2011 International Symposium on Nonlinear Theory and its Applications
NOLTA2011, Kobe, Japan, September 4-7, 2011

On-chip chaos lasers for fast non-deterministic random bit generation

S. Sunada[1] T. Harayama[1†] , K. Arai[1], K. Yoshimura[1] P. Davis[1‡] , K. Tsuzuki[2], and A. 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 Science, Saitama University
255 Shimo-Okubo Sakura-ku Saitama city Saitama, 338-8570, Japan
Email: sunada.satoshi@lab.ntt.co.jp

Abstract—We theoretically show that non-deterministic random bits can be generated due to the mixing property of chaotic systems and microscopic noises. Moreover, it is reported that with chaos laser chips which are designed on the basis of the theory, non-deterministic random bit sequences can be generated at fast rates up to 2.08 gigabit per second (Gbps).

1. Introduction

Random bit generation is important for many applications, such as cryptography, numerical computation, and stochastic modeling [1, 2]. In particular, fast generation of unpredictable truly random bit sequences is very important to achieve high security of communication systems.

The generation of such random bit sequences can be achieved by sampling observables obtained from physical phenomena which are expected to be random and converting them to bit sequences. The typical example is quantum physical random bit generators. They utilize quantum decision such as detection of single photon or vacuum fluctuation, which are in principle unpredictable [3, 4]. However, the sampling rate has been less than the order of GHz due to the limited bandwidth of detectors and amplifiers.

Recently, random bit generation using fluctuations in optical phenomena such as laser chaos or amplified spontaneous emission have been developed in order to obtain unpredictable random bit sequences extremely fast [5, 6, 7]. In particular, the use of laser chaos could make possible random bit generation which is efficient from the viewpoint of power consumption, since vary small noises such as spontaneous emission noise can be converted to macroscopic signals by the dynamical instability without additional high power amplfiers.

So far, many experimental demonstrations of random bit generation with laser chaos have been reported [5, 8, 9, 10, 11, 12]. However, the role of chaos in generating unpredictable random bits has not yet been studied in detail. The elucidation of the mechanism of the physical random bit generation is important in order to guarantee the unpredictability.

In this paper, we theoretically show that non-deterministic and unpredictable random bit sequences can be generated due to the mixing property of chaotic laser systems and microscopic noises, such as quantum noises due to spontaneous emission [13]. Moreover, we report an experimental demonstration of random bit generation using monolithically integrated chaos laser chips which are designed on the basis of the above theory and fabricated with photonic integration technologies. We experimentally show that random bit sequences passed standard statistical test suites for randomness can be generated at fast rates up to 2 Gbps [13].

2. Random bit generation with chaos

Here, let us consider the time evolution of an observable $I(t)$ in a dynamical system subject to random perturbation such as microscopic noise. (In laser system, the observable I is usually a output light intensity and the microscopic noise is quantum noise, such as spontaneous emission). Then, if the system is strongly chaotic, it has the mixing property. The mixing property of chaotic systems implies that any arbitrary smooth initial probability density of $I(t)$ converges to a unique invariant density, known as the natural invariant density $\rho(I)$. In principle, the non-determinism of $I(t)$ is based on non-determinism of the microscopic noise, but the asymptotic invariant density is a property of the chaotic dynamics. This convergence to the invariant density is a key fundamental point for the use of chaotic systems to generate large amplitude signals for robust non-deterministic random bit generation.

The binary signals can be extracted from the observable $I(t)$ by assigning bit 0(1) to it less (greater) than a threshold I_{th}, where I_{th} is defined by $\rho(I)$ so that it satisfies,

$$\int_0^{I_{th}} \rho(I)dI = \int_{I_{th}}^{\infty} \rho(I)dI. \quad (1)$$

When the chaotic dynamics starts from any arbitrary initial state and evolves in time subject to perturbation by mi-

† Presently at: Toyo University
‡ Presently at: Telecognix Corporation

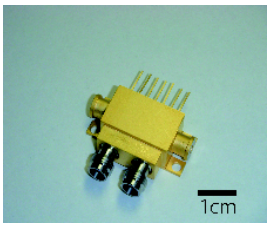


Figure 1: Photograph of a random signal generator module. The module contains two independent chaos laser chips, as shown in Fig. 2. The electrical signals obtained from the integrated PD in the laser chips (Fig. 2) are extracted from the high-frequency connectors via microstrip lines inside the module.

croscopic noise, and finally ends with an observation assigning a binary bit, 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.

