Performance of Random Number Generators Using Noise-Based Superluminescent Diode and Chaos-Based Semiconductor Lasers

Taiki Yamazaki and Atsushi Uchida, *Member, IEEE*

(Invited Paper)

***Abstract*—We investigate two optical sources used for random number generation: superluminescent diode (SLD) and semiconductor lasers. Amplified spontaneous emission noise is generated in the SLD and chaotic intensity fluctuation is generated in a semiconductor laser. We investigate the performance of random number generation for both optical sources. For single-bit generation of random numbers, the maximum generation rate is 8.33 Gb/s for both the SLD and the laser with a similar bandwidth of ∼15 GHz. For multibit generation schemes, we obtain the generation rate up to 400 Gb/s for both the SLD and the laser. The overall characteristics are similar between the SLD and the laser, since similar bandwidths of the RF spectra are used. The probability density function of the SLD is more symmetric than that of the chaotic laser. This fact results in slightly good performance of random number generation using the SLD for multibit generation.**

***Index Terms*—Chaos, information technology, noise, random number generation, semiconductor laser, superluminescent diode (SLD).**

I. Introduction

RANDOM numbers play crucial roles in recent communication and computing technologies such as information security [1], [2] and numerical computations [3], [4]. The techniques of random number generation can be classified into two categories: pseudorandom number generators and physical random number generators. Pseudorandom numbers are generated from a single random seed using deterministic algorithms, and these are used in modern digital computer systems [4]. 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 [5], [6]. For this reason, physically random processes are often used as entropy sources in random number generators [7], [8]. Random phenomena such as photon noise, thermal noise in resistors, and frequency jitter of oscillators have been used as physical entropy sources for nondeterministic random number generation in combination with deterministic pseudorandom number generators [9]. However, nondeterministic generators have been limited to much slower rates at megabit per second than pseudorandom number generators due to limitations of the rate and power of the mechanisms for extracting bits from physical noise [10], [11]. It is important to develop generators, which can operate at rates higher than gigabit per second.

Recently, new schemes for physical random number generators that utilize chaotic semiconductor lasers have been demonstrated intensively to generate nondeterministic random bits at rates of more than 1 Gb/s [12]–[32]. We have demonstrated that continuous streams of random-bit sequences that pass standard tests of randomness can be generated at fast rates of up to 1.7 Gb/s by directly sampling the output of two chaotic semiconductor lasers with 1-bit analog-to-digital converters (ADCs) [13]. Methods using multibit ADCs and digital processing of bits extracted from chaotic lasers have been proposed, and studies using offline computer processing of experimental laser data have reported [12]–[32]. Nonlinear amplification of intrinsic noise in chaotic semiconductor lasers is considered as the origin of randomness in these schemes, even though chaotic systems are deterministic [30], [31]. In addition, amplified spontaneous emission noise from erbium-doped fiber amplifiers or superluminescent diodes (SLDs) has been used as a seed of random number generation [33]–[36]. Moreover, quantum random number generators based on quantum noise have been developed intensively [37]–[40]. These noise-based and quantum-based systems are random from the quantum theory in principle. However, there has been no comprehensive investigation for which types of optical random number generators provide good performance and are suitable for the applications of information security and numerical simulations.

In this study, we investigate two types of random number generators: noise-based and chaos-based random number generators. We used an SLD as a noise source and unidirectionally coupled semiconductor lasers for bandwidth enhancement as a chaotic source. We adjusted the bandwidths of the RF spectra for the intensity fluctuations of the two optical sources for comparison. We used both single-bit and multibit generation schemes to evaluate random numbers generated from the two optical sources. Finally, we find similarity and discrepancy between the SLD and the semiconductor lasers as optical sources for random number generation.

Manuscript received November 8, 2012; revised January 13, 2013; accepted January 29, 2013. Date of publication February 12, 2013; date of current version May 13, 2013. This work was supported in part by Grant-in-Aid for Young Scientists and Management Expenses Grants from the Ministry of Education, Culture, Sports, Science and Technology in Japan.

The authors are with the Department of Information and Computer Sciences, Saitama University, Saitama 338-8570, Japan (e-mail: atmosty@gmail.com; auchida@mail.saitama-u.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2013.2246777

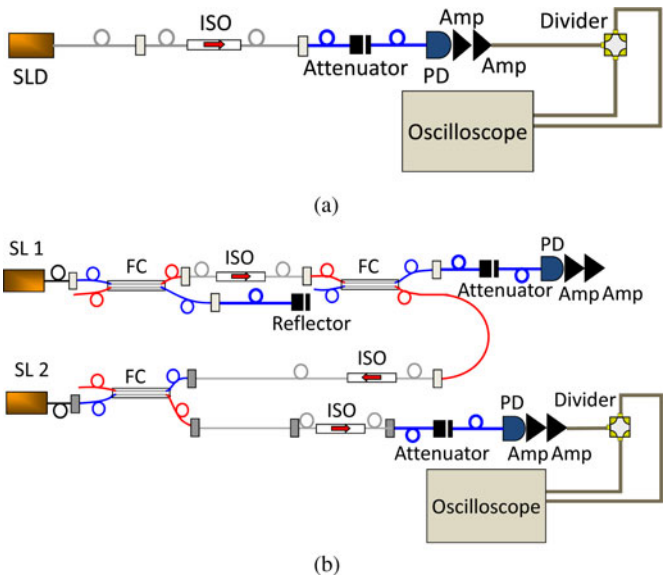

Fig. 1. Experimental setup for fast physical random number generation with (a) SLD and (b) bandwidth-enhanced chaotic semiconductor lasers. Amp: electronic amplifier, FC: fiber coupler, ISO: fiber isolator, PD: photodetector, SL: semiconductor laser, SLD: superluminescent diode.

