Optical Engineering

SPIEDigitalLibrary.org/oe

Frequency noise characteristics of a diode laser and its application to physical random number generation

Shinya Maehara
Kohei Kawakami
Hideaki Arai
Kenji Nakano
Kohei Doi
Takashi Sato
Yasuo Ohdaira
Shuichi Sakamoto
Masashi Ohkawa

Frequency noise characteristics of a diode laser and its application to physical random number generation

Shinya Maehara
Niigata University
Faculty of Engineering
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata 950-2181, Japan

Kohei Kawakami
Hideaki Arai
Kenji Nakano
Niigata University
Graduate School of Science and Technology
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata 950-2181, Japan

Kohei Doi
Niigata University
Gender Equality Office
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata 950-2181, Japan

Takashi Sato
Yasuo Ohdaira
Shuichi Sakamoto
Masashi Ohkawa
Niigata University
Faculty of Engineering
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata 950-2181, Japan
E-mail: tsato@eng.niigata-u.ac.jp

Abstract. We describe a method of generating physical random numbers by means of a diode laser that has an extremely wide-band frequency-noise profile. Fluctuations in the laser frequency affect the intensity of the light transmitted through the optical frequency discriminator, detected thereafter as random fluctuations. This allows us to simultaneously generate 8 random bit streams, due to the parallel processing of 8-digit binary numbers sampled by an 8-bit analog-to-digital converter. Finally, we generated physical random numbers at a rate of 3 Gbit/s, by combining one data stream with another stream that is delayed by 2 ms, by exclusive-OR.
 [DOI: 10.1117/1.OE.52.1.014302]

Subject terms: physical random number generation; diode laser; frequency noise; intensity noise.

Paper 121107P received Jul. 30, 2012; revised manuscript received Nov. 28, 2012; accepted for publication Nov. 30, 2012; published online Jan. 7, 2013.

1 Introduction

Today's diode lasers boast features that were unimaginable not long ago: ultra-compact, durable design, high power and high efficiency, low maintenance and low cost. In the interest of fairness, however, there are certain negative aspects that should be considered before moving to "upgrade" to these devices: a not-insignificant level of AM and FM quantum noise,[1–3] as well as optical feedback noise.[4] The former, generated by the spontaneous fluctuation of emissions, also cause fluctuations in carrier density and the refractive index of the cavity, which in-turn results in random fluctuations in optical power and frequency. The optical feedback noise, on the other hand, stems from the flow of light from an external reflector to the laser's active layer, which, in-turn causes unstable, i.e., oscillatory and/or chaotic, output and/or mode-hopping noises. It is therefore vitally important that users be able to correctly interpret these signals to ensure safe operation.

Our investigations of diode lasers' frequency-noise characteristics have led us to the conclusion that their oscillation frequency has a narrow linewidth and moves very fast at random. Owing to this frequency-noise characteristic, we can observe the large intensity fluctuation from the output beam of a diode laser through a frequency discriminator, such as a Fabry-Perot etalon or an absorption cell. This intensity fluctuation shows a random characteristic, so we could produce physical-random-numbers using the diode lasers' frequency fluctuation. While physical random numbers are currently being generated at a rate of 3 Gbit/s, we believe that far higher speeds are achievable if we simply take advantage of the wide and fast frequency noise characteristics of the diode laser.

The generation of physical random numbers has been approached from a number of different angles. One method, for example, is based on the rate of radioactive decay; another, from thermal noise of a resistor; and a third, from shot noise of a diode. While they are all capable of producing physical random numbers, the speeds at which they do so are slower than the typical pseudo-random number generator. There is yet another method of generating physical random numbers; measuring the phase noise of laser systems' spontaneously emitted light.[5,6] In this instance, a generation speed of 500 Mb/s has been reported. There are several other papers describing generators operating at the range of Gbit/s[7–10] that exploit the chaotic response of a diode laser whose light is reflected directly back to its source. Random numbers can be classified as either pseudo- or physical-random in character. Pseudo-random numbers are produced by deterministic algorithms characterized by a calculable periodicity, so they are thought to be ill-suited for the task

of creating safe cryptography in the era of ultra-high-speed data-processing, such as those provided by quantum computing. On the other hand, the noises emitted by Zener diodes and diode lasers are naturally-occurring random phenomena with no calculable periodicity, making them useful in applications such as next-generation cryptography and large-scale simulations required for understanding natural phenomena.

