Post-processing method for fast random bit generation with semiconductor lasers

Yasuhiro Akizawa †, Taiki Yamazaki †, 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: {s11mm301, auchida}@mail.saitama-u.ac.jp

Abstract– We propose a post-processing method for fast random bit generation with chaotic semiconductor lasers. Chaotic laser output and its time-delayed signal are sampled and converted into 8 bit values. The order of the 8 bit sequence of the time-delayed signal is reversed and bitwise exclusive-or operation is executed between the bit-order-reversed signal and the original chaotic signal, resulting in random bit sequences. For the proposed post-processing method, it is not necessary to extract the least significant bit from random bits to obtain good-quality random bit sequences. Experiments with off-line post-processing indicate that the equivalent generation rate of random bit sequences can be achieved up to 400 Giga bit per second (Gb/s) (8 bit/sample × 50 Gigasample/second). The randomness of the generated bit sequences are tested by using statistical tests of randomness. We investigate the bias of each significant bit and it is found that the proposed post-processing method can succeed in generating uniform distribution of the bias of each significant bit.

1. Introduction

Random numbers play extremely significant role in the cryptographic technology and large scale simulation such as Monte Carlo method [1]. The generation techniques of random numbers can be classified into two types: deterministic pseudorandom number generation and non-deterministic physical random-number generation. Pseudorandom numbers can be generated by a deterministic algorithm and seeds (initial conditions) implemented using digital logic, and fast generation of pseudorandom numbers can be achieved, determined by clock speed of digital circuits. However, pseudorandom number sequences have periodicity and reproducibility, which can be a weakness for applications in information security. On the other hand, non-deterministic physical random number sequences have aperiodicity and un-reproducibility because they are generated by non-deterministic physical phenomena. However, the generation speed of physical random numbers devices has been limited at hundreds of Megabit per second (Mb/s) due to the limitation of randomness extraction speed. Fast physical random number generators are required for new types of security systems such as quantum cryptography [2] and information-theoretic security [3] as well as large scale numerical computations [1].

Recently, new techniques for physical random number generators that utilize chaotic semiconductor laser to generate random bits at the speed of more than 1 Gigabit per second (Gb/s) has been introduced and demonstrated experimentally [4-8]. The generation speed of a physical random number generator has been reported at 1.7 Gb/s in real time using 1-bit analog-to-digital converters (ADCs) and a 1-bit exclusive-OR (XOR) gate for post-processing [4]. Moreover, random bit generators using chaotic lasers with the equivalent generation rates ranging from 12.5 ~ 300 Gb/s have been reported by using multi-bit ADCs and off-line post processing methods [5-8]. These multi-bit post-processing methods require the elimination of some of the most significant bits (MSBs) to generate uniformly distributed multi-bit random sequences, which can cause the reduction of the generation rates [5-8]. Developing more effective post-processing techniques without MSB elimination are important for implementing fast random bit generators with chaotic lasers from an engineering point of view.

In this study we propose a new post-processing method for a fast random bit generator with chaotic semiconductor lasers. A chaotic signal and its time-delayed signal are sampled by 8-bit ADCs and the order of 8-bit sequences of the time-delayed signal is reversed. Bitwise XOR operation is carried out between the bit-order-reversed signal and the original chaotic signal to generate random bit sequences. The equivalent generation rate up to 400 Gb/s is demonstrated in an experiment with the post-processing done off-line.

2. Random bit generation with post-processing

Random bit sequences can be generated from a temporal waveform of bandwidth-enhanced chaotic signal and its time-delayed signal [6]. Figure 1(a) shows the scheme of random bit generation with the proposed post-processing method. The output of a chaotic semiconductor laser with optical feedback is injected into another semiconductor laser which has no optical feedback. The

bandwidth of the injected chaotic semiconductor laser is enhanced due to the optical injection. The output of the bandwidth-enhanced chaotic laser is detected and converted into an electric signal by photodetector. The electric chaotic signal is divided into two signals, and one signal is electrically time-delayed through an additional transmission line. The two chaotic signals are sampled and converted into 8 bits value by an 8-bit analog-to-digital converter (ADC).

