IEICE Proceeding Series

Random number generation with a photonic integrated circuit for fast chaos generation

Rie Takahashi, Yasuhiro Akizawa, Taiki Yamazaki, Atsushi Uchida, Takahisa Harayama, Ken Tsuzuki, Satoshi Sunada, Kazuyuki Yoshimura, Ken-ichi Arai, Peter Davis

Vol. 1 pp. 138-141
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Random number generation with a photonic integrated circuit for fast chaos generation

Rie Takahashi[1], Yasuhiro Akizawa[1], Taiki Yamazaki[1], Atsushi Uchida[1],
Takahisa Harayama[2,3], Ken Tsuzuki[4], Satoshi Sunada[2,5],
Kazuyuki Yoshimura[2], Ken-ichi Arai[2], and Peter Davis[2,6]

[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,
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237, Japan
[3]Department of Mechanical Engineering, Toyo University,
2100 Kujirai, Kawagoe, Saitama, 350-8585, Japan
[4]NTT Photonics Laboratories, NTT Corporation,
3-1 Morinosatowakamiya, Atsugi, Kanagawa, 243-0198, Japan
[5]Institute of Science and Engineering, Kanazawa University,
Kakuma-machi, Kanazawa, Ishikawa, 920-1192, Japan
[6]Telecognix Corporation, Japan
58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto, 606-8314, Japan
Emails: {s12mm320, auchida}@mail.saitama-u.ac.jp

Abstract– Random number generation is experimentally demonstrated with a photonic integrated circuit (PIC) consisting of a semiconductor laser and a short external cavity. Broadband optical chaos with flat radio-frequency spectrum can be generated by adjusting the injection current and the feedback strength of the PIC. A chaotic waveform and its time-delayed signal are sampled with a 1-bit analog-to-digital (AD) converter, and exclusive-or (XOR) operation is carried out to obtain random bit sequences. We used several PICs with different external-cavity lengths. It is found that the maximum rate of the random number generation is dependent on the external cavity length.

1. Introduction

Random numbers are used for information security and numerical simulation. Random numbers can be categorized into two types: pseudorandom numbers and physical random numbers. Pseudorandom numbers are generated from a seed and a deterministic algorithm, and can be generated at high speed in a computer. However, pseudorandom numbers have reproducibility and periodicity. On the contrary, physical random numbers are generated from physical random phenomena such as thermal noise and quantum noise, and they do not have reproducibility and periodicity. However, the speed of existing physical random number generators is limited up to hundreds of Megabit per second (Mb/s).

Recently, fast physical random-number generators using chaotic lasers have been proposed at rates ranging from 1 to 400 Gigabit per second (Gb/s) [1-12]. Fast physical random-number generators can be useful for quantum cryptography and a new type of information-theoretic security systems [13,14]. It has been theoretically guaranteed that chaotic lasers can be used for nondeterministic random bit generators [15].

These laser-chaos-based random number generators reported in the literature utilize commercially available semiconductor lasers and photodetectors, which require large space on an optical table for experimental apparatus. To minimize random number generators, photonic integrated circuits (PICs) are more desirable for practical applications. From the application point of view, it is important to show that PICs are useful for random numbers generators.

Random number generators using a PIC with 10-mm-long external cavity has been reported [5,6]. However, the condition for generating broadband chaos and fast random numbers with certified randomness has not been well investigated so far. In particular, the effect of the external cavity length on the performance of random number generation has not been clarified. It is theoretically expected that PICs with shorter external cavity lengths produce broader chaotic radio-frequency (RF) spectrum.

In this study, we used a PIC with a 5-mm-long external cavity for random number generation using 1-bit analog-to-digital conversion and exclusive-or operation. We investigated the condition for generating fast random numbers for different sampling rates. We also used PICs with different external cavity lengths and generated random bit sequences at various sampling rates.

2. Random numbers generation using the PIC with a 5-mm-long external cavity

Figure 1(a) shows the schematics of a PIC used for random number generation. The PIC consists of a photodetector (PD), a distributed-feedback (DFB) semiconductor laser, two optical semiconductor amplifiers (SOA 1 and 2), a short passive waveguide (PW), and an external mirror (M) for optical feedback. The distance between the right facet of DFB and M is 5 mm. The optical output from the DFB laser is reflected by the mirror M, and re-injected into the laser to produce chaotic intensity fluctuations. The injection currents for the DFB laser and for the SOAs are adjusted to generate chaos. We observed different temporal dynamics, which can be classified into seven dominant regimes: periodic state, quasi-periodic state, chaotic state, pulse package, intermittency, stable state, and no lasing state [16].