Yabuzaki et al.[11] used diode laser frequency noise in their high-resolution spectroscopy. The setup consists of nothing more than a diode laser, a frequency discriminator (such as an atomic absorption line), a very fast optical detector, and a spectrum analyzer. They observed that the light transmitted through the atomic absorption cell emitted a significant amount of noise during a slow sweep of the laser frequency. They also observed signals originating from the hyperfine structure of Cs, without sweeping the laser frequency.

In this paper, we propose a novel method for the first physical random number generation utilizing the frequency noise of a diode laser.[12–14] That is to say that we converted laser frequency fluctuations directly to fluctuations in the intensity of the light transmitted through the optical frequency discriminator, and then to 8-digit binary numbers by means of an analog-to-digital converter (ADC). The present work carries forward our research in the area of physical-random number generation using the unique noise-profile of the Fabry-Perot diode laser.

2 Detection of Frequency Noise

Using a frequency discriminator, for example, an Rb absorption line or a Fabry-Perot etalon, we can convert frequency noise to intensity noise, generating physical random numbers in the process. Figure 1 shows the optical setup used to detect the signals that are proportional to the frequency noise produced by the diode laser. In this work, the Rb-D_2 absorption line was used as an optical frequency discriminator for converting the diode laser's 780 nm frequency noise to transmitted intensity noise signals. We used a 70 mW, single-mode diode laser (Sanyo, DL-7140-201) operating at 780 nm, and driven by a low-noise current source. The laser's thermostat (Yamaki, KLT-2E) controls temperature to within ± 0.01 K. We operated the diode laser at 73 mA (threshold current: 30 mA), controlling both injection current and temperature conditions, in order to tune the laser frequency to the Rb absorption line. As shown in Fig. 2, the spectral linewidth was determined to be 3 MHz at full width at half maximum

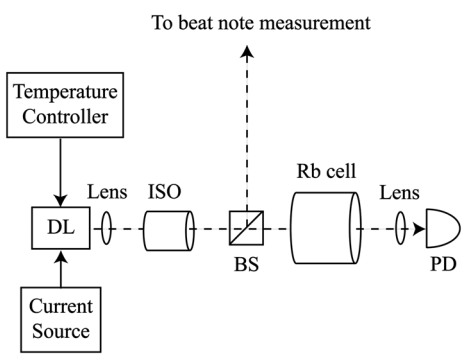

Fig. 1 Optical setup. DL: diode laser; ISO: optical isolator; BS: beam splitter; PD: photo detector.

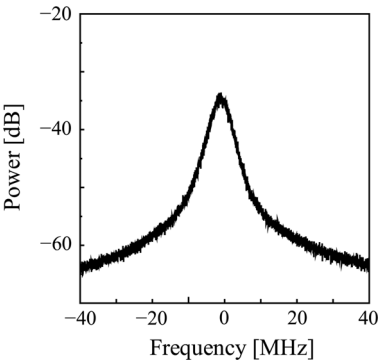

Fig. 2 The spectrum of beat note between two identical, independent diode lasers.

(FWHM) from the beat note between identical, temperature-controlled, free-running diode lasers. When the laser linewidth is too narrow, the intensity noise converted from the frequency noise in our system is reduced. If, on the other hand, the laser linewidth is too broad, most of frequency noise components are far from the absorption line, making it difficult to acquire an intensity noise of sufficient amplitude.

