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

Experiment on fast physical random bit generation with bandwidth-enhanced chaotic semiconductor lasers

Taiki Yamazaki†, Yasuhiro Akizawa†, Shinichiro Morikatsu†, Hiroki Aida†, Atsushi Uchida†,
Takahisa Harayama‡, Satoshi Sunada‡, Ken-ichi Arai‡, Kazuyuki Yoshimura‡, and Peter Davis‡

†Department of Information and Computer Sciences, Saitama University,
255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama, 338-8570, Japan
‡NTT Communication Science Laboratories, NTT Corporation,
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237, Japan
Emails: {s10mm332, auchida}@mail.saitama-u.ac.jp

Abstract– We experimentally demonstrate random bit generation using multi-bit samples of bandwidth-enhanced chaos in semiconductor lasers. Chaotic fluctuation of laser output is generated in a semiconductor laser with optical feedback and the chaotic output is injected into a second semiconductor laser to obtain a chaotic intensity signal with bandwidth enhanced up to 16 GHz. The chaotic signal is converted to an 8-bit digital signal by sampling with a digital oscilloscope at 12.5 Giga samples per second (GS/s). Random bits are generated by bitwise exclusive-OR operation on corresponding bits in samples of the chaotic signal and its time-delayed signal. Statistical tests verify the randomness of bit sequences obtained using 1 to 6 bits per sample, corresponding to fast random bit generation rates from 12.5 to 75 Gigabit per second (Gb/s) (= 6 bit × 12.5 GS/s).

1. Introduction

Random numbers are widely used in communication and computing, such as information security, quantum cryptography system and computer simulations. The techniques of random number generation can be classified into two categories: deterministic pseudorandom number generators and non-deterministic physical random number generators. Deterministic pseudorandom number sequences are generated from a single random seed using deterministic algorithms. However, sequences of pseudorandom 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 non-deterministic random number generators. 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 pseudorandom number generators.

Recently, several non-deterministic physical random number generators have been demonstrated with generation rates exceeding gigabit per second (Gb/s) using the outputs of chaotic semiconductor lasers with optical feedback [1-7] and amplified spontaneous emission from an optical noise source [8,9]. It is an ongoing challenge to increase the speed of non-deterministic physical random number generators and to develop bit extraction mechanisms which increase the random bit generation capacity.

In this study we experimentally demonstrate the generation of random bits by using bandwidth-enhanced chaos in semiconductor lasers [5]. Chaotic fluctuation of laser output is generated in a semiconductor laser with optical feedback and the chaotic output is injected into a second semiconductor laser for bandwidth enhancement [10-12]. Random bit sequences are generated by bitwise exclusive-OR operation on corresponding bits in samples of the bandwidth-enhanced chaotic signal and its time-delayed signal.

2. Experimental setup

Figure 1 shows our experimental setup for fast physical random bit generation [5]. We used two distributed-feedback (DFB) semiconductor lasers. One laser (referred to as Laser 1) was used for the generation of chaotic intensity fluctuations induced by optical feedback. The other laser (referred to as Laser 2) was used for the bandwidth enhancement of chaotic waveforms. Laser 1 was connected to a fiber coupler and a variable fiber reflector which reflects a fraction of the light back into the laser, inducing high-frequency chaotic oscillations of the optical intensity. The amount of the optical feedback light was adjusted by the variable fiber reflector. On the other hand, there was no optical feedback for Laser 2.

A portion of the chaotic Laser 1 beam was injected into Laser 2. Two optical isolators were used to achieve one-way coupling from Laser 1 to Laser 2. The wavelengths of Laser 1 and 2 were precisely adjusted in order to generate bandwidth-enhanced chaotic output of Laser 2. A portion of Laser 2 output was extracted by a fiber coupler, and divided into two beams by another fiber coupler. An extra optical fiber (1-meter length) was inserted into one of the optical paths after the two beams were divided, so that a chaotic waveform and its time-delayed signal (5.0 nanosecond delay) could be detected by two photodetectors. The converted electric signal at the photodetectors were amplified by electric amplifiers and sent to a digital oscilloscope and a radio-frequency (RF) spectrum analyzer to observe temporal waveforms and the corresponding RF spectra, respectively.

