2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Fast physical random bit generation using a photonic integrated circuit

Yuta Terashima[1], Kazusa Ugajin[1], Atsushi Uchida[1], Takahisa Harayama[2,3] and Kazuyuki Yoshimura[2,4]

[1] Department of Information and Computer Sciences, Saitama University
255 Shimo-Okubo Sakura-ku, Saitama City, Saitama 338-8570, Japan
[2] NTT Communication Science Laboratories, NTT Corporation
3-1 Morinosato, Wakamiya, Atsugi-Shi, Kanagawa 243-0198, Japan
[3] Department of Applied Physics, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, Japan
[4]Department of Information and Electronics Graduate school of Engineering, Tottori University
4-101 Koyama-Minami, Tottori 680-8552, Japan
Emails: s15mm318@mail.saitama-u.ac.jp, auchida@mail.saitama-u.ac.jp

Abstract—We propose random bit generation by using laser chaos generated from a photonic integrated circuit. We obtain smooth and symmetrical distribution of the amplitude of a chaotic temporal waveform by using a differential method. We generate random bit sequence by applying the differential method and XOR-operation, and the generated bits pass all of the NIST Special Publication 800-22 tests and TestU01 tests.

1. Introduction

Random number generation based on physical phenomena is useful for information security and cryptographic communication. Recently, random number generation using chaotic semiconductor lasers has been intensively investigated and high generation rates over Gigabit per second (Gb/s) have been reported [1–6]. In these systems, chaotic generators are usually composed of several devices such as a laser, a photodetector, and an external mirror. Therefore, photonic integrated circuits (PICs) have been proposed to reduce the size of physical random number generators [2, 3].

The statistical histogram of chaotic signals typically shows asymmetric distribution for laser-chaos-based random bit generation. The quality of the randomness of the random numbers generated from the chaotic signal is degraded due to the asymmetric distribution. To solve this problem, a differential method has been proposed to produce symmetric statistical distribution of the chaotic signals [4, 5].

To evaluate the randomness of the random bit sequence, NIST Special Publication 800-22 (NIST SP 800-22) have been commonly used. The length of the random number by the NIST evaluation requires only 1 Gigabits (10^9 bits). The statistical tests that treat with larger amounts of random numbers are necessary, and one of these statistical tests is known as TestU01 [9]. The maximum random bit length required for TestU01 is about 410 Gigabits.

In this study, we experimentally generate random bit sequences from chaotic temporal waveforms obtained from a PIC by using a differential method and exclusive-or (XOR) operation. We evaluate large amount of random bit sequences by using NIST SP 800-22 and TestU01.

2. Experimental setup

Figure 1 shows the schematics of the PIC used for random bit generation. The PIC consists of a semiconductor laser, two semiconductor optical amplifiers, a 10-mm-long waveguide, an external mirror, and a photodetector. A chaotic laser output is generated by the optical feedback from the mirror. The feedback strength can be tuned by varying the injection currents of the optical amplifiers. The chaotic optical signal of the laser is converted into an electrical signal by the photodetector.

Figure 2 shows the experimental setup for random bit generation. The temporal waveform of the laser output from the PIC is divided into the alternating current (AC) and the direct current (DC) components by a bias tee. The AC component is amplified by using an electrical amplifier, and sampled by an analog-to-digital converter with 8-bit resolution.

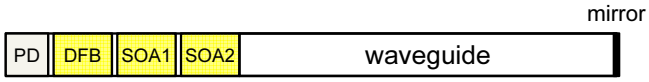

Figure 1: Schematics of photonic integrated circuit (PIC). The PIC consists of a photodetector (PD), a distributed-feedback (DFB) semiconductor laser, two semiconductor optical amplifiers (SOA 1 and 2), a passive waveguide, and an external mirror.

3. Experimental results of chaotic temporal waveform

Figure 3 shows a typical example of the chaotic temporal waveform and the radio-frequency (RF) spectrum generated from the PIC. An irregular temporal waveform is

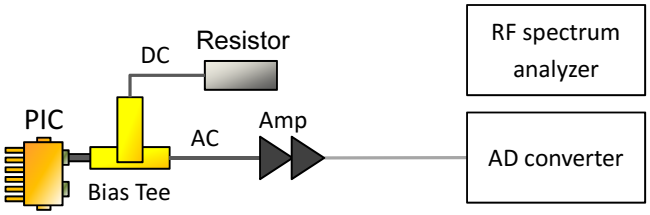

Figure 2: Experimental setup for random bit generation using the PIC.

observed in Fig. 3(a). A broadband spectrum is obtained in Fig. 3(b).

Figure 4 shows the probability distributions of the original temporal waveform and that generated from the difference between the original and time-delayed temporal waveforms by using the differential method. The histogram is obtained by sampling the amplitude of the chaotic temporal waveform with the vertical resolution of 256 points. The histogram shows irregularities due to the quantization error of the AD converter as shown in Fig. 4(a). Such a quantization error can cause artificial randomness of the generated random bits. To eliminate these quantization errors, we apply the differential method to the chaotic signal [4, 5]. The histogram after applying the differential method shows a smooth and normal distribution as shown in Fig. 4(b).

