IEICE Proceeding Series

Noise amplification based on dynamical instabilities in semiconductor laser systems and its application to nondeterministic random bit generators

S. Sunada, T. Harayama, P. Davis, K. Arai, K. Yoshimura, K. Tsuzuki, M. Adachi, A. Uchida

Vol. 1 pp. 263-267
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Noise amplification based on dynamical instabilities in semiconductor laser systems and its application to nondeterministic random bit generators

S. Sunada[1], T. Harayama[2,3], P. Davis[3,4], K. Arai[3], K. Yoshimura[3], K. Tsuzuki[5], M. Adachi[1], and A. Uchida[6]

[1] Institute of Science and Engineering, Kanazawa University, Kakuma-machi, Kanazawa, 920-1192, Japan
[2]Department of Mechanical Engineering, Toyo University, 2100 Kujirai, Kawagoe, Saitama 350-8585, Japan
[3] NTT Communication Science Laboratories, NTT Corporation,
2-4 Hikaridai Seika-cho Soraku-gun Kyoto, 619-0237, Japan
[4] Telecognix Corporation, 58-13 Yoshida Shimooji-cho Sakyo-ku, Kyoto, 606-8314, Japan
[5] NTT Photonics Laboratories, NTT Corporation,
3-1 Morinosato-Wakamiya Atsugi Kanagawa, 243-0198, Japan
[6] Department of Information and Computer Science, Saitama University
255 Shimo-Okubo Sakura-ku Saitama city Saitama, 338-8570, Japan
Email: sunada@se.kanazawa-u.ac.jp

Abstract—We experimentally demonstrate amplification of intrinsic microscopic noises by the dynamical instabilities in high dimensional chaotic laser systems, semiconductor lasers with delayed optical feedback. Then we discuss nondeterministic random bit generation using chaotic lasers, and show that the relation between the entropy of the bit sequences obtained by using chaotic lasers and the rates of the bit extraction can be understood in terms of the effect of the noise amplification.

1. Introduction

Fast generation of random bit sequences that are practically indistinguishable from unpredictable truly random bit sequences is important to achieve higher security of communication systems. The generation of nondeterministic random bit sequences can be achieved by sampling observables obtained from non-deterministic physical phenomena and converting them to bit sequences, but it is generally difficult in practice to avoid correlations and statistical bias when bits are generated at high speed.

Recently, methods for random bit generation using fluctuations in optical phenomena have been developed in order to obtain unpredictable truly random bit sequences at fast rates over giga bit per second (Gbps) [1, 2, 3, 4]. In particular, fast random bit generation using chaotic lasers have attracted much attention. Many experimental and theoretical studies have been done for further improving of the bit generation rate using bandwidth enhanced chaotic lasers [5] and complex post-processing techniques [6, 7], the miniaturization of the generators using photonic integration technologies [8, 9, 10], and realizing all optical random bit generators [11, 12]. However, it is still unclear whether nondeterministic bit sequences that are practically indistinguishable from truly random bit sequences can be really generated by using chaotic lasers. Although it has been theoretically studied that amplification of intrinsic microscopic fluctuation by dynamical instabilities of chaos plays an important role in generating nondeterministic random bits [13, 14], detailed experimental investigation of this aspect has not yet been performed.

In this presentation, we provide an experimental method for directly observing the effect of amplification of intrinsic microscopic noise in chaotic lasers [15]. In the experiment, the chaotic laser system is repeatedly operated, and the time evolution of an ensemble of chaotic trajectories starting from a same initial state is measured. It is experimentally demonstrated that intrinsic microscopic noises amplified by the chaotic dynamics are transformed into macroscopic fluctuating signals, and the probability density of the output light intensity exponentially converges to the natural invariant probability density in a strongly chaotic regime. On the basis of the convergence toward the natural invariant density, we discuss the relation between the randomness of the bit sequences obtained by using the chaotic lasers and the rate of random bit extraction.

