2009 International Symposium on Nonlinear Theory and its Applications
NOLTA'09, Sapporo, Japan, October 18-21, 2009

Amplification of noise in chaotic semiconductor lasers used for fast physical random bit generation

Kota Aoyama[1)], Atsushi Uchida[1)], Kazuyuki Yoshimura[2)], and Peter Davis[2)]

[1)] Department of Information and Computer Sciences, Saitama University,
255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama, 338-8570, Japan
[2)] NTT Communication Science Laboratories, NTT Corporation,
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237 Japan

Abstract– We investigate the effect of noise amplification by chaotic dynamics in semiconductor lasers used for generation of random bit sequences. We measure the memory time of initial conditions after noise is added in the chaotic lasers. We found that the memory time decreases as the noise strength is increased. We also measure the predictability time in the case where an ensemble of states which correspond to the same bit sequence in the past bit is used for the prediction of random bit sequences. It is found that the predictability time can be shorter than the interval between samples used to obtain bits, so the bit sequences cannot be predicted even using optimal nonlinear laser models.

1. Introduction

Physical random processes are often used as entropy sources in random number generators used for information security and computations [1,2]. Random phenomena such as photon noise, thermal noise in resistors and frequency jitter of oscillators have been used as physical entropy sources for physical random number generators [3-11]. However, non-deterministic generators have been limited to much slower rates than pseudo-random number generators up to tens of megabit per second (Mbps) due to limitations of the rate and power of the mechanisms for extracting bits from physical noise [3,4].

Recently, a fast physical random bit generator using chaotic semiconductor lasers has been demonstrated that generate random bit sequences that pass standard tests of randomness at a rate of up to 1.7 gigabit per second (Gbps) [12]. The performance of physical random number generation could be greatly improved by using chaotic laser devices as physical entropy sources. The output of chaotic devices can be both unpredictable as well as statistically random because they generate large amplitude random signals from microscopic noise by nonlinear amplification and mixing mechanisms [13,14]. It is important to measure the effect of noise amplification by chaotic dynamics to estimate predictability of random numbers generated by chaotic semiconductor lasers.

In this study, we present a numerical analysis of the characteristic time for amplification of noise by chaotic dynamics in semiconductor lasers, and its dependence on the noise strength. We define and estimate two characteristic times, the memory time and the predictability time, and present them as evidence for the unpredictability of bit sequences obtained by sampling the optical output of the chaotic lasers.

2. Method

A sequence of bits obtained by sampling a theoretically ideal deterministic chaos system is, in principle, completely predictable if the initial states of the system are known with infinite precision. However, a sequence generated by a real chaotic laser is predictable only if the rate of information about the laser state obtained by observing the generated sequence is greater than the rate of entropy production by amplification of noise by the chaotic dynamics in the laser.

Theoretically, the behavior of the chaotic state of the laser can be modeled by a set of equations of motion for the dominant macroscopic (large amplitude) degrees of freedom, and a stochastic noise due to huge number of microscopic (small amplitude) degrees of freedom. The chaotic state of a laser is a distinct state of the laser clearly distinguishable from the stable lasing state (which is obtained at different parameter settings) by the large amplitude, wildly varying oscillations [15-18]. When the oscillation of the macroscopic degrees of freedom is chaotic, the effects of microscopic noise are rapidly and continuously amplified [13,14]. So even if the macroscopic state of the laser is observed with high resolution at some time instant, at some time T later it will not be possible to predict whether the state corresponds to a "1" or a "0", if T is longer than a characteristic time. In the case of random bit generation, this unpredictability is a desired feature, so it is important to sample at time intervals longer than the characteristic time. The characteristic time depends on the amplification and mixing properties of the chaos dynamics, and the amplitude of the microscopic noise.