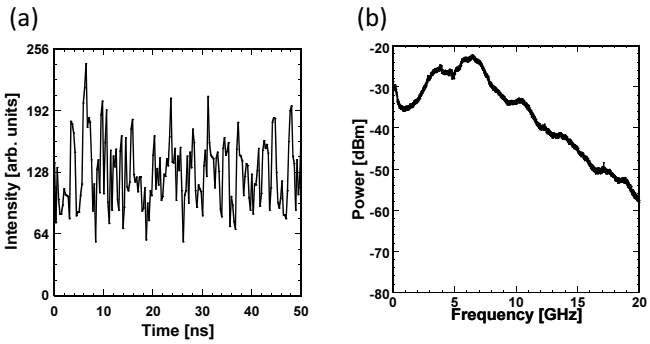

Figure 3: (a) Temporal waveform and (b) RF spectrum of the output of the PIC.

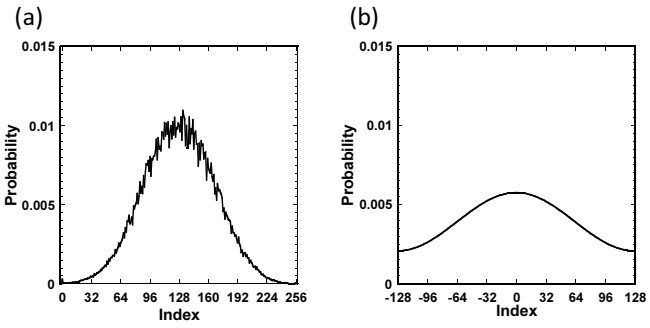

Figure 4: (a) Probability distribution of the chaotic temporal waveform and (b) that obtained from the differential method.

4. Random bit generation method

We generated a random bit sequence from the chaotic temporal waveforms by using the post-processing, consisting of the differential method, the bit-order reversal, and XOR operation. First, we apply a differential method to the chaotic signal to prevent the undesired asymmetric distribution of the histogram of the laser intensities, as shown in Fig. 5. Next, we generate three time-delayed 8-bit signals (called D1, D2, and D3) from the original signal (called D0). Then, we generate two differential signals (called DS1 and DS2) by calculating the differences between D0 and D1, and between D2 and D3 respectively. It is expected that the statistical histograms of DS1 and DS2 show symmetric distributions. Next, the bit order of DS2 is reversed, i.e., the most significant bit (MSB) changes to the least significant bit (LSB), the second MSB changes to the second LSB and so on [6] as shown in Fig. 6. Bitwise exclusive-OR (XOR) operation is then carried out between the bit-order reversed DS2 and the original DS1. Finally, some of the LSBs are extracted from the 8-bit signal, and they are used as a random bit sequence.

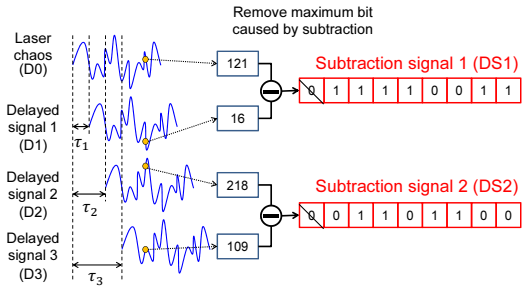

Figure 5: Schematics of differential method.

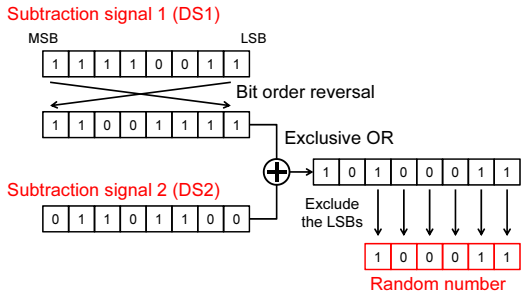

Figure 6: Schematics of physical random number generation method with bit-order reversal, XOR operation, and LSBs extraction.

5. Evaluation of generated random bits

To evaluate the randomness of a long random bit sequence, we calculate the statistical bias b of the occurrence of bit '1'. The bias b is defined as follows.

$$b = | p(1) - 0.5 | \quad (1)$$

where $p(1)$ is the probability of the occurrence of '1'. Smaller bias indicates higher randomness of generated random bit sequences. For the finite length N of the random bit sequence, the statistical bias b needs be less than the three-standard-deviations, defined as $3\sigma = 1.5N^{-0.5}$ [7]. We calculated the statistical bias b as a function of the length of the generated bit sequence N, and confirm that the bias is less than the 3σ line for all N.

The generated random bits are evaluated using National Institute of Standards and Technology Special Publication 800-22 (NIST SP 800-22) [8]. The NIST tests are performed for 1000 sequences of 1 Mbit length. Typical results of the NIST tests are shown in Table 1. The random bit sequence generated from the post-processing with 8 LSBs passes all of the NIST tests.