Figure 3 shows the conversion principle used to measure variations in intensity and voltage, based on frequency-shifts. Figure 3(a) describes the intensity of the transmitted signal, i.e., the absorption profile of the Rb-D_2 line obtained by sweeping the laser injection current. When absorption line spectra are characterized by steep slopes, small fluctuations in frequency translate to significant changes in light intensity. Therefore, the laser frequency was set at point P_1, where the slope of the absorption line spectrum is steepest. As Fig. 3(b) shows, frequency noise is converted to intensity noise by the frequency discriminator, i.e., the Rb absorption cell, when the laser frequency shifts around point P_1. Point P_1 has a steep slope that allows us to obtain a strong intensity noise signal, and then generate a physical random number originating from the frequency noise rather than having to rely on the amplifier's noise. Frequency noise, such as at P_2, P_3, or P_4, is not converted to transmitted light intensity noise, so we pick up only their small intensity noise emanating from the region where the laser frequency does not match the resonant frequency of Rb. So, the purpose of our study is to shine a bit more light on the mechanics of diode lasers' frequency noise and its potential applicability to such tasks as the generation of physical random numbers. The system we currently rely on for physical-random number-generation is quite simple, requiring nothing more than a diode laser, a frequency discriminator, and a photo detector.

3 Physical Random Number Generation System

Figure 4 shows the experimental setup for the physical random number generator. The laser beam passes through an optical isolator and then the Rb cell. Light intensity is detected by an avalanche photo diode (Hamamatsu, S2381, 1 GHz bandwidth), while voltage signals are amplified by a radio-frequency amplifier (COSMOWAVE, LPA-G39WD, 50 MHz to 8 GHz bandwidth). We used a digital oscilloscope (LeCroy, Wave Runner 62Xi-A, 600 MHz bandwidth, 10 GS/s) as an 8-bit ADC.

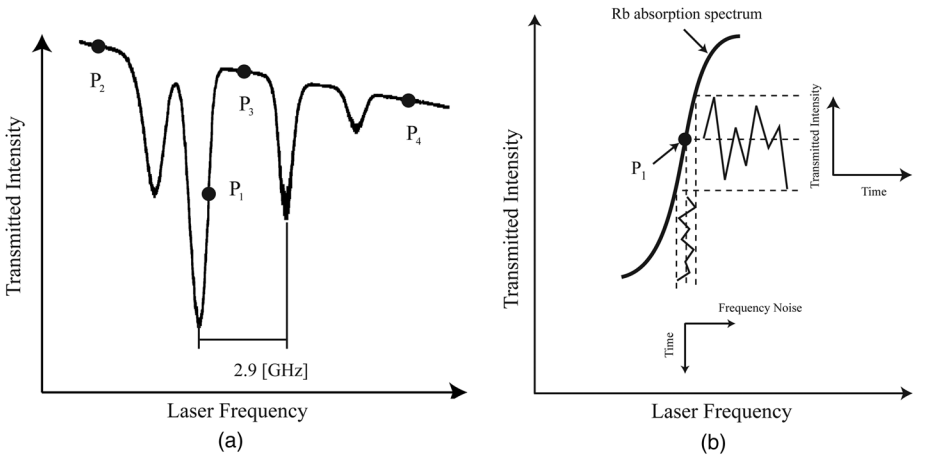

Fig. 3 (a) Observed Rb-D_2 absorption line and (b) conversion of laser frequency noise to laser intensity variation. The laser frequency is set at point P_1, by tuning the injection current. Off-resonant points P_2, P_3, and P_4 are used for references.

