Invited Paper

Physical random bit generators and their reliability: focusing on chaotic laser systems

Masanobu Inubushi1a), Kazuyuki Yoshimura1, Kenichi Arai2, and Peter Davis3

1 NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya Atsugi-shi, Kanagawa 243-0198, Japan
2 NTT Communication Science Laboratories, NTT Corporation, 2-4 Hikaridai Seika-cho, “Keihanna Science City” Kyoto 619-0237, Japan
3 Telecognix Corporation, 58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto 606-8314, Japan

a) inubushi.masanobu@lab.ntt.co.jp

Received October 1, 2014; Revised December 5, 2014; Published April 1, 2015

Abstract: Physical random bit generators (RBGs) that generate unpredictable bits at high speed are now of increasing importance in information science and technology, since they are expected to generate unpredictable random bits with high speed. From the viewpoint of applications for security, it is a crucial issue to be able to give a guarantee of the unpredictability of random bits. In this paper, we review research on physical RBGs, particularly focusing our attention on the studies of the unpredictability of random bits generated by laser systems, which are promising entropy sources for physical RBGs. Finally, we report recent research results on noise-robustness, which could be crucial for reliability of physical RBG.

Key Words: physical random bit generator, chaos, semiconductor laser, unpredictability, noisy dynamics

1. Introduction

A bit sequence which does not appear to have any rules is called a random bit sequence. Random bits are used in security technologies such as secret key generation and secure computation, scientific calculations such as Monte Carlo method, and gambling. The properties required of random bits depend on how they are applied. With respect to applications for security technologies, the following properties of random bits are important: (i) statistical homogeneity: passing all statistical tests for randomness, (ii) unpredictability: difficulty of predicting future bits from information of generated bits, and (iii) unreproducibility: completely uncorrelated random bit sequences obtained from completely identical input. Security of information technologies strongly depend on the above properties of the RBG [1]. When discussing RBG, it is important to distinguish whether the RBG is deterministic...
or nondeterministic. A deterministic RBG generates a bit sequence which is uniquely determined by its input, and a nondeterministic RBG generates a bit sequence which is not determined only by its input. By definition, the deterministic RBG does not have the property (iii) unreproducibility. However, with respect to cryptographic applications, both deterministic and nondeterministic RBGs are utilized. For instance, in applications for stream cipher and SSL, random bits generated by ‘cryptographically secure pseudo random number generator’ which is deterministic RBG are used for the encryption/decryption with common secret keys generated by nondeterministic RBG.

Deterministic random bits, or pseudo-random bits, can be generated using algorithms on digital computers. The generation speed of pseudo random bits can be fast, since it is limited by nothing but the speed of the computer processor. However, pseudo random bits can be predictable in principle, since if attackers get the inputs, such as the initial “seed” state, and the algorithm for generating bits, the future bits can be calculated deterministically.

Actually, it is well known that, in 1995, a flaw was discovered in the generating method of pseudo-random numbers in the SSL implementation of Netscape Navigator by I. Goldberg and D. Wagner [2–4]. They reported that the encryption scheme of Netscape used keys of just 40 bits, and thus, it only took 30 hours to recover SSL-encrypted data by using computers at that time. Recently, an inappropriate way of distribution of secret keys was pointed out [5]. Furthermore, it is said that a new random-number standard including an algorithm called Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generation) might contain a backdoor. It has been claimed that “If you know the secret numbers, you can predict the output of the random-number generator after collecting just 32 bytes of its output” [6]. As of September 2013, National Institute of Standards and Technology (NIST) strongly recommends that the Dual_EC_DRBG no longer be used [7].

On the other hand, non-deterministic random bits, or physical random bits, are generated from non-deterministic physical phenomena, such as thermal or quantum noise. Although the generation speed of physical random bits was typically slower than pseudo-random bits, in recent years high speed physical random bit generators have been developed. For example, in 2008 a fast physical bit generator employing chaotic semiconductor laser was proposed by Uchida et al. [8]. In 2012, Intel introduced the micro processor Ivy Bridge equipped with a high-speed physical RBG [10, 11], and NIST has started to standardize requirements for non-deterministic random bit generators [12]. Therefore, physical RBGs are now of increasing importance in physical science and industry, and are expected to become a fundamental component in future information technology.