Figure 1(b) shows the experimental setup for random number 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 divided into two electronic signals by a power divider. One of the temporal waveforms is time-delayed by adding an additional 1-m-long coaxial cable, whose delay time corresponds to 4.6 ns. The chaotic electronic signal and its time-delayed signal are detected using a digital oscilloscope. Random bits are generated from the two chaotic waveforms using post processing. We used a simple post-processing method [1,6] as shown in Fig. 1(c), so that we can clarify which chaotic states are useful for fast random number generation. A chaotic waveform and its time-delayed signal are sampled with a 1-bit analog-to-digital (AD) converter, and bitwise exclusive-or (XOR) operation is carried out for the two 8-bit sequences to generate random numbers.

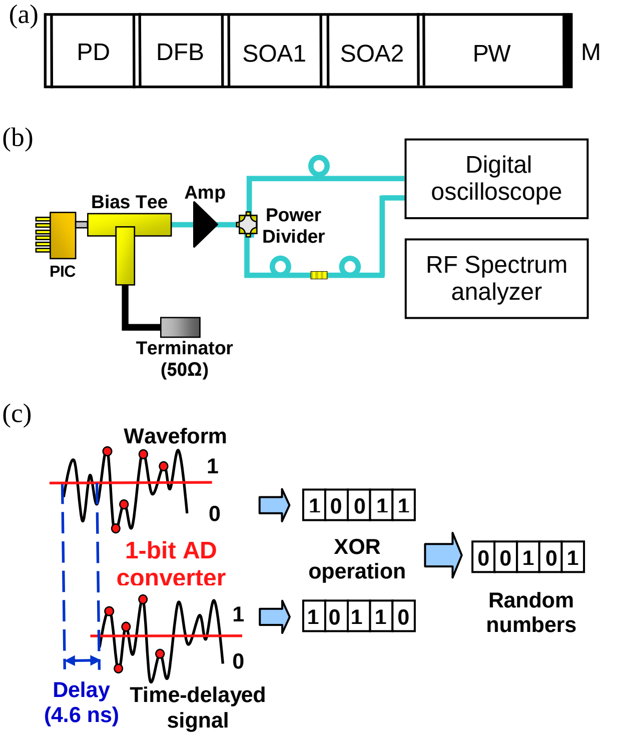

Fig. 1 (a) Schematics of the PIC. The PIC consists of a photodetector (PD), a distributed-feedback (DFB) semiconductor laser, two semiconductor optical amplifiers (SOA 1 and 2), a passive waveguide (PW), and an external mirror (M). (b) Experimental setup for random number generation. (c) Method for random number generation with 1-bit AD conversion and XOR operation.

The generated random numbers are evaluated using National Institute of Standards and Technology Special Publication 800-22 (NIST SP 800-22) [17]. This is a de-fact standard statistical test of randomness, and consists of 15 tests. Random numbers that can pass all the 15 tests indicate that their randomness is statistically equivalent to ideal random numbers.

First, we observed temporal dynamics that are suitable for random number generation using the PIC with 5-mm-long external cavity. We generated random bit sequences from quasi-periodic, pulse-package, and chaotic temporal waveforms. We found that good random numbers can be generated only from chaotic waveforms, but not from quasi-periodic or pulse-package waveforms. Table 1 shows the experimental result of NIST SP 800-22 for random numbers generated from chaotic waveforms. Random numbers generated at sampling rate of 4.55 Gb/s can pass all the statistical tests of randomness.

Table 1 Result of NIST SP 800-22 for random numbers generated from chaotic waveforms at rate of 4.55 Gb/s.

NIST SP800-22		P-value	Proportion	Result
1	frequency	0.682823	0.9840	SUCCESS
2	block-frequency	0.002058	0.9820	SUCCESS
3	cumulative-sums	0.165340	0.9860	SUCCESS
4	runs	0.397688	0.9920	SUCCESS
5	longest-run	0.940080	0.9940	SUCCESS
6	rank	0.990138	0.9910	SUCCESS
7	fft	0.177628	0.9870	SUCCESS
8	nonperiodic-templates	0.008326	0.9810	SUCCESS
9	overlapping-templates	0.054661	0.9830	SUCCESS
10	universal	0.319084	0.9830	SUCCESS
11	apen	0.583145	0.9880	SUCCESS
12	random-excursions	0.173269	0.9790	SUCCESS
13	random-excursions-variant	0.018845	0.9790	SUCCESS
14	serial	0.146152	0.9960	SUCCESS
15	linear-complexity	0.192724	0.9910	SUCCESS
TOTAL		15		