However, it is usually difficult to observe the convergence process to the invariant density in real experimental systems, because the states of the system are needed to reset to the same initial state many times, or wait long times until the laser revisits the neighborhood of the same initial state many times. Observation of the autocorrelation is a more practical way to 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,

$$C(\tau) =< I(t+\tau)I(t) >_t - < I(t) >_t^2 \to_{|\tau|\to\infty} 0, \qquad (2)$$

where the bracket defines the time average, $< X >_t = \lim_{T\to\infty} 1/T \int X(t)dt$. In particular, if the system is strongly chaotic, i.e., hyperbolic, the autocorrelation exponentially decays. The decay rate is the same as the rate of convergence to the invariant density. If the time interval between the observations, i.e., the bit-extraction time is much longer than the time required for the time-evolving probability density to converge to the natural invariant density, then the statistical correlation between bits will be zero and the sequence will be truly random. It is important to increase the decay rate of the autocorrelation in order to generate unpredictable random bit sequences as fast as possible.

3. Chaos laser chips

In order to carry out the above method with a small optoelectronic device, a random signal generator module was fabricated (see Fig.1). This module contains two chaos laser chips, which are designed so that the autocorrelation of the output signal vanishes as fast as possible, and fabricated with photonic integration technologies in InGaAsP material systems.

Fig. 2 shows the schematic and picture of the chaos laser chip. The laser chip consists of a distributed feedback

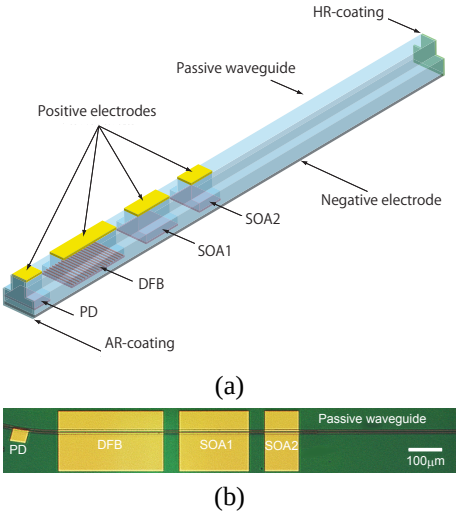
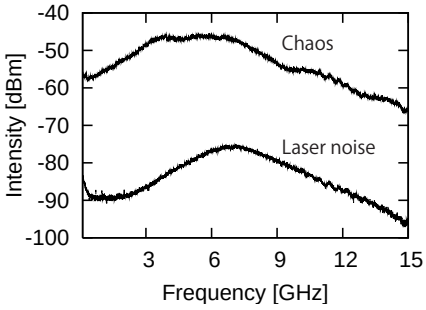


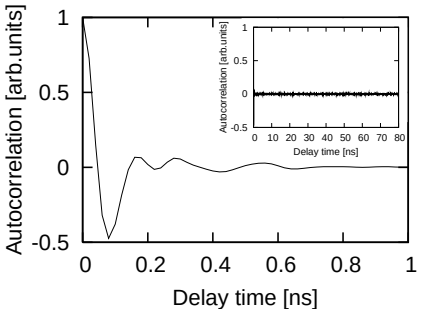
Figure 2: A schematic (a) and photograph (b) of the fabricated chaos laser device. The laser is contained in the module shown in Fig. 1. The lengths of DFB, SOA1, SOA2, PD, and passive waveguide are respectively 300 μm, 200 μm, 100 μm, 50 μm, and 10 mm. The width of the waveguide is 2 μm. DFB, SOAs, PD sections contain the strained InGaAs/InGaAsP multi-quantum well active layer bounded by the non-doped InGaAsP separate-confinement-heterostructure layer. For the DFB laser, a grating is fabricated so that the laser emits light around the wavelength λ_a= 1.55 μm. The passive region contains the intrinsic InP cladding layer and the non-doped InGaAsP waveguiding core layer with the bandgap corresponding to the wavelength λ_b = 1.3 μm, which is shorter than λ_a, to avoid light absorption. These layers are made by butt-joint selective growth.