In §2, we present a general description of a physical RBG and review recent progress on physical RBG. Chaotic semiconductor lasers are one of the promising entropy sources for physical RBG, because of their fast generation speed and randomness with quantum mechanical origin. Thus, we focus our attention on physical RBG by a chaotic laser system, and review studies on its mechanisms and unpredictability in §3. Beyond the verification of unpredictability, a novel concept of noise-robustness is essential for developing a reliable physical RBG. In §4, we describe the importance of the noise-robustness, and introduce a recent study on the noise-robustness with respect to noise correlation of a chaotic laser system. Results of numerical experiments of robustness of chaotic laser system to noise bias are shown in §5. Finally, in §6, we give conclusions and discussions.

2. Physical random bit generators

Here, we describe components of physical RBG. Figure 1 is an illustration of a conceptual model of physical RBG. First, a microscopic noise source, which contains intrinsically unpredictable physical

![Fig. 1. Conceptual model of physical RBGs.](image-url)
phenomena, such as thermal or quantum noise, generates a non-deterministic random signal. Usually, the amplitude of the random signal is too small to convert to digital bits directly. Therefore, some kind of mechanism is required to amplify the amplitude of the microscopic randomness. And then, the amplified analog random signal is digitalized to generate random bits. These components constitute the core of a physical RBG, known as the entropy source. When the output digital bit sequence has a statistical bias, a conditioning component is required to reduce the bias\(^1\).

The randomness of the output of a RBG is often tested using a battery of statistical tests, such as frequency test, serial test, and gap test. NIST Special Publication 800-22 statistical tests [13] and the Diehard tests [14] are often used for cryptographic applications. However, these tests focus only on statistical homogeneity, and cannot be used for testing whether the random bits have been generated by a non-deterministic generator or not.

Nowadays, many microprocessors contain physical RBGs. Intel has produced the micro processor Ivy Bridge equipped with a high-speed physical RBG since 2012 [10, 11]. The microscopic noise source is thermal noise. The amplification mechanism is the so-called metastable bistable circuit, which is a digital circuit consisting of two inverters being connected to each other as shown in Fig. 2(a). When the logical state of Node A is 1(0) and the logical state of Node B is 0(1), the circuit state is consistent as a whole. When the clock input is low, the transistors are on and force Node A and Node B into the same metastable state. When the clock input is high, the transistors are off, the metastable state becomes unstable, and the state of the Node A (Node B) goes to logical 1(0) or 0(1) depending on the thermal noise within the inverters - that is, the circuit amplifies the uncertainty of the microscopic thermal noise to macroscopic logical states. Finally, the logical state of one of the nodes, Node A for instance, is output as a random bit. Repeating this procedure, i.e. turning on/off the transistors repeatedly at discrete time intervals, generates a sequence of bits corresponding to the logical states of the Node.

The dynamics of random bit generation by the bistable circuit can be understood by a schematic illustration (Fig. 2(b)) of a conceptual model of the circuit state and its dynamics when the transistors are turned off. The black dot represents the logical state of the circuit, and here we consider it is governed by a gradient dynamical system with double-well potential as shown in Fig. 2(b). When the transistors are turned off, the circuit can be considered as the state on the top of the potential mountain, and thus unstable, i.e. a small perturbation added to the state grows. The thermal noise within the transistors kicks the state infinitesimally, and the state falls into a valley of the potential. A random bit is generated according to which valley the final state is in, and then, the state is forced to move back on to the top of the potential hill after the transistors are turned on again.

In real implementations, the bit sequence obtained by the circuit (Fig. 2(a)) typically has a statistical bias, i.e. the frequency of the logical state 0 is not equal to that of the logical state 1, and a temporal bias\(^1\). In NIST publications, they refer to these three components (Microscopic Noise Source, Amplification & Digitalization, and Conditioning component) as ‘entropy source’ [12].
correlation. Therefore, a conditioning component is used in the Intel’s physical RBG to reduce the bias and the correlation of the random bits. Also, the output from the conditioning component is used as a seed for a deterministic pseudo-random algorithm to generate the random bits that are provided for applications at high bit rate (3 Gbps).

Phenomena of quantum physics are an excellent source of randomness, since they are fundamentally non-deterministic, compared to those of classical physics such as thermal noise. In principle, an observed value in quantum physics is unpredictable if it is in a superposition state. For instance, it is intrinsically random whether a semi-transparent mirror reflects or transmits a photon being sent from a photon source. A random bit can be generated from observation of the exclusive events, i.e. the reflection or the transmission of the photon, for instance, assigning 0 and 1 to the two events respectively. Quantis developed and now sells a physical RBG based on this quantum phenomenon [15]. However, while the unpredictability of the generated random bits is guaranteed by quantum physics, the generating speed is not high (16 Mbps), limited by the speed of the detection system.