3. Numerical model

The set of equations for the semiconductor laser with delayed optical feedback is described as follows (Lang-Kobayashi equations) [19].

$$\frac{dE(t)}{dt} = \frac{1}{2}\left[G_N\left(N(t) - N_0\right) - \frac{1}{\tau_p} \right] E(t) + \frac{\kappa}{\tau_{in}} E(t-\tau)\cos(\theta(t)) + \xi(t) \quad (1)$$

$$\frac{d\phi(t)}{dt} = \frac{\alpha}{2} G_N\left(N(t) - N_{th}\right) - \frac{\kappa}{\tau_{in}} \frac{E(t-\tau)}{E(t)} \sin(\theta(t)) \quad (2)$$

$$\frac{dN(t)}{dt} = J - \frac{N(t)}{\tau_s} - G_N\left(N(t) - N_0\right)\left|E(t)\right|^2 \quad (3)$$

$$\theta = \omega\tau + \phi(t) - \phi(t-\tau) \quad (4)$$

$$\left\langle \xi(t)\xi(t-\tau) \right\rangle = D\delta(\tau) \quad (5)$$

where, E is the electric field amplitude, ϕ is the phase, N is the carrier density. G_N is the gain coefficient, N_0 is the carrier density at the transparency, $N_{th} = N_0 + 1/(G_N \tau_p)$ is the threshold carrier density for the solitary laser, κ is the feedback coefficient, τ_p is the photon lifetime, τ_{in} is the optical round-trip time in the cavity of the semiconductor laser, τ_s is the carrier lifetime, τ is the external cavity round-trip time, α is the linewidth enhancement factor, and J is the injection current density. ω is the angular optical frequency. D is the noise strength. An additive white Gaussian noise is added in Eq. (1). We numerically integrated these equations by employing the Runge-Kutta-Gill method. The parameters are set as follows: G_N =8.4 × 10^{-13} m^3s^{-1}, N_0 =1.4 × 10^{24} m^{-3}, τ_p =1.927 ps, τ_{in} =8.0 ps, τ_s =2.04 ns, τ =2.0 ns, α =5, J =1.44J_{th} ($J_{th} = N_{th}/\tau_s$), κ=0.04.

4. Temporal waveforms and random bit generation

Figure 1 shows an example of five trajectories starting from the same initial state and separating due to noise. Different time series of noise are added at t = 0 and chaotic trajectories are plotted. The trajectories start to diverge after 2 ns. The change in trajectories indicates the loss of the memory of the initial conditions due to the additive internal noise mixed by chaotic dynamics.

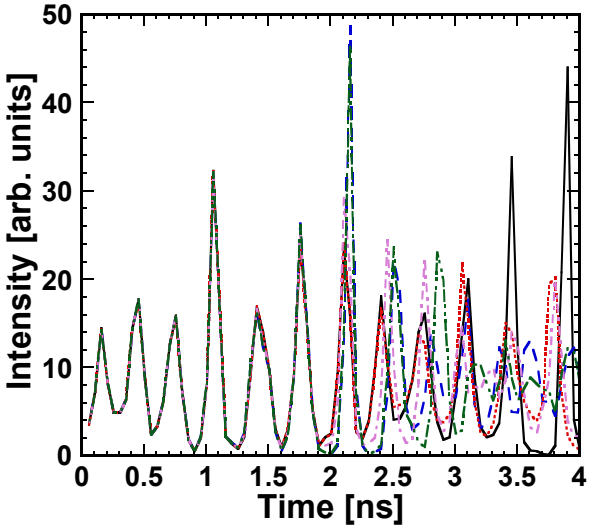

Fig. 1 Five temporal waveforms of chaotic laser outputs when different noise sequences are added at t = 0.

