2] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC, IEEE Trans. Comput. 52 (2003) 403–409.
[3] S. Maehara, K. Kawakami, H. Arai, K. Nakano, K. Doi, T. Sato, Y. Ohdaira, S. Sakamoto, M. Ohkawa, Frequency noise characteristics of a diode laser and its application to physical random-number generation, Opt. Eng. 52 (2013) 014302.
[4] M. Stipcevic, B. Medved Rogina, Quantum random number generator based on photonic emission in semiconductors, Rev. Sci. Instrum. 78 (2007) 045104.
[5] J.F. Dynes, Z.L. Yuan, A.W. Sharpe, A.J. Shields, A high speed, postprocessing free, quantum random number generator, Appl. Phys. Lett. 93 (2008) 031109.
[6] W.T. Holman, J.A. Connelly, A.B. Dowlatabadi, An integrated analog/digital random noise source, IEEE Trans. Circuits Syst. I: Fundam. Theory Appl. 44 (1997) 521–528.
[7] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, P. Davis, Fast physical random-bit generation with chaotic semiconductor lasers, Nat. Photonics 2 (2008) 728–732.
[8] I. Reidler, Y. Aviad, M. Rosenbluh, I. Kanter, Ultrahigh-speed random-number generation based on a chaotic semiconductor laser, Phys. Rev. Lett. 103 (2009) 024102.
[9] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, D. Syvridis, Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit, Opt. Express 18 (2010) 18763–18768.
[10] Y. Wang, P. Li, J. Zhang, Fast random-bit generation in optical domain with ultrawide bandwidth chaotic laser, IEEE Photonics Technol. Lett. 22 (2010) 1680–1682.
[11] N. Oliver, M.C. Soriano, D.W. Sukow, I. Fischer, Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random-bit generation, Opt. Lett. 36 (2011) 4632–4634.
[12] R.M. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijten, J. Bolk, G.V. Der Sande, Fast random bits generation based on a single chaotic semiconductor ring laser, Opt. Express 20 (2012) 28603–28613.
[13] A. Uchida, Optical Communication with Chaotic Lasers: Applications of Nonlinear Dynamics and Synchronization, Wiley-VCH Verlag GmbH & KGaA, Weinheim, Germany, 2012.
[14] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, P. Davis, Characteristics of fast physical random-bit generation using chaotic semiconductor lasers, IEEE J. Quantum. Electron. 45 (2009) 1367–1379.
[15] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, P. Davis, Fast random-bit generation with bandwidth-enhanced chaos in semiconductor lasers, Opt. Express 18 (2010) 5512–5524.
[16] J.G. Wu, X. Tang, Z.M. Wu, G.Q. Xia, G.Y. Feng, Parallel generation of 10 Gbits/s physical random number streams using chaotic semiconductor lasers, Laser Phys. 22 (2012) 1476–1480.
[17] T. Yamazaki, A. Uchida, Performance of random number generators using noise-based super-luminescent diode and chaos-based semiconductor lasers, IEEE J. Sel. Top. Quantum Electron. 19 (2013) 0600309.
[18] X. Li, S.-C. Chan, 40 Gps random-bit generation by oversampling chaos from an injected semiconductor laser, Proc. SPIE 8552 (2012) 85520K-1-7.
[19] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, Ken-ichi Arai, A. Uchida, P. Davis, Theory of fast nondeterministic physical random-bit generation with chaotic lasers, Phys. Rev. E 85 (2012) 046215.
[20] N. Li, W. Pan, L. Yan, B. Luo, X. Zou, S. Xiang, Enhanced two-channel optical chaotic communication using isochronous synchronization, IEEE J. Sel. Top. Quantum Electron. 19 (2013) 0600109.
[21] S. Xiang, W. Pan, B. Luo, L. Yan, X. Zou, N. Li, H. Zhu, Wideband unpredictability-enhanced chaotic semiconductor lasers with dual-chaotic optical injections, IEEE J. Quantum Electron. 48 (2012) 1069–1076.
[22] N. Li, W. Pan, S. Xiang, L. Yan, B. Luo, X. Zou, L. Zhang, P. Mu, Photonic generation of wideband time-delay-signature-eliminated chaotic signals utilizing an optically injected semiconductor laser, IEEE J. Quantum Electron. 48 (2012) 1339–1345.
[23] C.R.S. Williams, J.C. Salevan, X. Li, R. Roy, T.E. Murphy, Fast physical random number generator using amplified spontaneous emission, Opt. Express 18 (2010) 23584–23597.
[24] J. Zhang, Y. Wang, M. Liu, L. Xue, P. Li, A. Wang, M. Zhang, A robust random number generator based on differential comparison of chaotic signals, Opt. Express 20 (2012) 7496–7506.
[25] V.N. Chizhevsky, Symmetrization of single-sided or nonsymmetrical distribution: the way to enhance a generation rate of random bits from a physical source of randomness, Phys. Rev. E 82 (2010) 050101.
[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Nat. Inst. Standards and Technology, Special Publication 800-22, 2001, Revision 1, 2008, Available: http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf (online).
[27] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, M. Rosenbluh, An optical ultrafast random bit generator, Nat. Photonics 4 (2010) 58–61.

Please cite this article in press as: N. Li, et al., Influence of statistical distribution properties on ultrafast random-number generation using chaotic semiconductor lasers, Optik - Int. J. Light Electron Opt. (2014), http://dx.doi.org/10.1016/j.ijleo.2014.01.052