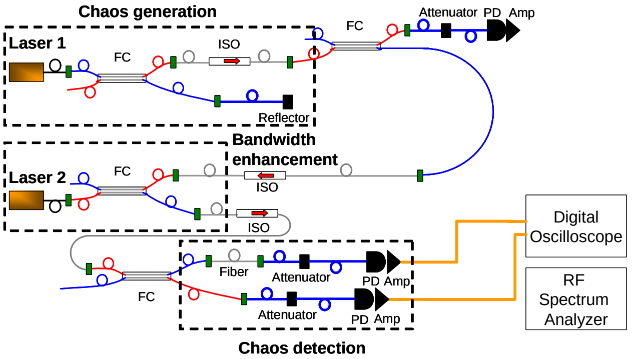


Fig. 1 Experimental setup for random bit generation with bandwidth-enhanced chaotic semiconductor lasers. Amp: electric amplifier, FC: fiber coupler, ISO: optical isolator, PD: photodetector.

3. Experimental results

3.1. Bandwidth enhancement of chaos

We set the relaxation oscillation frequencies to be 6.5 GHz for both Laser 1 and 2 by adjusting the injection current of the lasers. These values were close to the maximum relaxation oscillation frequencies that can be observed for solitary lasers in the experiment. To enhance the bandwidth of chaos, we detuned the optical wavelength of Laser 2 to the positive direction with respect to that of Laser 1, i.e., we set the optical wavelength to be 1547.585 nm for Laser 1 and 1547.677 nm for Laser 2, by controlling the temperature of the two lasers. The optical wavelength for Laser 2 was shifted to 1547.718 nm due to the presence of the optical injection from Laser 1. The optical wavelength detuning was defined as $\Delta\lambda = \lambda_2 - \lambda_1$, where λ_1 and λ_2 indicate the optical wavelengths of Laser 1 and 2 in the presence of the optical injection, respectively. $\Delta\lambda$ was set to 0.133 nm (16.6 GHz in frequency), which corresponds to the positive detuning condition in the literature [11]. The existence of the frequency component corresponding to the optical wavelength detuning is crucial for the bandwidth enhancement of the laser chaos [12]; it results in nonlinear frequency mixing between the optical wavelength detuning and the relaxation oscillation frequency of the laser.

Figures 2(a) and 2(b) show the RF spectra of Laser 1 and 2. The RF spectra in Figures 2(a) and 2(b) show bandwidth enhancement of Laser 2 by the optical injection of the Laser 1 output, where the center frequencies of Laser 1 and 2 are 6.6 and 16.1 GHz, respectively. We define the bandwidth of the chaotic signals as the frequency band starting at zero frequency and containing 80% of spectrum power [10,12]. The bandwidth of Laser 1 and 2 are 9.5 and 16.1 GHz, respectively. The bandwidth enhancement of chaotic signals is achieved up to approximately 16 GHz by optical injection of chaotic signal. It can also be seen that the RF spectrum of the output of Laser 2, shown in Fig. 2(b), is much flatter than that of Laser 1 in Fig. 2(a). Flatness of the RF spectrum is advantageous for the generation of random bit sequences [5]. The enhancement of chaos bandwidth up to 16 GHz enables to generate random bit sequences by sampling at the rate of 12.5 GS/s.

Figure 2(c) shows the temporal waveform of the Laser 2 output and the same output optically delayed by 5.0 ns, as detected by the two photodetectors. These two chaotic signals are used for the generation of random bit sequences. The temporal waveforms of the AC-signals from the photodetectors are detected using a dual-channel 8-bit oscilloscope sampling at 12.5 GS/s, with the 8-bit range adjusted symmetrically to ±2 standard-deviations of the signal amplitude. The match between the signal amplitudes and the range of the 8-bit detectors in the oscilloscope was adjusted using the optical attenuators.

