PHYSICAL REVIEW A **83**, 031803(R) (2011)

Fast nondeterministic random-bit generation using on-chip chaos lasers

Takahisa Harayama,[1] Satoshi Sunada,[1] Kazuyuki Yoshimura,[1] Peter Davis,[1] Ken Tsuzuki,[2] and Atsushi Uchida[3]
[1]*NTT Communication Science Laboratories, NTT Corporation, 2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan*
[2]*NTT Photonics Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3]*Department of Information and Computer Sciences, Saitama University, 255 Shimo-Okubo, Sakura-ku, Saitama City, Saitama 338-8570, Japan*

(Received 27 May 2010; published 15 March 2011)

It is shown that broadband chaos suitable for fast nondeterministic random-bit generation in small devices can be achieved in a semiconductor laser with a short external cavity. The design of the device is based on a theoretical model for nondeterministic random-bit generation by amplification of microscopic noise. Moreover, it is demonstrated that bit sequences passing common tests of statistical randomness at rates up to 2.08 Gbits/s can be generated using on-chip lasers with a monolithically integrated external cavity, amplifiers, and a photodetector.

DOI: 10.1103/PhysRevA.83.031803 PACS number(s): 42.65.Sf, 05.45.Gg, 05.45.Jn

Random-bit generators are widely used in communication and computation systems, and they are key devices for achieving ultimate performance and reliability [1–4]. Nondeterministic random bits are generated by sampling random physical phenomena but it is difficult in practice to avoid correlations and statistical bias when bits are generated at high speeds in small devices. Hence it has been an urgent but difficult challenge to find physical phenomena suitable for fast, reliable nondeterministic random-bit generation in small physical devices. Recently optical turbulence due to chaotic mechanisms in semiconductor lasers with oscillations at high frequencies above the order of GHz has been used to achieve fast random-bit generation [5–11]. However, these chaotic lasers used long optical feedback over 1 m. Monolithically integrated chaotic lasers with short delay have been developed for data transmission with chaotic optical carriers [12,13]. However, it has not been known whether such on-chip devices with short optical feedbacks are sufficiently chaotic and robust to generate random-bit sequences reliably at high rates.

In this Rapid Communication, we report that we have succeeded in generating random-bit sequences at rates up to 2.08 Gbits/s using monolithically integrated chaotic semiconductor lasers. Chaotic lasers have been integrated with photodiodes in a structure specifically designed to achieve robust generation of random bits at high bit rates. The design is based on a theoretical model for nondeterministic bit generation using chaotic laser dynamics seeded by the quantum noise of spontaneous emission.

The scheme for generating random-bit sequences using a module with two chaos laser chips (we call them laser 1 and laser 2) is shown in Fig. 1(a). Two chaos laser chips are contained in a single module with two high-frequency connectors to output the electrical signals from the integrated photodiodes (PDs) as shown in Figs. 1(b) and 1(c). The ac components of the electrical signals from the PDs are digitized at a 2.08-GHz sampling rate. The ac signals are converted to binary signals by comparing with a threshold voltage, and finally the binary bit signals are combined by a logical exclusive-OR (XOR) operation to generate a single random-bit sequence. No other digital postprocessing is required. This method is similar to that used for bit extraction in a previous demonstration of fast physical random-bit generation [5,7]. Figure 1(d) shows an optical image of the monolithically integrated optical components in a chaos laser chip. High-reflective coating at the edge of the passive waveguide reflects the light back into the distributed feedback (DFB) laser, inducing high-frequency chaotic oscillations in the gigahertz regime. The feedback delay length L is just 10 mm. The strength and phase of the optical feedback is controlled with the current to the semiconductor optical amplifiers (SOAs). The temporal wave forms of the signals from the two photodiodes of the chaos laser chips in the random signal generator module are shown in Fig. 2. The sequence of random bits is obtained as the output from the XOR operation.

The statistical randomness of digital bit sequences was verified using the statistical test suite for random number generators provided by the National Institute of Standard Technology (NIST) and the DIEHARD test suite [14,15]. Bit sequences obtained from the experimental device for sampling rates up to 2.08 Gbits/s passed all of the NIST and DIEHARD tests at the common statistical significance level of $\alpha = 0.01$ [16]. The tests were performed using 1000 instances of 1 Mbit sequences for NIST tests and using 92 Mbit sequences for DIEHARD tests. The random signal generation is stable with respect to mechanical and thermal perturbations, to the extent that statistical properties of the sequences were maintained over multiple trials during continual operation of the device.

