Theory of fast nondeterministic physical random-bit generation with chaotic lasers

Takahisa Harayama,[1] Satoshi Sunada,[1] Kazuyuki Yoshimura,[1] Jun Muramatsu,[1] Ken-ichi Arai,[1]
Atsushi Uchida,[2] and Peter Davis[1]
[1]*NTT Communication Laboratories, NTT Corporation, 2-4 Hikaridai Seika-cho, Soraku-gun, Kyoto, 619-0237, Japan*
[2]*Department of Information Science, Saitama University, 255 Shimo-okubo, Sakura-ku, Saitama city, Saitama, 338-8570, Japan*
(Received 16 September 2011; published 23 April 2012)

We theoretically show that completely stochastic fast physical random bit generation at a rate of more than one gigabit per second can be realized by using lasers with optical delayed feedback which creates high-dimensional chaos of laser light outputs. The theory is based on the mixing property of chaos, which transduces microscopic quantum noise of spontaneous emission in lasers into random transitions between discrete macroscopic states.

DOI: 10.1103/PhysRevE.85.046215 PACS number(s): 05.45.Gg, 42.65.Sf

I. INTRODUCTION

Random numbers are very important for many applications, including cryptography [1], numerical computation [2], and stochastic modeling [3]. Various methods are used to generate random numbers depending on the properties required by the applications. Applications such as quantum cryptography require true random number generators [4]. On the other hand, many applications in computing and communications use pseudorandom numbers, which mimic some statistical property of randomness, but can be generated with deterministic algorithms [5]. Applications that require true randomness extract random numbers from random physical processes. Common physical random number generators utilize randomness of noises or turbulence [6–13]. A fundamental source of randomness for physical random number generation is detection of quantum mechanical phenomena [14,15], which is unpredictable in principle. A practical problem of physical random number generators is that it is difficult to extract bits with good randomness properties at high bit rates.

Recently it has been demonstrated that bit sequences that pass strict statistical tests of randomness can be robustly generated at more than one gigabit per second (Gbps) by sampling the output of chaotic semiconductor lasers [16–20]. It has been also experimentally demonstrated that it is possible to achieve the fast generation of random bit sequences passing statistical tests of randomness even with compact on-chip chaos lasers [21,22] in contrast to previous laser systems with many discrete optical components. However, it is still unclear whether such random bit generation methods are really nondeterministic. As yet there have been no detailed theoretical or numerical investigations of this aspect. The purpose of this paper is to provide a theoretical description of the role of chaos in random bit generation and a numerical verification of fast nondeterministic random bit generation for chaotic laser systems based on the theory.

A chaotic laser can be modeled by using deterministic equations of motion for a set of macroscopic observables coupled with small amplitude perturbations caused by intrinsic noise such as thermal and quantum mechanical fluctuations. The properties of randomness required by true random number generators depend essentially on the effect of perturbations on the evolution of macroscopic observables. It is important to analyze this effect to understand the randomness of the bits extracted from the macroscopic observables.

In this paper, by considering the mixing property of chaos, it is theoretically shown that nondeterministic random bit sequences can be generated at a gigabit per second rate by using chaotic lasers with optical delayed feedback. It is shown that nondeterminism is guaranteed by the presence of spontaneous emission noise, which is quantum mechanical in origin. The relation between the randomness of the bit sequences and the rate of random bit extraction can be understood in terms of the convergence toward the natural invariant density due to the dynamical mixing process.

II. MICROSCOPIC NOISE AND MACROSCOPIC PROBABILITY

Let us consider a physical device whose input and output are respectively microscopic noises and discrete macroscopic random state sequences as shown in Fig. 1.

We assume that the microscopic noises have an infinite bandwidth and the physical device has a finite dynamical response. Even if the microscopic noise can be assumed to be truly random, the randomness of the sequence depends on the dynamical properties of the physical device and the method of extracting discrete sequences.

There are various methods for realizing physical random number generators by amplifying the microscopic noises and assigning discrete symbols to ranges (i.e., partitions) of the values of the macroscopic observables.

For example, thermal noise can be amplified with an amplifier to produce a large amplitude noise signal that is input into a bistable system, causing transitions between two stable states corresponding to macroscopic observables. The first amplifier stage may not be necessary if the bistable system is repeatedly reset precisely to an unstable point separating the basins of the two stable states.

In practice a common method is to use electrical amplifiers to amplify intrinsic electronic noise which is input into a threshold device such as a D-type flip flop (D-FF), driven by a periodic clock signal to produce a stream of random binary states [7,8,23].

The finite bandwidth of amplifiers and threshold devices, and the finite accuracy of the threshold level with respect to the distribution of the fluctuations make it difficult in practice to achieve random bit sequences at high bit rates.

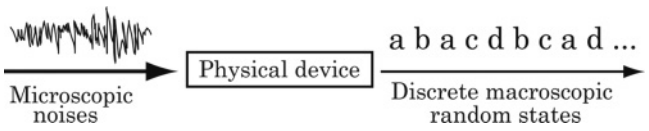

FIG. 1. Schematic illustration of a physical device producing sequences of discrete macroscopic states a, b, c, and d appearing randomly. Microscopic noises act as entropy sources.

On the other hand, it is known that chaotic devices are able to generate large amplitude signals that depend sensitively on microscopic noise, and so chaotic devices are of interest from the viewpoint of overcoming the practical problems of generating random sequences at high rates. In this paper we consider this issue from the viewpoint of basic dynamical theory, and its application to large bandwidth chaotic lasers.

Let us start with a brief review of fundamental properties of dynamical mixing [24] in a chaotic dynamical system with noise, which can be used to describe physical randomness.

