Noise-robustness of Random Bit Generations by Chaotic Semiconductor Lasers

Masanobu Inubushi†, Kazuyuki Yoshimura†, and Peter Davis‡

†NTT Communication Science Laboratories, NTT Corporation
2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237 Japan
‡Telecognix Corporation
58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto, 606-8314, Japan
Email: inubushi.masanobu@lab.ntt.co.jp

Abstract—We claim that a property of *noise-robustness* is important for reliable physical random bit generators (RBGs), and we report that RBGs using chaotic semiconductor lasers are noise-robust, i.e. insensitive to properties of a noise source. Employing the Lang-Kobayashi model, we study an influence of variations of noise properties on unpredictability of the laser chaos, and compare it with that of a bistable RBG.

1. Introduction

Random bit generation is one of the important technologies of the information security, such as secret key generation, secret calculation, and secret distribution. For the information security technology, random bits should be hard to predict. Thus, *physical* random bit generation is expected to be employed for the technologies, since the physical random bits are generated from unpredictable physical phenomena, as thermal noise and quantum noise. Recently, many researchers study and develop physical RBGs by using semiconductor lasers [1], a superluminescent LED [2], and hybrid Boolean networks [3]. These studies mainly focus their attention on the generation speed of the random bits, and less attention is being paid to reliability of the RBGs.

In this paper, for the reliable physical RBG, we emphasize that physical RBGs should be *noise-robust*. In general, physical RBGs use some kind of noise source as a black box, which means noise is generated by unknown rules and it is hard to control. Therefore, the properties of noise can be changed unexpectedly or some hidden properties of noise might exist or appear because of our limited knowledge of noise source. For instance, the noise distribution get to be biased or the noise sequence can get to have a temporal correlation accidentally. Even so, the reliable physical RBGs are required to be less affected by the changes of noise properties and/or appearing the hidden noise properties, particularly for the usage of the security technology. More concretely, we say that physical RBGs are noise-robust if the unpredictability of the physical RBGs is not sensitive to the noise properties.

The Physical RBG by the semiconductor laser chaos is one of the promising physical RBGs since it can generate random bits fast enough [1] and its unpredictability is theoretically examined by Harayama *et al.* [7]. Hence, we study the noise-robustness of physical RBG by the laser chaos in this paper. Dependency of the noise strength on the unpredictability of physical RBG by the laser chaos is studied by Mikami *et al.* [6]. Here, we consider the bias of the noise-distribution and the temporal correlation of noise time sequence. Specifically, by employing Lang-Kobayashi model, we study the noise-robustness of physical RBG by the laser chaos, and also we compare it with that of the bistable RBG which is now commonly used, for instance, in Intel's Ivy Bridge [4].

The numerical model of the laser chaos, the numerical method, and the noise sequence is described in Sec. 2 briefly. The noise-robustness of RBGs by chaotic laser to the bias of the noise-distribution and the temporal correlation of noise sequence are studied in Sec. 3 and Sec.4 respectively. In Sec. 5, we give conclusions and discussions.

2. Numerical model and method

The chaotic dynamics of the semiconductor laser with delayed feedback can be studied by the Lang-Kobayashi model equation:

$$\begin{aligned}
\frac{dE(t)}{dt} &= \frac{1}{2}\Big[-\frac{1}{\tau_p}+F\Big(E(t),N(t)\Big)\Big]E(t)\\
&\quad +\kappa E(t-\tau_D)\cos\theta(t)+\xi_E(t),\\
\frac{d\phi(t)}{dt} &= \frac{\alpha}{2}\Big[-\frac{1}{\tau_p}+F\Big(E(t),N(t)\Big)\Big]\\
&\quad -\kappa\frac{E(t-\tau_D)}{E(t)}\sin\theta(t)+\xi_\phi(t),\\
\frac{dN(t)}{dt} &= -\frac{N(t)}{\tau_s}-F\Big(E(t),N(t)\Big)\,E(t)^2+J,
\end{aligned}\tag{1}$$

where $E(t)\in\mathbb{R}$ is an amplitude of a complex electric field, $\phi(t)\in\mathbb{R}$ is a phase of a complex electric field, $N(t)\in\mathbb{R}$ is a career density, $\theta(t) := \omega\tau+\phi(t)-\phi(t-\tau)$, and $F\Big(E(t),N(t)\Big) := G_N\frac{N(t)-N_0}{1+\epsilon E(t)^2}$. The parameter in the equations and their values used in the numerical experiments