II. Experimental Setup

A. Superluminescent Diode

Fig. 1(a) shows the experimental setup for fast physical random number generation with an SLD. The optical center frequency of the SLD used in the experiment (DenseLight Semiconductors, DL-CS5254A-FP) was 1552 nm, and the full-width half-maximum (FWHM) of the optical spectra was 32 nm (4.0 THz in frequency). The lasing threshold of the injection current $I_{\rm th}$ for the SLD was 85.0 mA. The injection current was set to 115.0 mA ($1.35I_{\rm th}$) in this experiment. Spontaneous emission noise was amplified and noisy temporal waveform of the optical output was obtained in the solitary SLD. The optical output of the SLD was adjusted by a variable attenuator and sent to a photodetector (New Focus, 1434, 25 GHz bandwidth). The converted electronic signal at the photodetector was amplified by two electronic amplifiers (New Focus, 1422-LF, 20 GHz bandwidth). It is worth noting that the bandwidth of the detected signal is limited by the bandwidth of the photodetector or the electronic amplifier. The electronic signal is divided into two signals, one of which is time-delayed to avoid cross correlation between the two signals. In the experiment, the delay was implemented using a 1-m-long coaxial cable with a 4.6-ns delay time. The alternate-current (ac) components of the two electronic signals are simultaneously sampled at a fixed clock rate by ADCs with 8-bit vertical resolution to obtain two 8-bit sequences. Temporal waveforms of the electronic signals were sampled at 50 Giga Samples per second (GS/s) using an 8-bit digital oscilloscope (Tektronix, DPO71604B, 16 GHz bandwidth, 50 GS/s). The radio-frequency (RF) spectra of the electronic signals were observed by using an RF spectrum analyzer (Agilent, N9010 A-526, 26.5 GHz bandwidth). The optical wavelength of the lasers was measured by an optical spectrum analyzer (Yokogawa, A06370B).

B. Bandwidth-Enhanced Chaotic Semiconductor Lasers

Fig. 1(b) shows our experimental setup for fast physical random number generation with bandwidth-enhanced chaotic semiconductor lasers [19]. We used two distributed-feedback (DFB) semiconductor lasers (NTT Electronics, NLK1C5GAAA, the optical wavelength of 1547 nm), developed for optical fiber communications. 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. The injection current and the temperature of the semiconductor lasers were adjusted by a current–temperature controller (Newport, 8000-OPT-41-41). The optical wavelength of the lasers was precisely controlled by the temperature of the laser. The lasing thresholds of the injection current $I_{\rm th}$ for solitary Lasers 1 and 2 were 9.43 and 9.31 mA, respectively. Both Lasers 1 and 2 were prepared without standard optical isolators, to allow optical feedback and injection. 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. The fiber length between Laser 1 and the variable fiber reflector was 4.55 m, corresponding to a feedback delay time (round-trip) of 43.8 ns. On the other hand, there was no optical feedback for Laser 2. Polarization maintaining fibers were used for all the optical fiber components.

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 Lasers 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 detected by the photodetector. The converted electronic signal at the photodetector was amplified by two electronic amplifiers and sent to the 8-bit digital oscilloscope, as described in Section II-A. The RF spectra of the electronic signals were observed by using the RF spectrum analyzer, and the optical wavelength of the lasers was measured by the optical spectrum analyzer.

We set the relaxation oscillation frequencies to be 6.5 GHz for both Lasers 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. The injection currents for Lasers 1 and 2 were set to 50.00 mA (5.30 $I_{\rm th}$) and 59.00 mA (6.34 $I_{\rm th}$), respectively. 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 1547.733 nm for Laser 1 and 1547.822 nm for Laser 2, by controlling the temperature of the two lasers. The optical wavelength for Laser 2 was shifted to 1547.856 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 Lasers 1 and 2 in the presence of the optical injection, respectively. $\Delta\lambda$ was set to 0.123 nm (-15.4 GHz in frequency), so that similar bandwidth could be obtained between the SLD and the bandwidth-enhanced semiconductor lasers used in this experiment. The bandwidth was enhanced from 9.50 to 14.93 GHz. Under this condition, no injection locking was achieved between Lasers 1 and 2, where injection locking was defined as the matching of optical wavelengths between the two lasers due to the coherent unidirectional coupling [12]. The existence of the frequency component corresponding to the optical wavelength detuning is crucial for the bandwidth enhancement of the laser chaos [19]; it results in nonlinear frequency mixing between the optical wavelength detuning and the relaxation oscillation frequency of the laser.

III. Experimental Result

We measured temporal waveforms and RF spectra of both the SLD and the chaotic semiconductor lasers. Fig. 2(a) shows the temporal waveforms of the SLD and the bandwidth-enhanced chaotic semiconductor lasers. Both of the temporal waveforms oscillate irregularly and no significant difference is found from the temporal waveforms. However, low-frequency oscillation components are observed in the temporal waveform of the SLD, compared with the semiconductor laser. Fig. 2(b) shows the RF spectra of the SLD and the semiconductor laser. The spectrum of the SLD is very flat over wide frequency range. On the contrary, a top-hat-shaped spectrum is obtained for the semiconductor lasers, where a flat spectrum is observed from 6 to 16 GHz. Low-frequency components are missing in the RF spectrum of the semiconductor laser. This RF spectrum is obtained from the nonlinear frequency mixing effect between the relaxation oscillation frequency (6.5 GHz) and the optical frequency detuning (15.4 GHz) of the two semiconductor lasers. There are continuous spectral components between these two frequencies; however, the frequency components below the relaxation oscillation frequency are very low. The bandwidth is defined as the maximum frequency where 80% of the spectral power is included within the maximum frequency [19]. The bandwidths of the SLD and the semiconductor laser are 15.10 and 14.93 GHz, respectively. Note that the bandwidth of the SLD is limited by the bandwidth of the electronic amplifiers (20-GHz bandwidth), even though the intrinsic optical bandwidth (linewidth) of the SLD is 4.0 THz. The bandwidth of the semiconductor laser is adjustable up to $\sim$16 GHz by changing the optical-carrier frequency detuning between the two lasers. We adjusted these bandwidths so that similar bandwidths can be obtained between the SLD and the semiconductor laser.