Suppose that the time evolution of a system state $x(t)$ is defined by a differential equation $dx/dt = F(x) + n(x,t)$, where n represents random perturbations caused by other degrees of freedom, which we call "noise." First let us focus on the deterministic part of the evolution of a system obtained in the limit of zero noise amplitude. Suppose that the deterministic part of the time evolution of a system (i.e., without the noise term) on a manifold M is described as $x(t) = f^t x(0)$, and this flow is chaotic. If the flow is chaotic, then the flow has the mixing property. The mixing property means that statistical correlations between observables seen at different times decrease as the length of time between the observations increases. The mixing property also implies that the flow is ergodic. These mean that any arbitrary smooth initial state probability density distribution converges to a unique density distribution, known as the natural invariant density $\rho(x)$. Let us describe each of these.

First we introduce the correlation function

$$C_{AB}(\tau) = \langle A[f^{t+\tau}x(0)]B[f^t x(0)]\rangle_t - \langle A\rangle_t\langle B\rangle_t, \qquad (1)$$

where observables A and B are differentiable functions on M, and it is assumed that the time averages $\langle X\rangle_t \equiv \lim_{T\to\infty} 1/T \int_0^T X dt$ converge. The mixing property means that the correlation between observables seen at different times decreases as the length of time between the observations increases, which is expressed as follows,

$$C_{AB}(\tau) = \langle A(f^\tau x)B(x)\rangle - \langle A\rangle\langle B\rangle \xrightarrow[|\tau|\to\infty]{} 0 \qquad (2)$$

for arbitrary square integrable functions A and B.

The mixing property also implies ergodicity, namely that the time average $\langle X\rangle_t$ is equal to the ensemble average $\langle X\rangle \equiv \int \rho(dx)X$, where ρ is the invariant density.

In Eq. (2), choosing $B(x) = \rho_0(x)/\rho(x)$, where $\rho_0(x)$ represents the initial density yields

$$\int_M A(f^\tau x)\rho_0(x)dx - \langle A\rangle \xrightarrow[|\tau|\to\infty]{} 0. \qquad (3)$$

Since $A(x)$ is an arbitrary function, the following equation is satisfied:

$$\lim_{t\to\infty} L^t\rho_0(x) = \rho(x) \text{ almost surely}, \qquad (4)$$

where the initial density $\rho_0(x)$ is an arbitrary smooth function, and L^t is the Frobenius-Perron operator defined by using the Dirac δ function as $L^t\rho_0(x) \equiv \int_M \delta(x - f^t y)\rho_0(y)dy$. The mixing property means that any arbitrary smooth initial density function converges to the natural invariant density.

The distribution function of an observable Y also converges to a unique invariant distribution function $D(Y)$,

$$D(Y) = \int_M \delta[Y - \tilde{Y}(x)]\rho(x)dx. \qquad (5)$$

By using $D(Y)$, we can define a discrete number N of macroscopic states such that the probabilities of the macroscopic states X_i are all equal, that is, $1/N$. Specifically, we define $(N-1)$ thresholds S_i of the observable Y such that

$$\int_{S_0}^{S_1} D(Y)dY = \int_{S_1}^{S_2} D(Y)dY = \cdots = \int_{S_{N-1}}^{S_N} D(Y)dY. \qquad (6)$$

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

$$H(\mathbf{X}) \equiv -K\sum_{i=1}^{N} p(X_i)\log p(X_i), \qquad (7)$$

where $\mathbf{X} = \{X_i, i = 1,2,\ldots,N\}$ and $K = 1/\log N$ [25]. With the macroscopic states defined using the thresholds in Eq. (6), the Shannon entropy has a maximum value of unity.

The convergence toward the invariant density due to the mixing property is a very important feature of the transduction of microscopic noise to macroscopic randomness by chaotic dynamics. No matter how accurately we observe the state of the system, the effect of microscopic noise after the observation means that the state should be modeled by an ensemble. If the ensemble due to microscopic noise has a smooth probability distribution, then from Eq. (4) one can easily see that the time evolution of such an ensemble is ruled by the Frobenius-Perron operator and always converges to the natural invariant density in the long time limit if the system has the mixing property. Moreover, if discrete macroscopic states are defined appropriately, the probability of asymptotically being in any of the macroscopic states is equal, and the Shannon entropy is unity.

Now let us describe a method of generating random sequences. Assuming that microscopic noise is random, corresponding to a smooth probability distribution, and the time between observations of the state is sufficiently long, then the correlation (mutual information) between successive states (symbols) will be zero, so the sequence will be truly random.

Strictly zero correlation is obtained only in the limit of infinite time between observations. In practice, it is important to quantitatively estimate the time T_ϵ when the entropy becomes $1-\epsilon$ where ϵ is a small finite value.

Figure 2 shows a schematic illustration of the typical time dependence of the entropy of discrete macroscopic states. The time T_ϵ will depend on the initial distribution and on the rate of mixing by the flow. In order to achieve a fast rate of generation

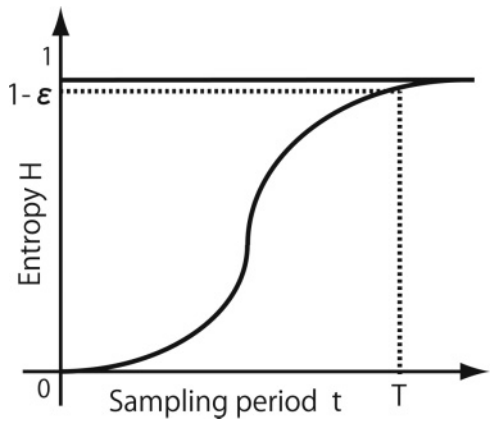

FIG. 2. Schematic illustration of the growth of entropy during the convergence of an initial microscopic noise distribution to the natural invariant density, due to the mixing property Eq. (4).

of random state sequences, physical devices should have a strongly chaotic property. Then the correlation function decays exponentially fast and the time T_ϵ can be made short.

(Note: Polygonal billiards are examples of dynamical systems that have the mixing property, but they are not hyperbolic and thus not strongly chaotic. Their Lyapunov exponents are zero and the correlation function decays slowly in an algebraic manner [26,27].)