We use chaotic temporal waveforms to generate random binary bits. We consider two situations where one laser or two lasers are used. For both cases, we set a threshold value for each chaotic signal and sample the chaotic signal at the constant clock frequency of 1.7 GHz, as previously reported in Ref. [12]. The clock frequency is lower than the dominant frequency of the chaotic waveforms (~ 3 GHz). We convert the sampled data to a binary signal (0 and 1) by comparing with the set threshold value for each chaotic signal. The threshold levels are selected at the condition where the frequency of 0 becomes the closest value to 50%. For the two-laser case, two binary signals are obtained from the two lasers, and the two binary signals are combined by a logical Exclusive-OR (XOR) operation to generate a single random bit sequence.

5. Amplification of noise

We consider the situation where an attacker tries to predict the physical bit sequences generated by chaotic semiconductor lasers. We assume that the attacker not only observes the bit sequence, but that they have a computational dynamical model of the laser and statistical model of the noise, and they are able to make a prediction based on the observed sequence and numerical simulation of the model. We consider the two following cases:

Case 1: All the generated bit sequences, all the parameter values of the laser, and all the initial states of the laser are known with high precision by attackers. Note that a large number of initial states exist in the time-delayed feedback loop (external cavity) and the system becomes very high dimensional. This is not a realistic assumption, but very advantageous for attackers.

Case 2: All the generated bit sequences and all the parameter values of the laser are known by attackers, but initial states of the laser are unknown. This is a more realistic situation for attackers.

5.1 Memory time

Let us first consider the case 1. Figure 2(a) shows a plot of bit entropy against time. This is obtained with the following procedure. We execute the simulation of the dynamical equations of motion with noise added. The state of the laser is recorded at a particular time. We repeatedly re-run the simulation from that same initial state to obtain a set of different waveforms corresponding to different noise instances. We then convert each waveform to a binary signal by comparing with a fixed threshold level. Finally we compute the entropy of the set of binary signals as a function of time. The time-dependent entropy is defined as:

$$H(t) = -\sum_{i=0}^{1} P_i(t) \log_2 P_i(t) \quad (6)$$

where $P_i(t)$ is the probability of the occurrence of i (i = 0 or 1) at the time t for an ensemble of different waveforms with different additive noise instances.

It can be seen that the entropy reaches 1 after about three nanoseconds in Fig. 2(a). This indicates that even if we know the state of the laser in the dynamical model to high precision at some time, we are unable to predict whether the waveform will correspond to a "1" or a "0" at three nanoseconds later. In other words, there is no information about the initial state in the bit after this time. We define the "memory time" of the initial conditions T_m as the time when the entropy reaches more than 0.9 in this calculation.

