Fast Random-Number Generation Using a Diode Laser's Frequency Noise Characteristic

Hiroki Takamori†, Kohei Doi†, Shinya Maehara†, Kohei Kawakami
Takashi Sato‡, Masashi Ohkawa‡, and Yasuo Odaira‡
†C/O Sato Lab., Graduate School of Science and Technology, Niigata University
‡Faculty of Engineering, Niigata University
Ikarashi 2-no-cho, Nishi-ku, Niigata 950-2181, Japan

ABSTRACT

Random numbers can be classified as either pseudo- or physical-random, in character. Pseudo-random numbers are generated by definite periodicity, so, their usefulness in cryptographic applications is somewhat limited. On the other hand, naturally-generated physical-random numbers have no calculable periodicity, thereby making them ideal for the task. Diode lasers' considerable wideband noise gives them tremendous capacity for generating physical-random numbers, at a high rate of speed. We measured a diode laser's output with a fast photo detector, and evaluated the binary-numbers from the diode laser's frequency noise characteristics. We then identified and evaluated the binary-number-line's statistical properties. We also investigate the possibility that much faster physical-random number parallel-generation is possible, using separate outputs of different optical-path length and character, which we refer to as "coherence collapse".
Keywords: laser diode, physical-random number, rapid generation, frequency noise

1. INTRODUCTION

In troubled times such as these, the need to protect our online personal, public and corporate information can never be overemphasized. Because of the calculable periodicity of the pseudo-random numbers used in today's cryptographic applications for cloud-, or grid computing, previously "secure" systems are now under grave threat, from dedicated hackers and crackers. It is believed, however, that physical random number-based encryption still provides a good level of protection. Laser diodes naturally produce wideband noise signals considered to have tremendous capacity and great promise, for the rapid generation of physical-random numbers for use in cryptographic applications.

Where before, we employed Fabry-Perot type diode lasers' frequency noise to generate physical random numbers, in the current undertaking, we used a VCSEL characterized by broader oscillation-linewidth and frequency-noise bandwidth, than Fabry-Perot type devices. This system allowed us to easily measure the intensity of the light transmitted, through the frequency reference, which converts frequency noise to intensity noise, and quickly obtain physical-random numbers, using an analog-digital converter (ADC) that produces 8-digit binary numbers from detected light intensity signals from the laser diode passing through the frequency reference.

Physics and Simulation of Optoelectronic Devices XX, edited by Bernd Witzigmann, Marek Osinski, Fritz Henneberger, Yasuhiko Arakawa, Proc. of SPIE Vol. 8255, 825521

2. PRINCIPLES

Diode lasers are characterized by a broad spectrum of naturally-occurring frequency noise. Using a frequency discriminator, -for example a Rb absorption line, or a Fabry-Perot etalon to convert this to intensity noise, we can generate physical-random numbers. Figure 1 shows the conversion principle used to measure variations in intensity and voltage, from shifts in frequency.

It is possible to detect frequency noise as strong intensity noise signals, by using saturated absorption spectroscopic measurements of Rb absorption lines. When the slopes of absorption line spectra are steep, small fluctuations in frequency translate to large variations in light intensity. So, we set the laser diode's oscillation frequency at the point where the slope of the absorption-line spectrum is steepest. The intensity and frequency of this transmitted light depend on the laser diode's frequency noise rate and the frequency discriminator's characteristics. Therefore, the system we rely on, for ultra-fast physical-random number-generation is quite simple, requiring only a laser diode, a frequency discriminator, such as a Fabry-Perot etalon, and a fast photo detector.

The word "coherence" is a property of waves that can make stationary interference. With regard to optics, it can convey two different ideas; the first, -"spatial coherence", the concept that allows for the observance of interference fringes by combining laser beams from two optical sources, or splitting a single in-two. This means that the similarities of two light wave-fronts, especially those having only one source. The second meaning is "temporal coherence"; that it is technically possible to obtain interference, i.e., the maxima and minima, when we aim two laser beams at a single detector. This means that two light beams can possess similar temporal characteristics, especially in case of one source, that corresponds to the light waves' linewidth or spectrum.

