# IEICE Proceeding Series

Fast random number generation with bandwidth-enhanced chaos and post-processing

Taiki Yamazaki, Yasuhiro Akizawa, Atsushi Uchida, Kazuyuki Yoshimura, Kenichi Arai, Peter Davis

Vol. 1 pp. 142-145
Publication Date: 2014/03/17
Online ISSN: 2188-5079

# Fast random number generation with bandwidth-enhanced chaos and post-processing

Taiki Yamazaki[1], Yasuhiro Akizawa[1], Atsushi Uchida[1],
Kazuyuki Yoshimura[2], Kenichi Arai[2], and Peter Davis[2,3]

[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]Telecognix Corporation,
58-13 Shimooji-cho, Yoshida, Sakyo-ku, Kyoto, 606-8314, Japan
Email: auchida@mail.saitama-u.ac.jp

**Abstract–** We experimentally demonstrate random number generation using multi-bit samples of bandwidth-enhanced chaos in two pairs of semiconductor lasers. Chaotic fluctuations of laser output are generated in two semiconductor laser with optical feedback independently. The chaotic outputs are injected into the corresponding semiconductor lasers to obtain chaotic intensity signals and their time-delayed signals for bandwidth enhancement. The four chaotic signals are converted to 8-bit digital signals by sampling at 50 Giga samples per second (GS/s). Random bits are generated by the combination of bit-order-reversal method, bitwise exclusive-OR operation, and extraction of some least significant bits. The maximum generation rate at 1.05 Tb/s (= 3 data × 7 bit × 50 GS/s) can be achieved for random bit sequences with certified randomness.

## 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 [1].

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 [1-13] and amplified spontaneous emission from an optical noise source [14,15] at rates ranging from 1 to 400 Gb/s. It is an ongoing challenge to increase the speed of non-deterministic physical random number generators more than 1 Terabit per second (Tb/s) and to develop bit extraction mechanisms which increase the random bit generation capacity.

In this study we evaluate a hybrid scheme for random number generation consisting of multi-bit samples of bandwidth enhanced chaos and digital post-processing. The bandwidth enhancement is achieved using optical injection [16,19]. 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. Random bit sequences are generated by the combination of the bit-order-reversal method [13], bitwise exclusive-OR operation [6], and the extraction of some least significant bits [3].

## 2. Experimental setup for bandwidth enhancement

Figure 1 shows our experimental setup for fast physical random bit generation. We used four distributed-feedback (DFB) semiconductor lasers (referred to as Laser 1, 2, 3 and 4, respectively). Laser 1 and 3 were used for the generation of chaotic intensity fluctuations induced by optical feedback. The other lasers, Laser 2 and 4, were used for the bandwidth enhancement of chaotic waveforms. Laser 1 (or Laser 3) 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.

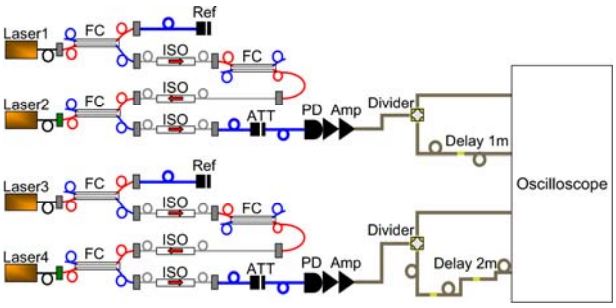


Fig. 1 Experimental setup for random number generation. Amp: electronic amplifier, ATT: fiber attenuator, FC: fiber coupler, ISO: optical isolator, PD: photodiode, Ref: fiber reflector.

A portion of the chaotic Laser 1 (or Laser 3) beam was injected into Laser 2 (or Laser 4). An optical isolators were used to achieve one-way coupling from Laser 1 (3) to Laser 2 (4). The wavelengths of the four lasers were precisely adjusted in order to generate bandwidth-enhanced chaotic outputs of Laser 2 and 4. A portion of Laser 2 (4) 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 (4.62 and 9.01 ns delays for Laser 2 and 4, respectively) were 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. Four bandwidth-enhanced chaotic signals, including two time-delayed signals, were obtained in this experiment.