The design of the chaos laser is based on a theoretical model for nondeterministic random-bit generation by amplification of microscopic noise. From the fundamental point of view, it is important that there is a theoretical basis for expecting this device to achieve truly random-bit sequences. The theoretical basis is obtained by considering the mechanism by which chaotic dynamics amplifies and mixes intrinsic quantum laser noise. Let us suppose that time evolution of output light intensity $I(t)$ of strongly chaotic lasers is given at discrete sampling times $t = 0, \tau, 2\tau, \ldots$, where τ is a sampling clock time. Then the mixing property of strong chaos implies that any arbitrary smooth initial probability density of $I(t)$ converges to the invariant density $\rho(I)$ corresponding to the natural invariant density of this chaos laser dynamical system. We emphasize that the asymptotic invariant density of the light intensity does not depend on the initial noise density. In principle the nondeterminism of the microscopic noise is the

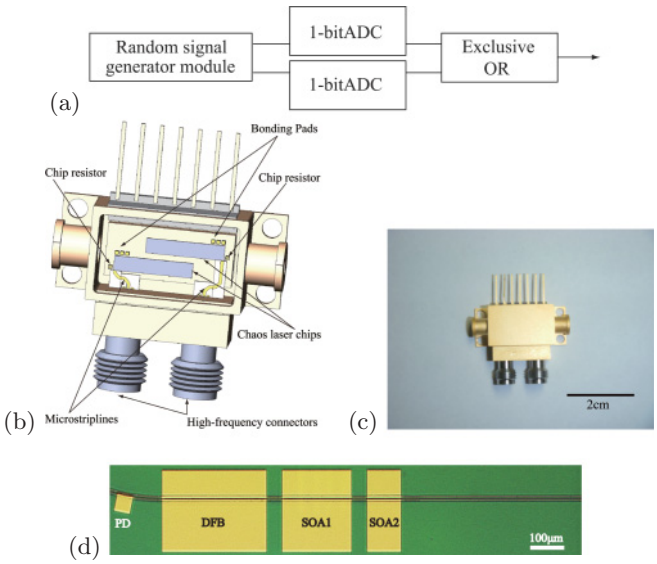

FIG. 1. (Color) Random-bit generation scheme and device structures. (a) Schematic diagram of random-bit generation. ADC denotes the analog-digital converter. (b) Schematic of the random signal generator module consisting of two chaos laser chips. Chip resistors are used for impedance matching and current is injected to the distributed feedback (DFB) laser and semiconductor optical amplifier (SOA) contacts of the chaos laser chips via bonding pads (wires not shown here). Electrical signal is output from the photodiodes (PDs) in the chaos laser chips via microstriplines to high-frequency connectors. (c) Photo of a random signal generator module. (d) Optical image showing the monolithically integrated optical components. A small section of the 10-mm-long passive waveguide for optical feedback can be seen. DFB laser, semiconductor distributed feedback laser; SOA1 and SOA2, semiconductor optical amplifiers, The width of the waveguide is 2 μm. The lengths of the PD, DFB laser, SOA1, SOA2, and passive waveguide are, respectively, 50 μm, 300 μm, 200 μm, 100 μm, and 10 mm.

origin of the nondeterminism of the output light intensity, but the asymptotic invariant density of the large-amplitude light intensity is a property of the chaotic dynamics. This convergence to the invariant density is a key fundamental point for the use of chaotic devices to generate large-amplitude signals for robust nondeterministic random-bit generation.

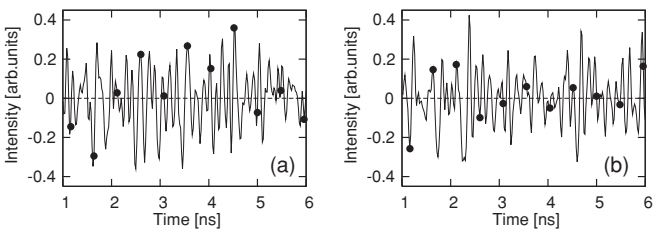

FIG. 2. Random-bit generation using the random signal generator module. Temporal wave forms of the two module outputs and corresponding binary digitized signals (a) 00111111010... and (b) 0110010110.... Dots mark points sampled with 2.08 GHz sampling rate. The threshold value for the ADC is zero, shown as a solid line. The random bit sequence output after the XOR operation is 01011010111....