The time evolution of the density function is ruled by the resonances of the Frobenius-Perron operator. Let us give an example to illustrate this. The spectral decomposition of the Frobenius-Perron operator of the r-adic map $x_{t+1} = rx_t(\mathrm{mod}\ 1)$, where r is an integer larger than 1, yields the expansion of the time evolving density function by the Bernoulli polynomials $B_m(x)$,

$$L^t\rho_0(x) = \rho(x) + \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m!r^{mt}} c_m B_m(x), \tag{8}$$

where $\rho(x) = 1$, m is the mode index, and the coefficients c_m are given as follows [28]:

$$c_m = \int_0^1 [\delta^{(m-1)}(x-1) - \delta^{(m-1)}(x)]\rho_0(x)dx. \tag{9}$$

Therefore, the difference between the time evolving density function and the natural invariant density decreases at least as fast as the slowest decay mode, $1/r^t$. For example, it is less than 10^{-5} when $r = 2$ and $t = 17$. This means that the frequencies of bits 0 or 1, which can be obtained by the integrals of the density function over the intervals (0,0.5) and (0.5,1), respectively, is approximately $(50 \pm 10^{-3})\%$ at the 17th iteration.

It is important to note that the density can approach the natural invariant density much faster than estimated from the slowest decay mode if the decay mode is only a small part of the initial density. For example, let us suppose that the initial distribution is distributed normally with average $\mu = 10^{-2}$ and variance $\sigma^2 = 10^{-6}$ for the r-adic map with $r = 2$. A numerical evaluation of the time evolution of the entropy is shown in Fig. 3. Notice that the numerically calculated entropy approaches 1 much faster than the slowest decay mode.

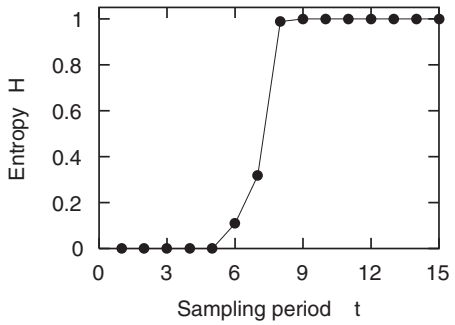

FIG. 3. Numerical calculation of the time dependence of the entropy of the bit obtained by using the r-adic map with $r = 2$. The entropy actually approaches 1 much faster than the theoretical prediction.

In this solvable example of a prototype chaotic system we considered the effect of microscopic noise only in terms of an ensemble of initial states. In physical systems the action of the noise is continuous in time. When the noise is sufficiently small and additive, and the system is strongly chaotic, it is expected that the natural invariant density and the rate of the convergence from the initial density to the natural invariant density will not be drastically affected by the addition of microscopic noise during the time evolution. This is confirmed by the numerical result in Fig. 3 for the map with microscopic noise added at each iteration. The numerical simulations show that a lower bound of the convergence rate can be estimated from just the deterministic part of the equation.

We emphasize that the property that the asymptotic invariant probability density and the rate of convergence to the invariant density do not depend on details of the microscopic noise is an important feature for ensuring the robustness of the randomness in chaotic random number generators.

Finally, we comment that in practice, it is difficult to precisely set the thresholds in Eq. (6). Moreover, the speed of the detector response may limit the generation rate. Such detector system issues are not dealt with in this paper.

III. CHAOS LASERS WITH DELAYED OPTICAL FEEDBACK

In this section we study the dynamics of mixing in chaotic lasers with delayed optical feedback and spontaneous emission noise. In the following section, we will apply the results of this section and the previous section to random bit generation using chaotic lasers.

In a single-mode semiconductor laser with delayed optical feedback, the dynamics of the macroscopic variables of light field amplitude E and the carrier density N is described by the Lang-Kobayashi equations [29] as

$$\frac{dE}{dt} = \frac{1+i\alpha}{2}\left(G - \frac{1}{\tau_p}\right)E + \frac{\kappa}{\tau_{in}}E(t-\tau_D)e^{-i\theta} + \sqrt{\frac{C_s N}{\tau_s}}\xi \tag{10}$$

and

$$\frac{dN}{dt} = J - \frac{1}{\tau_s}N - G|E|^2, \tag{11}$$

where the gain G depends on E and N,

$$G \equiv \frac{G_0(N - N_0)}{1 + \epsilon |E|^2}. \tag{12}$$

ξ is white Gaussian noise with zero mean and unitary variance so that the last term of the right-hand side of Eq. (10) represents the effect of the quantum noise of a spontaneous emission. The value of the parameters are fixed by taking account of the phase diagrams in Fig. 8: The linewidth enhancement factor is $\alpha = 5$, the differential gain $G_0 = 10^{-12}$ m^3 s^{-1}, the gain saturation coefficient $\epsilon = 8.16 \times 10^{-24}$ m^3, the propagation time in the DFB laser $\tau_{\text{in}} = 14$ ps, the delay time $\tau_D = 0.182$ ns, the delay phase shift $\theta = 0$ rad, the carrier lifetime $\tau_s = 2.04$ ns, the feedback strength $\kappa = 0.32$, and the transparent carrier density $N_0 = 1.4 \times 10^{24}$ m^{-3}. The spontaneous emission factor is set at $C_s = 10^{-3}$ by taking account of the properties of the the optical integrated circuits used for physical random number generation with laser chaos [21].

The Lang-Kobayashi (LK) model has been studied extensively, and has been used to explain chaotic phenomena observed in laser experiments. The phase space of the LK model is infinite dimensional because of the delayed feedback. In general, it is difficult to theoretically analyze high-dimensional chaos, and the dynamical properties of the LK model have not been fully elucidated although it has been studied for 30 years. Most works on the LK model have focused on cases of long delay time, typically several tens of nanoseconds, since most laser experiments have used discrete optical components such as optical fibers in order to put the light back into the laser and easily control the delay. However, when the delay time is long there are significant recurrences in autocorrelations at multiples of the delay times. For this reason, lasers with shorter delay times are expected to be more suitable for fast physical random bit generation.

