2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Nondeterministic Random Bits Extraction from Injected Chaotic Semiconductor Lasers

Xiao-Zhou Li[1], Jun-Ping Zhuang[1], Song-Sui Li[1], and Sze-Chun Chan[1,2,*]

[1]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[2]State Key Laboratory of Millimeter Waves, City University of Hong Kong, Hong Kong, China
*Email: scchan@cityu.edu.hk

Abstract– Randomness extraction from an optically injected semiconductor laser is investigated. The generation of randomness from the chaotic intensity time series is examined by estimating the time-dependent exponents through state-space reconstruction. Chaotic dynamics enables fast divergence of neighboring states with positive exponents, while the possible effects of negative exponents have to be ruled out by using a sufficiently long sampling interval. This guarantees successful extraction of nondeterministic random bits at 200 Gbps from experimentally injected chaotic lasers.

1. Introduction

Fast physical random bit generation (RBG) is of great importance for a range of applications in computation and secure communication [1]. Despite the simplicity in using deterministic algorithms for generating pseudo-random bits, nondeterministic RBG has been intensively investigated using broadband photonic sources including quantum measurements of photons, optical noise, and optical chaos [1-12]. Amongst the different approaches for physical RBG, semiconductor laser chaos-based RBGs have attracted much attention as pioneered by Uchida *et al*. [4-12]. The chaotic dynamics typically produces fast temporal fluctuations that can be digitized for extraction into random bits at rates exceeding 1 Tbps [5]. Different schemes of chaos-based RBG have been reported using combinations of semiconductor lasers with optical feedback and optical injection [4, 9].

The randomness of such chaos-based RBG schemes can be examined by statistical evaluations using autocorrelation functions and power spectra [9, 13]. Practical tests from the National Institute of Standards and Technology (NIST) are also widely employed for verifying the randomness of the output bits [4]. These tests mainly focus on the statistical properties of the examined data, while the fundamental randomness for bits extraction is not guaranteed. Besides, it has been reported that pseudo-random bits from deterministic schemes can have sufficient quality for passing the NIST tests [14]. Therefore, randomness generation from chaotic semiconductor lasers needs to be investigated for nondeterministic RBG. Fundamentally, randomness is originated from the divergence of neighboring states through chaotic mixing. The divergence rate has been investigated in laser systems by estimating the largest Lyapunov exponents [13]. Randomness generation was also investigated by resetting the laser state repeatedly to the same initial state [15]. However, previously reported works on randomness evaluation for RBG are all based on semiconductor lasers with optical feedback, randomness extraction from an optically injected laser has not been much reported so far.

In this work, randomness extraction for chaos-based RBG is investigated using an optically injected semiconductor laser. Compared with optical feedback, chaos generated from optically injected lasers possesses the advantage of having no undesirable time-delay signatures that are commonly observed in time-delay systems [9, 10]. By numerically reconstructing the state space from an intensity time series, divergence of neighboring states is verified through the positive time-dependent exponents (TDEs). Negative exponents are also eliminated when the evolution time is sufficiently long. Furthermore, chaotic mixing is found to be essential for randomness generation, as compared with period-one (P1) dynamics. Successful RBG at 200 Gbps is demonstrated experimentally, as verified by the NIST tests. In particular, we examine the spread of the time-dependent exponent as a function of the initial distances between neighbors. Chaotic dynamics, as compared to P1 dynamics, is found to give much greater exponents with a significantly broader spread.

2. Schematic Setup

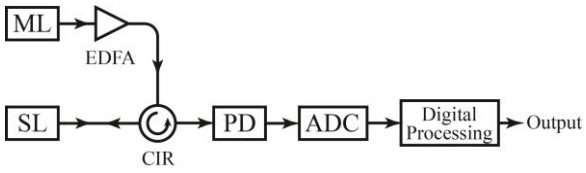

Fig. 1. Schematic of nondeterministic RBG using an optically injected semiconductor laser in chaos. ML, master laser; SL, slave laser; EDFA, erbium-doped fiber amplifier; CIR, circulator; PD, photodetector; ADC, analogue-to-digital converter.

