2009 International Symposium on Nonlinear Theory and its Applications
NOLTA'09, Sapporo, Japan, October 18-21, 2009

Characteristics of robust random bit generation using fast chaotic semiconductor lasers

Kunihito Hirano[1)], Kazuya Amano[1)], Atsushi Uchida[2)], Masaki Inoue[1)], Sunao Naito[1)], Shigeru Yoshimori[1)], Kazuyuki Yoshimura[3)], and Peter Davis[3)]

1) Department of Electronics and Computer Systems, Takushoku University,
815-1 Tatemachi, Hachioji, Tokyo, 193-0985, Japan
2) Department of Information and Computer Sciences, Saitama University,
255 Shimo-Ohkubo, Sakura-ku, Saitama City, Saitama, 338-8570, Japan
3) NTT Communication Science Laboratories, NTT Corporation,
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237,, Japan
Email: hirano.kunihito@gmail.com, auchida@mail.saitama-u.ac.jp

Abstract– We generate physical random bit sequences at the fast rate of 1 gigabit per second using two chaotic semiconductor lasers with external cavities. The bit sequences pass statistical tests of randomness. Bit sequences generated by binary sampling of the intensity of two independent chaotic lasers are combined using Exclusive-OR to obtain a single random sequence. We investigate the dependence of randomness of generated bit sequences on laser parameters. It is shown that randomness can be robustly achieved if the external cavity frequencies for the two lasers and the sampling clock frequency avoid low order incommensurate ratios.

1. Introduction

Random numbers are often used in the field of information security, such as codes, keys and challenges to ensure confidentiality, authenticity and integrity of information [1]. Future deployments of quantum cryptography systems will require the generation of trusted random numbers to select photon detection parameters [2-4]. Random numbers are also used for sampling in numerical computations to solve problems in many fields including materials science and biophysics [5].

The techniques of random-number generation can be classified into two categories: pseudo random-number generators and physical random-number generators. Pseudo-random numbers are generated from a single random seed using deterministic algorithms, and these are used in modern digital electronic information systems. However, sequences of pseudo-random numbers generated deterministically from the same seed will be identical, and this can cause serious problems for applications in security or parallel computation systems. Truly random numbers should be un-predictable, un-reproducible, and statistically unbiased. For this reason, physically random processes are often used as entropy sources in random number generators [6]. Random phenomena such as photon noise, thermal noise in resistors and frequency jitter of oscillators have been used as physical entropy sources for non-deterministic random number generation in combination with deterministic pseudo-random number generators [3,7,8]. However, non-deterministic generators have been limited to much slower rates than pseudo-random generators due to limitations of the rate and power of the mechanisms for extracting bits from physical noise. For example, typical rates are 10 megabit per second (Mbps) using electronic oscillator jitter [7], 40 Mbps using a set of interleaved chaotic maps [8], and 4 Mbps using quantum optical noise [3].

Recently, we have demonstrated that continuous streams of random bit sequences that pass standard tests of randomness are generated at fast rates of up to 1.7 gigabit per second (Gbps) by directly sampling the output of two chaotic semiconductor lasers with external cavities [9].

In this study, we investigate the dependence of the quality of random bit sequences on laser parameters in detail, in particular, external cavity frequency and clock frequency.

2. Experimental setup

Figure 1 shows our experimental setup for physical random number generation. We use two distributed-feedback (DFB) semiconductor lasers developed for optical fiber communications. The two lasers are called Laser 1 and 2, respectively. The injection current and the temperature of the semiconductor lasers are adjusted by a current-temperature controller. The optical wavelength of the lasers is precisely controlled by the temperature of the laser. We use space-optic components, rather than fiber optics as in Ref. [9], in order to investigate the parameter dependence of random number generation in detail.