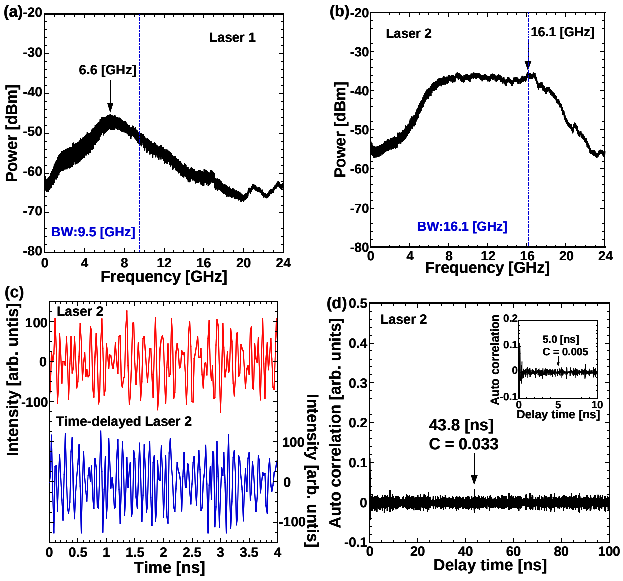


Fig. 2 (a) RF spectrum of Laser 1, (b) RF spectrum of Laser 2, (c) temporal waveforms of Laser 2 output and the same output optically delayed in time (5.0 ns delay), and (d) autocorrelation function of the temporal waveform of Laser 2 output. The inset is the enlargement of (d). (a), (b) BW: bandwidth.

The autocorrelation function of the Laser 2 output is shown in Fig. 2(d). The peak of the autocorrelation appears at 43.8 ns, corresponding to the round-trip time of the external cavity for Laser 1. The peak value of the autocorrelation function at 43.8ns is only 0.033, showing that periodicity due to the external cavity of the Laser 1 is suppressed in the Laser 2 output. We note that the correlation is 0.005 at the time of 5.0 ns corresponding to the delay between the two detected signals, as shown in the inset of Fig. 2(d).

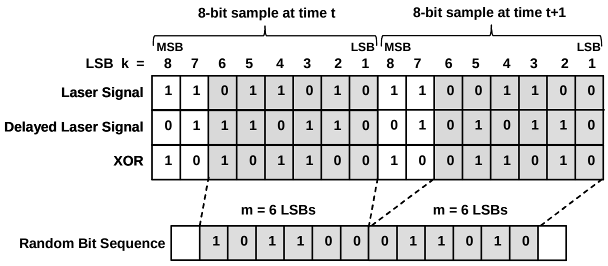
3.2. Generation of random bits

We generate random bits using two chaotic waveforms; the output of Laser 2 and the output of Laser 2 optically delayed by 5.0 ns. The two chaotic optical signals are detected by AC-coupled photodetectors, amplified and converted to digital 8-bit signals by a dual channel oscilloscope sampling at 12.5 GS/s per channel. Corresponding pairs of bits in the two 8-bit digital signals are combined by bitwise exclusive-OR (XOR) operation, giving a single 8-bit digital signal. A subset of *m* least significant bits (LSBs) from each sample are then selected and interleaved to generate a single bit sequence [5], which can be specified as follows:

$\ldots, s_m(t), s_{m-1}(t), \ldots, s_1(t), s_m(t+1), s_{m-1}(t+1), \ldots, s_1(t+1), \ldots$

where $s_k = 0$ or 1 $(k = 1, 2, \ldots, m)$ is the *k*-th LSB of the selected *m* LSBs. The method is illustrated in Fig. 3.

In our experimental system, the XOR operation and bit interleave are done off-line after acquisition by the oscilloscope. The record length of each continual data frame acquired by the oscilloscope is 1M samples. 1000 frames are recorded for each channel to obtain sufficient data for the statistical tests of randomness.



LSB k =	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
Laser Signal	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0
Delayed Laser Signal	0	1	1	1	0	1	1	0	0	1	0	1	0	1	1	0
XOR	1	0	1	0	1	1	0	0	1	0	0	1	1	0	1	0

Random Bit Sequence		1	0	1	1	0	0	0	1	1	0	1	0	

Fig. 3 Method for generating a random bit sequence using multiple (*m* = 1,…, 8) significant bits. Example for *m* = 6. LSB, least significant bit; MSB, most significant bit; XOR, exclusive-OR operation.