Let us extract binary bits from the chaotic laser intensity by assigning bit 0 (1) to the output intensity I less (greater) than the threshold $I_{\rm bit}$, where $I_{\rm bit}$ is defined by $\rho(I)$ so that it satisfies $\int_0^{I_{\rm bit}} \rho(I)dI = \int_{I_{\rm bit}}^{\infty} \rho(I)dI$. If the chaotic 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, and then if the interval between observations is sufficiently long, then the bits will be random with equal probabilities of 0 or 1, that is, probability 1/2.

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 done with infinite precision. In our experimental system, $I(t)$ is measured with 8-bit precision, and we combine the outputs of two chaos laser chips by a logical exclusive-OR operation, a simple and common way to make the bit frequency ratio closer to 50%.

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

$$C(\tau) = \langle I(t+\tau)I(t)\rangle_t - \langle I\rangle_t^2 \underset{|\tau|\to\infty}{\longrightarrow} 0, \tag{1}$$

where the bracket defines the time average: $\langle X(t)\rangle_t \equiv \lim_{T\to\infty} 1/T \int_0^T X(t)dt$. Therefore, observation of the autocorrelation is a practical way to monitor the rate of convergence of the probability distribution. If the probabilities of successive bits are to be independent and depend only on the invariant density and the bit-extraction threshold, then the autocorrelation vanishing time should be smaller than the bit extraction interval. Conversely, if the bit extraction interval is smaller than the vanishing time of the autocorrelation, then successive bit probabilities cannot be described by the above theory.

Based on the above theoretical principle, the chaos laser chips are designed so that the probability density function and autocorrelation function converge as fast as possible. We use a Lang-Kobayashi model as a reference model for optimizing the device parameters. The dynamics of the light field E and the carrier density N in a laser with delayed optical feedback is described by the Lang-Kobayashi equations [17] as

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

$$\frac{dN}{dt} = J - \frac{1}{\tau_s}N - G|E|^2, \tag{3}$$

where the gain G depends on E and N as $G \equiv G_0(N-N_0)/(1+\epsilon|E|^2)$. ξ is white Gaussian noise with zero mean and unitary variance. The last term of the right-hand side of Eq. (2) represents the effect of spontaneous emission. The linewidth enhancement factor is $\alpha = 5$, the differential gain $G_0 = 10^{-12}$ m^3 s^{-1}, the gain saturation coefficient $\epsilon = 4.08 \times 10^{-24}$ m^3, the propagation time in the DFB laser $\tau_{\rm in} = 7$ ps, the delay time $\tau_D = 0.303$ ns, the delay phase shift $\theta = 0$ rad, the carrier life time $\tau_s = 2.04$ ns, and the transparent carrier density $N_0 = 1.4 \times 10^{24}$ m^{-3}. Several values of the spontaneous emission factor C_s were used between 10^{-5} and 10^{-3}.

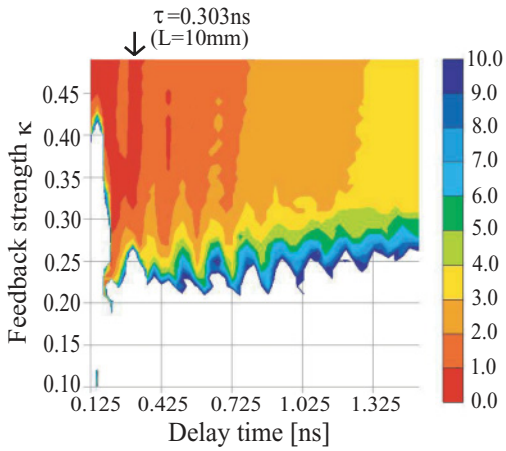

FIG. 3. (Color) The "vanishing time" of the autocorrelation functions. The colors indicate the time (ns) required for the exponentially decaying envelope of the autocorrelation function to becomes less than 0.1.

We calculated the dependence of the autocorrelation decay on values of parameters, in particular delay time τ_D and feedback strength κ. The parameter dependence of the times required for autocorrelation to become less than 0.1 are shown in Fig. 3. One can see that although strong chaos disappears when the delay time becomes too short, over most of this range the autocorrelation function vanishes faster as the feedback strength becomes larger and the delay time becomes shorter. 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 [12,13,18,19].