The schematic of the setup for nondeterministic random bits extraction is shown in Fig. 1, where an optically injected semiconductor laser is utilized for chaos generation. The continuous-wave emission from a master laser ML is transmitted through an erbium-doped fiber amplifier EDFA and a circulator CIR for optically injecting a slave laser SL. Both ML and SL are single-mode semiconductor lasers. The injection parameters

include the normalized injection strength ξ_i and the frequency detuning f_i of ML from SL. By adjusting the injection parameters (ξ_i, f_i), SL can be driven into chaotic dynamics. After optical to electrical conversion by a photodetector (PD), it produces fast intensity fluctuations for digitization by analogue-to-digital converter (ADC) in an real-time oscilloscope, which is followed by digital processing for extraction into random bits.

For numerical simulations, the dynamics of a semiconductor laser can be described by the normalized complex intracavity optical field amplitude $a(t)$ and the normalized charge carrier density $\tilde{n}(t)$. With optical injection from ML, the dynamics of SL can be modeled by the following rate equations [16]:

$$\frac{\mathrm{d}a}{\mathrm{d}t} = \frac{1-\mathrm{i}b}{2}\left[\frac{\gamma_c\gamma_n}{\gamma_s\tilde{J}}\tilde{n} - \gamma_p(|a|^2-1)\right]a + \xi_i\gamma_c e^{-\mathrm{i}2\pi f_i t} \quad (1)$$

$$\frac{\mathrm{d}\tilde{n}}{\mathrm{d}t} = -(\gamma_s + \gamma_n|a|^2)\tilde{n} - \gamma_s\tilde{J}\left(1-\frac{\gamma_p}{\gamma_c}|a|^2\right)(|a|^2-1), \quad (2)$$

where $\gamma_c = 5.36\times10^{11}\ \mathrm{s}^{-1}$ is the cavity decay rate, $\gamma_s = 5.96\times10^{9}\ \mathrm{s}^{-1}$ is the spontaneous carrier relaxation rate, $\gamma_n = 7.53\times10^{9}\ \mathrm{s}^{-1}$ is the differential carrier relaxation rate, $\gamma_p = 1.91\times10^{10}\ \mathrm{s}^{-1}$ is the nonlinear carrier relaxation rate, $b = 3.2$ is the linewidth enhancement factor, and $\tilde{J} = 1.222$ is the normalized bias current above threshold. The relaxation resonance frequency of the laser is $f_r = 10.25$ GHz. These parameters are extracted from a commercial semiconductor laser [16]. For simplicity, the spontaneous emission noise is not considered. Using second-order Runge-Kutta integration on Eqs. (1)–(2), an intensity time series $I(t)$ is recorded with a sampling period of $\tau_s = 2.38$ ps. The injection parameters are chosen as (ξ_i, f_i) = (0.05, 6.26 GHz) for inducing chaotic dynamics in SL. The simulated chaos intensity is shown in Fig. 2(a). Due to chaotic dynamics, the time series contains quick and irregular temporal fluctuations faster than 100 ps, which is comparable to the reciprocal of the relaxation resonance frequency of the laser.

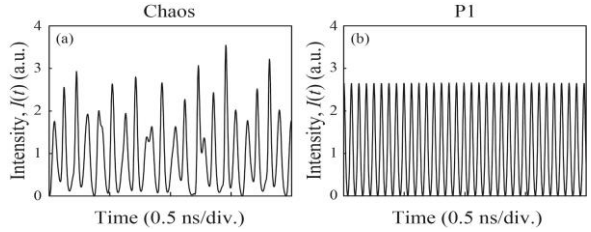

Fig. 2. Intensity time series $I(t)$ recorded from numerical simulations for (a) chaotic and (b) P1 dynamics of the optically injected semiconductor laser.

3. Numerical State-space Reconstruction

To verify the divergence of neighboring states through chaotic mixing, the evolution of the trajectories needs to be examined. As only the emission intensity of the injected laser is usually measured in practical experiments, reconstruction of the state space from the intensity time series is sought. For a normalized intensity time series $I(t)$, a reconstructed state vector is given by $\boldsymbol{x}(t) = [I(t), I(t+\tau_e), \ldots, I(t+(m_e-1)\tau_e)]$, where m_e and τ_e are the embedding dimension and embedding delay time, respectively. Since $I(t)$ is usually recorded at a sampling period of τ_s, the i-th reconstructed state can be notated by $\boldsymbol{x}_i = \boldsymbol{x}(i\tau_s)$, where i is the index of time. Suppose states $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$ form a pair $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ that describes two initial states. After an evolution time of τ_s for some integer k, the separation distance between the two states is given by $d_{ij}(k) = \|\boldsymbol{x}_{i+k} - \boldsymbol{x}_{j+k}\|$, where $\|\cdot\|$ denotes the Euclidean norm in the state space. So $d_{ij}(0)$ is the initial distance between the two states. The evolution of the trajectories can be examined by the change of separation distance $d_{ij}(k)$ over the evolution time $k\tau_s$. Then the TDE is described by [17-19]:

$$\Lambda_{ij}(k) = \ln\frac{d_{ij}(k)}{d_{ij}(0)}. \quad (3)$$

The effect of divergence can be examined by the TDE when pairs of neighboring states are identified for $d_{ij}(0)$ with sufficiently small values. Different pairs of neighbors give different initial separation distances $d_{ij}(0)$, thus resulting in different TDEs $\Lambda_{ij}(k)$ for a given evolution time $k\tau_s$. It is of essence to scrutinize the effect of the choice of such initial distances on the statistics of the TDEs.

Figure 3(a) shows the so-called divergence plots for TDEs obtained from different pairs of neighboring states. An intensity time series of 10^4 data points is used for state-space reconstruction, where embedding parameters of $m_e = 8$ and $\tau_e = 5\tau_s$ are adopted. Similar reconstruction parameters have been utilized for optical injection chaos [18]. In Fig. 3(a-i), the evolution time is only 2.38 ps for $k = 1$. The time is too short for any pair of states to diverge, so most of the TDEs are concentrated at around 0. In Fig. 3(a-ii), the TDEs spread out when the evolution time increases to 0.05 ns for k = 21. Most of the neighboring states diverge due to chaotic dynamics, so their separation distances increase such that positive TDEs are observed. Negative TDEs are also identified, showing the existence of convergence between states. Interestingly, the TDEs spread more as the initial distance increases. This is because of associated increase of the number of initial states, which more completely probe the neighboring space. The evolution time further increases to 0.2 ns in Fig. 3(a-iii) for k = 84. Most of the neighbors keep diverging such that most TDEs continue to increase, while the number of negative TDEs also reduces. In Fig. 3(a-iv), as the evolution time is increased to 0.5 ns for k = 210, the TDEs generally keep increasing and nearly all TDEs become positive, as long as the evolution time is sufficiently long for the neighbors to diverge. Finally in Fig. 3(a-v), the evolution time is 1 ns for k = 420. The TDEs become more concentrated with positive values.

As the overall size of the chaotic attractor is not infinite, there is an upper bound for TDEs that decreases as the initial distance increases, as Figs. 3(a-iv) and 3(a-v) show. In fact, as the evolution time increases, the structure of the divergence plot becomes progressively invariant. The invariance is reached less quickly for states with small initial distances. The initially identified neighboring states, after the sufficiently long evolution time, are finally randomly located around the attractor. Therefore, any neighboring states are finally independent with each other, ensuring the fundamental randomness generation for RBG.

In order to examine the divergence of neighbors without chaotic mixing, Fig. 3(b) is shown by simulating the slave laser in P1 dynamics instead of chaotic dynamics. The P1 dynamics is obtained by adjusting the injection strength ξ_i to 0.10. The emission intensity oscillates periodically at a microwave frequency of 16 GHz, as detailed in Fig. 2(b). The TDEs always stay at around 0, so nearby neighbors keep highly correlated even if the evolution time is long enough. Therefore, periodic oscillations without chaotic dynamics cannot support efficient divergence of neighboring states for randomness generation.

Summarizing Fig. 3, due to chaotic dynamics, TDEs spread out quickly and positively with the increase of time. Chaos is found to be essential for providing quick increase of TDEs for randomness generation.