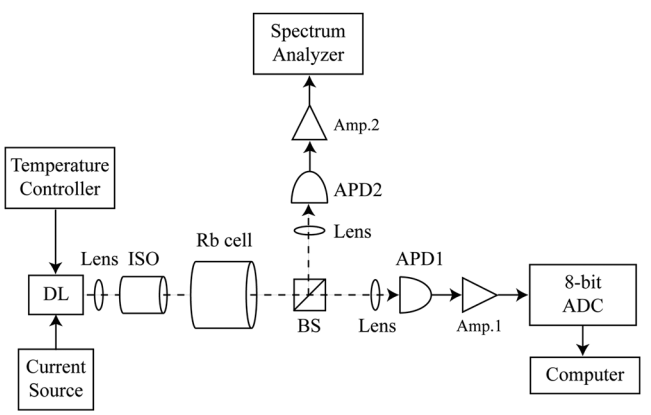

Fig. 4 Experimental setup. DL: diode laser; ISO: optical isolator; BS: beam splitter; APD: avalanche photo diode; Amp: amplifier; ADC: analog/digital converter.

As indicated in Fig. 5, we can generate 8 random bit-streams at a time, because the light intensity is sampled by an 8-bit ADC and converted to 8 digit binary data. They are uploaded to a computer, and verified in accordance with the National Institute of Standard Technology (NIST)'s test suites.[15,16] We also used a spectrum analyzer (ROHDE&SCHWARZ, FSU3, 20 Hz to 3.6 GHz bandwidth) to measure the noise of the light transmitted at several oscillation frequencies.

4 Experimental Results and Discussions

Yabuzaki et al. described significant intensity fluctuation or noise of the beam transmitted through the Cs cell near steeply-sloped areas of the absorption signal when the laser frequency was swept slowly around the Cs-D_1 absorption line.[11] In Fig. 6, the transmitted beam is viewed in a test using the Rb-D_2 absorption line. Here, we can demonstrate that the strongest signal is observed where the slope-angle is the steepest. We obtained high-intensity noise-signals proportional to the diode laser's frequency-fluctuation. Figure 7(a) shows the waveform of the discriminator output. In this experiment, by adjusting the injection current to about 73 mA, we set the laser frequency at position P_1, where the slope of Rb-D_2 absorption line is at its sharpest inclination, as shown in Fig. 3(a). The trace (1) is the signal waveform displayed on the digital oscilloscope, with signal waveforms being observed at different frequencies [see Fig. 3(a)]. When the laser beam was blocked at the entrance of the APD, a trace (3) [Fig. 7(b)] was obtained. Figure 7(c) represents the noise spectra of the transmitted light as measured by the spectrum analyzer; the results of which indicate that we can take full advantage of frequency noise components

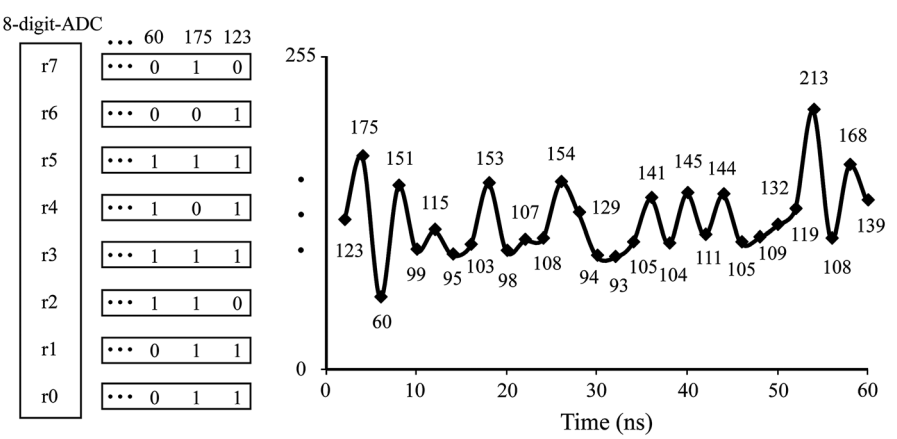

Fig. 5 Random number generation by means of transmitted light signals. A transmitted light signal is sampled at 500 MHz. Its voltage is converted to 8-bit binary data, from which we obtain 8 random bit streams at a time.