Fast random bit generation based on quantum physics was experimentally accomplished by employing a chaotic semiconductor laser with delayed feedback [8]. The microscopic noise includes quantum noise in the semiconductor laser, and is amplified by the chaotic dynamics of the semiconductor laser with delayed feedback (see the next section for theoretical details). In [8], the output intensity is sampled with a binary detector at discrete time intervals, and the resulting streams of random bits passed standard statistical tests for randomness at generation speeds up to 1.7 Gbps. Recently, a bandwidth enhancement technique for the chaotic semiconductor laser was proposed, and the generating speed of random bits with this technique attains 50 Gbps [16, 17].

3. Physical RBGs using chaotic lasers

In this section, we review studies on unpredictability of random bits generated by chaotic laser systems. Harayama et al. explained that the origin of the non-determinism of bits generated by a physical RBG using a chaotic laser system is the intrinsic quantum noise (the spontaneous emission). The quantum noises introduces uncertainty in the laser state and the chaotic dynamics amplifies the uncertainty to the macroscopic level [18–20]. The chaotic semiconductor laser with delayed feedback is modeled by the chaotic dynamical system defined by the Lang-Kobayashi delay differential equations [21, 22]. In a chaotic dynamical system, an infinitesimal difference between two states exponentially grows. Thus, fluctuation caused by microscopic quantum noise grows and become macroscopic fluctuation which can be detected by a digital bit detector. Figure 3(a) shows a schematic illustration of the state space of the chaotic laser system. Harayama et al. emphasized that, due to the mixing property of the chaotic dynamical system, an asymptotic distribution of the observable converges to an invariant distribution determined by the Lang-Kobayashi equations which does not depend on the distribution of the microscopic fluctuation. Moreover, they showed numerically that the convergence...
is exponentially fast, and such strongly chaotic behavior is robust with respect to the perturbations of laser parameters. Setting a threshold which divides the invariant probability distribution of the observable into two parts that have equal probability and generating a 0(1) output when the observed value is below (above) the threshold, random bits can be obtained by sampling the observable with a time interval which is large enough for convergence of the initial noise distribution to the invariant distribution of the chaotic dynamical system (Fig. 3(b)). Since the uncertainty of the next bit originates from the fluctuation by the quantum noise, the future bit sequence is unpredictable. The combination of the intrinsic randomness of quantum physics and the rapid amplification effect of the microscopic noise by the chaotic laser dynamics with the mixing property enables the fast generation of the unpredictable random bits.

Mikami et al. studied the evolution of bit entropy in physical random bit generation modeled by the Lang-Kobayashi equations with a white Gaussian noise [23]. They investigated how the entropy of bits depends on the amplitude of the noise. They defined the memory time as the time to reach a particular threshold value of entropy close to one, and they showed that the average memory time scales inversely with logarithm of the noise amplitude, which can be used to estimate the average dynamical entropy rate independently of the noise amplitude or the initial laser state. Moreover, they showed that the average entropy rate coincides with the average maximum Lyapunov exponent over a wide range of laser parameters (feedback strength). For reliable physical RBGs, their study on the response of the chaotic laser system to the change in the noise amplitude is important, and is closely related to the concept of the noise-robustness as described in the next section.

4. Noise-robustness of physical RBGs

The next crucial step of verifying reliability of a physical RBG is to study whether the physical RBG has a property of noise-robustness, which was first introduced by Inubushi et al. [24]. In general, any physical RBG uses some kind of microscopic noise source, such as thermal or quantum noise as mentioned before. It is unavoidable that there exist some limitations in control accuracy and knowledge of noise properties. Therefore, the concept of noise-robustness is crucial for physical RBG, since this concept allows us to guarantee reliability of physical RBGs without accurate control and precise knowledge of noise sources.

4.1 Definition of noise-robustness

We describe the formal definition of noise-robustness. The noise-robustness is defined by an inclusion relation of two regions in a noise parameter space, ‘noise-controllable region $C$’ and ‘noise-robust region $R$’, as $C \subset R$. Below, we present formal definitions for noise-controllable region $C$, noise-robust region $R$, and noise-robustness of physical RBGs.