Fig. 2(c) shows the probability density function (histogram) of the temporal waveforms observed in the 8-bit digital oscilloscope. The amplitudes of the temporal waveforms are adjusted so that most of the signals are included within 8-bit vertical resolution (see Section V-B for details). It is worth noting that the histogram of the SLD output is almost symmetric and looks like a Gaussian distribution. On the contrary, the histogram of the chaotic semiconductor laser is slightly asymmetric and negative values (i.e., less than the mean value "0") appear more often.

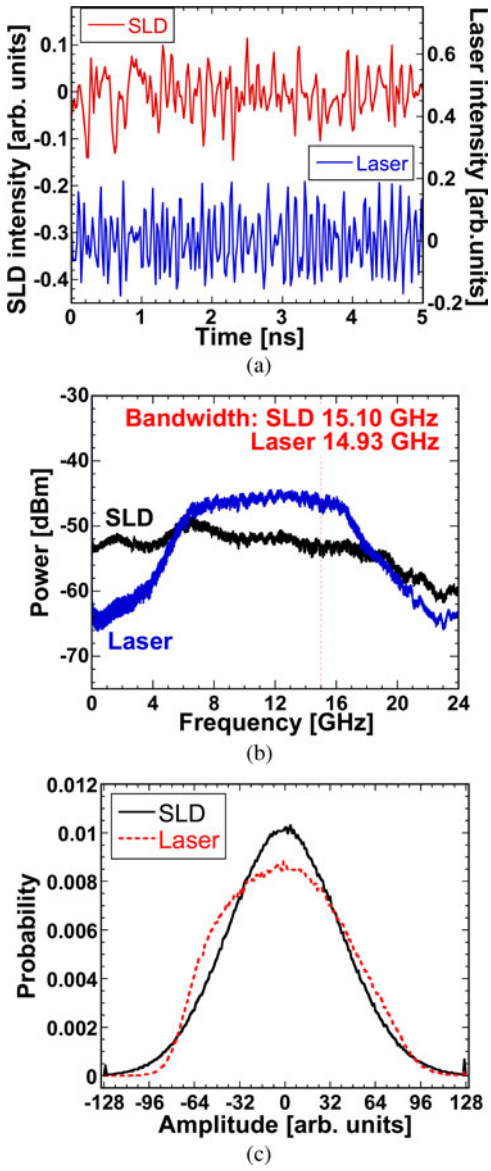

Fig. 2. Experimental results of (a) temporal waveforms, (b) RF spectra, and (c) probability density function (histogram) of the temporal waveforms of the SLD and the bandwidth-enhanced chaotic semiconductor lasers. (b) Bandwidths of the SLD and the semiconductor laser are 15.10 and 14.93 GHz, respectively.

This asymmetric characteristic results from the chaotic pulsations of the semiconductor lasers, where low values appear more frequently than high values in the vertical axis of the temporal waveform. The degree of symmetry of the histogram affects the characteristics of random number generation, as described in Section V.

IV. One-Bit Random Number Generation

First, we used a 1-bit generation scheme of random numbers [13], [15], [22] to simply evaluate the characteristics of random number generators based on the SLD and the semiconductor lasers. The 1-bit random number generation scheme is shown in Fig. 3. An irregular temporal waveform and its time-delayed signal are used for 1-bit random number

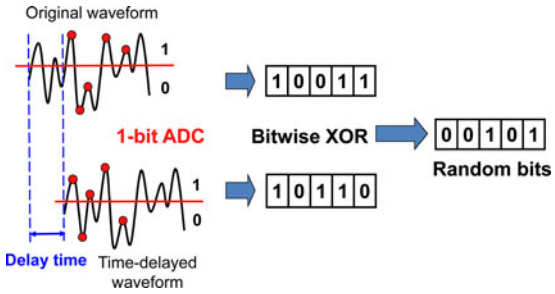

Fig. 3. Schematics of 1-bit random number generation method. ADC: analog-to digital conversion, XOR: exclusive-OR.

generation. A threshold value for each temporal waveform is selected around the mean value to satisfy the condition where the probability of the occurrence of bit "0" is as close to 50% as possible for generated random bits [15]. The temporal waveforms are sampled at a fixed clock rate and compared with the threshold values. A bit "0" or "1" is generated from one sampled data when the sampled data are below or above the threshold value. A logical exclusive-OR (XOR) operation is executed between two bits generated from the original and time-delayed temporal waveforms at one sampling point, and used as a random bit. This procedure is repeated to generate a random-bit stream. The random-bit generation rate matches the sampling rate in this scheme.

The randomness of bit sequences is tested using a standard statistical test suite for random number generators provided by the National Institute of Standard Technology (NIST), known as NIST Special Publication 800-22 (NIST SP 800-22) [41]. The NIST SP 800-22 test consists of 15 statistical tests, and the tests are performed using 1000 samples of 1 Mb sequences (=1 Gb) and the significance level $\alpha = 0.01$ [41].

We changed the sampling rate and evaluate the randomness of bit sequences generated from the SLD and the semiconductor laser by using the NIST SP 800-22 tests. Fig. 4(a) shows the number of passed NIST tests as a function of the sampling time (i.e., the inverse of the sampling rate) for the 1-bit random number generation with the SLD. Five 1-Gb 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 in Fig. 4(a). "15" indicates that all the NIST tests are passed on the vertical axis of Fig. 4. When the sampling time is long and the sampling rate is slow, we succeeded in generating random bits that can pass all the 15 statistical tests of randomness with the SLD. As the sampling time is decreased and the sampling rate is increased, some of the random bits cannot pass all the NIST tests. The maximum random-bit generation rate is 8.33 Gb/s for the SLD, as shown in Fig. 4(a). In the case of the semiconductor laser shown in Fig. 4(b), the whole characteristic is similar to the case for the SLD. However, more random bits are failed in some of the NIST tests even for slow sampling rate (long sampling time). The maximum random-bit generation rate is 8.33 Gb/s for the semiconductor laser, when it is evaluated by the median [black dots in Fig. 4(b)]. This is the same result as the case for the SLD. This similarity results from the fact that similar bandwidths of the flat RF spectra are used