Symbols	Parameters	Values
τ_D	External-cavity round-trip time	0.25ns
τ_p	Photon lifetime	1.927ps
τ_s	Carrier lifetime	2.04 ns
α	Linewidth enhancement factor	5.0
G_N	Gain coefficient	$8.4 \times 10^{-13}\mathrm{m}^3\mathrm{s}^{-1}$
N_0	Carrier density at transparency	$1.400 \times 10^{24}\mathrm{m}^{-3}$
ϵ	Gain saturation coefficient	2.5×10^{-23}
κ	Feedback strength	$6.25\ \mathrm{n}s^{-1}$
J	Injection current	$1.42 \times 10^{33}\mathrm{m}^{-3}\mathrm{s}^{-1}$
ω	Optical angular frequency	$1.225 \times 10^{15}\mathrm{s}^{-1}$
D	Noise amp.	1.0×10^{-4}

Table 1: The parameters in the Lang-Kobayashi equation and their values used in the numerical experiments.

are shown in Tab.1. The period of the relaxation oscillation is $T_{\mathrm{relax}} = 2\pi/\omega_{\mathrm{relax}} = 0.35$[ns], the external cavity length is $L = c\tau_D/2 = 0.037$[m], and $J/J_{\mathrm{th}} = 1.44$. $\xi(t)$ is a model of the noise in the laser system such as the spontaneous emission, which is usually assumed as a white Gaussian process. Here we consider $\xi(t)$ as a biased white Gaussian process in Sec. 3, and as a Ornstein- Uhlenbeck (OU) process in Sec.4. Numerical solutions of the Lang-Kobayashi equation are calculated by using 4th order Runge-Kutta method (the time step $\Delta t = 1.0\times10^{-3}$), and the Ornstein- Uhlenbeck (OU) process is calculated by using the method of Fox *et al.*[5].

3. Bias of noise-distribution

Here, we study the robustness of the chaotic laser RBGs to a bias in a noise distribution. Usually, in studies of chaos in the Lang-Kobayashi model, the center of the noise distribution is set to be zero: $\langle\xi(t)\rangle = 0$, where the bracket denotes a long time average $\langle\cdot\rangle = \lim_{T\to\infty}\frac{1}{T}\int_0^T \cdot\, dt$. Realistically, it is difficult to set and keep the center of the distribution to be zero. Thus, reliable RBGs are expected to be robust to a bias in a noise distribution. In this section, we study robustness of RBGs using Lang-Kobayashi model chaos to changes in the center of the noise distribution.

Let us consider a white Gaussian process $\xi_E(t)$ ($\xi_\phi(t)$) whose mean value is $\epsilon\sqrt{D}$ (zero) as a biased noise sequence, i.e.

$$\langle\xi_E(t)\rangle = \epsilon\sqrt{D},\ \ \langle\xi_\phi(t)\rangle = 0, \tag{2}$$

$$\langle\xi'_E(t)\xi'_E(s)\rangle = \langle\xi'_\phi(t)\xi'_\phi(s)\rangle = D\delta(t-s), \tag{3}$$

where $\xi'(t) = \xi(t) - \langle\xi(t)\rangle$, $\sqrt{D}$ is a noise strength, ϵ denotes the normalized strength of the bias. To study the robustness of RBG, we calculate probability $p(\epsilon)$ defined by

$$p(\epsilon) = \int_{E_t}^{\infty} P(E,\epsilon)dE, \tag{4}$$

where $P(E,\epsilon)$ is probability density function of the amplitude of the electric field E when the chaotic laser is affected by ϵ-biased noise sequence, and E_t is a threshold to generate a bit from an analog sample of signal $E(t)$ when $\epsilon = 0$: $p(0) = 1/2 = \int_{E_t}^{\infty} P(E,0)dE = \int_{-\infty}^{E_t} P(E,0)dE$. Employing the probability $p(\epsilon)$, we can measure the robustness of RBGs: for a given ϵ, the smaller the probability deviation $|p(\epsilon) - 1/2|$ is, the more robust the RBG is. Specifically, $dp(0)/d\epsilon$ can be used for measuring a "local" robustness, which means the RBG is robust to infinitesimal changes in noise properties.

Figure 1 shows the numerically calculated probability $p(\epsilon)$: the red, green, blue, and purple line is the case of $D = 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}$ respectively. The error bar is the standard deviation of the ensemble average, where we use ten different initial conditions with different noise realizations. The horizontal axis is ϵ. Except for the large noise case ($D = 10^{-3}$), the probability deviation $|p(\epsilon)-1/2|$ is less than 0.01 for $\epsilon < 1$, i.e. the error by the bias is less than 1 %.