Next we changed the sampling rate to generate random numbers and examined the relationship between the autocorrelation function and randomness of generated bit sequences. Figure 2(a) shows the number of passed NIST tests when the sampling time is changed. The lower horizontal axis shows the sampling time, and the upper horizontal axis shows the corresponding sampling rate (i.e., inverse of the sampling time) for random numbers generation. We changed the sampling rate and evaluated the randomness by using NIST SP 800-22. We obtained that the maximum rate of the random number generation is 4.55 Gb/s. Figure 2(b) shows the relationship between the autocorrelation function of the chaotic temporal waveform and the number of passed NIST tests for the random bits generated from the chaotic waveform and the sampling rate. The red circles in Fig. 2(b) represent the sampling rates where all the 15 NIST tests are passed, whereas the blue triangles represent the rates where some NIST tests are failed. We found that more random bits can be generated when a sampling rate corresponding to a lower autocorrelation value in Fig. 2(b) is used.

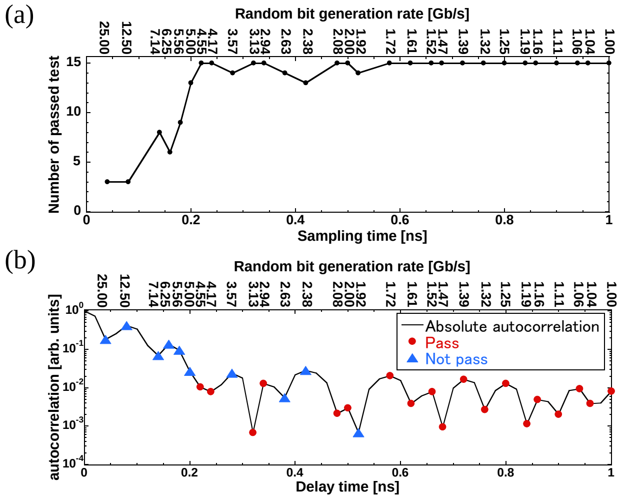

Fig. 2 (a) Number of passed NIST tests for generated random bit sequences as a function of the sampling time (i.e., the sampling rate). (b) Autocorrelation function (absolute value) of the chaotic temporal waveform and result of NIST tests for generated random bit sequences. Red circles: all the NIST tests are passed. Blue triangles: some NIST tests are failed.

We examined the conditions of different chaotic states for good random number generation. The shape of radio-frequency (RF) spectra is changed by adjusting the injection current and the feedback strength of the PIC in the chaotic regimes. Figures 3(a) and 3(b) show the RF spectra for different chaotic states. In Fig. 3(a), broadband chaotic spectrum is observed. The maximum rate of random number generation is 4.55 Gb/s by using this chaotic state. On the contrary, a low frequency peak exists and the low frequency peak is higher than the peak of the broadband chaotic component in Fig. 3(b). The maximum rate of random number generation is 1.04 Gb/s by using this chaotic state.

We estimated the difference in the heights between the low-frequency peak and that of the chaotic broadband component in RF spectra, and investigated the maximum rate of random number generation, as shown in Fig. 3(c). A larger peak difference results in a higher rate of random number generation. Therefore, the adjustment of RF spectra is crucial for random number generation. The low frequency peak needs to be eliminated for fast random number generation.

3. Random numbers generation using the PICs with different cavity length

We next investigated the condition for generating fast random numbers using PICs with different external cavity lengths (2, 3, 4, 5, and 10 mm-long). Chaos is generated by nonlinear interaction between the external cavity frequency and the relaxation oscillation frequency. A shorter external cavity corresponds to a higher external cavity frequency that results in faster chaotic dynamics. Therefore, it is expected to observe higher chaotic oscillations for a shorter external cavity length.

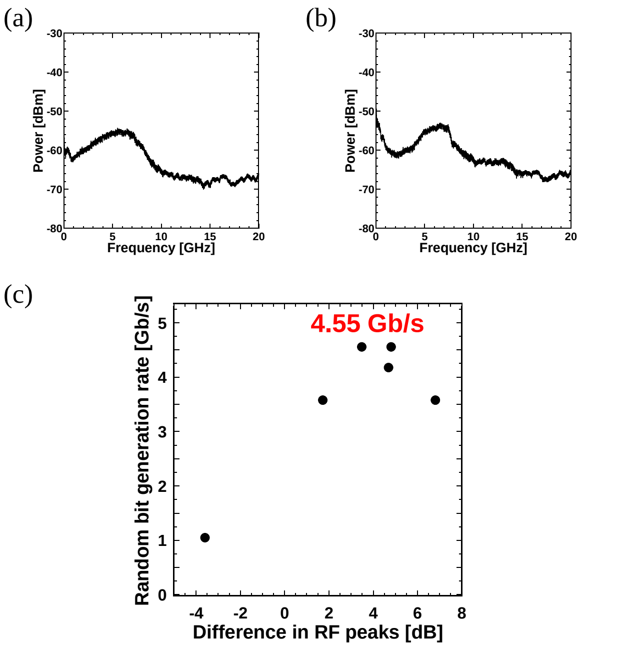

Fig. 3 (a), (b) RF spectra of chaotic temporal waveforms used for random number generation. The maximum rates of random number generation with these RF spectra are (a) 4.55 Gb/s and (b) 1.04 Gb/s, respectively. (c) Difference in the heights between the low frequency peak and the peak of chaotic broadband spectrum component.