The randomness of obtained random bit sequences was tested using a standard statistical test suite for random number generators provided by the National Institute of Standards Technology (NIST), known as NIST Special Publication 800-22 (NIST SP 800-22) [13,14]. The NIST SP 800-22 test consists of 15 statistical tests as shown in Table 1. The tests are performed using 1000 samples of 1 Mbit sequences and the significance level $\alpha = 0.01$ [13].

Typical results of the NIST tests are shown in Table 1 for a set of sequences generated using 6 consecutive LSBs (see Fig. 3). We confirmed that random bit sequences obtained from the bandwidth-enhanced chaos by 8-bit sampling at 12.5 GS/s are sufficiently random that they pass all the statistical tests of NIST SP 800-22. Moreover, sequences obtained by interleaving up to 6 consecutive LSBs at each sample also passed the statistical tests of randomness. These results correspond to random bit generation rates from 12.5 to 75 Gb/s (= 6 bit × 12.5 GS/s).

Table 1 Result of the NIST SP 800-22 tests.

STATISTICAL TEST	P-VALUE	PROPORTION	RESULT
frequency	0.219006	0.9880	SUCCESS
block-frequency	0.000387	0.9860	SUCCESS
cumulative-sums	0.572847	0.9870	SUCCESS
runs	0.000550	0.9860	SUCCESS
longest-run	0.917870	0.9900	SUCCESS
rank	0.440975	0.9910	SUCCESS
fft	0.933472	0.9860	SUCCESS
nonperiodic-templates	0.013856	0.9810	SUCCESS
overlapping-templates	0.777265	0.9890	SUCCESS
universal	0.518106	0.9880	SUCCESS
apen	0.087692	0.9910	SUCCESS
random-excursions	0.013411	0.9868	SUCCESS
random-excursions-variant	0.112047	0.9851	SUCCESS
serial	0.162606	0.9870	SUCCESS
linear-complexity	0.989425	0.9900	SUCCESS
Total			15

4. Statistical characteristics of random bits

We investigate the dependence of the randomness test performance on the number of LSBs used. Figure 4 shows the number of passed NIST SP 800-22 tests as a function of the number of LSBs. The number of LSBs is increased from “1”, corresponding to just the LSB, to “8” corresponding to all bits including the MSB. All the 15 tests are passed when the number of LSBs is set to a value between 1 and 6. In the case of 7 LSBs, only 13 tests are passed. For 8 LSBs, only 7 tests are passed. The maximum length of LSBs used for random bits that pass all the NIST tests is 6 LSBs. The use of 6 LSBs obtained at the sampling rate of 12.5 GS/s corresponds to the generation rate of 75 Gb/s.

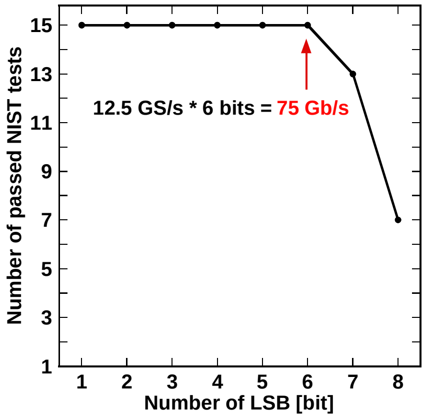


Fig. 4 The number of passed NIST SP 800-22 tests as a function of the number of least significant bits (LSBs) used to generate the bit sequence. “15” indicates that all the tests are passed.

Next we investigate the probability density function of multi-bit states obtained from various LSBs. Figure 5(a) shows the distribution for 8-bit samples from one chaotic waveform. Figure 5(b) shows the distribution of 8-bit XOR samples after bitwise XOR of 8-bit samples from a chaotic waveform and the delayed waveform. The distribution becomes more uniform, but there are some discontinuities in the distribution of Fig. 5(b). When only 7 LSBs of the 8-bit XOR data are selected (Fig. 5(c)), the distribution becomes flatter. In the case of 6 LSBs of the 8-bit XOR data (Fig. 5(d)), the distribution appears almost uniform. From these results, randomness of generated bit sequence improves by decreasing the number of LSBs.

