Estimation of entropy rate for random bit generators with chaotic semiconductor lasers

Takuya Mikami†, Kazutaka Kanno†, Kota Aoyama†, Atsushi Uchida†,
Takahisa Harayama‡, Satoshi Sunada‡, Ken-ichi Arai‡, Kazuyuki Yoshimura‡, Peter Davis‡

†Department of Information and Computer Sciences, Saitama University
255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama, 338-8570 Japan
‡NTT Communication Science Laboratories, NTT Corporation
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237 Japan
Emails: {s10mm326, auchida}@mail.saitama-u.ac.jp

Abstract– We estimate the entropy rate of a fast physical random bit generator using a chaotic semiconductor laser with intrinsic noise. The entropy is generated by the amplification of microscopic noise by chaotic dynamics. The relationship between the time for the loss of the memory of initial conditions and the intrinsic noise strength is investigated quantitatively. The entropy rate is evaluated from the memory time of the initial conditions and almost coincides with the maximum Lyapunov exponent of the dynamical laser system.

1. Introduction

Physical random processes can be used to realize non-deterministic random number generators for use in information security and computations [1,2]. Random phenomena such as photon noise and thermal noise in resistors have been used for physical random number generators [3,4]. However, it is difficult to realize non-deterministic generators which generate random bits at the communications over a Gigabit per second (Gb/s). Recently, fast physical random bit generators using chaotic semiconductor lasers have been demonstrated [5-13] and generate random bit sequences that pass standard tests of randomness at rates ranging from 1 to 300 Gb/s. From the point of view of information security applications, it is important to know not only that a sequence does not show statistically significant deviations from randomness, but also that the source is non-deterministic, in the sense that repeated operations of the device from the same initial state produce statistically independent sequences.

In this study we present numerical analysis which shows how unpredictable random bits can be generated at fast rates in a chaotic laser system, and estimate the rate of generation of non-deterministic bits, which is referred to as the entropy rate.

2. Numerical model

A set of equations for a semiconductor laser with time-delayed optical feedback from an external mirror is well known as the Lang-Kobayashi equations [14-16]. We include the gain saturation effect to reproduce a similar histogram of the laser intensity distribution to that observed in experiments [11,15]. The Lang-Kobayashi equations with the gain saturation effect are described as follows [15,16].

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

$$\frac{d\phi(t)}{dt}=\frac{\alpha}{2}\left[\frac{G_N\left(N(t)-N_0\right)}{1+\varepsilon E^2(t)}-\frac{1}{\tau_p}\right]-\kappa\frac{E(t-\tau)}{E(t)}\sin\left(\theta(t)\right)+\eta(t) \tag{2}$$

$$\frac{dN(t)}{dt}=J-\frac{N(t)}{\tau_s}-\frac{G_N\left(N(t)-N_0\right)}{1+\varepsilon E^2(t)}\left|E(t)\right|^2 \tag{3}$$