Lasers with shorter delay times require higher feedback strength to achieve strong chaos [30]. Recently chaotic laser chips have been fabricated using optical circuit integration technologies, which enable strong delayed optical feedback [21,22]. Therefore, our study focuses on lasers with short delay times corresponding to chaotic laser chips.

First we show a typical example of the evolution of a smooth initial probability density of the light intensity $I(t)$ and the carrier density $N(t)$ for a laser exhibiting chaotic oscillations. An example of the time evolution of the probability density in the most strongly chaotic regime is shown in Fig. 4. Irrespective of the initial probability density of $I(t)$ and $N(t)$, the distribution converges to a unique distribution, which is a natural invariant density for the specified parameters.

In this example, an ensemble of trajectories is calculated for one initial state of I and $N10^5$ different trajectories representing perturbations due to the spontaneous emission noise. The ensemble distribution is stretched and folded in the phase space by the chaotic dynamics as shown in Figs. 4(b)–4(g), and finally converges to an invariant distribution as shown in Fig. 4(h). The invariant probability density $\rho(I)$ of the light intensity is compared with the transient distribution after 1.25 ns time evolution in Fig. 5. Here the invariant probability density is obtained by long time evolution of a typical orbit. The difference between the time-evolving density and the

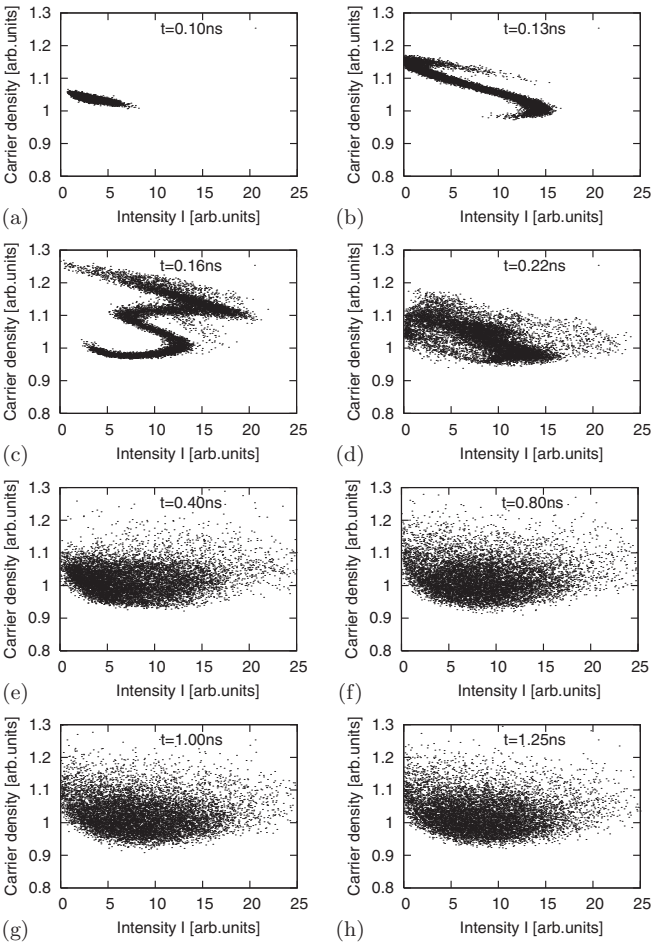

FIG. 4. The time evolution of the probability density distribution of the light intensity and the carrier density at times (a) 0.1 ns, (b) 0.13 ns, (c) 0.16 ns, (d) 0.22 ns, (e) 0.40 ns, (f) 0.86 ns, (g) 1.00 ns, and (h) 1.25 ns.

invariant probability density decays exponentially due to the strongly chaotic dynamics, as shown in Fig. 6.

The transient probability density is difficult to obtain experimentally because of the need to reset the laser to the same initial state many times, or to wait a long time until the laser revisits the neighborhood of the same initial state many times. Observation of the autocorrelation is a more practical way to

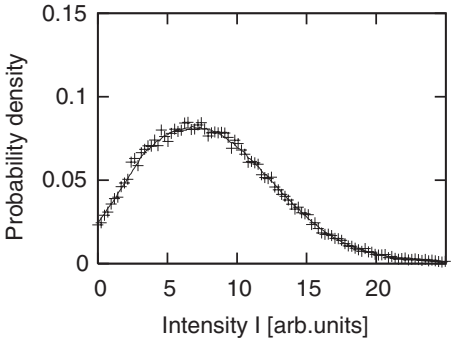

FIG. 5. The invariant probability density of the light intensity (solid curve) and the time-evolving probability density of the light intensity after 1.25 ns (crosses).

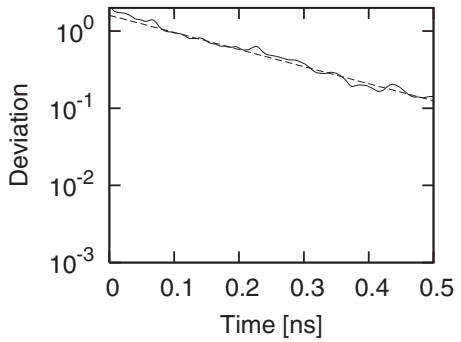

FIG. 6. The difference between the average transient probability density and the invariant probability density (solid curve). The average transient probability density was averaged over the transient probability densities obtained for 10 different randomly chosen initial states of N and I on the chaotic attractor. The transient probability density for each initial condition was obtained using 10^5 different microscopic noise trajectories. The dotted line represents $\exp(-5.3t)$.

monitor the rate of convergence of the probability distribution. The mixing property of the convergence to the invariant density implies the decay of the autocorrelation function $C(\tau)$,

$$C(\tau) = \langle I(t+\tau)I(t)\rangle_t - \langle I\rangle_t^2 \xrightarrow[|\tau|\to\infty]{} 0, \qquad (13)$$

where the bracket defines the time average: $\langle X(t)\rangle_t \equiv \lim_{T\to\infty} 1/T \int_0^T X(t)dt$. Figure 7 shows that the autocorrelation function decays exponentially with the same decay rate as the difference between the time-evolving density and the invariant probability density.