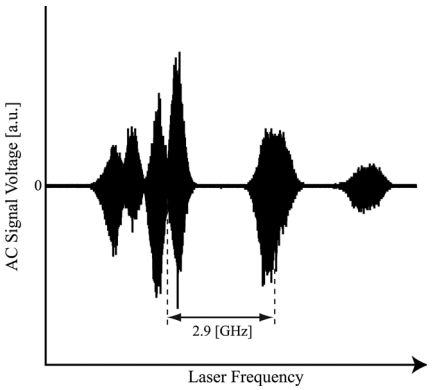

Fig. 6 Conversion of a frequency noise to a transmitted light intensity noise. As the laser frequency was slowly swept through the Rb-D_2 absorption line, we recorded the alternative current (AC) voltage output.

observed at point P_1, as high as 1 GHz, detected by an APD for physical random number generation.

Applying the method shown in Fig. 5, we can obtain 8 binary number streams, in-parallel, such as "r0," referring to the lowest digit, "r1," the second lowest, and so on. Our method follows the approach used by Saito et al.[17] to generate a physical random number. The 8 bit-sequences that were generated were subsequently evaluated, using NIST FIPS140-2[15] in the early stages of the experiment. As shown in Table 1, we obtained a high examination pass rate for bit-sequences r0 through r5. We also wanted to use NIST SP 800-22 tests,[16] which require a bit sequence of 1 Gbit length and are commonly used in other reports as an evaluation test for the pseudo-random numbers' randomness, to compare our result with other reports. Therefore, we prepared a 1 Gbit length bit sequence using binary numbers from r0 to r5, which have already been evaluated as random numbers in NIST FIPS140-2 tests. Here, we can obtain the equal probability of occurring "0" and "1" in bit-sequences using the exclusive OR operation between the bit-sequence and itself, delayed by 2 ms. This method is cited in Ref. 10. This operation is an integral part of any evaluation of physical-random-numbers when we use the examination method for pseudo-random number's randomness, such as NIST SP 800-22 tests. We evaluated our data using the NIST SP 800-22 statistical tests; Table 2 describes the outcome. In these tests, the statistical randomness for a binary stream is verified. The stream, which satisfies all tests, is considered to be a correct random number. From Table 2, we found that 1Gbit streams generated by frequency noise passed all test items. At other measurement points (P_2, P_3, P_4), results were similar to a "laser off" condition. Parameters, such as the laser's frequency, the laser's power, and the optical thickness of the Rb vapor, change and determine the intensity of the transmitted laser signal. When the variation is significant, the balance of "0's" and "1's" in the upper bits (for