Figure 7 shows the number of the passed NIST tests when the number of extracted LSBs is changed. We carried out the NIST tests with 1-Gbit sequences for five times, and the median of the five test results is plotted with error bars of the maximum and minimum values, as shown in Fig. 7. We succeeded in passing all of NIST tests in the cases from 1 to 8 LSBs except LSB 3.

Table 1: Result of NIST SP 800-22 for random bit sequences generated from the post-processing with 8 LSBs. Significance level is set to $\alpha = 0.01$. To pass the tests, the P-value of the uniformity of p-values should be larger than 0.0001, and the proportion of sequences satisfying p-value $> \alpha$ for 1000 samples of 1 Mbit data should be in the range of 0.99 ± 0.0094392 [8]. For tests which produce multiple P-values and proportions, the worst case is shown.

	Test	P-value	Proportion	Result
1	frequency	0.429923	0.985000	Success
2	block-frequency	0.641284	0.993000	Success
3	cumulative-sums	0.034257	0.983000	Success
4	runs	0.203351	0.987000	Success
5	longest-run	0.890582	0.995000	Success
6	rank	0.145326	0.986000	Success
7	fft	0.701366	0.985000	Success
8	nonoverlapping-template	0.000181	0.982000	Success
9	overlapping-templates	0.949278	0.988000	Success
10	universal	0.119508	0.989000	Success
11	approximate-entropy	0.705466	0.990000	Success
12	random-excursions	0.102624	0.996800	Success
13	random-excursions-variant	0.086176	0.998400	Success
14	serial	0.534146	0.986000	Success
15	linear-complexity	0.591409	0.991000	Success
Result				**15/15**

We also used TestU01 to evaluate the randomness of a longer random bit sequence. TestU01 consists of five package: Rabbit, Alphabit, SmallCrush, Crush and BigCrush. The BigCrush test requires the longest random bit length of ~410 Gbits (4.1×10^{11} bits). We carried out the TestU01 tests while the number of the extracted LSBs is changed. It found that all of the Rabbit, Alphabit, and SmallCrush tests are passed from 1 to 8 LSBs, and all of the Crush and BigCrush test are passed from 5 to 8 LSBs.

6. Conclusions

We experimentally demonstrated fast physical random bit generation by using laser chaos generated from a photonic integrated circuit. We generated random bit sequence by applying the differential method, bit-order reversal, and XOR operation. The randomness of the generated random bit sequences is verified by using NIST Special Publication 800-22 and TestU01.

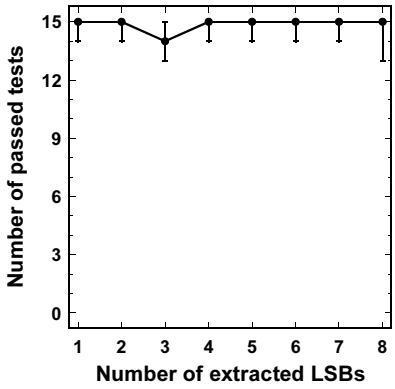

Figure 7: Number of passed NIST tests as a function of the extracted LSBs for the post-processing for the random bit generation. "15" on the vertical axis indicates that all the NIST tests are passed. Five 1-Gbit sequences of random bits are used for each NIST test and the median of the five test results is plotted with error bars of the maximum and minimum values.

Acknowledgments

We acknowledge support from Grants-in-Aid for Scientific Research from Japan Society for the Promotion of Science (JSPS KAKENHI Great Number JP24686010), and Management Expenses Grants 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, "Fast physical random bit generation with chaotic semiconductor lasers.", *Nature Photonics*, Vol. 2, pp. 728-732 (2008).

[2] R. Takahashi, Y. Akizawa, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation.", *Opt. Express*, Vol. 22, pp. 11727-11740 (2014).

[3] A. Argyris, et al., 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).

[4] 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, pp. 024102 (2009).

[5] J. Zhang, Y. Wang, M. Liu, L. Xue, P. Li, A. Wang, and M. Zhang, "A robust random number generator based on differential comparison of chaotic laser signals.", *Opt. Express*, Vol. 20, pp. 7496-7506 (2012).

[6] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, P. Davis, "Fast Random Number Generation With Bandwidth-Enhanced Chaotic Semiconductor Lasers at 8×50 Gb/s.", *IEEE Photon. Tech. Lett*, Vol. 24, pp. 1042-1044 (2012).

[7] V. N. Chizhevsky, "Symmetrization of single-sided or nonsymmetrical distributions: The way to enhance a generation rate of random bits from a physical source of randomness." *Phys. Rev. E*, Vol. 82, pp. 050101 (2010).

[8] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, and S. Vo, "Statistical test suite for random and pseudorandom number generators for cryptographic applications.", Special Publication 800-22, Revision 1a (2010).

[9] P. L. Ecuyer, R. Simard. "TestU01: AC library for empirical testing of random number generators.", ACM Transactions on Mathematical Software, Vol. 33, Article No. 22 (2007).