The obtained 8-bit sequences and the post-processing procedure are shown in the step 1 of Fig. 1(b). We call the 8-bit chaotic signal "Ch1" and its time-delayed signal "Ch2", respectively. In the step 2 of Fig. 1(b), the order of 8-bit sequence of the Ch2 signal is reversed for each sampling point, i.e., the 8-bit sequence $a_8a_7\ldots a_1$ is changed to $a_1a_2\ldots a_8$, where a_i is the i-th significant bit of the 8-bit sequence. The reversed 8-bit Ch2 signal is referred to as $Ch2^R$. In step 3, bitwise XOR operation is carried out between the Ch1 and $Ch2^R$ signals at each sampling point, and random bit sequences are generated. It is worth noting that no elimination of some of MSBs is required for the proposed post-processing method, unlike for the previous methods [5-8]. The random bit sequence generated by this post-processing method is referred to as Ch1 XOR $Ch2^R$.

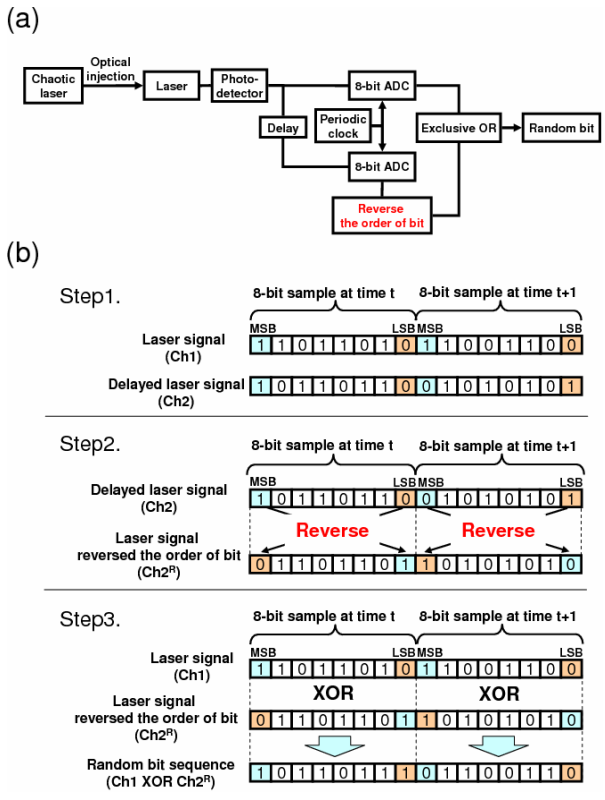

Fig. 1 (a) Scheme of random bit generation. (b) Detail steps of the proposed post-processing method.

Table 1 Result of the NIST SP 800-22 tests. The P-value should be larger than 0.0001, and the proportion should be in the range of 0.99 ± 0.0094392 to pass the tests. For the tests which produce multiple P-values and proportions, the worst case is shown.

STATISTICAL TEST	P-value	Proportion	RESULT
frequency	0.709558	0.9910	SUCCESS
block-frequency	0.193767	0.9920	SUCCESS
cumulative-sums	0.399442	0.9920	SUCCESS
runs	0.928857	0.9820	SUCCESS
longest-run	0.388990	0.9840	SUCCESS
rank	0.970302	0.9930	SUCCESS
fft	0.836048	0.9810	SUCCESS
nonoverlapping-templates	0.003322	0.9820	SUCCESS
overlapping-templates	0.548314	0.9860	SUCCESS
universal	0.275709	0.9850	SUCCESS
apen	0.348869	0.9880	SUCCESS
random-excursions	0.122900	0.9825	SUCCESS
random-excursions-variant	0.002748	0.9809	SUCCESS
serial	0.027313	0.9930	SUCCESS
linear-complexity	0.397688	0.9910	SUCCESS
Total			15

Table 2 Result of the Diehard tests. "KS" indicates the Kolmogorov-Smirnov (KS) test. For the tests which produce multiple P-values without the KS test, the worst case is shown.

STATISTICAL TEST	P-VALUE	RESULT	
birthday spacing	0.038946	SUCCESS	KS
overlapping 5-permutation test	0.688794	SUCCESS	
binary rand test for 31 × 31 matrices	0.922511	SUCCESS	
binary rand test for 32 × 32 matrices	0.555641	SUCCESS	
binary rand test for 8 × 6 matrices	0.115215	SUCCESS	KS
bitstream test	0.005530	SUCCESS	
overlapping-pairs-space-occupancy test	0.012400	SUCCESS	
overlapping-quadruples-space-occupancy test	0.004800	SUCCESS	
DNA test	0.005300	SUCCESS	
count-the-1's test on a stream of bytes	0.614364	SUCCESS	
count-the-1's test for specific bytes	0.008804	SUCCESS	
parking lot test	0.666387	SUCCESS	KS
minimum distance test	0.632756	SUCCESS	KS
3D-spheres test	0.961739	SUCCESS	KS
squeeze test	0.707630	SUCCESS	
overlapping sums test	0.139870	SUCCESS	KS
runs test	0.075993	SUCCESS	KS
craps test	0.436289	SUCCESS	
Total			18

3. Result of random bit generation

3.1. Statistical tests of randomness

A random bit sequence is generated at the rate of 50 Gigasample per second (GS/s) in the off-line post processing. The equivalent generation rate of the random bit is 400 Gb/s (= 8 bit × 50 GS/s). In order to evaluate the randomness of the generated bit sequences, we use de-facto standard statistical tests of randomness: National Institute of Standard Technology Special Publication 800-22 (NIST SP 800-22) and Diehard tests [9,10].