As a reference, the probability deviation $|p(\epsilon) - 1/2|$ in the bistable RBG case is also shown in Figure 1 (the blue broken line). In the bistable RBG case, the probability $p(\epsilon)$ is given by the integration of the Gaussian distribution, which is the complementary error function: $p(\epsilon) = 1/2\ \mathrm{erfc}(\epsilon)$.

Although the large deviation from $p(\epsilon) = 1/2$ is found in the large biased case in the large noise case (i.e. $\epsilon > 0.3, D = 10^{-3}$), $dp(0)/d\epsilon$ is quite small for all noise amplitude D ($dp(0)/d\epsilon \simeq 0$), particularly smaller than $dp(0)/d\epsilon = 1/\sqrt{2\pi}$ in the bistable case. Thus, the laser chaos RBG is robust to the infinitesimal bias in noise distribution, particularly more robust than the bistable RBG.

4. Correlated noise

Next, we study the robustness of RBGs using chaotic laser to the temporal correlation of noise sequence. As mentioned in Sec. 2, we use the Ornstein- Uhlenbeck (OU) process $\xi(t)$ governed by

$$\frac{d\xi}{dt} = -\gamma\xi + \sqrt{2\gamma D}\zeta, \tag{5}$$

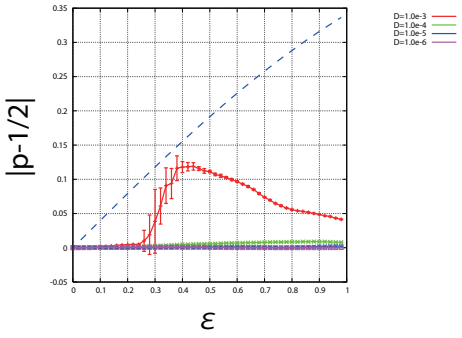

Figure 1: The probability deviation $|p(\epsilon) - 1/2|$. The red, green, blue, and purple line is the case of $D = 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}$ respectively. In the bistable RBG case, $p(\epsilon) = 1/2\ \mathrm{erfc}(\epsilon)$, as depicted by the blue broken line.

where ζ is the white Gaussian process, i.e. $\langle\zeta(t)\rangle = 0$, $\langle\zeta(t)\zeta(s)\rangle = \delta(t-s)$. Then, the OU process has following properties [8]: $\langle\xi(t)\rangle = 0$, $\langle\xi(t)\xi(s)\rangle = De^{-\gamma|t-s|}$. D is fixed as shown in the Tab.1, and the correlation time $T_\gamma := 1/\gamma$ is a control parameter.

To measure the unpredictability of the laser chaos, we define a correlation coefficient of the amplitude of the electric fields $E(t)$. Here, we write the laser state and the noise state as (x, ξ), and their time evolutions as

$$(x(T), \xi(T)) = \varphi^T_{\gamma,i}(x(0), \xi(0)), \tag{6}$$

where $\varphi^T_{\gamma,i}$ is a time evolution operator defined by the evolution equations (1), (5) with the parameter γ. The subscript i represents the index of the noise realization, i.e. the different indices mean the different noise realizations, which cause the different time evolutions though the initial conditions are same; $\varphi^T_{\gamma,1}(x(0), \xi(0)) \neq \varphi^T_{\gamma,2}(x(0), \xi(0))$. Using these notation, we define the correlation coefficient as

$$C(T_\gamma, T_s) := \frac{\left\langle \tilde{E}\left(\varphi^{T_s}_{\gamma,1}(x,\xi)\right)\tilde{E}\left(\varphi^{T_s}_{\gamma,2}(x,\xi)\right)\right\rangle}{\mathrm{Var}(\tilde{E})} \tag{7}$$

where $\tilde{E}$ is a fluctuation part of E; $\tilde{E}(x) = E(x) - \langle E\rangle$, and T_s is the RBG sampling time. The correlation coefficient $C(T_\gamma, T_s)$ evaluates how fast the correlation vanishes by the difference of the noise realization only. $C(T_\gamma, T_s)$ can be used as an indicator of the unpredictability of the RBG, i.e. $C(T_\gamma, T_s) = 0$ indicates that the RBG is unpredictable.