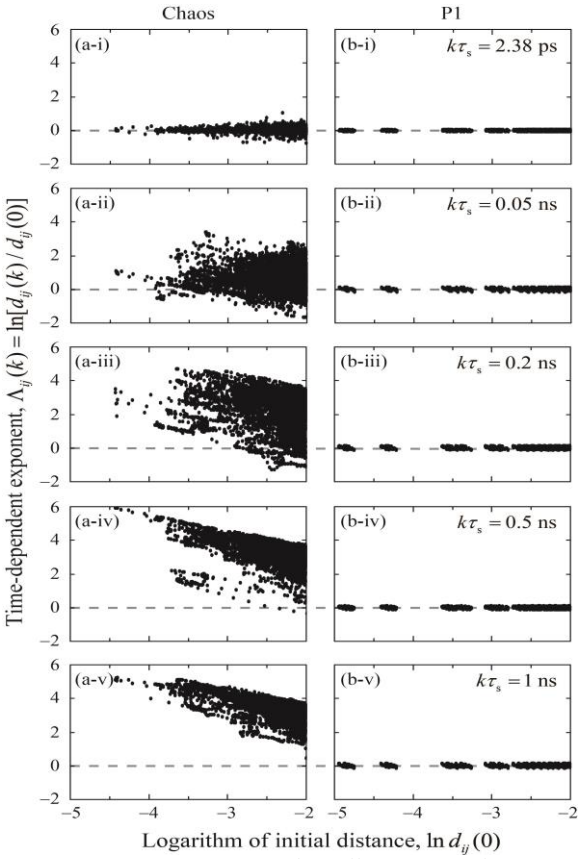

Fig. 3. Time-dependent exponents for different pairs of neighboring states estimated from (a) chaotic and (b) P1 dynamics of an optically injected laser. The evolution time $k\tau_s$ increases for (i) k = 1, (ii) k = 21, (iii) k = 84, (iv) k = 210, and (v) k = 420.

4. Experimental RBG by Optical Injection

Based on the schematic setup detailed in Fig. 1, experiments are further conducted using a distributed-feedback semiconductor laser as the slave laser. In free-running, it emits at about 1550 nm with an optical power of 2.2 mW. The relaxation resonance frequency is f_r = 7 GHz. The maser laser ML is a tunable laser, and the detuning frequency is f_i = 4 GHz. The EDFA gain is controlled such that, with an injection power of 0.8 mW, chaotic dynamics is invoked in SL.

The emission light is converted to electrical signal through a PD, which is followed by a 13-GHz ADC with 8-bit resolution for digitization, where the sampling rate is set as 40 GHz. To ensure randomness, only 5 least significant bits are selected from each digitized sample. To reduce the bias introduced from imperfect detection, each sample is then compared with its 1-ns delayed replica through an exclusive-OR (XOR) operation. The output from the XOR is a stream of bits generated at an output bit rate of 200 Gbps. For comparison, by increasing the injection power to 1.6 mW, SL demonstrates P1 dynamics with its intensity oscillating at 9 GHz.

Then RBGs by chaotic dynamics and P1 dynamics are compared experimentally through taking the NIST tests. A total of 1000 sequences, each of size 1 Mbit, are collected for testing. At significance level α = 0.01, the success proportion has to be in the range of 0.99 ± 0.0094392 for passing a test. The composite *P*-value should be larger than 0.0001 to ensure uniformity. The testing results for chaos and P1 are respectively summarized in Tables 1 and 2, where the worst case is shown for tests producing multiple *P*-values and proportions.

Random bits generated by chaotic dynamics can successfully pass all the 15 NIST tests, while most of the tests are failed using P1 dynamics. This again verifies the randomness generation requires using chaotic dynamics of an optically injected semiconductor laser.

Table 1. NIST tests results for RBG using chaos from an optically injected semiconductor laser

Statistical test	*P*-value	Proportion	Result
Frequency	0.007862	0.9810	Success
Block-frequency	0.206629	0.9920	Success
Cumulative-sums	0.007975	0.9820	Success
Runs	0.725829	0.9850	Success
Longest-run	0.415422	0.9860	Success
Rank	0.773405	0.9870	Success
FFT	0.204439	0.9900	Success
Nonoverlapping-templates	0.340858	0.9820	Success
Overlapping-templates	0.695200	0.9900	Success
Universal	0.927677	0.9920	Success
Approximate-entropy	0.769527	0.9920	Success
Random-excursions	0.478196	0.9834	Success
Random-excursions-variant	0.158133	0.9834	Success
Serial	0.655854	0.9930	Success
Linear-complexity	0.637119	0.9820	Success
Total			15

Table 2. NIST tests results for RBG using P1 from an optically injected semiconductor laser