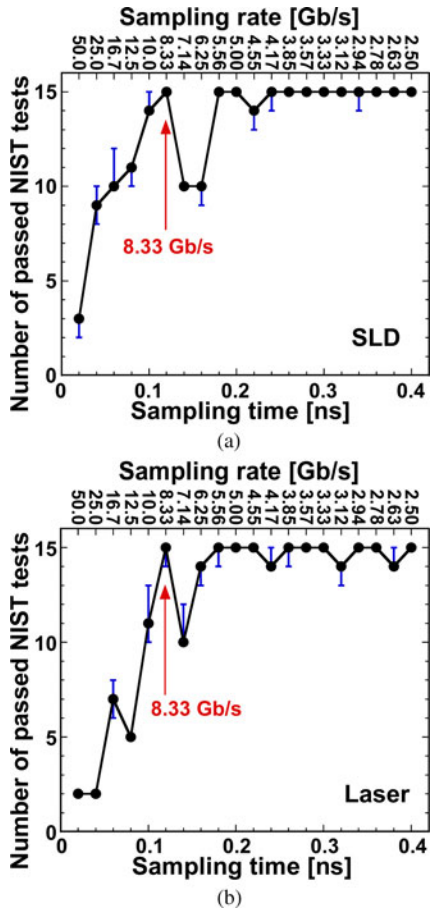

Fig. 4. Number of passed NIST tests as a function of the sampling time (i.e., the inverse of the sampling rate) for the 1-bit random number generation with (a) SLD and (b) semiconductor laser. Five 1-Gb sequences of random bits are used for each NIST test and the median of the five test results is plotted with error bars of the maximum and minimum values. "15" indicates that all the NIST tests are passed on the vertical axis.

(∼15 GHz) for 1-bit random number generation. We found that the maximum frequency component affects the characteristics of generated random numbers if the spectrum is flat over some frequency range, even though low-frequency components are missing for the chaotic semiconductor laser.

We evaluated the relationship between the sampling rate succeeded in generating good random bits and the autocorrelation function of the temporal waveforms generated from the SLD and the semiconductor laser. Fig. 5(a) shows the absolute value of the autocorrelation function of the SLD. The red circles indicate the sampling time (sampling rate) where generated random bits pass all the 15 NIST tests, and the blue squares indicate the sampling time where random bits fail some of the NIST tests. It is found that good random bits can be generated when the autocorrelation value is less than 4×10^{-2}. Therefore, the characteristics of Fig. 4(a) can be explained from the autocorrelation function shown in Fig. 5(a), i.e., lower autocorrelation values result in good random-bit generation. Fig. 5(b) shows the autocorrelation function and the results of the evaluation of random bits generated at different sampling times for the chaotic semiconductor laser. Compared with the case of the SLD in

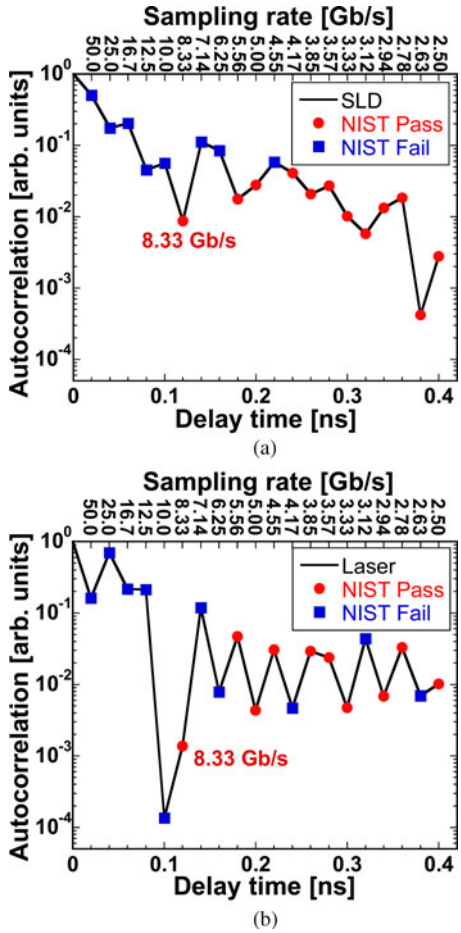

Fig. 5. Absolute value of the autocorrelation function of the temporal waveform generated from (a) SLD and (b) chaotic semiconductor laser used for 1-bit random number generation. The red circles indicate the sampling time where generated random bits pass all the 15 NIST tests, and the blue squares indicate the sampling time where random bits fail some of the NIST tests. The sampling rate is the inverse of the sampling time.