We examine the parameter dependence of the correlation coefficient $C(T_\gamma, T_s)$ as shown in Fig.2. The darker area corresponds to the lower correlation $C(T_\gamma, T_s) \simeq 0$, and the lighter area corresponds to the higher correlation $C(T_\gamma, T_s) \simeq 1$. Let us consider the functional relation $T_s = f(T_\gamma)$ defined by the boarder between the area $C(T_\gamma, T_s) > 0$ and the area $C(T_\gamma, T_s) = 0$. The light blue curve in the figure is defined by $C(T_\gamma, T_s) = 0.1$ as a reference. The results show that the longer the noise correlation time T_γ is, the longer the required sampling interval T_s is. Interestingly, in the long correlation time region ($T_\gamma \gg 1$), the required sampling interval depends on the noise correlation time T_γ logarithmically as $T_s \propto \log T_\gamma$.

As a reference, in the case of the bistable RBG, the required sampling interval is linearly proportional to the correlation time as $T_s \propto T_\gamma$ for all T_γ. Thus, as we increase the noise correlation time T_γ, the sampling interval T_s in the case of the chaos laser gets longer with a slower speed than that in the case of the bistable case. In this sense, the laser chaos RBG is robust to the noise correlation, and in particular more robust than the bistable RBG.

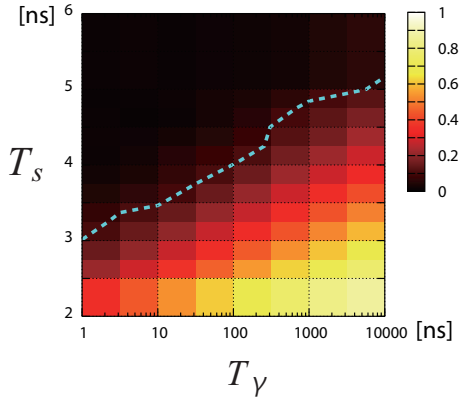

Figure 2: The correlation coefficient $C(T_\gamma, T_s)$ for temporally correlated noise. The light blue curve is defined by $C(T_\gamma, T_s) = 0.1$.

5. Conclusions and discussions

The noise-robustness of an RBG using a chaotic laser modeled by the Lang-Kobayashi equation.

Firstly, we consider the robustness of the chaos laser RBG to the bias of the noise-distribution, and we found that the chaos laser RBG is robust in the sense that the error in the probability $p(\epsilon)$ is less than 1 % for $\epsilon < 1$ except for the large noise case ($D = 10^{-3}$). Also, the chaos laser RBG is locally robust: $dp(0)/d\epsilon$ is quite small, particularly smaller than $dp(0)/d\epsilon = 1/\sqrt{2\pi}$ in the bistable case.

Secondly, we consider the robustness of the chaotic laser RBG to the temporal correlation of the noise. It is found that the RBG by the chaos laser is robust in the sense that the required sampling interval depends on the noise correlation time T_γ logarithmically as $T_s \propto \log T_\gamma$ in the long correlation time region ($T_\gamma \gg 1$), which is more robust than the bistable RBG case ($T_s \propto T_\gamma$ for all T_γ).

In the study of the robustness of RBG to the bias in the noise-distribution, we considered the quantity $dp(0)/d\epsilon$. The quantity is formulated in the linear response theory for general dynamical systems developed by Ruelle [9] under several assumptions. They considered the vector field $X + aX$ on a state space M which defines a flow (f^t_a) with a

hyperbolic attractor K_a depending continuously on a, and they obtained a general formula:

$$\frac{d}{da}\rho_a(A)|_{a=0} = \int_0^\infty dt \int \rho_0(dx)X(x)\cdot\nabla_x(A\circ f_0^t), \quad (8)$$

where ρ_a is the so-called *SRB measure* with the parameter a, $A : M \to \mathbb{R}$ is an observable, and $\rho_a(A) = \int \rho_a(dx)A(x)$. In our context, $A = H(E(x) - E_t)$ where $H(\cdot)$ is the Heaviside step function and $E(x)$ is the amplitude of electric field at state $x \in M$. The situations of the local robustness of the RBG differ from those of the Ruelle's linear response theory since they considered the finite dimensional dynamical system, the hyperbolic attractor, A is C^2 function, and so on. However, their theory is expected to be useful for studying the robustness of a RBG by a chaotic attractor in a general frame work, and the study in this direction will be tackled in the future.

Appendix A. Why $T_s \propto \log T_\gamma$ ($T_\gamma \gg 1$) ?

Let us consider an equation of motion with noise $dx/dt = F(x) + \xi_x$ and $dy/dt = F(y) + \xi_y$. Initially, we suppose $\delta(0) = \Delta(0) = 0$, where $\delta(t) = y(t) - x(t)$ and $\Delta(t) = \xi_y(t) - \xi_x(t)$. An error vector δ is governed by a variational equation $d\delta(t)/dt = DF_x\delta(t) + \Delta(t)$, where DF_x is Jacobian matrix at x.