### 3. Post-processing for random bit generation

We generate random bits using four chaotic waveforms; the outputs of Laser 2 and 4, and the corresponding time-delayed outputs. The four chaotic optical signals are detected by AC-coupled photodetectors, amplified and converted to digital 8-bit signals by a digital oscilloscope sampling at 50 GS/s per channel. The four chaotic outputs are referred to as signal A (Laser 2 output), B (Laser 2 delayed signal), C (Laser 4 output), and D (Laser 4 delayed signal).

Figure 2 shows our proposed post-processing method based on the combination of three techniques: bit-order-reversal, bitwise exclusive-or (XOR), and extraction of least significant bits (LSBs). First, we apply bit-order-reversal method for the signal A, B, and D (referred to as $A^R$, $B^R$, and $D^R$). Next, bitwise XOR is executed to pairs of A and $B^R$, $A^R$ and D, and C and $D^R$ (see Fig. 2), and the resultant 8-bit signals $X = A \oplus B^R$, $Y = A^R \oplus D$, and $Z = C \oplus D^R$ are obtained. 7 LSBs of these 8-bit signals $X_{7\sim1}$, $Y_{7\sim1}$, and $Z_{7\sim1}$ are extracted and combined as random bit.

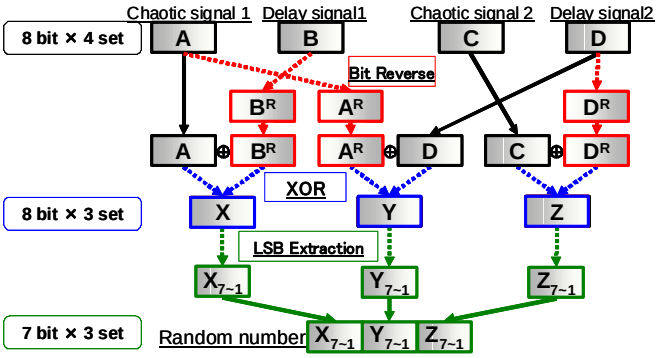


Fig. 2 Proposed scheme for random bit generation. The combination of three techniques: bit-order-reversal, bitwise exclusive-or (XOR), and extraction of least significant bits (LSBs) are used.

Here, 21 bits (= 3 data × 7 bit) can be obtained from 32 bit (= 4 data × 8 bit) by the post-processing. This procedure is carried out at each sampling point at 50 GS/s. The equivalent rate of random bit generation is 1.05 Tb/s (=3 data × 7 bit × 50 GS/s).

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) [20]. The NIST SP 800-22 test consists of 15 statistical tests. The tests are performed using 1000 samples of 1 Mbit sequences and the significance level $\alpha = 0.01$. A typical result of the NIST tests is shown in Table 1. We confirmed that random bit sequences are sufficiently random that they pass all the 15 statistical tests of NIST SP 800-22.

Table 1 Result of NIST SP 800-22 for random numbers generated at a rate of 1.05 Tb/s.

| STATISTICAL TEST | P-VALUE | PROPORTION | RESULT |
|---|---|---|---|
| frequency [1test] | 0.796268 | 0.9870 | SUCCESS |
| block-frequency [1test] | 0.010911 | 0.9850 | SUCCESS |
| cumulative-sums [2test] | 0.031848 | 0.9880 | SUCCESS |
| runs [1test] | 0.893482 | 0.9880 | SUCCESS |
| longest-run [1test] | 0.281232 | 0.9810 | SUCCESS |
| rank [1test] | 0.029996 | 0.9890 | SUCCESS |
| fft [1test] | 0.162606 | 0.9870 | SUCCESS |
| nonoverlapping-template [148test] | 0.007918 | 0.9820 | SUCCESS |
| overlapping-templates [1test] | 0.066465 | 0.9870 | SUCCESS |
| universal [1test] | 0.005280 | 0.9880 | SUCCESS |
| approximate-entropy [1test] | 0.530120 | 0.9950 | SUCCESS |
| random-excursions [8test] | 0.014059 | 0.9811 | SUCCESS |
| random-excursions-variant [18test] | 0.028787 | 0.9795 | SUCCESS |
| serial [2test] | 0.647530 | 0.9880 | SUCCESS |
| linear-complexity [1test] | 0.624627 | 0.9850 | SUCCESS |
| Total | | | 15 |

## 4. Evaluation of random bit generation rate

Next we investigated the effect of post-processing by changing the number of XORed data (*n* data) and the number of extracted LSBs (*m* LSBs). We generated random bits by changing both *n* and *m*, and evaluate the randomness by using NIST SP 800-22 tests.