Table 1 shows the result of NIST SP 800-22 for the generated random bit sequences. The NIST SP 800-22 test consists of 15 statistical tests as shown in Table 1. The tests are performed by using 1000 samples of 1-Mbit sequences with the significance level of $\alpha = 0.01$. The generated random bits pass all the NIST SP 800-22 tests as shown in Table 1.

Table 2 shows the result of Diehard tests for the generated random bit sequences. The Diehard tests is performed by using a 74-Mbit sequence. The significance level of $\alpha = 0.01$ is used for the Diehard tests. The generated random bits pass all the Diehard tests as shown in Table 2. Therefore, we found that the random bit sequence generated by the proposed post-processing method can pass all the statistical tests of NIST SP 800-22 and Diehard.

3.2. Histogram of generated bit sequences

We investigate the histogram of the 8-bit chaotic signal and the signal generated after the XOR operation. Figures 2(a) and 2(b) show the 8-bit histogram of the chaotic signal (Ch1) and its time-delayed signal (Ch2), respectively. Figure 2(c) shows the 8-bit histogram of the bit-order-reversed signal ($Ch2^R$). Figure 2(d) shows the histogram of random bit sequence generated by two post-processing methods. One is the proposed post-processing method shown in Fig. 1 (referred to as Ch1 XOR $Ch2^R$). For the other method, only bitwise exclusive-or between Ch1 and Ch2 is used (referred to as Ch1 XOR Ch2) [6]. In Fig. 2(d), the histogram of Ch1 XOR $Ch2^R$ is more uniform than that of Ch1 XOR Ch2. This result supports the fact that the random bit sequences generated by the proposed post-processing method (Ch1 XOR $Ch2^R$) pass all the statistical tests as shown in Tables 1 and 2.

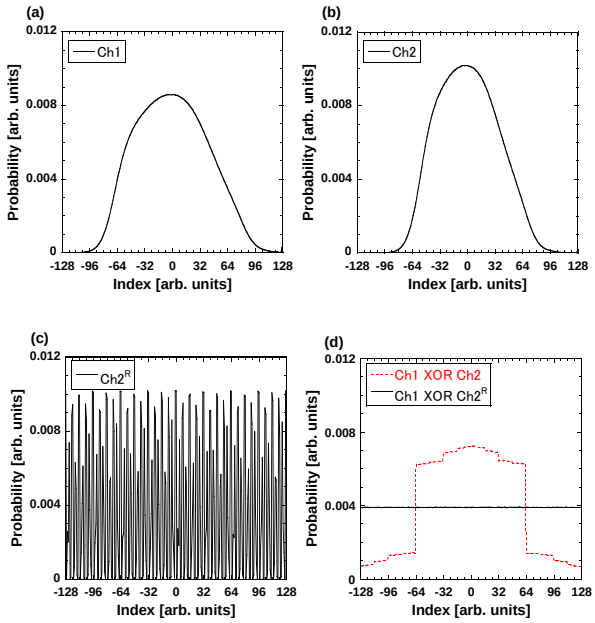

Fig. 2 Histogram of 8-bit sequences. (a) Chaotic signal (Ch1), (b) time-delayed chaotic signal (Ch2), (c) bit-order-reversed time-delayed signal ($Ch2^R$), and (d) random bits generated by the methods of Ch1 XOR $Ch2^R$ (solid curve) and Ch1 XOR Ch2 (dotted curve).