The decay rate λ can be estimated solely from the deterministic part of the LK equation corresponding to the eigenvalue of the Frobenius-Perron operator with the second largest absolute value.

We point out that for the specific value of microscopic noise amplitude corresponding to the spontaneous emission which is expected to be truly random due to its quantum mechanical origin, the correlation value reaches a value of 0.1 in 1 ns.

In terms of the tolerances for the errors that occurs in the fabrication processes of the actual devices and the fluctuations in their operating environments, it is important that the continuous region in the parameter space where the autocorrelation function decays quickly is large enough to produce strong chaos stably. The parameter dependence of the time required for autocorrelation functions to become less

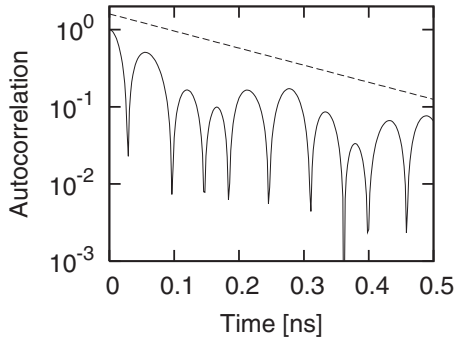

FIG. 7. The autocorrelation function of the time evolution of the light intensity. The dotted line represents $\exp(-5.3t)$.

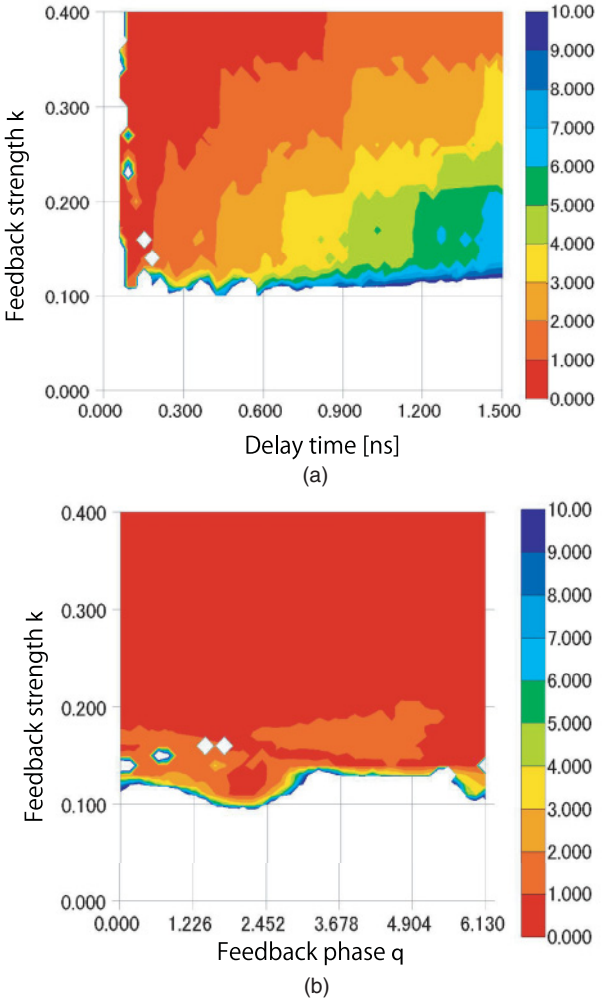

FIG. 8. (Color) The "vanishing time" of the autocorrelation functions. The colors indicate the time (ns) required for the exponentially decaying envelope of the autocorrelation function to become less than 0.1 calculated numerically with the spontaneous emission factor $C_s = 10^{-5}$. (a) Phase diagram of time delay and feedback strength for a fixed phase $\theta = 0$. (b) Phase diagram of the delay phase shift and feedback strength for a fixed time delay $\tau_D = 0.182$ ns.

than 0.1 is shown in Fig. 8(a). One can see that there are continuous areas where the autocorrelation function becomes less than 0.1 within 1 ns as long as the feedback strength is high and the delay time is short. Although strong chaos disappears when the delay time becomes too short, over most of this range the autocorrelation function vanishes faster as the delay time decreases. It is important to note that this range is not the so-called "short cavity regime," where the inverse delay time exceeds the relaxation oscillation frequency and the dynamical behavior sensitively depends on the phase of the delayed feedback field [22,31–33]. Indeed, Fig. 8(b) clearly shows that the vanishing time is almost independent of the delay phase shifts if the feedback strength κ is higher than about 0.2.

The power spectrum of the time evolution of the light intensity is also a convenient measure to check the strong chaotic property since it can be measured as the radio frequency (rf) spectrum in an actual experiment. The peaks

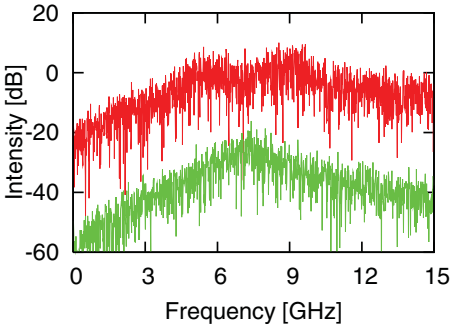

FIG. 9. (Color) The rf spectra of the chaos laser with delayed optical feedback (red curve) and a solitary laser (green curve). The spontaneous emission factor C_s is 10^{-3} for the chaos laser and 10^{-5} for the solitary laser in correspondence with laser experiments (see text).

in the rf spectrum correspond to the recurrences contained in the autocorrelation function. Therefore, there are no large peaks in the rf spectrum of the light intensity of a strongly chaotic laser.