The noise controllable region is defined as follows. Considering some stochastic noise model generating noise signal, we write parameters of the noise model as $p = (p_1, p_2, \ldots, p_m) \in \mathbb{R}^m$, where $m$ is the number of noise parameters characterizing the noise source. Here, we assume that the noise model can be characterized by a finite number of parameters, i.e. $m < \infty$. The subscript $i$ of $p_i$ is just a label of a noise parameter and there is no particular order. In actual implementations, noise parameters of physical RBG cannot be fixed within infinite precision. In other words, we can at best control noise parameters to be in some finite region in noise parameter space. $C(p^\star)$ denotes this finite region around specific target value of noise parameters $p^\star = (p_1^\star, p_2^\star, \ldots, p_m^\star)$ in noise parameter space, and we refer to $C(p^\star)$ as the noise controllable region of $p^\star$.

The noise-robust region is defined as follows. Let $Q(p) = (Q_1(p), Q_2(p), \ldots, Q_n(p))$ denote some quantities evaluating properties of random bits. The subscript $j$ of $Q_j$ is just a label of a property of random bits and there is no particular order. In general, properties of random bits depend on properties of noise source, and thus, we write $Q(p)$ as a function of $p$. Then, we define noise-robust region as $R(p^\star) := \{p \in \mathbb{R}^m | Q_j(p) = Q_j(p^\star) \ (j = 1, 2, \ldots, n)\}$, i.e. properties of random bits do not depend on noise parameters $p$ if $p \in R(p^\star)$. The definition of the noise-robust region described above may be too idealistic. For practical use of this concept, we need to modify the definition of
the noise-robust region as \( R_\Delta(p^*) := \{ p \in \mathbb{R}^m | |Q_j(p) - Q_j(p^*)| < \Delta_j \ (j = 1, 2, \cdots, n) \} \), where \( \Delta_j \) is tolerance in the properties of random bits.

We define that a physical RBG has noise-robustness at \( p^* \) if an inclusion relation \( C(p^*) \subset R(p^*) \) holds. Figure 4 shows schematic examples of a case with noise-robustness (Fig. 4(a)) and a case without noise-robustness (Fig. 4(b)).

Furthermore, introducing \( p^*_i = (p^*_{i1}, p^*_{i2}, \cdots, p^*_{in}) \) to denote the noise parameter vector which is equal to \( p^* \) except for the \( i \)-th component, we define the noise-robust region with respect to the \( i \)-th noise property as \( R_i(p^*) := \{ p_i \in \mathbb{R} | Q_j(p^*_{i}) = Q_j(p^*) \ (j = 1, 2, \cdots, n) \} \), i.e. properties of random bits do not depend on the \( i \)-th noise parameters \( p_i \) if \( p_i \in R_i(p^*) \). We say that physical RBG has noise-robustness with respect to the \( i \)-th noise property if \( C_i(p^*) \subset R_i(p^*) \) [24]. This framework allows us to consider in a general framework various types of robustness with various types of randomness properties and various types of noise properties, as in the following sections.

4.2 Robustness of chaotic laser RBG to noise correlation

As mentioned in the previous section, unpredictability of semiconductor laser chaos in the context of physical RBG has been examined by Harayama et al. specifically with respect to white Gaussian noise added to the electric field parameter [18]. Noise-robustness can be seen in the results for the dependence of auto-correlation on noise variance. In addition, dependency of the unpredictability of the laser chaos RBG on the noise amplitude has been studied by Mikami et al. [23]. Noise-robustness can be seen in the results for dependence of bit entropy on the amplitude of white Gaussian noise added to the laser light intensity.