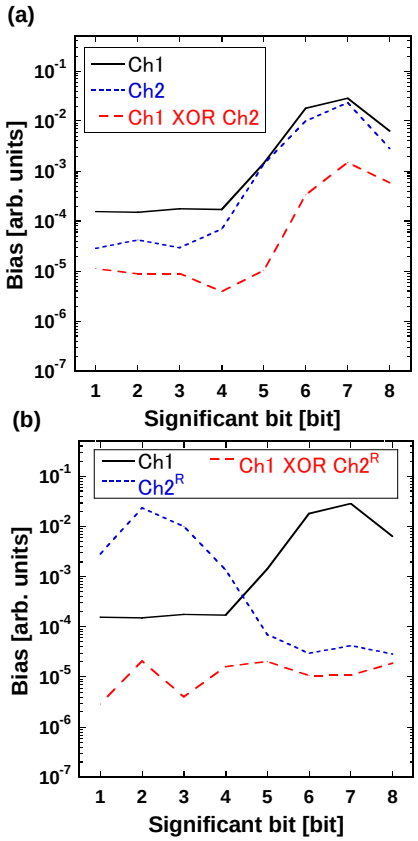

Fig. 3 Bias of each significant bit for Ch1, Ch2, and $Ch2^R$ signals. The post-processing methods of (a) Ch1 XOR Ch2 and (b) Ch1 XOR $Ch2^R$ are used.

3.3. Bias of significant bit

In order to investigate the effect of the post-processing, we examine the "bias" of significant bit. The bias of i-th ($i = 1,\ldots,8$) significant bit b_i can be defined as the following equation,

$$b_i = \left|0.5 - P_i\right|. \qquad (1)$$

where P_i represents the probability of the occurrence of bits 1 for the i-th significant bit. Larger bias of a bit means less randomness.

Figure 3 shows the bias of the significant bit of the two chaotic signals and the multi-bit sequences generated by the two post-processing methods of Ch1 XOR Ch2 (Fig. 3(a)) and Ch1 XOR $Ch2^R$ (Fig. 3(b)). The bias of significant bit is calculated by using 1-Gbit sequences for each significant bit. In Fig. 3(a), the original chaotic signals have different bias for each significant bit. It is found that a higher-order (larger i) significant bit has larger bias, except the MSB ($i = 8$). After the XOR operation, this characteristic remains for the bias of the bits generated by Ch1 XOR Ch2, even though the bias becomes smaller, as shown in Fig. 3(a). Larger bias for

some MSBs needs to be eliminated to produce good-quality random numbers, as in the previous post-processing methods [5-8]. On the contrary, the bias of the bit-order-reversed signal $Ch2^R$ shows the opposite bias distribution, where a lower-order (smaller *i*) significant bit has larger bias, as shown in Fig. 3(b). Due to the XOR operation between Ch1 and $Ch2^R$, the bias of the output bits are reduced and a more uniform distribution is obtained after the post-processing of Ch1 XOR $Ch2^R$, as shown in Fig. 3(b). The bias of each significant bit for the sequences generated by Ch1 XOR $Ch2^R$ is thus very small ($\sim 10^{-5}$) and more uniformly distributed than the bias for the original chaotic signal.

4. Conclusion

We have proposed a post-processing method for fast random bit generation with chaotic semiconductor lasers. Chaotic laser output and its time-delayed signal are sampled and converted into 8 bit values. The order of the 8 bit sequence of the time-delayed signal is reversed and bitwise XOR operation is executed between the bit-order-reversed signal and the original chaotic signal, resulting in random bit sequences. For the proposed post-processing method, no elimination of some of MSBs is required to obtain good-quality random bit sequences, unlike previous techniques. The equivalent generation rate of random bit sequences can be achieved up to 400 Gb/s (= 8 bit × 50 GS/s). The randomness of the generated bit sequences are tested by using the statistical tests of randomness. We investigate the bias of each significant bit of random bit sequences and found that the proposed post-processing method can succeed in generating almost uniform distribution of the bias for each significant bit.

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] N. Metropolis, and S. Ulam, "The Monte Carlo method," *Journal of the American Statistical Association*, Vol. 44, pp. 335-341 (1949).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Review of Modern Physics*, Vol. 74, No. 1, pp. 145-195 (2002).
[3] J. Muramatsu, K. Yoshimura, and P. Davis, *Lecture Notes in Computer Science,* Vol. 5973, pp. 128-139 (2010).
[4] 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, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, Vol. 2, no. 12, pp. 728-732 (2008).
[5] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Physical Review Letters*, Vol. 103, no. 2, pp. 024102-1-024102-4 (2009).
[6] 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," *Optics Express*, Vol. 18, no. 6, pp. 5512-5524 (2010).
[7] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photonics*, Vol. 4, pp.58-61, (2010).
[8] 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," *Optics Express*, Vol. 18, no. 18, pp. 18763-18768 (2010).
[9] 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, "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).
URL:http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf
[10] G. Marsaglia, "The Marsaglia random number CD-ROM including the Diehard battery of tests of randomness," (1995).
URL: http://www.stat.fsu.edu/pub/diehard/