Initially, the error vector δ is governed by $d\delta(t)/dt \simeq \Delta(t)$. Considering $\xi_x(t), \xi_y(t)$ as the OU process (see (5)) and the evolution equation $d\delta(t)/dt = \Delta(t)$, we can obtain

$$\langle\Delta^2(t)\rangle = 2\langle\xi^2(t)\rangle = 2D(1 - e^{-2\gamma t}) \quad (9)$$

$$\langle\delta^2(t)\rangle = \frac{4D}{\gamma}\left(t - \frac{2}{\gamma}(1 - e^{-\gamma t}) + \frac{1}{2\gamma}(1 - e^{-2\gamma t})\right). \quad (10)$$

Here we study the case of $\gamma \ll 1$ ($T_\gamma \gg 1$) and $t = O(1)$ (or $t \ll 1$), thus, the variance mentioned above can be approximated by [8]

$$\langle\Delta^2(t)\rangle = 4\gamma Dt \quad (11)$$

$$\langle\delta^2(t)\rangle = \frac{4\gamma D}{3}t^3. \quad (12)$$

We compare the term in the variation equation $d\delta(t)/dt = DF_x\delta(t) + \Delta(t)$, and we find that there is a γ independent transition time $\tilde{t}$ as follows: the evolution of the error vector is dominated by the OU noise $d\delta(t)/dt \simeq \Delta(t)$ $(0 \le t \ll \tilde{t})$ and by the chaotic dynamics $d\delta(t)/dt \simeq DF_x\delta(t)$ $(t \gg \tilde{t})$. The transition time is $\tilde{t} = \sqrt{3}c$ (c = const.), which is given by $c\sqrt{\langle\delta^2(\tilde{t})\rangle} = \sqrt{\langle\Delta^2(\tilde{t})\rangle}$.

The time taken until a microscopic noise δ grows to be a macroscopic one A is

$$T := \tilde{t} + \frac{1}{\lambda}\ln\left(\frac{A}{\sqrt{4\gamma D/3}\,\tilde{t}^{3/2}}\right). \quad (13)$$

Here, we assume that the maximum Lyapunov exponent λ *does not* depend on the existence of the noise term. If $T_s \gg T$, there are no correlation between states x and y, i.e. $C \simeq 0$, and if $T_s \ll T$, the states x and y are correlated, i.e. $C > 0$. Therefore, $T_s = f(T_\gamma)$ is given by

$$T_s = f(T_\gamma) = \tilde{t} + \frac{1}{\lambda}\ln\left(\frac{A}{\sqrt{4D/3}\,\tilde{t}^{3/2}}\right) + \frac{1}{2\lambda}\ln T_\gamma. \quad (14)$$

When the system is purely deterministic (no noise), the maximum Lyapunov exponent is calculated as $\lambda \sim 2.6$. Using this result, the slope of the function $T_s = f(T_\gamma)$ at $T_\gamma \gg 1$ is $\frac{1}{2\lambda\log_{10}e} \sim 0.45$ from the above argument, which is near the slope in the Figure 2.

References

[1] 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. Photonics* 2, 728 (2008).

[2] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED", *Opt. Lett*. 36, 1020 (2011).

[3] D. P. Rosin, D. Rontani, and D. J. Gauthier, "Ultrafast physical generation of random numbers using hybrid Boolean networks", *Phys. Rev. E* 87, 040902(R) (2013).

[4] M. Hamburg, P. Kocher, and M. E. Marson, "Analysis of Intel's Ivy Bridge digital random number generator", Cryptography Research, Inc., (2012).

[5] R. F. Fox, I. R. Gatland, R. Roy, and G. Vemuri, "Fast, accurate algorithm for numerical simulation of exponentially correlated colored noise", *Phys. Rev. A*, Vol. 38, Number 11 (1988).

[6] T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Estimation of entropy rate in a fast physical random-bit generator using a chaotic semiconductor laser with intrinsic noise", *Phys. Rev. E* 85, 016211 (2012).

[7] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers", *Phys. Rev. A* 83, 031803(R) (2011).

[8] C. Gardiner, Stochastic Methods: A Handbook for the Natural and Social Sciences, Springer; 4th ed. (2009).

[9] D. Ruelle, "A review of linear response theory for general differentiable dynamical systems", Nonlinearity 22 (2009).