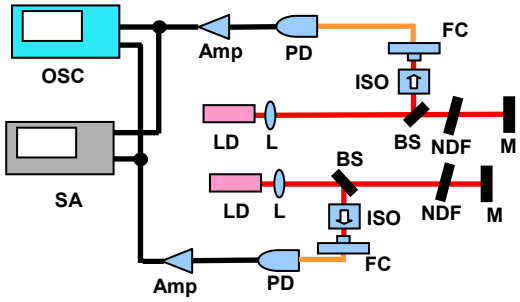

Fig. 1 Experimental setup for random bit generation using two chaotic semiconductor lasers with optical feedback.

3. Generation of random bit sequences

Our scheme of random bit generation with two independent chaotic semiconductor lasers is shown in Fig. 2. The output intensities of the two chaotic lasers are converted to electrical signals by photo-detectors, and sampled and stored by the digital oscilloscope. The digital oscilloscope acquires 8-bit samples of signal amplitude at 20 Giga samples per second (Gsps). We set a threshold value for each chaotic signal and sample the chaotic signal at the constant clock frequency of 1.0 GHz. We convert the sampled data to a binary signal (0 and 1) by comparing with the set threshold value for each chaotic signal. Note that the clock frequency (1.0 GHz) is slower than the dominant frequency of the chaotic waveforms (the dominant frequency of 3.0GHz) to avoid periodicity of chaotic signals. The two binary signals are combined by a logical Exclusive-OR (XOR) operation to generate a single random bit sequence. These processing steps are performed off-line, after the two chaotic waveforms are acquired by the digital oscilloscope, for the purpose of the investigation of the relationship between original chaotic waveforms and generated random bit sequences in detail.

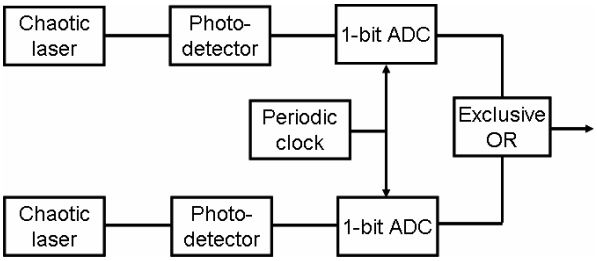

Fig. 2 Schematic diagram of random bit generation with two independent chaotic lasers.

The adjustment of the threshold values is important to obtain good-quality random bits with a proper balance of 0/1 ratio. Figure 3 shows the frequency (occurrence) of "0" of 1-Gbit random bit sequences as a function of the threshold value for Laser 1 and 2, respectively. The threshold for Laser 1 is first changed at the condition where a threshold value for Laser 2 is selected at around the mean value of the temporal waveform. Figure 3(a) indicates that the frequency of 0 is almost linearly decreased with the increase of the threshold value for Laser 1. We select the threshold for Laser 1 at the condition where the frequency of 0 becomes the closest value to 50%, i.e., V_{Th1} = 0.008 V in Fig. 3(a). We next change the threshold for Laser 2 with the selected threshold for Laser 1 (V_{Th1} = 0.008 V), as shown in Fig. 3(b). The frequency of 0 is decreased linearly as the threshold value for Laser 2 is increased, as well as Fig. 3(a). We then select the threshold value of V_{Th2} = 0.008 V to obtain the closest frequency to 50 %. This selection of the two threshold values results in the frequency of 0 of 49.996 % for the 1-Gbit random bit sequences.

It is worth noting that the resolution of vertical axis for Fig. 3(b) is higher than that for Fig. 3(a), and the slopes of Figs. 3(a) and 3(b) are -6.4 and -1.5 %/V, respectively. This indicates that the frequency of 0 adjusted by two threshold values for the two lasers is more precisely controllable than that adjusted by only one threshold value. The frequency of 0 for 1-Gbit random bit sequences must be set within the range of 50 ± 0.02 % (see the range between the dotted lines in Figs. 3(a) and 3(b)) to pass the frequency test in the NIST Special Publication 800-22 statistical test (see Section 4). Several data points exist within this range in Fig. 3(b). On the other hand, only one data point exists within this range in Figure 3(a). These results show that the use of two lasers and two threshold values enhances the controllability and robustness of the randomness.