Recently, the noise-robustness of correlations between successive bits with respect to the temporal correlation of noise in the chaotic laser system was studied by Imbusch et al. [24]. They employed the Lang-Kobayashi equations with a correlated noise source of correlation time \( T_\gamma \) which includes white Gaussian noise as a limit \( T_\gamma \to 0 \). They found numerically that there exists a characteristic timescale \( \bar{T} \) of the noise correlation time such that the sampling time \( T_s \) required for small correlations between successive bits is constant for \( T_\gamma \ll \bar{T} \) and \( T_s \propto \log T_\gamma \) for \( T_\gamma \gg \bar{T} \). This result shows that there exists a value of the noise correlation time \( \bar{T} \) below which the correlation of the noise does not affect the unpredictability in the chaotic laser system. Therefore, if the noise correlation time is kept under the limit \( (T_\gamma \ll \bar{T}) \), the noise-robustness of the physical RBG is guaranteed. In other words, using the formulation of noise-robustness described above, they identified the region of noise-robustness with respect to the noise correlation time as \( R_{corr.} = \{ 0 \leq T_\gamma < \bar{T} \} \), since the unpredictability does not change if \( T_\gamma \in R_{corr.} \). If the noise correlation time exceeds the limit \( (T_\gamma \gg \bar{T}) \), the required sampling time \( T_s \) needs to be made longer depending on the noise correlation time \( T_\gamma \). However, the required sampling time \( T_s \) depends on the noise correlation time \( T_\gamma \) logarithmically \( (T_s \propto \log T_\gamma) \), which means the dependency is ‘weak’ compared with linear dependence.
For theoretical interpretation of the numerical experiment, they proposed a simple model of tangent space dynamics, and they obtained the theoretical curve of $T_s = f_{th}(T_\gamma)$, by employing this model. This theoretical curve agrees well with the numerical results, i.e. their theory explains numerically obtained functional dependency $T_s = f(T_\gamma) = \text{const}$. ($T_\gamma < \tilde{T}$) and $T_s = f(T_\gamma) \propto \log T_\gamma$ ($T_\gamma \gg \tilde{T}$). Furthermore, they obtained a theoretical limit of the noise-robustness as $\tilde{T} = 1/\lambda$, where $\lambda$ is the maximum Lyapunov exponent of the noiseless (deterministic) chaotic laser system. When constructing the simple model, they did not use any details of the laser system, but they only assumed existence of an unstable direction along the solution orbit. Therefore, it is expected that the properties obtained by the simple model are general properties for a variety of chaotic systems with correlated noise, and useful for realizing reliable non-deterministic RBGs using chaotic physical devices.

The correlation time of the intrinsic laser noise of spontaneous emission (SE) is usually much less than the photon life time $\tau_p$ [22]. Thus, the noise controllable region with respect to the SE noise correlation is $C_{\text{corr.}} = \{0 \leq T_\gamma < \tau_p\}$. In their calculation, the boundary of the noise-robust region is $\tilde{T} = 1/\lambda = 0.38[\text{ns}]$, and it is much larger than the photon life time, i.e. $\tau_p \ll \tilde{T}$ since $\tau_p = 1.927[\text{ps}]$. Therefore, the results of [24] shows that $C_{\text{corr.}} \subset R_{\text{corr.}}$, i.e. the chaotic laser RBGs has noise-robustness with respect to the SE noise correlation.

5. Robustness of chaotic laser RBG to noise bias

Here, we study the noise-robustness with respect to the bias of noise distribution in the chaotic laser system, by employing the Lang-Kobayashi equations. And also, we compare results of the chaotic laser system with that of a bistable system.

5.1 Model and Numerical method

The chaotic dynamics of a single mode semiconductor laser with delayed feedback can be modeled with the Lang-Kobayashi model equation:

$$
\frac{dE(t)}{dt} = \frac{1}{2} \left[ -\frac{1}{\tau_p} + F\left(E(t),N(t)\right) \right] E(t) + \kappa E(t-\tau_D) \cos \theta(t) + \xi_E(t),
$$

$$
\frac{d\phi(t)}{dt} = \frac{\alpha}{2} \left[ -\frac{1}{\tau_p} + F\left(E(t),N(t)\right) \right] - \kappa \frac{E(t-\tau_D)}{E(t)} \sin \theta(t) + \xi_\phi(t),
$$

$$
\frac{dN(t)}{dt} = -\frac{N(t)}{\tau_s} - F\left(E(t),N(t)\right) E(t)^2 + J,
$$

(1)

where $E(t) \in \mathbb{R}$ is the amplitude of the complex electric field, $\phi(t) \in \mathbb{R}$ is the phase of the complex electric field, $N(t) \in \mathbb{R}$ is the carrier density, $\theta(t) := \omega \tau + \phi(t) - \phi(t - \tau)$, and $F\left(E(t),N(t)\right) := G_N N(t) - N_0 \right) \in \mathbb{R}$. The parameters in the equations and their values used in the numerical experiments are shown in Table I. The period of the relaxation oscillation is $T_{\text{relax}} = 2\pi/\omega_{\text{relax}} = 0.35[\text{ns}]$ and $J/J_{\text{th}} = 1.44$. The variables $\xi_E(t)$ and $\xi_\phi(t)$ are the amplitude and phase components in a model of the optical noise in the lasing mode. Usually this is considered to be spontaneous emission with white Gaussian characteristics. However, in practical systems it may be difficult to ensure that the distribution does not change. Thus RBGs should be required to be robust with respect to changes in the noise distribution. Here, we study the robustness of RBGs 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 particular example of a biased noise process, i.e.