Figure 9 shows the rf spectra of the chaos laser with the same parameters as when the convergence of the probability density and the decay of the autocorrelation function are exponential. One can see that the intensity of the rf spectrum is about 30 dB larger than that obtained without the delayed optical feedback.

IV. FAST NONDETERMINISTIC PHYSICAL RANDOM BIT GENERATION BY CHAOS LASERS

We apply the random bit generation method that we proposed in Sec. II to chaos lasers with the parameter values of the strongly chaotic regime shown in Sec. III.

To extract binary bits from the observed chaos laser intensity, a threshold $I_{\rm bit}$ is set so that $\int_0^{I_{\rm bit}} \rho(I)dI = \int_{I_{\rm bit}}^{\infty} \rho(I)dI$, and bit 0(1) is assigned to the light intensity less (greater) than the threshold $I_{\rm bit}$, where $\rho(I)$ is the invariant probability

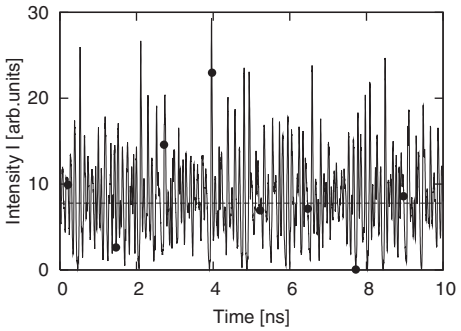

FIG. 10. An example of the time series and the bit sequences obtained by numerically solving the Lang-Kobayashi Eqs. (10) and (11). Temporal waveforms of the light intensity, and corresponding binary digitized signals 10110001$\cdots$. The dots mark points sampled with a 0.8 GHz sampling rate. The broken line represents the threshold value for digitizing the light intensity. The random bit sequences are generated after the XOR operation combining two bit sequences extracted from two different time series starting from different initial states.

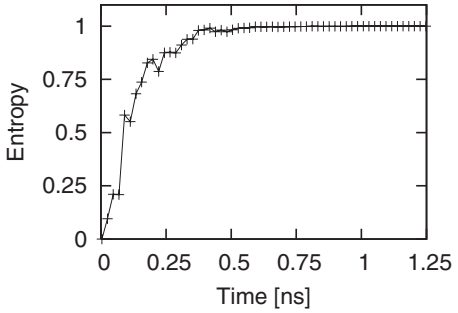

FIG. 11. The entropy averaged over 10^5 random bit sequences generated by sampling the time series numerically produced by the Lang-Kobayashi model with the clock times corresponding to the horizontal axis.

density. According to Eq. (6), it is possible to extract more bits from one sampling of the light intensity by increasing the number of thresholds and assigning bit sequences to each section divided by the thresholds. The bit generation rate depends not only on the convergence rate to the invariant probability density but also on the number of thresholds, that is, the resolution of analog-digital converters. However, in practice, the extraction of more bits could be more susceptible to external noise, which is unrelated to chaos lasers. In this paper we focus on the above bit extraction method using a single threshold, which is the simplest and robust method for directly investigating the statistical property of the bit sequences generated from the chaotic light intensity.

If the chaos laser dynamics starts from an arbitrary initial state and evolves in time subject to perturbations by microscopic noise, such as spontaneous emission, and finally ends with an observation assigning a binary bit, then if the interval between observations is sufficiently long, the bits will be random with equal probabilities of 0 or 1, that is,

TABLE I. Results of NIST Special Publication 800-22(rev. 1a) statistical tests. The tests have been performed using 1000 samples of 1 Mbit data and a significance level $\alpha = 0.01$. The P value (uniformity of p values) should be larger than 0.0001 and the proportion should be in the 0.99 ± 0.0094392 range. For the tests that produce multiple P values and proportions, the worst case is shown.

Statistical test	P value	Proportion	Result
Frequency	0.000181	0.9820	Success
Block frequency	0.080519	0.9890	Success
Cumulative sums	0.000294	0.9810	Success
Runs	0.224821	0.9880	Success
Longest runs	0.783019	0.9870	Success
Rank	0.388990	0.9940	Success
FFT	0.000390	0.9870	Success
Nonoverlapping templates	0.000799	0.9830	Success
Overlapping templates	0.262249	0.9870	Success
Universal	0.410055	0.9880	Success
Approximate entropy	0.380407	0.9840	Success
Random excursions	0.102098	0.9860	Success
Random excursions variant	0.072585	0.9825	Success
Serial	0.508172	0.9860	Success
Linear complexity	0.684890	0.9890	Success

TABLE II. Typical results of the "Diehard" statistical test suite. KS denotes the Kolmogorov-Smirnov test. Significance level $\alpha = 0.01$. For tests with multiple p values, the worst case is shown.

Statistical test	p value	Result
Birthday spacing	0.140624 [KS]	Success
Overlapping 5-permutation	0.875211	Success
Binary rank for 31×31 matrices	0.527490	Success
Binary rank for 32×32 matrices	0.362914	Success
Binary rank for 6×8 matrices	0.746760 [KS]	Success
Bitstream	0.015400	Success
Overlapping-Pairs-Sparse-Occupancy	0.030000	Success
Overlapping-Quadruples-Space-Occupancy	0.023100	Success
DNA	0.049200	Success
Count-the-1's on a stream of bytes	0.104320	Success
Count-the-1's for specific bytes	0.133742	Success
Parking lot	0.490047 [KS]	Success
Minimum distance	0.072981 [KS]	Success
3D spheres	0.827151 [KS]	Success
Squeeze	0.932692	Success
Overlapping sums	0.638165 [KS]	Success
Runs	0.723110 [KS]	Success
Craps	0.480631	Success

a probability of 1/2. Figure 10 shows an example of the time series of the light intensity of the chaos laser and the bits obtained every 1.25 ns. We can check the bit frequency ratio for the binary bit sequences by employing the Shannon entropy defined by Eq. (7) with $N = 2$. Figure 11 shows the entropy of the bit sequences obtained by averaging 10^5 different trajectories of the light intensity of the chaos laser. It is clearly seen that the entropy becomes very close to 1, more precisely the difference from 1 is less than 2.0×10^{-6}, when the sampling clock time is longer than 1.25 ns. This means that the bit sequences generated up to a rate of 0.8 Gbps by numerically solving the Lang-Kobayashi model of the chaos lasers with the parameter values fixed in this paper are almost random at least in the sense that the bit frequency ratio is $50 \pm 0.08\%$.