We examined temporal dynamics by adjusting the injection current of the DFB laser and the feedback strength. We observed chaotic outputs for all the PICs with different external cavity lengths. We succeeded in generating random numbers from the chaotic states of all the PICs.

We generated random bits sequences from the different PICs and changed the sampling rate of random number generation. We then evaluated the randomness of generated bits by using NIST SP 800-22 tests. Figure 4 shows the sampling rates for random bit sequences that pass all the NIST tests for the PICs with different external cavity lengths. The sampling rates are changed from 1 to 6 GHz. The solid black dots indicate the sampling rates that pass all the NIST tests. We succeeded in generating random bit sequences, except the 2-mm-long PIC. It is found that most bits generated at the sampling rates below 2 Gb/s can pass all the NIST tests. For the sampling rates higher than 2 Gb/s, the sampling rates for good random number generation are discretized. We can generate random bits at rates up to 5.56 Gb/s using the 4-mm-long PIC.

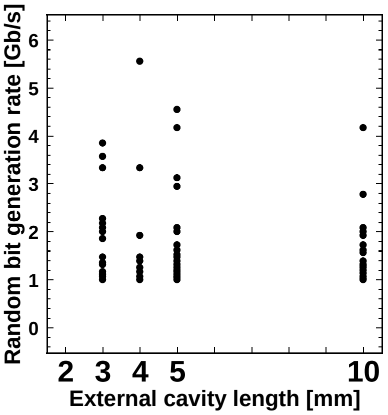

Fig. 4 Sampling rates generated for the random bit sequences that pass all the NIST tests for PICs with different external cavity lengths. Solid black dots indicate the sampling rates that pass all the NIST tests.

4. Conclusion

We have experimentally generated random numbers using PICs. We have observed temporal dynamics using a PIC with a 5-mm-long external cavity, and evaluated the condition for generating good random numbers by using 1-bit AD conversion and XOR operation. We found that random numbers with certified randomness can be generated when the sampling rate is adjusted to low autocorrelation values of the chaotic temporal waveforms. In addition, a low frequency peak in the RF spectrum needs to be eliminated. We have generated random numbers using PICs with different external cavity lengths. We succeeded in generating certified random numbers at rates up to 5.56 Gb/s.

Acknowledgments

We acknowledge support from Grant-in-Aid for Young Scientists 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, *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] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, *Nature Photonics*, Vol. 4, pp. 58-61 (2010).

[4] 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).

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

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

[7] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, *Optics Express*, Vol. 19, No. 7, pp. 5713-5724 (2011).

[8] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, *Optics Letters*, Vol. 36, No. 23, pp. 4632-4634 (2011).

[9] Y. Zhang, J. Zhang, M. Zhang, and Y. Wang, *Chinese Optics Letters*, Vol. 9, No. 3, pp. 031404 (2011).

[10] P. Li, Y. Wang, A. Wang, L. Yang, M. Zhang, and J. Zhang, *Optics Express*, Vol. 20, No. 4, pp. 4297-4308 (2012).

[11] J. Zhang, Y. Wang, M. Liu, L. Xue, P. Li, A. Wang, and M. Zhang, *Optics Express*, Vol. 20, No. 7, pp. 7496-7506 (2012).

[12] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, *IEEE Photonics Technology Letters*, Vol. 24, No. 12, pp. 1042-1044 (2012).

[13] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, *Optics Express*, Vol. 17, No. 11, pp. 9053-9061 (2009).

[14] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, *Physical Review Letters*, Vol. 108, pp. 070602-1-5 (2012).

[15] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K. Arai, A. Uchida, and P. Davis, *Physical Review E*, Vol. 85, No. 4, pp. 046215-1-9 (2012).

[16] Y. Akizawa, R. Takahashi, H. Aida, T. Yamazaki, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Yoshimura, K. Arai, and P. Davis, *Proceedings of Nonlinear Theory and Its Applications 2012* (NOLTA 2012), (2012).

[17] 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).