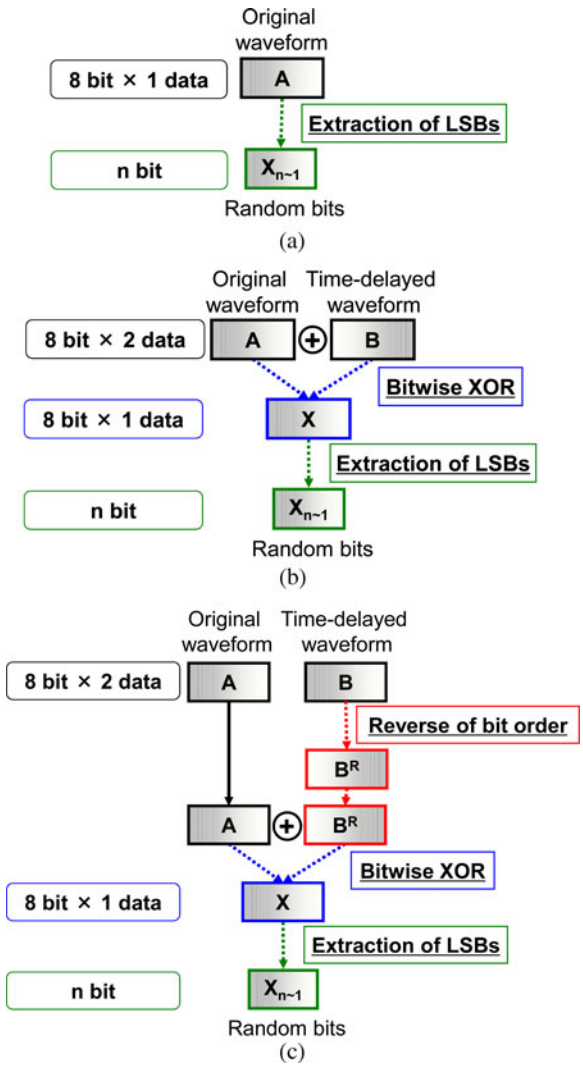

Fig. 6. Schematics of multibit random-number generation methods used in this experiment. (a) LSB method [17], [20]: some LSBs are extracted from a single irregular waveform. (b) XOR method [19]: an irregular temporal waveform and its time-delayed signal are converted into 8-bit signals in the digital oscilloscope and bit-wise XOR operation is carried out between the two 8-bit signals. Some LSBs of the resultant 8-bit signal are extracted and used for random numbers. (c) Reverse method [29]: the order of the 8-bit time-delayed signal is reversed. The original signal and bit-order-reversal signal of the time-delayed waveform are used for the bit-wise XOR operation, and some LSBs are extracted.

Fig. 5(a), the characteristics of the autocorrelation function are not directly related to the sampling times succeeded in generating good random bits. For example, the random bits sampled at 0.1 ns cannot pass all the NIST tests, even though the autocorrelation value is $\sim 10^{-4}$. This result will be investigated in detail in our future work.

V. Multibit Random Number Generation

A. Methods

Next, we used some multibit schemes for random number generation to evaluate the characteristics of random number generators based on the SLD and the semiconductor lasers. Fig. 6 shows the schematics of multibit random-number generation methods used in this experiment. The simplest method in Fig. 6 is the extraction of some least significant bits (LSBs) from a single irregular waveform [17], [20], as shown in Fig. 6(a). The number of LSBs can be changed to control the randomness of generated bits. This method is referred to as the LSB method. Fig. 6(b) shows another method [19], where an irregular temporal waveform and its time-delayed signal are used for random-bit generation. The two signals are converted into 8-bit signals in the digital oscilloscope and bit-wise exclusive-OR (XOR) operation is carried out between the two 8-bit signals. Some LSBs of the resultant 8-bit signal are extracted and used for random bits. This method is referred to as the XOR method. Fig. 6(c) shows a similar method to the XOR method; however, one additional procedure is included. An irregular temporal waveform and its time-delayed signal are used and the order of the 8-bit time-delayed signal is reversed, i.e., the most significant bit (MSB) becomes the LSB, the second MSB becomes the second LSB, and so on [29]. The original signal and the bit-order-reversal signal of the time-delayed waveform are used for the bit-wise XOR operation, and some LSBs are extracted. This method is

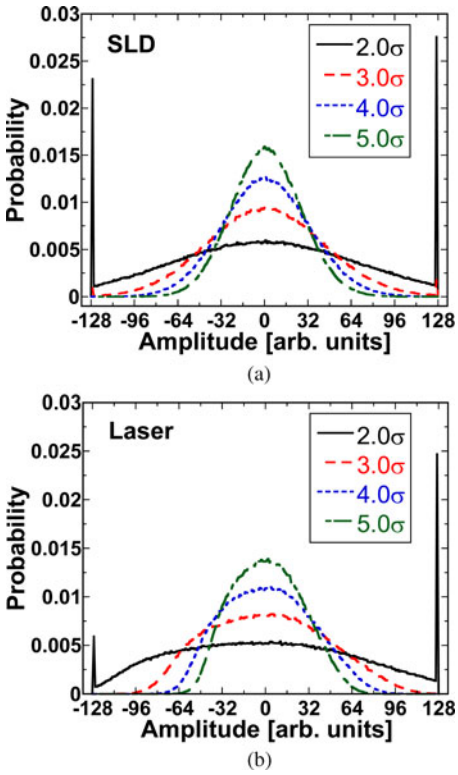

Fig. 7. Probability density functions of the temporal waveforms when the detection window size ($\pm n$ times σ) for the temporal waveforms is changed for (a) SLD and (b) semiconductor lasers. σ: standard deviation of the temporal waveforms.

referred to as the reverse method. We applied these three multibit schemes of random number generation for the SLD and the semiconductor lasers. For all the multibit generation methods, a threshold for the MSB is set to the mean value of the temporal waveform.

B. Results

It is important to adjust the amplitudes of irregular temporal waveforms to the 8-bit-vertical resolution (from -127 to $+127$ in integer) of the digital oscilloscope. We control the amplitude of the temporal waveform by using the variable attenuator in front of the photodetector (see Fig. 1). The amplitude of the temporal waveform is determined by the standard deviation σ of the temporal waveform. The width of the 8-bit vertical window of the digital oscilloscope (i.e., detection window size) is denoted as $\pm n$ times σ, where n is a positive number. Fig. 7 shows the probability density functions of the temporal waveforms when the detection window size for the temporal waveforms is changed for the SLD and the semiconductor lasers. When the 8-bit detection window size is set to ± 2.0 σ, where σ is 64 in the range of ± 127, large probabilities are obtained at the edges of ± 127, since too small or too large values are saturated and clipped at ± 127. As n is increased, the probability density function becomes sharper and the center peak value of the distribution becomes larger. Note that the distribution for the chaotic semiconductor lasers is more asymmetric than that for the SLD.