Figure 4 shows an example of random bits plotted in two-dimensional plane. Bits "1" and "0" are converted into white and black dots, respectively, and placed from left to right (and from top to bottom). 500 by 500 bits are shown in Fig. 4.

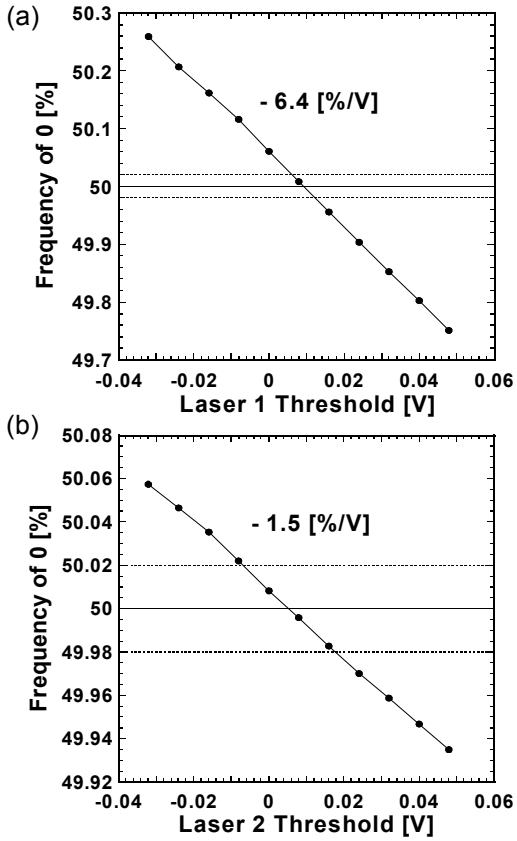

Fig. 3 Frequency (occurrence) of "0" of 1-Gbit random bit sequences as a function of the threshold value for (a) Laser 1 and (b) Laser 2.

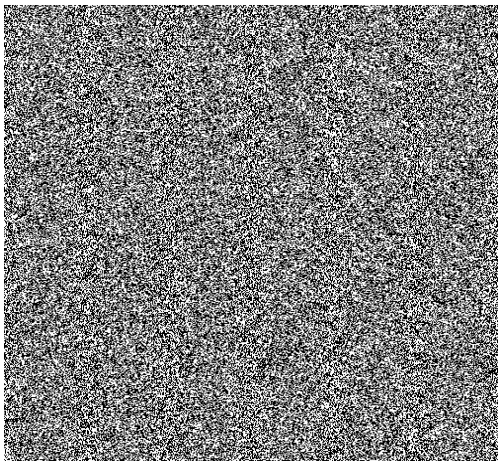

Fig. 4 Example of random bit sequence plotted in two-dimensional plane. Bits "1" and "0" are converted into white and black dots, respectively, and placed from left to right (and from top to bottom). 500 by 500 bits are shown.

4. Statistical evaluation of random bit sequences

To evaluate the randomness of digital bit sequences we use a standard statistical test suite for random number generators provided by National Institute of Standard Technology (NIST) test suite (NIST Special Publication 800-22) [10,11]. The test consists of 15 statistical tests, including frequency, runs, and entropy tests, as shown in Table 1. The tests are performed using 1000 instances of 1 Mbit sequences for all the NIST tests (the total amount of 1 Gbit data). Typical results of the NIST tests are shown in Table 1. For "success" using 1000 samples of 1Mbit data and 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 range of 0.99 ± 0.0094392 [10,11]. For the tests which produce multiple P-values and proportions, the worst case is shown in Table 1. We found that bit sequences obtained from the experiment pass all of the NIST SP 800-22 tests.