$$\theta=\omega\tau+\phi(t)-\phi(t-\tau) \tag{4}$$

$$\left\langle\xi(t)\xi(t-\tau)\right\rangle=D_E\delta(\tau) \tag{5}$$

$$\left\langle\eta(t)\eta(t-\tau)\right\rangle=D_\phi\delta(\tau) \tag{6}$$

where E is the electric field amplitude, ϕ is the electric field phase, N is the carrier density. G_N is the gain coefficient, N_0 is the carrier density at the transparency, $\kappa=\left(1-r_2^2\right)r_3/\left(r_2\tau_{in}\right)$ is the optical feedback strength, r_2 is the reflectivity of the internal cavity, r_3 is the reflectivity of the external mirror, τ_{in} is the optical round-trip time in the cavity of the semiconductor laser, τ_p is the photon lifetime, τ_s is the carrier lifetime, τ is the external-cavity round-trip time, α is the linewidth enhancement factor, J is the injection current density, ε is the gain saturation coefficient, $\omega=2\pi c/\lambda$ is the angular optical frequency, c is the speed of light, λ is the optical wavelength, and D is the noise strength. Additive white Gaussian noise $\xi(t)$ and $\eta(t)$ are added in Eqs. (1) and (2), respectively, as intrinsic noise. The parameter values are set as follows: $G_N = 8.4\times10^{-13}$ m^{3}s^{-1}, $N_0 = 1.4\times10^{24}$ m^{-3}, $\tau_p = 1.927\times10^{-12}$ s, $\tau_{in} = 8.0\times10^{-12}$ s, $\tau_s = 2.04\times10^{-9}$ s, $\tau = 2.0\times10^{-9}$ s, $\alpha = 5.0$, $J = 1.44\ J_{th}$ ($J_{th} = N_{th}/\tau_s$, $N_{th} = N_0 + 1/(G_N\tau_p)$), $\kappa = 6.25$ ns^{-1}, $\lambda =$

1.537×10^{-6} m, and $\varepsilon = 2.5\times10^{-23}$. The similarity of the dynamics in the numerical model and experiments has been confirmed. We numerically integrate the Lang-Kobayashi equations of Eqs. (1) ~ (3) with these parameter values by employing the Runge-Kutta method.

3. Noise amplification by chaotic dynamics

We add intrinsic noise in the deterministic model of Eqs. (1) ~ (3) to investigate the noise amplification effect by chaotic dynamics. All the time series are calculated from the same parameter values and the same initial conditions, however, different noise sequences are added to the same chaotic trajectory after $t = 0$. Figure 1 shows an example of three chaotic time series of the laser intensity ($I(t) = |E(t)|^2$) starting from the same initial conditions with different additive noise sequences. It is shown that the three chaotic time series are almost the same at around $t \approx 0$, however, they start separating to each other due to the effect of the intrinsic noise for the time evolution. On the scale of this plot, the time series appear to start diverging after a few nanoseconds. The difference in the trajectories indicates the loss of the memory of the initial conditions due to the nonlinear amplification of the additive internal noise by chaotic dynamics.

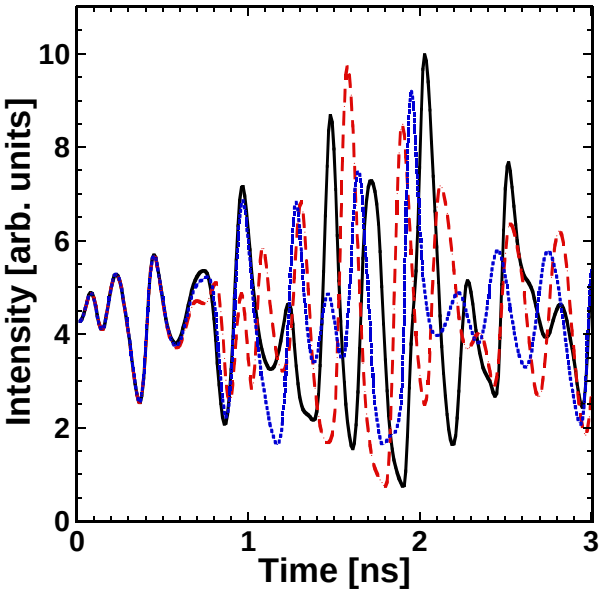

Figure 1 Three temporal waveforms of chaotic laser intensities starting from the same initial conditions when different noise sequences are added at time $t = 0$.