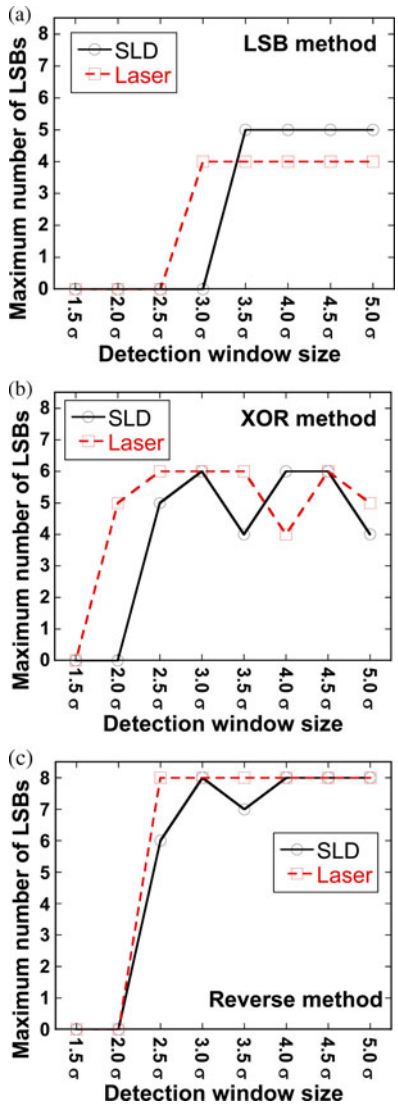

Fig. 8. Maximum number of LSBs as a function of the detection window size ($\pm n$ times σ) for the three multibit generation methods with the SLD and the semiconductor lasers. (a) LSB method, (b) XOR method, and (c) reverse method.

We evaluated the randomness of the generated bit sequences from the three multibit schemes with the SLD and the semiconductor lasers. We changed the number of LSBs and generated random bits for the three multibit generation schemes. We used the NIST SP 800-22 tests to evaluate the randomness of the generated bits, and determined the maximum number of LSBs for generated random bits that can pass all the NIST tests. We also changed the detection window size in the oscilloscope. Fig. 8 shows the maximum number of LSBs as a function of the detection window size ($\pm n$ times σ) for the three multibit generation methods with the SLD and the semiconductor lasers. Fig. 8(a)–(c) shows the results for the LSB, XOR, and reverse methods, respectively. In Fig. 8(a), the maximum numbers of LSBs are 5 for the SDL and 4 for the semiconductor lasers, corresponding to the equivalent generation rate of 250 Gb/s (=5 LSBs $\times$ 50 GS/s) and 200 Gb/s (=4 LSBs $\times$ 50 GS/s), respectively. These generation rates are obtained with a window size larger

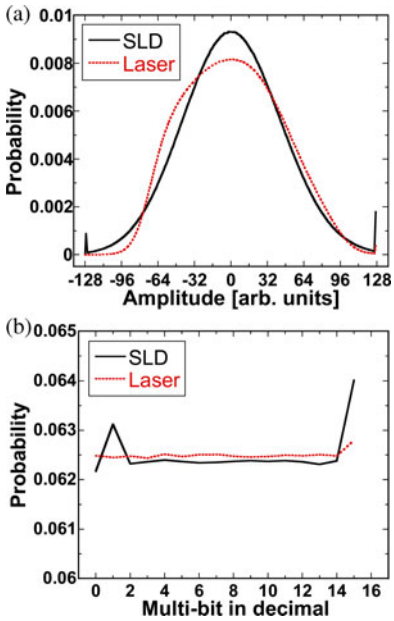

Fig. 9. (a) Examples of the probability density functions of the SLD and semiconductor laser when the amplitude is set to $\pm 3.0\,\sigma$. (b) Probability density functions for random bits generated by using the LSB method with the extraction of four LSBs.

than $\pm 3.5\sigma$ for the SLD and $\pm 3.0\sigma$ for the semiconductor laser. In Fig. 8(b), the maximum number of LSBs is 6 for both the SLD and the semiconductor lasers, corresponding to the equivalent generation rate of 300 Gb/s (=6 LSBs $\times$ 50 GS/s). There is also a difference in the maximum number of LSBs for small n between the SLD and the semiconductor lasers (e.g., $\pm 2.0\sigma$). In Fig. 8(c), the maximum number of LSBs is 8, corresponding to the equivalent generation rate of 400 Gb/s (=8 LSBs $\times$ 50 GS/s), for both the SLD and the laser. All the 8-bit information can be used effectively as random bits in the reverse method.

The discrepancy between the SLD and the laser shown in Fig. 8(a) results from asymmetry of the probability density functions. Fig. 9(a) shows examples of the probability density functions of the SLD and the semiconductor laser when the detection window size is set to $\pm 3.0\ \sigma$. The distribution for the chaotic semiconductor laser is more asymmetric than that for the SLD. It is worth noting that the peak values at ± 127 for the SLD are larger than those for the laser. These two peaks at ± 127 result in the degradation of symmetric distribution for random numbers. Fig. 9(b) shows the probability density functions for random bits generated by using the LSB method with the extraction of four LSBs. The distribution for the SLD is not as flat as that for the laser, particularly at 1 and 15, as shown in Fig. 9(b). These two peaks at 1 and 15 in Fig. 9(b) originate from the peaks at ± 127 in Fig. 9(a) for the SLD. Therefore, it is important to decrease the peak values at the edges of the distribution by adjusting the detection window size.

To evaluate the effect of the peaks at the edges of the distribution, we matched the sum of the two peak values at ± 127 in the distributions between the SLD and the laser. We also used small values of the sum of the two peaks so that the distribution becomes flat after the procedures of random number generation.

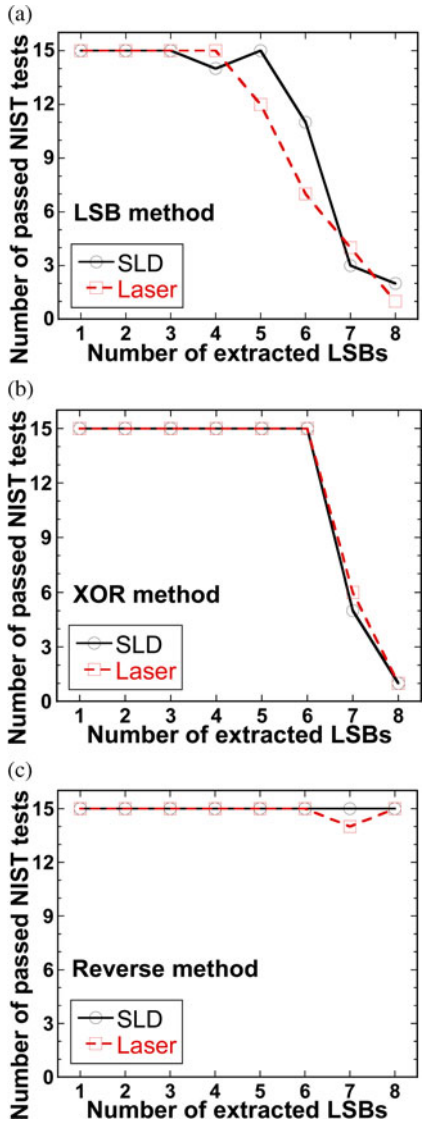

Fig. 10. Number of passed NIST tests as a function of the extracted LSBs for the three multibit generation methods with the SLD and the laser. "15" indicates that all the NIST tests are passed on the vertical axis. (a) LSB method, (b) XOR method, and (c) reverse method.