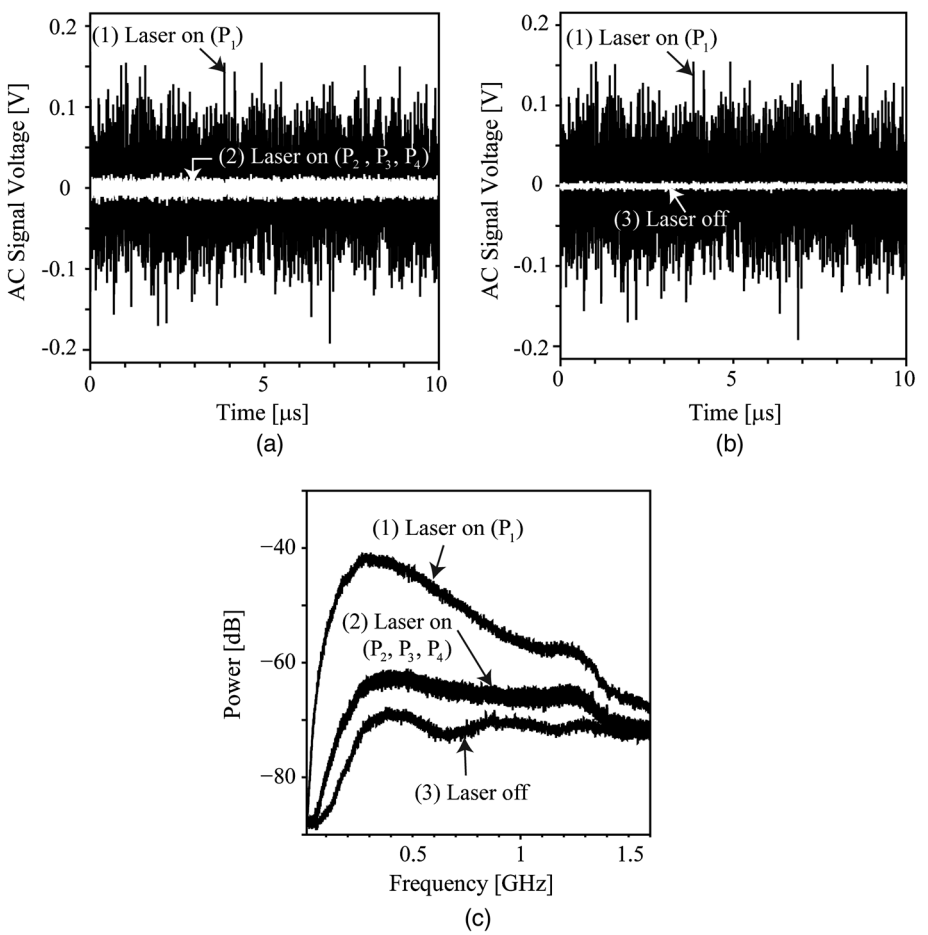

Fig. 7 Waveforms and spectra of transmitted light intensity signals. Detection of discriminator output: (Laser on/off) (1) the detection of the discriminator output at P_1, (2) the detection of the discriminator output at P_2, P_3 and P_4, and (3) the discriminator output is shut in front of the APD.

Table 1 Results of NIST FIPS 140-2 statistical tests. Statistical randomness for a binary stream consisted of 20,000 digits, verified by four tests consisting of the "monobit," the "poker," the "run," and the "longrun." We evaluated 10,000 sets of 20,000 binary numbers and calculated the examination pass rates, at every digit. "Total" means the examination pass rate of binary streams satisfied all four tests.

	r0	r1	r2	r3	r4	r5	r6	r7
Mono	99.96%	98.07%	99.87%	99.77%	99.96%	99.97%	99.11%	99.27%
Poker	99.99%	99.88%	99.99%	99.97%	100.0%	100.0%	97.57%	90.75%
Run	99.52%	98.23%	99.26%	99.29%	99.49%	99.50%	6.16%	0.01%
Longrun	99.94%	99.99%	99.97%	99.96%	99.96%	99.93%	99.98%	99.97%
Total	99.43%	96.55%	99.11%	99.07%	99.43%	99.43%	6.09%	0.016%

example, r7, r6, and r5 in our manuscript) approaches a rough equivalence, demonstrating its random nature. On the other hand, when the change is small, we cannot expect this randomness in the upper bits. Thus, we demonstrated the generation of physical random number based on the frequency noise of the diode laser. Because we used an 8-bit ADC at a sampling rate of 500 MS/s, we were able to obtain 4 Gbit/s at full speed when all binary streams passed the test. Hence, we generated physical-random numbers at a rate of 3 Gbit/s.

Our system allowed us to obtain results that were in good compliance with the standards set forth in NIST SP 800-22. Unfortunately, however, we still have a great deal of work ahead of us in our effort to accurately detect and measure random high-speed output, because of: (1) our inability to control the cut-off frequency of the APD; and (2) the limited performance of our ADC in regards to its analog bandwidth and sampling rate. So, it is of vital importance that we use a noise source having high speed random fluctuation in order to achieve faster physical random number generation. We

Table 2 Results of NIST Special Publication 800-22 statistical tests. A set of 1000 sequences generated using the lower 6-digits is evaluated. Each sequence contains 1 Mbits data. Significance level $\alpha = 0.01$, the P value (uniformity of p values) should be larger than 0.0001, while the proportion should be greater than 0.9805608.