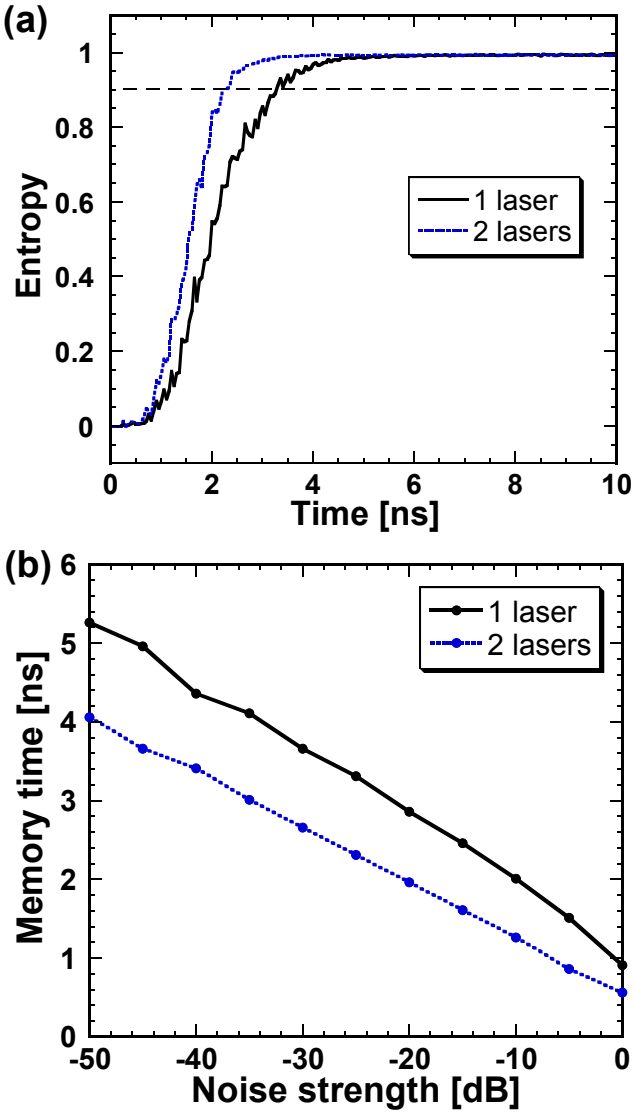

Fig. 2 (a) Bit entropy as a function of time. (b) Memory time as a function of noise strength.

Figure 2(b) shows the memory time as a function of noise strength. Note that noise strength -25 dB corresponds to the noise level in our experiment in Ref. [12], as evaluated by the signal-to-noise ratio. The plot is a straight line and the memory time decreases as the noise strength is increased. Even if the laser state is exactly known at some time t = 0, the entropy of the corresponding binary signal becomes unity after memory time T_m. For the noise level of -25dB observed in the experiment, the memory time T_m corresponds to 2.4 nanoseconds for the two-laser case.

5.2 Predictability time

We next consider the case 2 where the attacker cannot observe the analog initial state of the laser, but can only observe the bit sequence generated. In this situation, we should estimate the possible states of the laser based on the past bit sequence, then run our simulator forward in time to estimate the possible states of the laser at the time of the next bit. The entropy of the next bit depends on the ensemble of all the laser states which are consistent with the past bit sequence. This is a rather large computation for a system with large dimensions due to the time-delay. So instead we generate a representative ensemble in the following way. We start from a single state, assuming that we have somehow identified this state with a long bit sequence starting at minus infinity. We run the simulation with various noises, and keep a set of trajectories that correspond to the same bit pattern for the next M-bits. Now we have an ensemble of states which correspond to the same bit sequence in the past. We run the simulation forward for these states, and calculate the entropy of the next bit (that is the (M+1)th bit).

Figure 3 shows the entropy of the corresponding binary signal as a function of time from the M-th bit for M=5, in the case of bit sequences generated at 1.7 Gbps. It can be seen that at the time 0.05 nanoseconds (ns) later, the entropy has reached more than 0.9. This characteristic time is defined as the "predictability time" T_p. Note that T_p of 0.05 ns is shorter than the bit interval (0.59 ns, inverse of the sampling frequency of 1.7 GHz). This result supports unpredictability of random bit sequences from the attack with chaotic laser models [12].

Our numerical analysis supports the claim that if we can only observe the bit sequence (and not the internal analog state of the laser system itself) then even if we use a computational model of the chaotic dynamics, we cannot predict the next bit. This is because of the persistent uncertainty in the state of the laser, due to the property that the rate of the generation of entropy (due to amplification of noise by the chaotic dynamics) is large compared to the bit rate.

The results of the numerical analysis explained above support the claim of unpredictability. These can be reproduced by anyone using the well known nonlinear dynamical model for this type of chaotic laser. It is difficult to achieve this proof experimentally, because of the need to repeatedly prepare the laser in the same state.