2. Microscopic noise and macroscopic randomness

First, let us start with a brief review of fundamental statistical descriptions of chaotic systems and discuss extraction of randomness from observables of the systems [13]. Here suppose that the time evolution of a system state $x(t)$ is described as $x(t) = f^t x(0)$, where f is the time evolution operator of the system. If the system is strongly chaotic, then it has the mixing property, which can be expressed as follow,

$$C_{AB}(\tau) = \langle A(f^\tau x)B(x)\rangle - \langle A\rangle \langle B\rangle \to_{[|\tau|\to\infty]} 0, \qquad (1)$$

where A and B are arbitrary square integrable functions, and $\langle X\rangle$ denotes a statistical ensemble, $\langle X\rangle \equiv \int X\rho(dx)$. ρ is a unique invariant density of the system, natural invariant density, which does not depend on initial states and observables. In a statistical description, Eq. (1) implies that any arbitrary smooth initial density function $\rho_0(x)$ converges to the natural invariant density $\rho(x)$. The time evolution of the probability density is ruled by the Frobenius-Perron operator L^t:

$$\lim_{t\to\infty} L^t\rho_0(x) = \rho(x), \tag{2}$$

where L^t is defined by using the Dirac delta function as $L^t\rho_0(x) \equiv \int_M \delta(x - f^t y)\rho_0(y)dy$. The convergence toward the invariant density due to the mixing property is a very important feature of the amplification of initial small uncertainty and the transduction to unpredictable behavior of observables of the system.

Next, let us consider an observable Y and the extraction of the randomness from the observable. The distribution function of an observable Y also converges to a unique invariant distribution function $D(Y) = \int_M \delta(Y - \tilde{Y}(x))\rho(x)dx$. By using $D(Y)$, we can define a discrete number N of macroscopic states such that the probabilities of the macroscopic states X_i are all equal, that is, $1/N$. Specifically, we define $(N-1)$ thresholds S_i of the observable Y such that

$$\int_{S_0}^{S_1} D(Y)dY = \int_{S_1}^{S_2} D(Y)dY = \cdots = \int_{S_{N-1}}^{S_N} D(Y)dY. \tag{3}$$

Then we define a set of discrete macroscopic states X_i $(i = 1, 2, \cdots, N)$ of the system such that the system is in state X_i $(i = 1, 2, \cdots, N)$ when the observable Y is found in the interval between the thresholds S_{i-1} and S_i $(i = 1, 2, \cdots, N)$. The Shannon entropy is defined as

$$H(\mathbf{X}) \equiv -K \sum_{i=1}^{N} p(X_i) \log p(X_i), \tag{4}$$

where $\mathbf{X} = \{X_i, i = 1, 2, \cdots, N\}$ and $K = 1/\log N$. With the macroscopic states defined using the thresholds in Eq. (3), the Shannon entropy is the maximum value of unity.

In real physical systems, microscopic noise is always present. For instance, in the cases of laser systems, there exists quantum noise of spontaneous emission, which is in principle unpredictable but the amplitude of the noise is very small. No matter how accurately we observe the state of the system, the effect of microscopic noise after the observation means that the state should be modeled by an ensemble. If the ensemble due to microscopic noise has a smooth probability distribution, then from Eq. (2), one can easily see that the time evolution of such an ensemble is ruled by the Frobenius-Perron operator and always converges to the natural invariant density in the long time limit if the system has the mixing property. Moreover, if discrete macroscopic states are defined appropriately, the probability of asymptotically being in any of the macroscopic states is equal, and the Shannon entropy is unity. Therefore, in order to provide better understanding of physical mechanism of random number generation using chaotic lasers, it is important to confirm whether microscopic noise can be actually amplified and transduced into macroscopic randomness in chaotic laser systems.