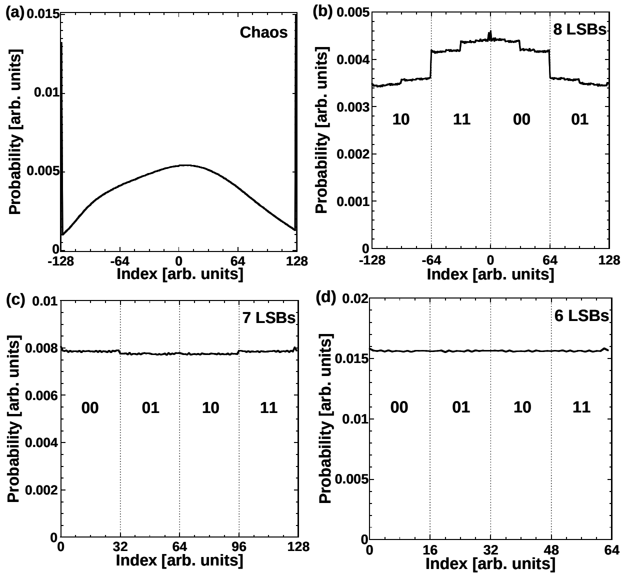


Fig. 5 Probability density functions for (a) 8-bit digitized chaotic waveform, (b) 8-bit random bits after bitwise XOR operation is applied to the two 8-bit digitized chaotic waveforms, (c) 7 LSBs selected from the 8-bit XOR data, and (d) 6 LSBs selected from the 8-bit XOR data. The two-bit labels shown in Figs. 5(b)-5(d) indicate the first two most significant bits (MSBs) of the data generated from *m* LSBs.

5. Conclusion

We have experimentally demonstrated a method for physical random bit generation using bandwidth-enhanced chaos in semiconductor lasers. Bandwidth-enhanced chaos is realized by taking the chaotic light from a semiconductor laser with optical feedback and injecting it into a second semiconductor laser. We have used this technique to achieve chaotic laser signals with bandwidth enhanced up to 16 GHz. In the experiment, we used a high-speed digital oscilloscope to record 8-bit samples at 12.5 GS/s simultaneously on two channels from a chaotic laser signal and its time-delayed signal. Random bits are then obtained by bitwise XOR operation on corresponding bits of the two digital signals. Sequences obtained by interleaving up to 6 LSBs passed the statistical tests of randomness. These results correspond to random bit generation rates from 12.5 to 75 Gb/s (= 6 bit × 12.5 GS/s). We also show the dependence of the randomness test performance on the number of LSBs used, and it is found that up to 6 LSBs can be combined to create sequences which pass the statistical tests of randomness.

Chaotic laser devices can be fast and reliable sources of physical entropy for fast physical random number generators for the applications in computing and information security.

Acknowledgments

We acknowledge support from TEPCO Research Foundation and Grant-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science and Technology in Japan.

References

[1] 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).

[2] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Physical Review Letters, Vol. 103, no. 2, pp. 024102-1-4 (2009).

[3] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, IEEE Journal of Quantum Electron., Vol. 45, no. 11, pp. 1367-1379 (2009).

[4] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nature Photonics, Vol. 4, pp.58-61, (2010).

[5] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, Optics Express, Vol. 18, no. 6, pp. 5512-5524 (2010).

[6] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, Optics Express, Vol. 18, no. 18, pp. 18763-18768 (2010).

[7] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, Physical Review A, Vol. 83, pp. 031803(R)-1-4 (2011).

[8] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Optics Express, Vol. 18, no. 23, pp. 23584-23597 (2010).

[9] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Optics Letters, Vol. 36, no.6, pp. 1020-1022 (2011).

[10] F. Y. Lin and J. M. Liu, Optics Communications, Vol. 221, no. 1-3, pp 173-180 (2003).

[11] J. Ohtsubo, "Semiconductor Lasers, -Stability, Instability and Chaos-," Second Ed., Springer-Verlag, Berlin Heidelberg (2008).

[12] H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, Optics Express, Vol. 17, no. 22, pp. 19536-19543 (2009).

[13] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. E. Bassham III, National Institute of Standards and Technology, Special Publication 800-22 Revision 1a (2010).

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