Figure 4 shows an example of convergence of the distribution and the autocorrelation function with time in the most strongly chaotic regime. It can be seen that the deviation of the distribution and the autocorrelation both decay at the same rate, and the autocorrelation decays to less than 0.1 within 1 ns. For small noise, the decay rate is roughly independent of the noise strength. However the curve shifts downward for larger noise amplitude, achieving shorter randomization times for larger noise strengths.

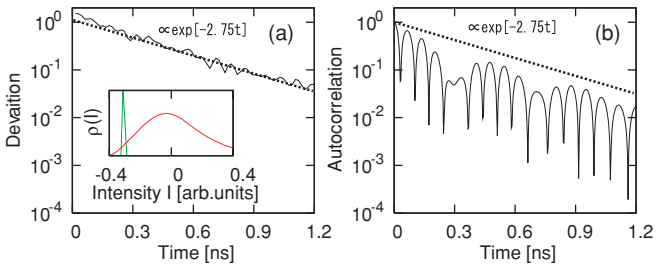

FIG. 4. (Color) Numerical results on the convergence of the density and autocorrelation function. (a) Difference between the evolving time density and the invariant density. Inset: Any smooth initial density (the green curve) converges to the invariant density (the red curve). (b) The autocorrelation function.

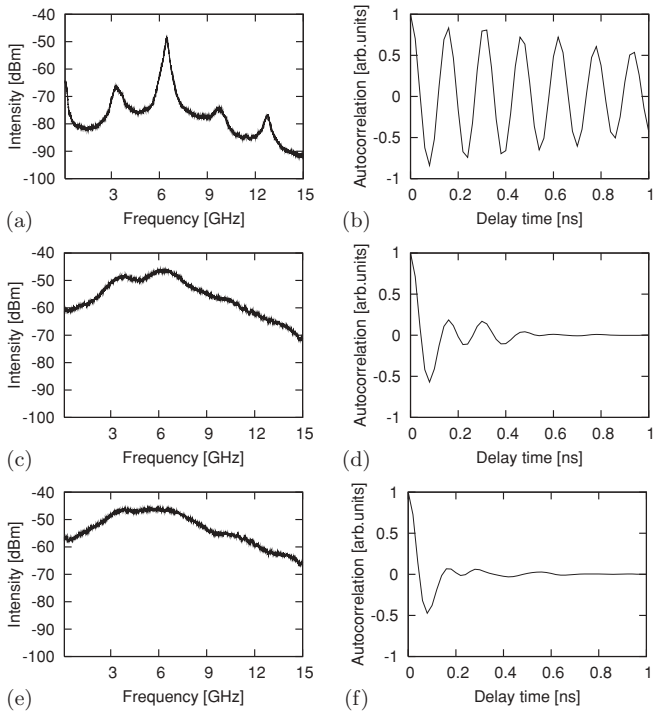

FIG. 5. Radio-frequency spectra and autocorrelation functions for I_{SOA1} = (a), (b) 2 mA; (c), (d) 6 mA; and (e), (f) 10 mA.

The experimental laser chaos chips were designed to operate in the regime where the correlation vanishes fastest, marked by the arrow in Fig. 3. In particular, the strong feedback and tunability, which have been shown to be necessary by the above theory, were achieved by integrating dual SOAs and a PD together with the optical waveguide. Figure 5 shows a typical scenario observed while tuning the experimental chip to minimize the correlation time. It is important to note that the decay of the autocorrelation function is closely related to the flatness of the power spectrum. Even small structures in the spectrum mean slower decay of the autocorrelation function. In this example, the current I_{SOA1} injected to the first optical amplifier SOA1 is increased while the injection currents of the DFB laser and the SOA2 are fixed at 42.5 and 5 mA, respectively. (The threshold current for the DFB laser is 12.69 mA.) When I_{SOA1} is 2 mA [Fig. 5(a)], the signal starts oscillating, and the relaxation oscillation frequency increases to 6.6 GHz while the inverse of the feedback delay time remains 3.3 GHz. These two peaks have come into resonance, so the peaks are sharp and higher harmonics are observed. The corresponding autocorrelation function takes a long time to decay, as shown in Fig. 5(b). When I_{SOA1} is increased to 6 mA, the signal becomes chaotic and the autocorrelation function decays faster as shown in Figs. 5(c) and 5(d). When I_{SOA1} is increased to 10 mA, the signal becomes more strongly chaotic and the rf spectrum becomes more similar to white noise, with intensity increased by more than about 30 dB compared to the solitary laser case, and the autocorrelation function decays much faster, as shown in Figs. 5(e) and 5(f). It can be seen that the correlation decays to less than 0.1 well within 1 ns, as anticipated from the Lang-Kobayashi model. The broadband chaos of the flat spectrum as in Fig. 5(f) and the corresponding

fast vanishing autocorrelation functions can be stably obtained in a wide range of I_{SOA1} between 8 and 20 mA.