4. Estimation of entropy rate

We compute the time-dependent entropy to calculate the entropy rate of the generated bits as a physical random bit generator. First we calculate a temporal waveform of chaotic laser intensity. We set a threshold level to detect whether the laser intensity is above or below a specified level at fixed time intervals for extracting random bits (i.e., 1-bit analog-to-digital conversion) [5,6,13]. The threshold level is pre-defined for digitizing a temporal waveform, and is adjusted to equalize the long-time average ratio of the number of 0 and 1 bits, i.e., the probability of the occurrence of each bit is set to 50 % as close as possible. Each point on the temporal waveform is compared with the threshold level, and bit 1 is generated when the sampled point is larger than the threshold level, and bit 0 is generated otherwise. The temporal waveform is thus converted into a bit sequence in time. We execute this procedure for 10^3 temporal waveforms which are generated from the same initial conditions, but added by different microscopic noise sequences. We then calculate the probability of bit 1 and 0 at time t, and time-dependent entropy $H(t)$ is estimated by the following equation.

$$H(t) = -\sum_{i=0}^{1} P_i(t)\log_2 P_i(t) \qquad (7)$$

where $P_i(t)$ is the probability of the occurrence of bits 'i' (i = 0 or 1) at the time t for an ensemble of the time series with different additive noise instances. The time-dependent entropy is also averaged over 10^3 different initial conditions.

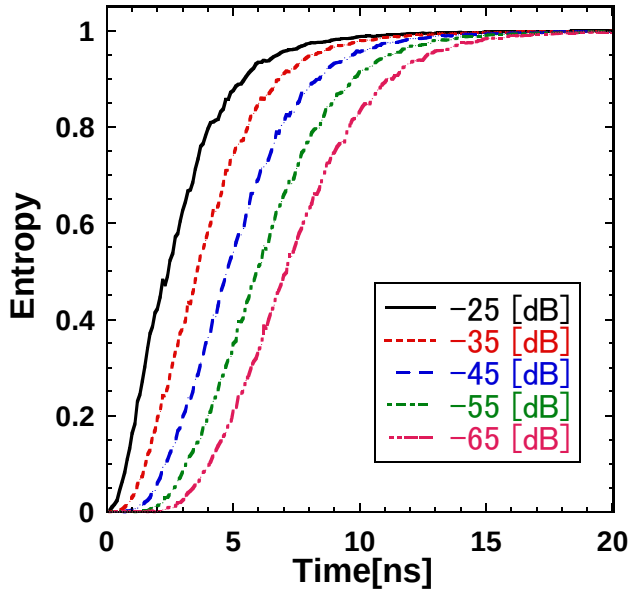

Figure 2 Entropy as a function of time for an ensemble of time series starting at exactly the same state at time $t = 0$ for different noise strengths. Solid line: noise strength of -25 dB, dotted line: -35dB, dashed line: -45 dB, dashed-dotted line: -55 dB, dashed double-dotted line: -65 dB. The noise strengths are evaluated by the signal-to-noise ratio in the power spectrum of the optical intensity signal.

Figure 2 shows an example of the plots of bit entropy as a function of time for an ensemble of time series starting at exactly the same state at time t = 0 for the different noise strengths. It can be seen that the entropy reaches ~1 after ~10 ns for the noise strength of -25 dB, where the noise strength is defined as the ratio of the signal (the peak value of the center frequency of chaotic waveforms) to noise (the noise floor level) in the power spectrum of the optical intensity signal. This fact indicates that even if we know the state of the laser in the dynamical model to high precision at t = 0, we are unable to predict whether the waveform corresponds to a bit '1' or '0' after the entropy reaches ~1. It is worth noting that there is no information about the initial conditions in the bit after this time. As shown in Fig. 2, more time is required to converge to $H(t) \approx 1$ as the noise strength is decreased. The time for the convergence to $H(t) \approx 1$ is thus dependent on the noise strength.

Let us define the "memory time" T_m of the initial conditions as the time when the time-dependent entropy $H(t)$ reaches more than 0.995, which corresponds to the pass criteria of the frequency (0/1 ratio) test for the length of 10^3 bits in the NIST Special Publication 800-22 statistical tests of randomness [17]. From Fig. 2, the memory times T_m are estimated as 13.0, 14.1, 15.3, 17.0, and 18.2 ns for the noise strengths of -25, -35, -45, -55, and -65 dB, respectively.