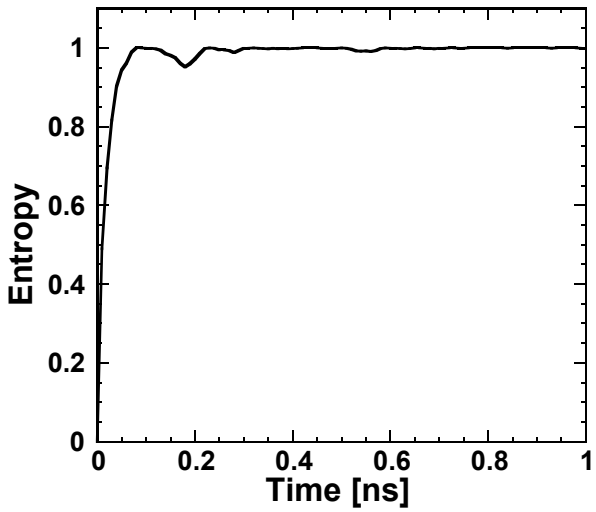

Fig. 3 Bit entropy as a function of time when only preceding bit sequence is known.

6. Conclusion

We have calculated the effect of noise amplification by chaotic dynamics in semiconductor lasers used to achieve generation of random bit sequences at the fast rate of 1.7 gigabits per second. We have measured the memory time of the initial conditions defined as the time when the entropy reaches more than 0.9 after noise is added in the chaotic lasers. We found that the memory time decreases as the noise strength is increased. We have also measure the predictability time when the entropy reaches more than 0.9 by using an ensemble of states which correspond to the same bit sequence in the past bit. It is found that the predictability time is shorter than the interval between samples used to obtain bits. This result supports the claim that the bit sequences are unpredictable even when chaotic dynamical models are used for prediction.

Acknowledgments

A. U. acknowledges support from TEPCO Research Foundation, JGC-S Scholarship Foundation, and Grants-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science and Technology.

References

[1] J. Kelsey, X9.82. NIST (2004)
[2] W. Schindler and W.Killmann, *CHES 2002, Lecture Notes in Computer Science* **2523** 431–449 (Springer-Verlag, Berlin Heidelberg) (2002).
[3] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.,* vol. 93, pp. 031109-1--031109-3, 2008.
[4] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, *IEEE Transactions on Computers* **52,** 403-409 (2003).
[5] B. Jun and P. Kocher, *White Paper Prepared for Intel Corporation,* Cryptography Research Inc., (1999). http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.
[6] W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, *IEEE Trans. Circuits and Systems I,* **44,** 521-528 (1997).
[7] F. Cortigiani, C. Petri, S. Rocchi, and V. Vignoli, *The 7th IEEE International Conference on Electronics, Circuits and Systems, 2000 (ICECS 2000)* **1,** 120 - 123 (2000).
[8] C. Tokunaga, D. Blaauw, and T. Mudge, *IEEE Journal of Solid-State Circuits* **43,** 78-85 (2008).
[9] T. Stojanovski, and L. Kocarev, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, **48,** 281-288 (2001).
[10] J. T. Gleeson, *Appl. Phys. Lett.* **81,** 1949 (2002).
[11] S. Callegari, R. Rovatti, and G. Setti, *IEEE Trans. Signal Processing* **53,** 793-805 (2005).
[12] 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, *Nature Photonics,* **2,** no.12, pp.728-732 (2008).
[13] R. F. Fox and J. Keizer, *Phys. Rev. A* **43,** 1709 (1991).
[14] C. Bracikowski, R. F. Fox, and R. Roy, *Phys. Rev. A* **45,** 403-408 (1992).
[15] G. D. VanWiggeren and R.Roy, *Science*, **279,** 1198-1200 (1998).
[16] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, *Nature* **438,** 343-346 (2005).
[17] J. M. Liu, H. F. Chen, and S. Tang, *IEEE Journal of Quantum Electronics* **38,** 1184- 1196 (2002).
[18] T. Yamamoto, I. Oowada, H. Yip, A. Uchida, S. Yoshimori, K. Yoshimura, J. Muramatsu, S. Goto, and P. Davis, *Optics Express,* **15,** no.7, pp.3974-3980 (2007).
[19] A. Uchida, N. Shibasaki, S. Nogawa, and S. Yoshimori, *Phys. Rev. E* **69,** 056201 (2004).