Table 1 Result of the NIST tests

STATISTICAL TEST	P-VALUE	PROPORTION	RESULT
frequency	0.058984	0.99000	SUCCESS
block-frequency	0.347257	0.99300	SUCCESS
cumulative-sums	0.917570	0.99100	SUCCESS
runs	0.048716	0.98800	SUCCESS
longest-run	0.846338	0.99200	SUCCESS
rank	0.595549	0.99000	SUCCESS
fft	0.228367	0.98900	SUCCESS
nonperiodic-templates	0.998474	0.99700	SUCCESS
overlapping-templates	0.410055	0.98600	SUCCESS
universal	0.968863	0.98700	SUCCESS
apen	0.169044	0.98500	SUCCESS
random-excursions	0.032518	0.09966	SUCCESS
random-excursions-variant	0.975708	0.99490	SUCCESS
serial	0.177628	0.98800	SUCCESS
linear-complexity	0.331408	0.99400	SUCCESS
total			15

5. Parameter dependence

We investigate the dependence of randomness of generated bit sequences on the laser parameters. We change the external cavity length of the two lasers. Table 2 shows the summary of the number of passed tests for NIST SP 800-22 at different combinations of the two external cavity lengths for the two lasers. "15" indicates that all the tests are passed. All of the 15 tests are passed for many combinations of the external cavity lengths, but not when the external cavity lengths are the same (diagonal components in Table 2) or when the lengths have the particular 1:2 combination of 1.4 and 2.8 m. In each case the 1/0 ratio was optimized by adjusting the threshold values.

Table 2 Number of passed tests for NIST SP 800-22 at different combinations of the two external cavity lengths.

	0.6 [m]	0.7 [m]	1.4 [m]	2.0 [m]	2.4 [m]	2.8 [m]	3.1 [m]
0.6 [m]	5	**15**	**15**	**15**	**15**	**15**	**15**
0.7 [m]	**15**	10	**15**	**15**	**15**	**15**	**15**
1.4 [m]	**15**	**15**	12	**15**	**15**	14	**15**
2.0 [m]	**15**	**15**	**15**	14	**15**	**15**	**15**
2.4 [m]	**15**	**15**	**15**	**15**	13	**15**	**15**
2.8 [m]	**15**	**15**	14	**15**	**15**	13	**15**
3.1 [m]	**15**	**15**	**15**	**15**	**15**	**15**	**15**

To explain the result of Table 2, we investigate the correlation function of the chaotic laser outputs and its corresponding digital bit sequences. Figure 5 shows the autocorrelation function of the two chaotic laser outputs and the corresponding random bit sequences as a function of delay time, when the external cavity lengths are set to different values (2.0 and 1.4 m) and the identical value (0.6 m). The autocorrelation function of chaotic laser outputs has two dominant peaks that correspond to the inverse of the relaxation oscillation frequency and the external cavity frequency as shown in Figs. 5(a) and 5(c). The inverse of the external cavity frequencies of the two lasers (13.35 ns and 9.30 ns) are incommensurate to each other. Figure 5(e) shows the autocorrelation function of the random bit sequences obtained from the two chaotic waveforms of Figs. 5(a) and 5(c) at the clock frequency of 1.0 GHz. There is no dominant peak in Figure 5(e) and all of the NIST tests are passed, according to Table 2. On the contrary, we set the same external cavity length of 0.6 m for the two lasers and plot the autocorrelation function as shown in Figs. 5(b) and 5(d). Both of the autocorrelation functions for the two lasers have a peak value around 4.0 ns, corresponding to the inverse of the external cavity

frequency. We generate random bit sequences by using these two chaotic waveforms of Figs. 5(b) and 5(d) and plot the autocorrelation function of the random bits in Fig. 5(f). A peak is observed at 4 bit, corresponding to the external-cavity round-trip delay time (4.0 ns) divided by the sampling time (1.0 ns). Since the external cavity lengths of the two lasers are set to the same value and the sampling time is low-order commensurate to the external-cavity delay time, the peak of autocorrelation remains at 4 bit in the generated random bits. These results show that the two external cavity frequencies and the clock frequency need to be set as incommensurate ratios to avoid the periodicity of random bit sequences.