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

$$
\langle \xi_E(t) \xi_E(s) \rangle = \langle \xi_\phi(t) \xi_\phi(s) \rangle = D \delta(t-s), \quad (3)
$$

where $\xi'(t) = \xi(t) - \langle \xi(t) \rangle$. $D$ is the noise strength, $\epsilon$ denotes the strength of the bias (Fig. 5(a)). We consider $\epsilon$ as a noise parameter $p$ described in the formulation of noise-robustness, and the target
Table I. The parameters in the Lang-Kobayashi equation and their values used in the numerical experiments [23].

| Symbols | Parameters | Values |
|---------|------------|--------|
| $\tau_D$ | External-cavity round-trip time | 0.25ns |
| $\tau_p$ | Photon lifetime | 1.927ps |
| $\tau_s$ | Carrier lifetime | 2.04 ns |
| $\alpha$ | Linewidth enhancement factor | 5.0 |
| $G_N$ | Gain coefficient | $8 \times 10^{-13} m^3 s^{-1}$ |
| $N_0$ | Carrier density at transparency | $1.400 \times 10^{24} m^{-3}$ |
| $\epsilon$ | Gain saturation coefficient | $2.5 \times 10^{-23}$ |
| $\kappa$ | Feedback strength | 6.25 ns$^{-1}$ |
| $J$ | Injection current | $1.42 \times 10^{13} m^{-3}s^{-1}$ |
| $\omega$ | Optical angular frequency | $1.225 \times 10^{15} s^{-1}$ |

Fig. 5. (a) Schematic illustration of the bias of the noise distribution. The blue dot line represents the noise distribution without the bias, and the red solid line represents the $\epsilon$-biased noise distribution. (b) The invariant distribution of the observable of the chaotic laser system. The horizontal dot line represents the threshold as in Fig. 3(b). The blue dot line represents $P(I,0)$, and the red solid line represents $P(I,\epsilon)$.

value of noise parameter is $p^* = \epsilon^* = 0$ (unbiased noise). Numerical solutions of the Lang-Kobayashi equation are calculated by using 4th order Runge-Kutta method with time step $\Delta t = 10^{-3}$. Note that numerical error due to finite bit representation and numerical integration scheme is very small compared to the noise amplitude considered here.

As the randomness property $Q$, we consider the noise-robust region with respect to the noise bias, and we calculate measure $p(\epsilon)$ defined by

$$p(\epsilon) = \int_{I_t}^{\infty} P(I,\epsilon) dI,$$

where $I$ is absolute value of amplitude of the electric field $E$ (i.e. $I = |E|$) and $P(I,\epsilon)$ is the density function when the chaotic laser is affected by the $\epsilon$-biased noise sequence (Fig. 5(b)). $I_t$ is a threshold to generate a bit from an analog sample of signal $I(t)$. The value of $I_t$ is chosen so that when $\epsilon = 0$: $p(0) = 1/2 = \int_{I_t}^{\infty} P(I,0) dI = \int_{0}^{I_t} P(I,0) dI$.

5.2 Numerical experiments

In this sub-section, we present numerical results for the model system. In practice, $p(\epsilon)$ is obtained by counting events $I(t) > I_t$ at each Runge-Kutta step for sufficiently long time ($T = 2.5 \times 10^4 [ns]$) to ensure the convergence in Fig. 6.

Figure 6 shows the numerically calculated bias of $p(\epsilon)$: the red, green, blue, and purple line is the case of $D = 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}$ respectively. The noise level observed in experiments is estimated to be $O(10^{-5}) \sim O(10^{-4})$ [8]. The error bar is the standard deviation of the ensemble average, for ten different initial conditions. The horizontal axis is $\epsilon$. Except for the large noise case ($D = 10^{-3}$), the bias $|p(\epsilon) - 1/2|$ is less than 0.01 for $\epsilon < 1$, i.e. the error due to the bias is less than 1%.