3. Experiment

For the above purposes, we experimentally study the transduction of initial uncertainty due to microscopic noise into macroscopic randomness. The chaotic system studied here is a semiconductor laser device with delayed optical feedback (see Fig. 1). The experiment is carried out by resetting the dynamical state of the laser to an initial state repeatedly and measuring the time-evolution of ensemble of the trajectories. In this experiment, we use a stable low dimensional state, stationary lasing state of the solitary laser without delayed feedback, as an initial state, because the stable state can be easily obtained by making the feedback strength zero. Then, the feedback strength is suddenly changed so that a chaotic state is obtained. Since the initial stationary lasing state is close to the chaotic attractor and the state rapidly approaches the attractor, the time-evolution of the signal obtained from the state evolving in the attractor can be clearly observed. The resetting to the same initial state is carried out by setting the feedback strength to zero again. Consequently, with this repeated switching of the feedback strength, the ensemble of the time evolution of the chaotic signals from the same initial state can be obtained.

The experimental setup for implementing the above method is shown in Fig.1. The feedback strength is switched with a periodic pulse signal while the other parameters are fixed. A typical example of the experimental result is shown in Fig. 2. This figure displays four different time series of the output light intensity signals obtained by switching the state of the system from stationary stable state to the chaotic one. The origin of time $t = 0$ denotes a time when the state of the laser is changed from stationary lasing state to chaotic one. One can clearly see that for the chaotic regime of $t > 0$, initial uncertainty due to small noise is amplified by the dynamical instability, and that the trajectories of the signals are rapidly separated. In order to evaluate the statistical property of the noise amplification, we obtained the transient probability density by sampling the light intensity signals observed at the same time t and making a histogram. Fig. 3 shows the time-dependence of the probability density. For $t = 0$, the initial probability density has one peak corresponding to the averaging value of the initial stationary lasing oscillation. For $t > 0$, the width of the probability is rapidly increased. The probability density converges to a probability density represented by a dotted curve, which is obtained from a single long chaotic trajectory observed in the case of the same parameters. That is, it is the invariant probability density characterized by the chaotic dynamical system. Its convergence to the invariant probability density implies that even if the initial state is known, the information whereabouts of the state in the chaotic attractor is completely lost within short times about 1 ns. This is important for knowing the lower limit of the sampling time interval of the light intensity for generating unpredictable random bits.

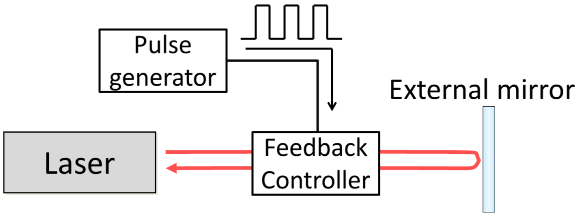

Figure 1: A schematic of experimental setup for measuring amplification of microscopic noise in a semiconductor laser with delayed optical feedback.

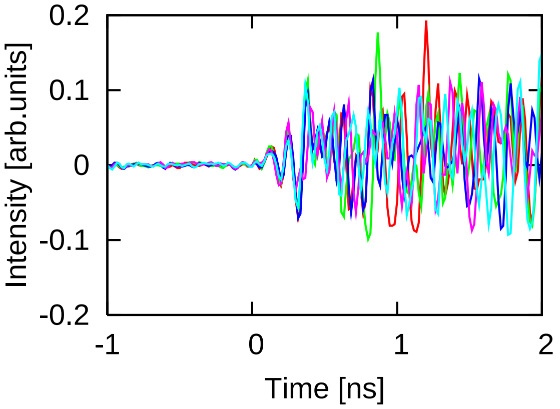

Figure 2: Four temporal waveforms of chaotic intensity starting from an initial state.