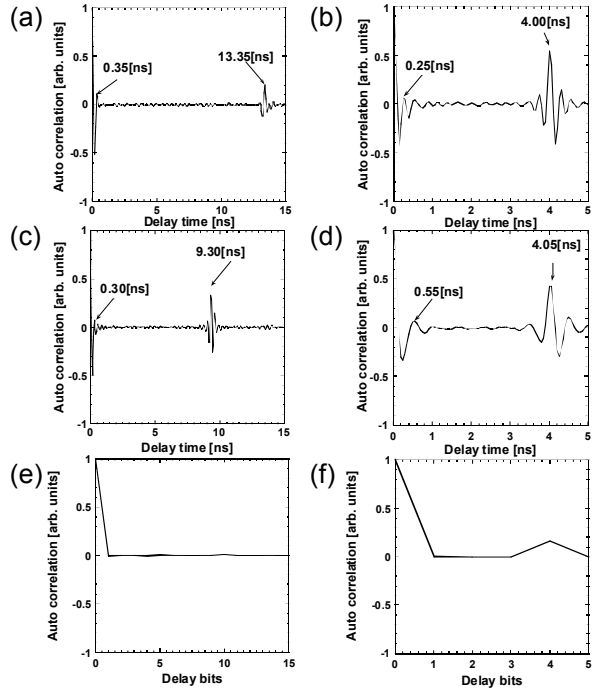

Fig. 5 Autocorrelation function of the two chaotic laser outputs and the corresponding random bit sequences as a function of delay time, when the external cavity lengths are set to (a), (c), (e) different values (L_1 = 2.0 m and L_2 = 1.4 m) and (b), (d), (f) the identical value ($L_1 = L_2$ = 0.6 m). (a), (b) Laser 1, (c), (d) Laser 2, (e), (f) Random bits.

6. Conclusion

We have investigated the characteristics of random bit generation using fast chaotic semiconductor lasers with external cavities. To generate random bits, the parameters of the two lasers are adjusted to detune the external cavity lengths so their frequency components and the sampling clock frequency are respectively incommensurate, and correlations are small. Finally, the levels of the threshold detectors are adjusted to equalize the ratio of 0 and 1 at the XOR output. With this procedure, we achieve physical random bit generation with a high speed of 1.0 Gbps. Randomness is verified by the standard statistical tests of NIST SP 800-22.

We show the dependence of the randomness on laser parameters. In particular, it is shown how the randomness can be robust if the external cavity frequencies for the two lasers and the clock frequency avoid low order incommensurate ratios. The use of optical fiber components may allow to assemble the whole system in a small package even for long external-cavity lengths.

The scheme of fast physical random bit generation with chaotic lasers is a new application of chaotic lasers to information technology. The performance of random number generation could be greatly improved by using chaotic laser devices as physical entropy sources.

Acknowledgments

A. U. acknowledges support from TEPCO Research Foundation, JGC-S Scholarship Foundation, and Grants-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science and Technology.

References

[1] Security requirements for cryptographic modules. FIPS 140-2 (2001)

[2] N. Gisin, G. Robordy, W. Tittel, and H. Zbinden, *Reviews of Modern Physics* **74,** 145-195 (2002).

[3] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.,* vol. 93, pp. 031109-1--031109-3, 2008.

[4] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29,** 2797 (2004).

[5] N. Metropolis and S. Ulam, *Journal of the American Statistical Association* **44,** 335-341 (1949).

[6] W. Schindler and W.Killmann, *CHES 2002, Lecture Notes in Computer Science* **2523** 431–449 (Springer-Verlag, Berlin Heidelberg) (2002).

[7] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, *IEEE Transactions on Computers* **52,** 403-409 (2003).

[8] S. Callegari, R. Rovatti, and G. Setti, *IEEE Trans. Signal Processing* **53,** 793-805 (2005).

[9] 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, *Nature Photonics,* vol.2, no.12, pp.728-732 (2008).

[10] A. Rukhin, et al., National Institute of Standards and Technology, Special Publication 800-22 Revision 1 (2008).

[11] S. J. Kim, K. Umeno, and A. Hasegawa, *arXiv:nlin.CD/0401040v1* (2004).