	Laser on (P_1)			Laser off		
Statistical test	P value	Proportion	Result	P value	Proportion	Result
Frequency	0.120909	0.9830	Success	0.000000	0.0310	Failure
Block frequency	0.099513	0.9880	Success	0.000000	0.0000	Failure
Cumulative sums	0.068999	0.9820	Success	0.000000	0.0200	Failure
Runs	0.803720	0.9930	Success	0.000000	0.0000	Failure
Longest run	0.494392	0.9900	Success	0.000000	0.0000	Failure
Rank	0.131122	0.9920	Success	0.000000	0.0000	Failure
Nonoverlapping template	0.022760	0.9890	Success	0.000000	0.0000	Failure
Overlapping template	0.560545	0.9890	Success	0.000000	0.0000	Failure
Universal	0.034942	0.9880	Success	0.000000	0.0000	Failure
Approximate entropy	0.352107	0.9950	Success	0.000000	0.0000	Failure
Random excursions	0.042950	0.9866	Success	—	—	Failure
Random excursions variant	0.064103	0.9900	Success	0.000000	1.0000	Failure
Serial	0.467322	0.9890	Success	0.000000	0.0000	Failure
Linear complexity	0.494392	0.9890	Success	0.618385	0.9930	Success

also need to introduce a photo detector with a faster response, a broad-range radio-frequency amplifier, and ADC with a broad analog bandwidth, high sampling rate, and high resolution. Although the frequency noise spectrum of the Fabry-Perot type diode laser extends to several GHz, vertical cavity surface emitting lasers (VCSEL) are characterized by even broader oscillation-linewidth and frequency-noise bandwidth, and therefore could be used as higher-speed noise sources. Therefore, we can expect further improvements in physical random number generation speed. Laser frequency is set in a sloped area of the Rb absorption line, under temperature-controlled free-running conditions. Therefore, we should generate physical random numbers with stable laser frequency in order to remove any useless low frequency components.

5 Conclusion

We proposed, designed, and built a system for generating physical random numbers using the frequency noise generated by a Fabry-Perot-type diode laser. We then evaluated the binary number line's statistical properties, and, in the end, achieved a physical random number generation speed of 3 Gbit/s, maximum.

The next step in this process will require the introduction of a photo detector with improved response-time, a broad-range radio-frequency amplifier and a broadband ADC, a high sampling rate, and a high resolution, i.e., more output digits. To improve the speed at which "fast physical random numbers" are generated, we need to apply the frequency noise characteristics of the diode laser in conjunction with a broad-spectrum, high FM noise-bandwidth light-source, such as a VCSEL.

Acknowledgments

We would like to thank Mr. Hiroki Takamori for his help in our experiment. This work is supported in part by a Grant-in-Aid for Scientific Research (No. 22560035) from the Japan Society for the Promotion of Science.