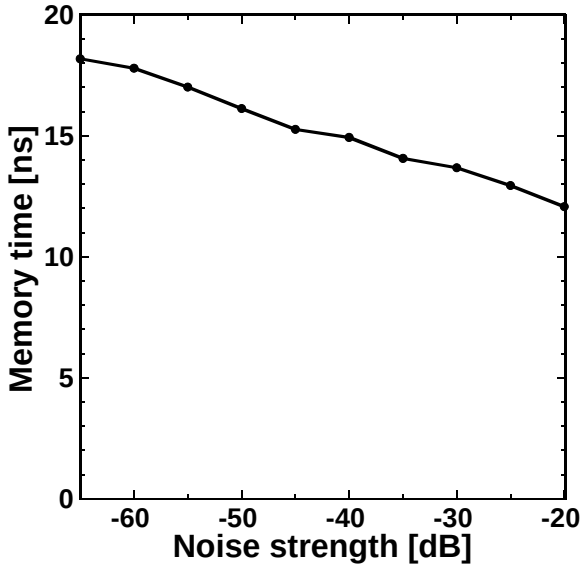

Figure 3 Memory time as a function of the noise strength. The memory time T_m of the initial conditions is defined as the time when the time-dependent entropy $H(t)$ reaches more than 0.995.

We investigate the memory time when the noise strength is changed continuously. Figure 3 shows the memory time as a function of the noise strength. The plot is an almost straight line on the semi-logarithmic plot, indicating that the memory time decreases as the noise strength is increased exponentially. This relationship can be fitted with the empirical relation as follows.

$$T_m - T_0 = L(10\log_{10} S_n) \tag{8}$$

where T_m is the memory time, T_0 is the offset time, S_n is the noise strength, and L is the slope of the straight line in Fig. 3. The value of L obtained from the plot in Fig. 3 is L = -0.14 ns/dB. The linear slope shows that we can estimate the entropy rate that is independent of the noise strength. The entropy rate can be defined as the rate of the increase of the noise strength (taking the natural logarithm) to the increase of the memory time,

$$R_e = \log_e(S_n)/(T_m - T_0) \tag{9}$$

The value of entropy rate R_e can be obtained from Eqs. (8) and (9),

$$R_e = 1/(|L| \times 10\log_{10} e) = 1.7\ ns^{-1} \tag{10}$$

The entropy rate can be a measure of the generation speed of uncertainty from intrinsic noise amplification by chaotic dynamics. Non-deterministic bit generation can be guaranteed when the entropy rate is larger than the bit generation rate. Therefore, these results show that non-deterministic bit generation at the maximum speed of 1.7 Gb/s can be achieved by using a chaotic semiconductor laser with 1-bit analog-to-digital conversion.

5. Comparison of entropy rate with maximum Lyapunov exponent and KS entropy

To investigate the influence of laser parameter values on the entropy rate, we calculate the maximum Lyapunov exponent of the chaotic semiconductor laser with the same parameter values by using the linear stability analysis [18,19]. The maximum Lyapunov exponent is obtained as a rate of the exponential growth of the norm of linearized variables in the logarithmic scale. We evaluate the entropy rate and the maximum Lyapunov exponent at different chaotic states by changing the optical feedback strength κ. Figure 4 shows the entropy rate R_e and the maximum Lyapunov exponent as a function of the optical feedback strength κ. It is worth noting that the entropy rate almost coincides with the maximum Lyapunov exponent for different chaotic states. This result indicates that the entropy rate defined as Eq. (9) can be estimated from the maximum Lyapunov exponent of the chaotic semiconductor laser. Therefore, the maximum Lyapunov

exponent can be a good measure to design random bit generators with large entropy rate.