If the probabilities of successive bits are to be independent and depend only on the invariant probability density $\rho(I)$

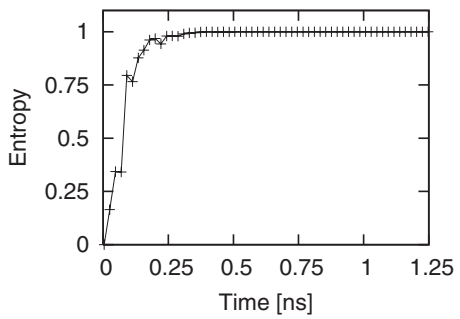

FIG. 12. The entropy averaged over 10^5 random bit sequences obtained by a logical XOR operation on pairs of bits generated by sampling the different time series produced numerically from the Lang-Kobayashi model with clock times corresponding to the horizontal axis.

TABLE III. Results of NIST Special Publication 800-22(rev. 1a) statistical tests for bit sequences obtained by a logical XOR operation on pairs of bits generated at the rate 1.6 Gbps by two chaotic lasers. The tests have been performed using 1000 samples of 1 Mbit data and a significance level of $\alpha = 0.01$. The P value (uniformity of p values) should be larger than 0.0001 and the proportion should be in the 0.99 ± 0.0094392 range. For the tests that produce multiple P values and proportions, the worst case is shown.

Statistical test	P value	Proportion	Result
Frequency	0.014150	0.9880	Success
Block frequency	0.798139	0.9920	Success
Cumulative sums	0.066051	0.990	Success
Runs	0.741918	0.9910	Success
Longest runs	0.651693	0.9890	Success
Rank	0.889118	0.9940	Success
FFT	0.759756	0.9880	Success
Nonoverlapping templates	0.001091	0.9810	Success
Overlapping templates	0.146982	0.9940	Success
Universal	0.516113	0.9820	Success
Approximate entropy	0.138860	0.9920	Success
Random excursions	0.082322	0.9811	Success
Random excursions variant	0.149786	0.9828	Success
Serial	0.020973	0.9920	Success
Linear complexity	0.127393	0.9910	Success

and the bit-extraction threshold, then the vanishing time of the autocorrelation function should be smaller than the bit extraction interval. Conversely, if the bit extraction interval is smaller than the vanishing time of the autocorrelation function, then successive probabilities of the appearances of bits 0 and 1 cannot be described by the theory introduced in Sec. II.

The sequences are only truly random in the limit of infinite sample intervals. Next we examine strict tests of the statistical randomness of bit sequences generated with finite sampling intervals. We use the statistical test suite provided by National Institute of Standard Technology (NIST) and the Diehard test suite [34,35]. Bit sequences generated by the above scheme with sampling rates up to 0.8 GHz passed all of the NIST and Diehard tests at a common statistical significance level of $\alpha = 0.01$ [34,35]. The tests were performed using 1000 instances of 1 Mbit sequences for the NIST tests, and 92 Mbit sequences for the Diehard tests. The results are shown in Tables I and II. Consequently, the bit sequences generated from the time series simulation of the light intensity of the chaos laser up to the generation rate of 0.8 Gbps are statistically random in the sense that they pass the standard statistical test suites of NIST and Diehard.

It is important to note that real systems cannot exactly achieve the above equality which assumes that the observation of intensities and comparison with the threshold value are performed with infinite precision. In the real experiments, $I(t)$ is typically measured with 8-bit precision. Therefore, taking the real chaos laser systems into consideration, we combine the bit sequences obtained from a numerically calculated time series of the light of two identical chaos lasers by a logical Exclusive-OR (XOR) operation, which is a simple and common way to make the bit frequency ratio closer to 50%.

TABLE IV. Typical results of "Diehard" statistical test suite for bit sequences obtained by a logical XOR operation on pairs of the bits generated at a rate of 1.6 Gbps by two chaotic lasers. KS denotes the Kolmogorov-Smirnov test. Significance level $\alpha = 0.01$. For tests with multiple p values, the worst case is shown.

Statistical test	p value	Result
Birthday spacing	0.902520 [KS]	Success
Overlapping 5-permutation	0.70349	Success
Binary rank for 31×31 matrices	0.499604	Success
Binary rank for 32×32 matrices	0.821451	Success
Binary rank for 6×8 matrices	0.62506 [KS]	Success
Bitstream	0.083190	Success
Overlapping-Pairs-Sparse-Occupancy	0.078500	Success
Overlapping-Quadruples-Sparse-Occupancy	0.039500	Success
DNA	0.011000	Success
Count-the-1's on a stream of bytes	0.263346	Success
Count-the-1's for specific bytes	0.061611	Success
Parking lot	0.180784 [KS]	Success
Minimum distance	0.166405 [KS]	Success
3D spheres	0.663964 [KS]	Success
Squeeze	0.988839	Success
Overlapping sums	0.256445 [KS]	Success
Runs	0.486020 [KS]	Success
Craps	0.486023	Success

Figure 12 shows the entropy of the bit sequences obtained by this XOR operation scheme. One can see that the entropy approaches 1 much faster than the case of single chaos laser shown in Fig. 11.