We used the detection window sizes of $\pm 4.0\sigma$ for the SLD and $\pm 3.5\sigma$ for the laser. We then evaluated the randomness of the generated bit sequences by using the NIST tests. Fig. 10 shows the number of passed NIST tests as a function of the extracted LSBs for the three multibit generation methods with the SLD and the laser. "15" indicates that all the NIST tests are passed on the vertical axis of Fig. 10. Overall characteristics of the results in Fig. 10(a)–(c) are matched well between the SLD and the laser. In Fig. 10(a), there is a discrepancy between the results of the SLD and the laser, where the maximum numbers of LSBs are 5 and 4 for the SLD and the laser, respectively. This results from the symmetry of the distribution for the SLD than that for the laser. Symmetric distribution results in more extraction of the LSBs after the procedure of multibit random number generation.

VI. Discussions

We investigated the characteristics of random numbers generated from the noisy SLD and the chaotic semiconductor laser. For single-bit generation of random numbers, the maximum generation rate is 8.33 Gb/s for both the SLD and the laser with the similar bandwidth of ∼15 GHz. Low autocorrelation values at the sampling time result in good random-bit generation for the SLD; however, it is not always the case for the chaotic laser. For multibit generation schemes, we obtained the generation rate up to 400 Gb/s for both the SLD and the laser. A discrepancy is found for a multibit generation scheme, where five LSBs can be used for the SLD and four LSBs are used for the laser to generate good random numbers using the LSB method. However, we cannot find significant difference between the noisy SLD and the chaotic semiconductor laser in terms of random number generation. One reason is that we used similar RF spectra for both cases: broad and flat spectra up to ∼15 GHz are used. From our results, both optical sources can be good candidates for fast physical random number generators.

For the 1-bit generation scheme (see Fig. 4), "block-frequency" and "runs" tests are the most difficult tests to pass in the 15 tests of NIST SP 800-22. This fact indicates that the structure of short-term correlation remains in random bits generated by the 1-bit generation scheme. Short-term correlation of temporal waveforms needs to be avoided to pass these two tests. For the multibit generation schemes (see Figs. 8 and 10), "nonoverlapping- template" and "random-excursions" tests are the most difficult tests to pass. Nonoverlapping-template tests consist of 148 pattern-matching tests and it is difficult to pass all the tests in general [41].

We did not consider the theoretical aspect of noise-based and chaos-based random number generators in this study. However, it is important to clarify the origin of randomness in both of the optical sources. In the case of SLDs, amplified spontaneous emission originates from random quantum noise. In the case of chaotic lasers, nonlinear amplification of intrinsic noise by chaotic dynamics is the origin of randomness [30], [31], [42], and the entropy rate can be evaluated from the maximum Lyapunov exponent [31]. These theoretical works guarantee randomness of these optical random number generators and are very important as pieces of evidence of randomness.

VII. Conclusion

We investigated two optical sources used for random number generation: SLD and semiconductor lasers. Amplified spontaneous emission noise is generated in the SLD and chaotic intensity fluctuation is generated in a semiconductor laser. We investigated the characteristics of random number generation for both of the optical sources. For single-bit generation of random numbers, the maximum generation rate is 8.33 Gb/s for both the SLD and the laser with the similar bandwidth of ∼15 GHz. For multibit generation schemes, we obtained the generation rate up to 400 Gb/s for both the SLD and the laser. The overall characteristics are similar between the SLD and laser, since similar bandwidths of the RF spectra are used. The probability density function of the SLD is more symmetric than that of the chaotic laser. This fact results in slightly good performance of random number generation used in the SLD for multibit generation.

References

[1] D. Eastlake, J. Schiller, and S. Crocker. (2005). "Randomness requirements for security," RFC4086, [Online]. Available: http://tools.ietf.org/html/rfc4086

[2] (2001). "Security requirements for cryptographic modules," FIPS 140-2, [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] N. Metropolis and S. Ulam, "The monte carlo method," *J. Amer. Statistical Assoc*., vol. 44, pp. 335–341, 1949.

[4] D. E. Knuth, *The Art of Computer Programming: vol. 2: Seminumerical Algorithms*, 3rd ed. Reading, MA, USA: Addison-Wesley, 1996.

[5] L. Dorrendorf, Z. Gutterman, and B. Pinkas, "Cryptanalysis of the windows random number generator," in *Proc. 14th ACM Conf. Comput. Commun. Security*, 2007, pp. 476–485.

[6] H. Miyazawa and M. Fushimi, "An implementation of a 5-term GFSR random number generator for parallel computations," in *Proc. Int. Symp. Operations Res. Appl*., 2009, pp. 448–452.

[7] J. Kelsey, Entropy and entropy sources in X9.82, National Inst. Standards and Technol., MD, USA, 2004.

[8] W. Schindler and W. Killmann, "Evaluation criteria for true (physical) random number generators used in cryptographic applications," in *Cryptographic Hardware and Embedded Systems-CHES 2002*. (Lecture Notes in Computer Science. vol. 2523). Berlin, Germany: Springer-Verlag, 2002, pp. 431–449.

[9] B. Jun and P. Kocher, "The Intel random number generator," White Paper Prepared for Intel Corporation, Cryptography Research Inc., [Online]. Available: http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf

[10] W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, "An integrated analog/digital random noise source," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl*., vol. 44, no. 6, pp. 521–528, Jun. 1997.