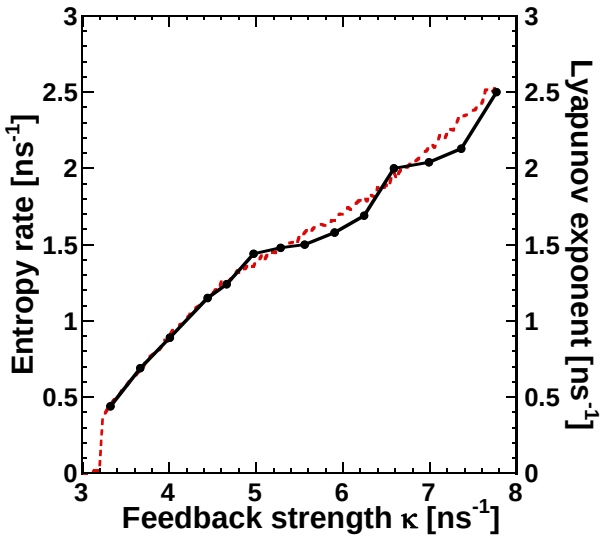

Figure 4 Entropy rate R_e (solid curve) and the maximum Lyapunov exponent (dotted curve) as a function of the optical feedback strength κ.

6. Conclusion

We have evaluated the entropy rate of a random bit generator using a chaotic semiconductor laser with intrinsic noise, and shown that bits are non-deterministic if extracted at rates slower than the entropy rate due to the nonlinear amplification of microscopic noise by chaotic dynamics. Using particular parameter values corresponding to semiconductor laser implementations, we show that non-deterministic bits can be generated in the gigabit per second regime. The persistent uncertainty in the state of the laser can be guaranteed because of the property that the rate of the generation of entropy (due to the amplification of intrinsic noise by chaotic dynamics) is larger than the bit generation rate. The technique used for the evaluation of the entropy rate can be useful for designing fast physical random bit generators with non-deterministic bits.

Acknowledgments

We gratefully acknowledge support from TEPCO Research Foundation and Grant-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science and Technology in Japan.

References

[1] W. Schindler and W.Killmann, CHES 2002, Lecture Notes in Computer Science **2523,** 431 (Springer-Verlag, Berlin Heidelberg) (2002).
[2] D. Eastlake, J. Schiller, and S. Crocker: "Randomness requirements for security," RFC4086 (2005).
[3] W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, IEEE Trans. Circuits and Systems I **44,** 521 (1997).
[4] C. Tokunaga, D. Blaauw, and T. Mudge, IEEE J. Solid-State Circuits **43,** 78 (2008).
[5] 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,** 728 (2008).
[6] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, IEEE J. Quantum Electron. **45,** 1367 (2009).
[7] T. E. Murphy and R. Roy, Nature Photonics **2,** 714 (2008).
[8] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103,** 024102 (2009).
[9] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, Optics Express **17,** 9053 (2009).
[10] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nature Photonics **4,** 58 (2010).
[11] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, Optics Express **18,** 5512 (2010).
[12] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Optics Express **18,** 18763 (2010).
[13] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Phys. Rev. A **83,** 031803(R) (2011).
[14] R. Lang and K. Kobayashi, IEEE J. Quantrum Electron. **16,** 347 (1980).
[15] D. W. Sukow, T. Heil, I. Fischer, A. Gavrielides, A. Hohl-AbiChedid, and W. Elsäßer, Phys. Rev. A **60,** 667 (1999).
[16] J. Ohtsubo, "*Semiconductor Lasers, -Stability, Instability and Chaos-*," Second Ed., Springer-Verlag, Berlin Heidelberg (2008).
[17] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. E. Bassham III, National Institute of Standards and Technology (NIST), Special Publication 800-22, Revision 1a (2010).
URL:http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf
[18] R. Vicente, J. Daudén, P. Colet, and R. Toral, IEEE J. Quantum Electron. **41,** 541 (2005).
[19] K. Pyragas, Phys. Rev. E **58,** 3067 (1998).