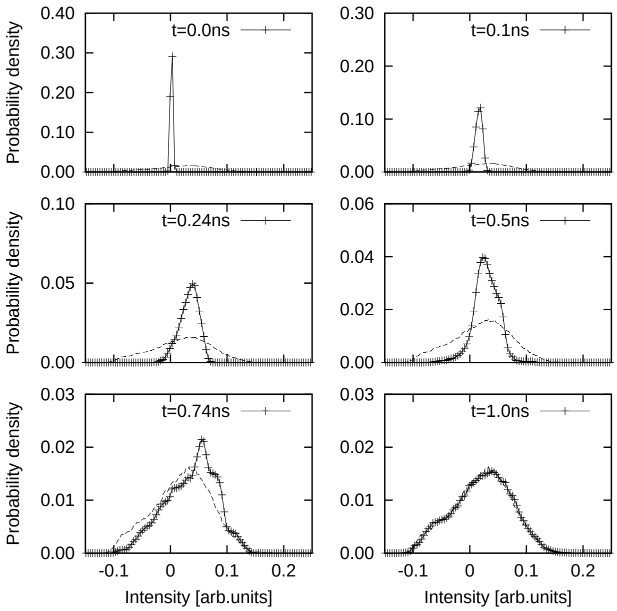

Figure 3: Time dependence of the probability density of the chaotic light intensity signals. The dotted curve represents the probability density obtained from a single long chaotic time series in the case of the same injection current value.

4. Random bit generation

In this section, we study random bit generation using the above chaotic laser device. The random bit generation method shown in Sec. 2 is applied to the chaotic lasers. In this experiment, the light intensity signals obtained by the repeated operation of the chaotic laser device are sampled and converted into binary bits 0 or 1 based on the natural invariant probability density $\rho(I)$ of the light intensity I. Fig. 4 shows the time dependence of the Shannon entropy H of the generated bits. As expected, the entropy is increased and becomes close to 1 within 1 ns. The rate of growth of the entropy is related to the rate of convergence to the invariant density.

It is important to note that in the present experiment, it is difficult to control threshold I_{th} with infinite precision. Actually, the threshold was set with 8 bit precision, so that a slight but significant statistical deviation from the bit probability 1/2 is caused by the lack of the resolution of the threshold. Also, precisely speaking, entropy equal to 1 is only achieved in the long time limit. With finite time, one cannot obtain completely random bits.

In order to reduce the statistical bias, a logical Exclusive-OR (XOR) operation is useful, where two independent bit sequences generated by using two chaotic laser systems are combined by the XOR operation and a single bit sequence with lower statistical bias is produced. In order to evaluate the XOR-ed bit sequences, we also measure the entropy of the random bit generation. The result is shown in Fig. 5. The entropy approaches 1 much faster than the case of the single chaotic laser system shown in Fig. 4.

For further evaluating the randomness of the generated bits, we used a standard statistical test for randomness, the NIST Special Publication 800-22 [16], consisting of 15 different tests. The test is performed using 100 M samples of a long bit sequences and a common significance level $\alpha = 0.01$. Here we emphasize that the bit sequences used for the tests are those obtained for the ensemble of the chaotic light intensity signals starting from the same initial state, while previous works have used bit sequences generated from a single chaotic trajectory of the light intensity obtained by continuous operation of chaotic lasers. If the generated bits are deterministic pseudo-random and reproducible, they would never pass this test. Accordingly, with this test, it is possible to test whether the bits appear to be nondeterministic and unpredictable.

We confirmed that the bit sequences generated at the sampling rate about 1.2 GHz pass all of the tests. A significant statistical correlation occurs for higher sampling rates, and the number of the passed tests is decreased. In particular, the bit sequences fail the test“block frequency”, where the ratio of the statistical frequencies of bits 0 and 1 within a specified block length is investigated. The result is related to the decrease of the entropy for the shorter sampling time interval, as shown in Fig. 5.