Bit sequences generated by this scheme with sampling rates up to 1.6 GHz passed all of the NIST and Diehard tests at a common statistical significance level of $\alpha = 0.01$ [34,35]. The tests were performed using 1000 instances of 1 Mbit sequences for the NIST tests, and 92 Mbit sequences for the Diehard tests. The results are shown in Tables III and IV. The results show that the bit sequences generated by this XOR operation on the pairs of bits obtained from the time series simulation of the light intensity of the chaos laser up to the generation rate of 1.6 Gbps are statistically random in the sense that they pass the standard statistical test suites of NIST and Diehard.

V. CONCLUSION

We have described theoretically the generation of nondeterministic random bits using chaotic physical systems, which transduce nondeterministic microscopic noise to nondeterministic macroscopic states based on the mixing property of chaos. We emphasized that while the nondeterminism has its origins in that of the microscopic noise, due to the mixing property the chaotic physical system can be characterized by a probability distribution of macroscopic states that does not depend on the details of the probability distribution of the microscopic noise. We also described how the rate of convergence of a probability distribution corresponding to a single macroscopic state with microscopic noise perturbations to an asymptotic probability distribution of macroscopic states can be estimated from the deterministic chaos obtained in the limit of vanishing noise amplitude.

We have also shown numerically that lasers with delayed optical feedback exhibit the mixing characteristic of strongly chaotic systems, with exponential convergence to the natural invariant probability density starting from an arbitrary smooth initial density. We also showed specifically that spontaneous emission noise, which is of quantum mechanical origin, can cause close to unity entropy of macroscopic states within a short time of the order of 1 ns. Moreover, such strongly chaotic behavior is robust with respect to the perturbations of laser parameters.

Finally, we applied the above results to show that bits with almost no correlation can be generated at fast rates of the order of gigabits per second. The sequences are sufficiently random to pass the common randomness statistical test suites of NIST and Diehard at statistical significance levels of 0.01.

The results confirm that physical devices such as the chaotic lasers reported in [21] can indeed be used for nondeterministic random bit generators operating at fast rates of over 1 Gbps.

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC, Boca Raton, FL, 1996).

[2] N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).

[3] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis* (Springer, New York, 2007).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[5] D. Knuth, *The Art of Computer Programming: Volume 2: Seminumerical Algorithms*, 3rd ed. (Addison-Wesley, New York, 1996).

[6] B. Jun and P. Krocher, The Intel RNG, white paper, [http://www.cryptography.com/intelRNG.pdf], (1999).

[7] C. S. Petrie and J. A. Connelly, IEEE ISCAS 1996, Vol. 4, p. 324.

[8] M. Bucci, L. Germani, R. Luzzi, and A. Trifiletti, IEEE Trans. Comput. **52**, 403 (2003).

[9] B. Sunar, W. J. Martin, and D. Stinson, IEEE Trans. Comput. **56**, 109 (2007).

[10] C. Petrie and J. Connelly, IEEE Trans. Circuits Syst. I **47**, 615 (2000).

[11] C. Tokunaga *et al.*, ISSCC Dig. Tech. Papers, Feb. 2007, p. 404.

[12] M. Matsumoto *et al.*, ISSCC Dig. Tech. Papers, Feb. 2008, p. 414.

[13] S. Srinivasan, S. Mathew, V. Erraguntla, and R. Krishnamurthy, *Proceedings of the 22nd International Conference on VLSI Design*, New Delhi, India, 5-9 January 2009 (IEEE Computer Society, Los Alamitos, CA, 2009), p. 301.

[14] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[15] B. Qi, Y-M. Chi, H-K. Lo and L. Qian, Opt. Lett. **35**, 312 (2010).

[16] J. Miller, Phys. Today **62**, 12 (2009).

[17] T. E. Murphy and R. Roy, Nat. Photon. **2**, 714 (2008).

[18] 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, Nat. Photon. **2**, 728 (2008).
[19] I. Kanter, Y. Aviad, I. Reidler, and E. Cohen, and M. Rosenbluh, Nat. Photon. **4**, 58 (2010).
[20] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).
[21] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Phys. Rev. A **83**, 031803(R) (2011).
[22] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, Phys. Rev. Lett. **100**, 194101 (2008).
[23] J. J. Lepley *et al*., Elec. Lett. **36**, 1480 (2000).
[24] P. Gaspard, *Chaos, Scattering and Statistical Mechanics* (Cambridge University Press, Cambridge, 1998).
[25] C. E. Shannon, Bell Syst. Tech. J. **27**, 379, 623 (1948).
[26] G. Casati and T. Prosen, Phys. Rev. Lett. **83**, 4729 (1999).
[27] E. Gutkin, J. Stat. Phys. **83**, 7 (1996).
[28] P. Gaspard, J. Phys. A **25**, L483 (1992).
[29] R. Lang and K. Kobayashi, IEEE J. Quantum Electron. **16**, 347 (1980).
[30] J. Otsubo, *Semiconductor Lasers: Stability, Instability and Chaos* (Springer, Berlin, 2006).
[31] K. E. Chlouverakis, A. Argyris, A. Bogris, and D. Syvridis, Phys. Rev. E. **78**, 066215 (2008).
[32] T. Heil, I. Fischer, W. Elsäßer and A. Gavrielides, Phys. Rev. Lett. **87**, 243901 (2001).
[33] T. Heil, I. Fischer, W. Elsäßer, B. Krauskopf, K. Green, and A. Gavrielides, Phys. Rev. E. **67**, 066214 (2003).
[34] A. Rukhin *et al*., A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology, Special Publication 800-22 Revision 1a (2010).
[35] G. Marsaglia, DIEHARD: A battery of tests of randomness [http://stat.fsu.edu/∼geo] (1996).