Figure 3 shows the evaluation of the generated random bits when the number of XORed data (*n*) and the number of extracted LSBs (*m*) are changed. The equivalent rate of random bit generation can be estimated from R = *n* data × *m* LSBs × 50 GS/s. The red solid dots represent that all the NIST tests are passed, whereas the open circles represent that some of the NIST tests are failed. The green and blue curves correspond to the equivalent generation rates of 0.5 and 1.0 Tb/s, respectively. For small *n* (n = 1, 2), random numbers can be generated for all the *m* ($1 \le m \le 8$). For *n* = 3, the maximum *m* is 7. For n ≥ 4, no random bits can be generated even for *m* = 1. We found that the maximum rate of random bit generation is 1.05 Tb/s for *n* = 3 and *m* = 7.

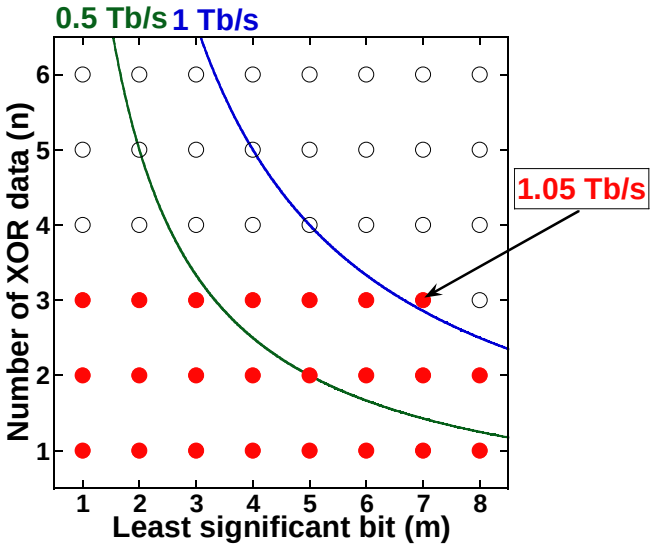


Fig. 3 Evaluation of the generated random bits as functions of the number of XORed data (*n*) and the number of extracted LSBs (*m*). The equivalent rate of random bit generation can be estimated from R = *n* data × *m* LSBs × 50 GS/s. The maximum rate of random bit generation is 1. 05 Tb/s.

## 5. Conclusion

We have experimentally demonstrated random number generation using a hybrid scheme of multi-bit samples of bandwidth enhanced chaos in two pairs of semiconductor lasers and digital post-processing. Chaotic fluctuations of laser output are generated in two semiconductor laser with optical feedback independently. The chaotic outputs are injected into the corresponding semiconductor lasers to obtain bandwidth-enhanced chaotic intensity signals and their time-delayed signals. The four chaotic signals are converted to 8-bit digital signals by sampling at 50 GS/s. Random bits are generated by the combination of bit-order-reversal method, bitwise exclusive-OR operation, and the extraction of some least significant bits. The maximum generation rate at 1.05 Tb/s (= 3 data × 7 bit × 50 GS/s) can be achieved for random bit sequences with certified randomness.


## 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, “Optical Communication with Chaotic Lasers, Applications of Nonlinear Dynamics and Synchronization,” Wiley-VCH, Weinheim (2012).

[2] 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).

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

[4] 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).

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

[6] 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).

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

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

[9] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Chaos laser chips with delayed optical feedback using a passive ring waveguide," Optics Express, Vol. 19, No. 7, pp. 5713-5724 (2011).

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

[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] T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, Physical Review E, Vol. 85, pp. 016211-1-7 (2012).
[13] 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).
[14] 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).
[15] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Optics Letters, Vol. 36, No. 6, pp. 1020-1022 (2011).
[16] F. Y. Lin and J. M. Liu, Optics Communications, Vol. 221, No. 1-3, pp. 173-180 (2003).
[17] J. Ohtsubo, “Semiconductor Lasers, Stability, Instability and Chaos,” Second Ed., Springer-Verlag, Berlin Heidelberg (2008).
[18] H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, Optics Express, Vol. 17, No. 22, pp. 19536-19543 (2009).
[19] A. Wang, Y. Wang, and H. He, IEEE Photonics Technology Letters, Vol. 20, No. 19, pp. 1633-1635 (2008).
[20] 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).