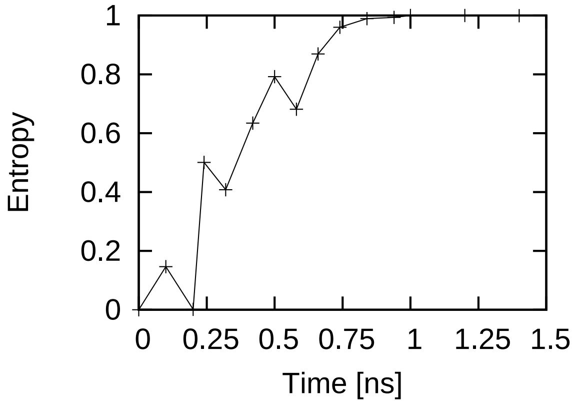

Figure 4: Time dependence of the Shannon's entropy of the bit sequences.

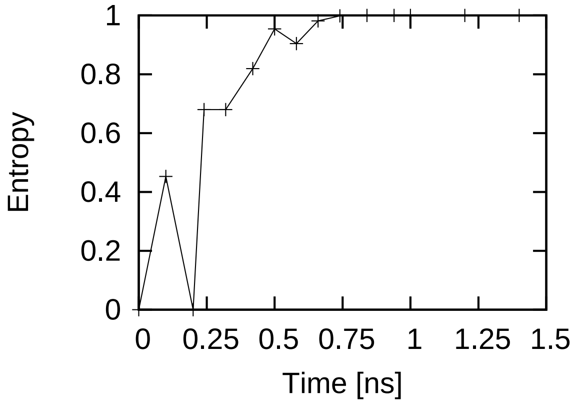

Figure 5: Time dependence of the Shannon's entropy of the XOR-ed bit sequences.

5. Summary

In summary, we experimentally demonstrated that the intrinsic microscopic noises can be rapidly amplified by the chaotic dynamics for very short time in the order of nano second by resetting the state of the system to a same initial state repeatedly. Then we investigated the non-determinism of random bit generation with chaotic laser systems in terms of the convergence property to the invariant density, and discussed the relation between the bit entropy and the convergence of initial probability density due to noise to the invariant density. It was confirmed that the entropy of the bit generation is related to the rate of convergence to the invariant density.

Acknowledgment

The first author was partially supported by Grant-in-Aid for Young Scientists (B) (Grant No. 10463704), Japan Society for the Promotion of Science.

References

[1] A. Uchida, et al, *Nature Photon.*, vol.2, pp.728–732, (2008).

[2] C. R. S. Williams, et al, *Opt. Express*, vol.18, pp. 23584–23597, (2010).

[3] X. Li, et al, *Opt. Lett.*, vol. 36, pp.1020-1022, (2011).

[4] K. Hirano, et al, *IEEE J. Quantum Electron.*, vol.45, pp.1367–1379, (2009).

[5] K. Hirano, et al, *Opt. Express*, vol.18, pp.5512–5524, (2010).

[6] I. Reidler, et al, *Phys. Rev. Lett.*, vol.103, 024102, (2009).

[7] I. Kanter, et al, *Nature Photon.*, vol. 4, pp.58–61, (2010).

[8] A. Argyris, et al, *Opt. Express*, vol.18, pp.18763–18768 (2010).

[9] T. Harayama, et al, *Phys. Rev. A*, vol.83, 031803(R) (2011).

[10] S. Sunada, et al, A. Uchida, *Opt. Express*, vol. 19(7) 5713-5724 (2011).

[11] P. Li, et al, *Opt. Express* vol.20(4) 4297-4308 (2012).

[12] P. Li, et al, *Opt. Express* vol.18(19) 20360-20369 (2010).

[13] T. Harayama, et al, *Phys. Rev. E* vol. 85(4) 046215 (2012).

[14] T. Mikami, et al, *Phys. Rev. E* vol.85 016211 (2012).

[15] S. Sunada, et al, submitted to Chaos: An Interdisciplinary Journal of Nonlinear Science.

[16] A. Rukhin, et al, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST Special Publication 800-22 Revision 1a, (2010).