References

1. Y. Yamamoto, "AM and FM quantum noise in semiconductor lasers–part I: theoretical analysis," *IEEE J. Quantum Electron.* **19**(1), 34–46 (1983).
2. Y. Yamamoto, S. Saito, and T. Mukai, "AM and FM Quantum noise in semiconductor lasers–part I: comparison of theoretical and experimental results for AlGaAs lasers," *IEEE J. Quantum Electron.* **19**(1), 47–58 (1983).
3. M. Ohtsu et al., "Estimation of the ultimate frequency stability of semiconductor lasers," *Jpn. J. Appl. Phys.* **22**(7), 1157–1166 (1983).
4. R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.* **16**(3), 347–355 (1980).
5. H. Guo et al., "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E* **81**(5), 051137 (2010).
6. B. Qi et al., "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett.* **35**(3), 312–314 (2010).
7. A. Uchida et al., "Fast physical random bit generation with chaotic semiconductor lasers," *Nat. Photon.* **2**, 728–732 (2008).
8. I. Reidler et al., "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.* **103**(2), 024102 (2009).
9. I. Kanter et al., "An optical ultrafast random bit generator," *Nat. Photon.* **4**, 58–61 (2009).
10. K. Hirano et al., "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt. Express* **18**(6), 5512–5524 (2010).
11. T. Yabuzaki, T. Mitsui, and U. Tanaka, "New type of high-resolution spectroscopy with a diode laser," *Phys. Rev. Lett.* **67**(18), 2453–2456 (1991).
12. H. Nishimura et al., "Physical-random number generation using laser diodes' inherent noises," *Proc. SPIE* **7597**, 75970M (2010).
13. T. Ushiki et al., "Super fast physical-random number generation using laser diode frequency noises," *Proc. SPIE* **7933**, 79332F (2011).
14. H. Takamori et al., "Fast random-number generation using a diode laser's frequency noise characteristic," *Proc. SPIE* **8255**, 825521 (2012).
15. Information Technology Laboratory, "Security requirements for cryptographic modules," NIST Federal Information Processing Standards Publication 140-2 (2001).
16. A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22 Revision 1a, http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html (2010).
17. T. Moro et al., "Generation of physical random number using the lowest bit of an A-D converter," *IEICE Trans. Electron.* **J88-A**(6), 714–721 (2005), (in Japanese).

Shinya Maehara received his BE in electrical and electronics engineering from Niigata University, Japan, in 2001. He received his ME from the Graduate School of Science and Technology, Niigata University, in 2003. He is currently a research assistant at Niigata University. His research subject is the frequency noise characteristic of a diode laser and its application.

Kohei Kawakami received his BE from Niigata University, Japan, in 2011. He is currently pursuing his ME degree from the Graduate School of Science and Technology, Niigata University.

Hideaki Arai received his BE from Niigata University, Japan, in 2008. He received his ME degree from the Graduate School of Science and Technology, Niigata University, in 2010. He is currently a doctoral course student at Niigata University.

Kenji Nakano received his BE from Niigata University, Japan, in 2005. He received his ME from the Graduate School of Science and Technology, Niigata University, in 2007. He is currently a doctoral course student at Niigata University.

Kohei Doi received his BE in electrical and electronics engineering from Niigata University, Japan, in 2004. He received his ME and Dr Eng degrees from Niigata University in 2006 and 2010, respectively. He currently works at the Gender Equality Office at Niigata University.

Takashi Sato received his BS, MS, and PhD in electronic engineering from Kyoto University in 1976, 1978, and 1983, respectively. He is currently a professor at Niigata University. His research subjects are in laser-production of Alkali Hydride particles, frequency stabilization of dye lasers and semiconductor lasers, the oscillation frequency shift of a semiconductor laser in a magnetic field, and the application of nonlinear optical effects for frequency stabilization of a semiconductor laser.

Yasuo Ohdaira received his BE, ME, and PhD degrees in electronics from Yamanashi University, in 1996, 1998, and 2003, respectively. He has been engaged in the research of high resolution laser spectroscopy and spin control in optical near-fields. He is currently an associate professor at Niigata University. His research interests lie in the area of near-filed signal control using nano-structured organic material systems.

Shuichi Sakamoto received his BE, ME, and PhD degrees in mechanical engineering from Niigata University, Japan, in 1986, 1988, and 1991, respectively. In 1992, he joined the faculty of engineering, Niigata University, Japan, as a research associate, and is currently an associate professor. His research interests include acoustics, noise control, and analysis of signal.

Masashi Ohkawa received his BE, ME, and PhD in electrical engineering from Osaka University, Japan, in 1984, 1986, and 1989, respectively. In 1989, he joined the faculty of engineering, Niigata University, Japan, as a research associate, and is currently a professor. His research interests include integrated optic devices and holography.