Statistical test	*P*-value	Proportion	Result
Frequency	0.000000	0.0450	Fail
Block-frequency	0.000000	0.0000	Fail
Cumulative-sums	0.000000	0.0380	Fail
Runs	0.000000	0.0000	Fail
Longest-run	0.000000	0.8940	Fail
Rank	0.842937	0.9860	Success
FFT	0.000000	0.6180	Fail
Nonoverlapping-templates	0.000000	0.0150	Fail
Overlapping-templates	0.000000	0.6530	Fail
Universal	0.000000	0.0710	Fail
Approximate-entropy	0.000000	0.0000	Fail
Random-excursions	0.155209	0.9846	Success
Random-excursions-variant	0.006582	0.9846	Success
Serial	0.000000	0.0000	Fail
Linear-complexity	0.222480	0.9910	Success
Total			4

5. Conclusion

In conclusion, nondeterministic RBG is investigated using a chaotic optically injected semiconductor laser. By estimating the TDEs from a reconstructed state-space, the divergence of neighboring states by chaotic dynamics is illustrated through a divergence plots (Fig. 3). Chaotic dynamics is also found to be essential for randomness generation, as compared with P1 dynamics, in the experiments at 200 Gbps.

Acknowledgments

The work described in this paper was fully supported by a grant from the National Natural Science Foundation of China (NSFC) (Grant 61308002).

References

[1] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photon*., vol. 9, pp. 151–162, 2015.

[2] T. Durt, C. Belmonte, L. P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, "Fast quantum-optical random-number generators," *Phys. Rev. A*, vol. 87, p. 022339, 2013.

[3] 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*, vol. 18, pp. 23584–23597, 2010.

[4] 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*., vol. 2, pp. 728–732, 2008.

[5] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Opt. Express*, vol. 23, pp. 1470–1490, 2015.

[6] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett*., vol. 103, p. 024102, 2009.

[7] 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*, vol. 18, pp. 18763–18768, 2010.

[8] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: approaching the information theoretic limit," *IEEE J. Quantum Electron.*, vol. 49, pp. 910–918, 2013.

[9] X. Z. Li and S. C. Chan, "Heterodyne random bit generation using an optically injected semiconductor laser in chaos," *IEEE J. Quantum Electron*., vol. 49, pp. 829–838, 2013.

[10] X. Z. Li, S. S. Li, J. P. Zhuang, and S. C. Chan, "Random bit generation at tunable rates using a chaotic semiconductor laser under distributed feedback," *Opt. Lett.*, vol. 40, pp. 3970–3973, 2015.

[11] X. Fang, B. Wetzel, J. M. Merolla, J. M. Dudley, L. Larger, C. Guyeux, and J. M. Bahi, "Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, pp. 888–901, 2014.

[12] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, "Physical random bit generation from chaotic solitary laser diode," *Opt. Express*, vol. 22, pp. 17271–17280, 2014.

[13] K. Kanno, A. Uchida, and M. Bunsen, "Complexity and bandwidth enhancement in unidirectionally coupled semiconductor lasers with time-delayed optical feedback," *Phys. Rev. E*, vol. 93, p. 032206, 2016.

[14] F. Arnault and T. P. Berger, "Design and properties of a new pseudorandom generator based on a filtered FCSR automaton," *IEEE Trans. Comput*., vol. 54, pp. 1374–1383, 2005.

[15] S. Sunada, T. Harayama, P. Davis, K. Tsuzuki, K. Arai, K. Yoshimura, and A. Uchida, "Noise amplification by chaotic dynamics in a delayed feedback laser system and its application to nondeterministic random bit generation," *Chaos*, vol. 22, p. 047513, 2012.

[16] S. C. Chan, "Analysis of an optically injected semiconductor laser for microwave generation," *IEEE J. Quantum Electron.*, vol. 46, pp. 421–428, 2010.

[17] J. Gao and Z. Zheng, "Direct dynamical test for deterministic chaos and optimal embedding of a chaotic time series," *Phys. Rev. E*, vol. 49, pp. 3807–3814, 1994.

[18] S. K. Hwang, J. B. Gao, and J. M. Liu, "Noise-induced chaos in an optically injected semiconductor laser model," *Phys. Rev. E*, vol. 61, p. 5162, 2000.

[19] X. Z. Li, J. P. Zhuang, S. S. Li, J. B. Gao, and S. C. Chan, "Randomness evaluation for an optically injected chaotic semiconductor laser by attractor reconstruction," *Phys. Rev. E* (submitted).