(DFB) laser with a single optical frequency, passive waveguides, two semiconductor optical amplifiers (SOAs), and a fast response photodiode (PD). The light emitted from the DFB propagates via the passive waveguide and two SOAs, reflected at high-reflection-coated edge of the passive waveguide, and fed back to the DFB, inducing high-frequency chaotic oscillations in the gigahertz regime. The feedback delay length is 10 mm. The strength and phase of the optical feedback is controlled with the current to the SOAs. The generated chaotic signal is detected with the integrated PD with coupling efficiency over 70 %.

Fig. 3(a) shows a typical power spectrum obtained from the chaos laser chip shown in Fig. 2. The injection current to DFB is 40 mA, which is about three times of the threshold current, while the injection currents to SOA1 and SOA2 are respectively 10 mA and 5 mA. The feedback power ratio corresponds to 9.5 %, which is larger than the chaos laser chip reported in [12]. One can see that the spectrum is very flat and there are no sharp peaks suggesting weak instability. This flatness of the spectrum is achieved by the stronger feedback and better tunability by the use of dual



(a)



(b)

Figure 3: (a) The rf-spectra of the chaotic light intensity and the laser noise. (b) The autocorrelation of the chaotic light intensity.

SOAs. Moreover, the intensity is increased by more than about 25 dB compared to the noise spectrum of the solitary laser noise measured when the injection currents to SOAs are not applied, suggesting that the chaotic signal is robust with respect to the external electrical perturbations.

Fig. 3(b) shows the autocorrelation function corresponding to the spectrum of Fig. 3(a). The correlation has a peak around the relaxation oscillation period, and the peak rapidly decays over just a few periods due to the strongly chaotic dynamics. Note that there are no significant peaks associated with the feedback delay time, unlike the chaotic laser systems with long feedback delay [5]. This means that tuning of the sampling interval is not necessary [5].

4. Random bit generation

The conversion to the binary signals from the generated chaotic signals is carried out on the basis of the method mentioned in sec. 2. First the chaotic signal is digitized at a sampling interval 0.48 ns (the sampling rate 2.08 GHz). As shown in Fig. 3(b), the autocorrelation of the chaotic signal has almost vanished at this time. The sampled signals can be converted to binary signal (1 or 0) by comparing a threshold value which is decided using the invariant density obtained from the time-series of the chaotic signal (see Eq.(1)). However, it is important to note that real systems cannot exactly achieve the equality (1) which assumes that the observation of the signal and comparison with the threshold value is done with infinite precision. In this experiment, the threshold is determined by a method with only 8-bit precision which cannot avoid some small statistical bias. In order to generate a random bit sequence with lower statistical bias, two independent bit sequences obtained from two chaos laser chips are combined by a logical Exclusive-OR (XOR) operation, which is a simple and common way to reduce statistical bias.

Statistical randomness of the generated bit sequence is evaluated using the standard test suites for random number generators provided by National Institute of Standard Technology (NIST), NIST Special Publication 800-22 (revision 1a) [14] and "Diehard" tests [15]. The NIST test consists of 15 statistical tests, as shown in Table 1, and each test was performed using 1000 instances of 1Mbit sequences generated with sampling rate 2.08GHz and significance level 0.01. To pass each test, the P-value (the uniformity of the p-value) should be larger than 0.0001 and the proportion should be in the range of 0.99 ± 0.0094392. Diehard tests consist of 18 statistical tests, as shown in Table 2. The tests were performed using 92 Mbit sequences and the same significance level 0.01, which means that the p-values should be larger than 0.01 and smaller than 0.99. We confirmed that the bit sequences obtained in this experiment pass all tests of both the NIST and Diehard tests. The results are shown in Tables 1 and 2.