As a comparison, here we consider the bias $|p(\epsilon) - 1/2|$ in the bistable RBG case (Fig. 2(b)). We here assume that the noise distribution is the Gaussian distribution, and also that the bistable mechanism
amplifies the microscopic noise to the macroscopic level directly, i.e. there is no mixing process such as in a chaotic dynamical system. Therefore, the noise amplitude is amplified with the initial bias. Under this assumption, the measure $p(\epsilon)$ of the bistable RBG is given by the integration of the biased Gaussian distribution, which is the complementary error function: $p(\epsilon) = 1/2 \text{erfc}(\epsilon)$, as shown in Fig. 6 (the blue broken line).

Focusing our attention on the small noise parameter region of $0 \leq \epsilon \leq \tilde{\epsilon}$ ($\tilde{\epsilon} \simeq 0.2$), $p(\epsilon)$ is almost constant for all noise strength $D$, i.e. $p(0) = p(\epsilon)$ for $0 \leq \epsilon \leq \tilde{\epsilon}$. By using the formulation of noise-robustness, we can say that the noise-robust region with respect to the noise bias is $R_{\text{bias}} = \{0 \leq \epsilon \leq \tilde{\epsilon}\}$ in the case of the chaotic laser RBGs. For example, we can say that if the tolerance of deviation is 0.01, and the control of noise keeps the noise bias less than 0.2, then the chaotic laser RBG is noise-robust with respect to noise bias. On the other hand, in the case of the bistable RBGs, $p(\epsilon)$ changes sensitively with the change of the noise bias parameter $\epsilon$, since $dp(0)/d\epsilon = 1/\sqrt{2\pi}$. If the bias tolerance is 0.01, and the noise bias controllability is 0.2, then the chaotic RBG is noise-robust but the bistable system is not.

6. Conclusions and discussions

In this paper, we reviewed recent progress on physical RBG, including the so-called bistable RBGs (Intel’s RBG) and RBG based on quantum physics (Quantis’s RBG). Next, we reviewed studies on physical RBG by chaotic semiconductor lasers as a promising entropy source. These studies show that the combination of the intrinsic uncertainty in microscopic noise due to quantum mechanics and the rapid amplification of microscopic uncertainty by the chaotic laser dynamics with the mixing property enables the fast generation of unpredictable random bits. Then, going beyond the verification of unpredictability, we introduce a novel concept of noise-robustness which is essential for realizing a reliable physical RBG, and describe a study on noise-robustness of chaotic laser system in the case of the noise correlation. Numerical results confirmed that the entropy source of the chaotic laser RBG is superior to that of a bistable RBG due to the property of mixing, which reduces the dependence of the distribution of observables on the bias of the noise distribution.

In the dynamical system theory, the quantity $dp(0)/d\epsilon$ is formulated in the linear response theory for general dynamical systems developed by Ruelle [25] under several assumptions. They considered the vector field $X + aX$ on a state space $M$ which defines a flow $(f_\alpha^t)$ with a hyperbolic attractor $K_\alpha$ depending continuously on $\alpha$, and they obtained a general formula:

$$\frac{d}{d\alpha}\rho_\alpha(A)|_{\alpha=0} = \int_0^\infty dt \int \rho_0(dx)X(x) \cdot \nabla_x(A \circ f_\alpha^t),$$

where $\rho_\alpha$ is the so-called SRB measure with the parameter $\alpha$, $A : M \to \mathbb{R}$ is an observable, and
\[ \rho_0(A) = \int \rho_0(dx) A(x) \]. In our context, \( A = H(I(x) - I_t) \) where \( H(\cdot) \) is the Heaviside step function and \( I(x) \) is the amplitude of electric field at state \( x \in M \) (we here neglect the noise effect but some constant perturbation \( aX \) as a bias). 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, the Ruelle approach is expected to be useful for studying the robustness of a RBG by a chaotic attractor in a general framework.

In applications for security technology, it is difficult to guarantee security only by using pseudo-random bits. It’s not too much to say that the physical random bits are now essential in applications, and the physical RBGs are expected to be mounted on many information devices in the future. However, it is not true that physical random bits are always reliable. If a conditional component contains inappropriate processes during the generation of ‘random’ bits from nondeterministic physical processes, the generated ‘physical random bits’ might be predictable. For instance, it was recently reported that it would be possible to insert Trojans in a stealthy manner into Intel’s physical RBG used in the Ivy Bridge processors, and Trojans could reduce the entropy rate of the generated bits to make an estimation easier [26]. Nevertheless, the Trojan passes both of the functional tests recommended by Intel for its physical RBG and the NIST random number tests.