[11] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, "A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC," *IEEE Trans. Comput*., vol. 52, no. 4, pp. 403–409, Apr. 2003.

[12] A. Uchida, *Optical Communication With Chaotic Lasers—Applications of Nonlinear Dynamics and Synchronization*. Weinheim, Germany: Wiley-VCH, 2012.

[13] 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," *Nat. Photon*., vol. 2, no. 12, pp. 728–732, 2008.

[14] T. E. Murphy and R. Roy, "The world's fastest dice," *Nat. Photon*., vol. 2, no. 12, pp. 714–715, 2008.

[15] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," *IEEE J. Quantum Electron*., vol. 45, no. 11, pp. 1367–1379, Nov. 2009.

[16] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," *Opt. Exp*., vol. 17, no. 11, pp. 9053–9061, 2009.

[17] 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. 024102-1–024102-4, 2009.

[18] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nat. Photon*., vol. 4, pp. 58–61, 2010.

[19] 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," *Opt. Exp*., vol. 18, no. 6, pp. 5512–5524, 2010.

[20] 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. Exp*., vol. 18, no. 18, pp. 18763–18768, 2010.

[21] P. Li, Y.-C. Wang, and J.-Z. Zhang, "All-optical fast random number generator," *Opt. Exp*., vol. 18, no. 19, pp. 20360–20369, 2010.

[22] T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," *Phys. Rev. A*, vol. 83, pp. 031803(R)-1–031803(R)-4, 2011.
[23] 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," *Opt. Exp.*, vol. 19, no. 7, pp. 5713–5724, 2011.
[24] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, K. Tsuzuki, A. Uchida, and P. Davis, "Random optical pulse generation with bistable semiconductor ring lasers," *Opt. Exp.*, vol. 19, no. 8, pp. 7439–7450, 2011.
[25] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation," *Opt. Lett.*, vol. 36, no. 23, pp. 4632–4634, 2011.
[26] Y. Zhang, J. Zhang, M. Zhang, and Y. Wang, "2.87-Gb/s random bit generation based on bandwidth-enhanced chaotic laser," *Chin. Opt. Lett.*, vol. 9, no. 3, pp. 031404-1–031404-3, 2011.
[27] P. Li, Y. Wang, A. Wang, L. Yang, M. Zhang, and J. Zhang, "Direct generation of all-optical random numbers from optical pulse amplitude chaos," *Opt. Exp.*, vol. 20, no. 4, pp. 4297–4308, 2012.
[28] 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. Exp.*, vol. 20, no. 7, pp. 7496–7506, 2012.
[29] Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8×50 Gb/s," *IEEE Photon. Technol. Lett.*, vol. 24, no. 12, pp. 1042–1044, Jun. 2012.
[30] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K. Arai, A. Uchida, and P. Davis, "Theory of fast nondeterministic physical random-bit generation with chaotic lasers," *Phys. Rev. E*, vol. 85, pp. 046215-1–046215-9, 2012.
[31] T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Estimation of entropy rate in a fast physical random-bit generator using a chaotic semiconductor laser with intrinsic noise," *Phys. Rev. E*, vol. 85, pp. 016211-1–016211-7, 2012.
[32] J. Zhang, Y. Wang, L. Xue, J. Hou, B. Zhang, A. Wang, and M. Zhang, "Delay line length selection in generating fast random numbers with a chaotic laser," *Appl. Opt.*, vol. 51, no. 11, pp. 1709–1714, 2012.
[33] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett.*, vol. 35, no. 3, pp. 312–314, 2010.
[34] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Opt. Exp.*, vol. 18, no. 23, pp. 23584–23597, 2010.
[35] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Opt. Lett.*, vol. 36, no. 6, pp. 1020–1022, 2011.
[36] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *J. Lightw. Technol.*, vol. 30, no. 9, pp. 1329–1334, 2012.
[37] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.*, vol. 71, no. 4, pp. 1675–1680, 2000.
[38] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Appl. Phys. Lett.*, vol. 93, no. 3, p. 031109, 2008.
[39] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nat. Photon.*, vol. 4, no. 10, pp. 711–715, 2010.
[40] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, pp. 1021–1024, 2010.
[41] 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. (Apr. 2010), "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, [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf
[42] C. Bracikowski, R. F. Fox, and R. Roy, "Amplification of intrinsic noise in a chaotic multimode laser system," *Phys. Rev. A*, vol. 45, pp. 403–408, 1992.

Taiki Yamazaki was born in Saitama, Japan. He received the B.E. and M.E. degrees in information and computer sciences from Saitama University, Saitama, Japan, in 2010 and 2012, respectively.

In 2012, he joined East Japan Railway Compary, Japan.

Atsushi Uchida (S'97–M'00) was born in Saitama, Japan. He received the B.S., M.S., and Ph.D. degrees in electrical engineering from Keio University, Yokohama, Japan, in 1995, 1997, and 2000, respectively.

In 2000, he joined the Department of Electronics and Computer Systems, Takushoku University, Tokyo, Japan, where he was a Research Associate. He was a Visiting Researcher at the ATR Adaptive Communications Research Laboratories, Kyoto, Japan, from 2001 to 2002. He was a JSPS Postdoctoral Fellow at the University of Maryland, College Park, USA, from 2002 to 2004. He was a Lecturer at the Department of Electronics and Computer Systems, Takushoku University, Tokyo, from 2005 to 2008. Since 2008, he has been an Associate Professor at the Department of Information and Computer Sciences, Saitama University, Saitama. He is currently involved in research on synchronization of chaotic lasers and its applications for optical secure communications, secure key generation using chaotic lasers for cryptography, fast physical random number generation using chaotic lasers, and synchronization of chaos in nonlinear dynamical systems.

Dr. Uchida is a member of the Optical Society of America, the American Physical Society, the Institute of Electronics, Information, and Communication Engineers of Japan, the Japan Society of Applied Physics, the Laser Society of Japan, and the Optical Society of Japan.