5. Summary

In summary, we showed a theory of non-deterministic random bit generation using strongly chaotic systems with microscopic noises. On the basis of the theory and using photonic integration technologies, monolithically integrated semiconductor chaotic laser chips were designed and fabricated. We also showed that at fast rates up to 2 Gbps, the chaos laser chips generate random bit sequences which pass standard statistical tests for randomness.

References

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

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

[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.*, vol.71, pp.1675–1680, (2000).

[4] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random

Table 1: Results of NIST Special Publication 800-22(rev. 1a) statistical tests. For the tests which produce multiple P-values and proportions, the worst case is shown.

Statistical test	P value	Proportion	Result
Frequency	0.194813	0.9900	Success
Block frequency	0.310049	0.9910	Success
Cumulative sums	0.285427	0.9890	Success
Runs	0.375313	0.9930	Success
Longest runs	0.504219	0.9900	Success
Rank	0.146152	0.9950	Success
FFT	0.792508	0.9860	Success
Nonoverlapping templates	0.005889	0.9820	Success
Overlapping templates	0.289667	0.9880	Success
Universal	0.222480	0.9880	Success
Approximate entropy	0.411840	0.9840	Success
Random excursions	0.164882	0.9835	Success
Random excursions variant	0.013808	0.9868	Success
Serial	0.823725	0.9920	Success
Linear complexity	0.331408	0.9970	Success

Table 2: Typical results of "Diehard" statistical test suite. KS - Kolmogorov-Smirnov test. For tests with multiple p-value, the worst case is shown.

Statistical test	p-value	Result
Birthday Spacing	0.577899 [KS]	Success
Overlapping 5-permutation	0.038679	Success
Binary rank for 31×31 matrices	0.348054	Success
Binary rank for 32×32 matrices	0.342725	Success
Binary rank for 6×8 matrices	0.187360 [KS]	Success
Bitstream	0.024130	Success
OPSO	0.020200	Success
OQSO	0.031500	Success
DNA	0.067300	Success
Count-the-1's on a stream of bytes	0.278065	Success
Count-the-1's for specific bytes	0.0357829	Success
Parking lot	0.793332 [KS]	Success
Minimum distance	0.430103 [KS]	Success
3D spheres	0.184534 [KS]	Success
Squeeze	0.267296	Success
Overlapping sums	0.506894 [KS]	Success
Runs	0.114851 [KS]	Success
Craps	0.112728	Success

numbers based on vacuum states," *Nature Photon.*, vol.4, pp.711–715, (2010).

[5] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Karashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol.2, pp.728–732, (2008).

[6] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Opt. Express*, vol.18, pp. 23584–23597, (2010).

[7] X. Li, A. B. Cohen, T. E. Murphy, R. Roy, "Scalable parallel physical random number generator based on superluminescent LED," *Opt. Lett.*, vol. 36, pp.1020-1022, (2011).

[8] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of Fast Physical Random Bit Generation Using Chaotic Semiconductor Lasers," *IEEE J. Quantum Electron.*, vol.45, pp.1367–1379, (2009).

[9] 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," *Opt. Express*, vol.18, pp.5512–5524, (2010).

[10] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol.103, 024102, (2009).

[11] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photon.*, vol. 4, pp.58–61, (2010).

[12] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," *Opt. Express*, vol.18, pp.18763–18768 (2010).

[13] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast photonics non-deterministic random bit generator using on-chip chaos lasers," *Phys. Rev. A*, vol.83, 031803(R) (2011).

[14] A. Rukhin, et al, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22 Revision 1a, (2010). http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

[15] G. Marsaglia, DIEHARD: A battery of tests of randomness, (1996). http://stat.fsu.edu/geo