Therefore, it is a crucial issue how to guarantee the quality and the reliability of bits generated by a physical RBG. Clearly, it is not enough to just check whether the generated bit sequences pass the standard statistical tests. With a growing awareness of this issue, NIST has recently proposed guidelines for the design and operation of non-deterministic RBG, including the requirement to make open a description of the physical origin of unpredictability. While this step is significant, the NIST requirements for the description of the physical origin of unpredictability are not concrete. Moreover, there does not seem to be a consensus about general criteria for the quality and reliability of physical RBG that could be used by NIST in the future. The studies reported in this review are aimed at clarifying the properties of unpredictability in physical RNG. We expect that such studies can contribute to the development of more rigorous methods and criteria for evaluating and optimizing the reliability of physical RBGs in the future.

Acknowledgments
The authors would like to thank the members of the NTT Communication Science Laboratories for their continuous encouragement and support.

References
[1] B. Schneier, Applied cryptography, Wiley, 1996.
[2] Software security flaw puts shoppers on internet at risk, New York Times, September 19, 1995.
[3] I. Goldberg, “Netscape SSL implementation cracked!,” cypherpunks list massage, 1995.
[4] I. Goldberg and D. Wagner, “Randomness and the netscape browser,” Dr. Dobb’s Journal, http://www.cs.berkeley.edu/~daw/papers/dlj-netscape.html, 1996.
[5] A.K. Lenstra, J.P. Hughes, M. Augier, J.W. Bos, T. Kleinjung, and C. Wachter, “Ron was wrong, Whit is right,” IACR Cryptology ePrint Archive, vol. 2012, p. 64, 2012.
[6] B. Schneier, “Did NSA put a secret backdoor in new encryption standard?,” https://www.schneier.com/essay-198.html, 2007.
[7] “Supplemental ITL bulletin for september 2013,” http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf, 2013.
[8] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” Nature Photonics, vol. 2, no. 12, pp. 728–732, 2008.
[9] T.E. Murphy and R. Roy, “Chaotic lasers: The world’s fastest dice,” Nature Photonics, vol. 2, no. 12, pp. 714–715, 2008.
[10] G. Taylor and G. Cox, “Digital randomness,” *Spectrum*, IEEE, vol. 48, no. 9, pp. 32–35, 56, 58, 2011.

[11] M. Hamburg, P. Kocher, and M.E. Marson, “Analysis of Intel’s Ivy Bridge digital random number generator,” *Cryptography Research, Inc.*, 2012.

[12] “Draft NIST special publication 800-90,” http://csrc.nist.gov/publications/PubsDrafts

[13] “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

[14] “The marsaglia random number cdrom including the diehard battery of tests of randomness,” http://www.stat.fsu.edu/pub/diehard/

[15] Quantis, http://www.idquantique.com/random-number-generators/products.html

[16] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, “Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers,” *Optics Express*, vol. 18, no. 6, pp. 5512–5524, 2010.

[17] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, “Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8 × 50 gb/s,” *Photonics Technology Letters*, IEEE, vol. 24, no. 12, pp. 1042–1044, 2012.

[18] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, “Fast nondeterministic random-bit generation using on-chip chaos lasers,” *Physical Review A*, vol. 83, no. 3, 031803, 2011.

[19] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K. Arai, A. Uchida, and P. Davis, “Theory of fast nondeterministic physical random-bit generation with chaotic lasers,” *Physical review E*, vol. 85, 046215, 2012.

[20] 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, 047513, 2012.

[21] R. Lang and K. Kobayashi, “External optical feedback effects on semiconductor injection laser properties,” *IEEE Journal of Quantum Electronics*, vol. 16, no. 3, pp. 347–355, 1980.

[22] J. Ohtsubo, *Semiconductor Lasers: Stability, Instability And Chaos (Third edition)*, Springer-Verlag New York Inc, 2012.

[23] 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,” *Physical Review E*, vol. 85, 016211, 2012.

[24] M. Imbishi, K. Yoshimura, and P. Davis, “Noise-robustness of unpredictability in a chaotic laser system: Toward reliable physical random bit generation,” (submitted to *Physical Review E*).

[25] D. Ruelle, “A review of linear response theory for general differentiable dynamical systems,” *Nonlinearity*, vol. 22, 2009.

[26] G.T. Becker, F. Regazzoni, C. Paar, and W.P. Burleson, “Stealthy dopant-level hardware trojans,” *Cryptographic Hardware and Embedded Systems CHES 2013*, pp. 197–214, Springer, 2013.