Previous lasers used for random-bit generation had a significant peak in the autocorrelation function corresponding to long feedback time delays longer than 50 ns [5,7,11]. This required the delay times and multiples of sampling intervals to be detuned when sampling in the gigahertz regime. In contrast, for the short cavity it is not necessary to detune the delay lengths since the delay time is shorter than the sampling interval. Moreover, the spectrum is flatter than previous reports for short cavity chaos lasers of the short cavity regime [12,13]. This is due to the tuning of the lasers to a more strongly chaotic regime which was achieved using a structure with integrated dual SOAs. Besides, it is theoretically shown that nondeterministic random-bit sequences can be obtained by this scheme using the quantum noises of spontaneous emission and the mixing property of the strongly chaotic dynamics. Together these results show not only that random signal generation is possible with smaller devices but also that the characteristics can be even better than the previous examples using macroscopic optical components [5,7].

Finally, we note that it is expected that this device could be used to generate sequences that pass the statistical randomness at higher effective bit rates by applying multibit sampling and postprocessing methods such as demonstrated recently, for example, in [9–11]. However, achieving *nondeterministic* random-bit generation at higher rates remains a difficult challenge as it is limited by the rate of amplification of microscopic noise.

In conclusion, we have demonstrated that continuous streams of random-bit sequences which pass standard tests of statistical randomness can be generated at fast rates of up to 2.08 Gbit/s using two monolithically integrated chaos laser chips with a scheme based on a theoretical model for nondeterministic random-bit generation. This achievement opens the door to reduction of size and cost of fast nondeterministic physical random-bit generators operating at rates beyond gigabits per second.

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 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-Verlag, New York, 2007).

[4] C. H. Bennett *et al.*, J. Cryptology **5**, 3 (1992).

[5] A. Uchida *et al.*, Nat. Photonics **2**, 728 (2008).

[6] Thomas E. Murphy and Rajarshi Roy, Nat. Photonics **2**, 714 (2008).

[7] K. Hirano *et al.*, IEEE J. Quantum Electron. **45**, 1367 (2009).

[8] T. Honjo *et al.*, Opt. Express **17**, 9053 (2009).

[9] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Phys. Rev. Lett. **103**, 024102 (2009).

[10] Ido Kanter *et al.*, Nat. Photonics **4**, 58 (2010).

[11] K. Hirano *et al.*, Opt. Express **18**, 5512 (2010).

[12] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, Phys. Rev. Lett. **100**, 194101 (2008).

[13] K. E. Chlouverakis, A. Argyris, A. Bogris, and D. Syvridis, Phys. Rev. E **78**, 066215 (2008).

[14] 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.

[15] G. Marsaglia, in *Computer Science and Statistics: The Interface*, edited by L. Billard (Elsevier, Amsterdam, 1985), p. 3. The software package DIEHARD, a battery of tests of randomness, is available via the WWW at [http://stat.fsu.edu/geo/diehard.html], 1996. The Marsaglia Random Number CDROM contains 4.8109 random bits obtained from a combination of several sources.

[16] For example, in the case of the monobit frequency test which tests the ratio of 1 and 0, the statistical significance value $\alpha = 0.01$ means that deviation δ from the ideal value of $1/2$ should be such that $\mathrm{erfc}(\delta\sqrt{2n} < \alpha$, where erfc is the complementary error function and n is the length of the bit sequence).

[17] R. Lang and K. Kobayashi, IEEE J. Quantum Electron. **16**, 347 (1980).

[18] T. Heil, I. Fischer, W. Elsasser, and A. Gavrielides, Phys. Rev. Lett. **87**, 243901 (2001).

[19] T. Heil *et al.*, Phys. Rev. E **67**, 066214 (2003).