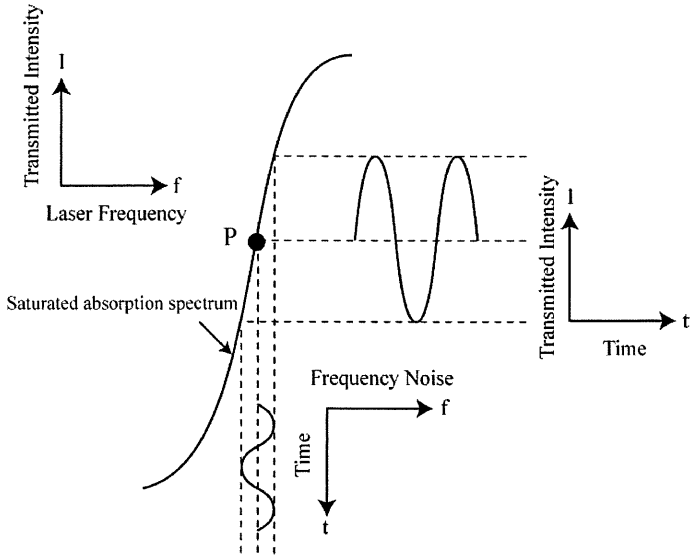

Fig. 1 Frequency-intensity converter

3. EXPERIMENTS

Due to the exceedingly large number of noise-types, and the mechanisms by which they are generated, we need to determine which method is most efficient, for the generation of physical-random numbers. We tackled the problem, by first working to correctly identified various intensity noises, such as already reported by Reidler et al. (Reference[6]) Once those were accounted for, we looked for signals unique to semiconductor lasers operating at very high frequencies, identifying them by the intensity of the light transmitted through the Rb absorption lines.

Fig. 2 and 3 show our experimental and optical setups. Using a VCSEL incorporating a laser mount, photo-detector circuit and various other components hand-built from the ground up, we introduced the laser beam to a photo-detector, such as Avalanche Photo Diode (APD) or PIN Photo diode, through the Rb cell as a frequency discriminator, at temperatures controlled to within ±0.01 K. The light received by a photo-detector is detected as a light intensity signal, and an RF amplifier increases the signal's power. This optical system was specifically designed for tasks related to frequency stabilization. We can use Rb absorption lines' frequency/ intensity conversion characteristics, to obtain the desired level of intensity noise.

We used a digital oscilloscope (LeCroy wave Runner 62Xi-A) as an A-D converter (ADC). A 10 GS/s ADC intensity noise signal is introduced at the PD through an RF amplifier (NOGAWA COMM WORKS MODEL NUL-5136). It generates a series of physical-random numbers; for example 8-digit binary numbers; -from the detected light intensity. This time, we obtained 8 series of binary numbers, as shown in Fig. 4. These are expected to have no cyclic period, and be physically-random, in character.

In addition to the investigation described up to this point, we were moving forward with another series of experiments aimed at testing the concept of "coherent collapse". A beam emitted from one diode laser is split and detected through a lens and an isolator, and the Rb cell as shown in Fig. 3. One of the split beams is traveling longer than our LD's coherent length, while the other is detected without any extra pass.

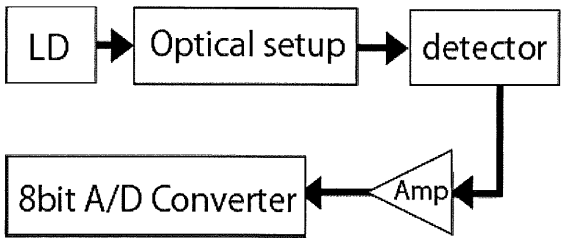

Fig. 2 Experimental Setup

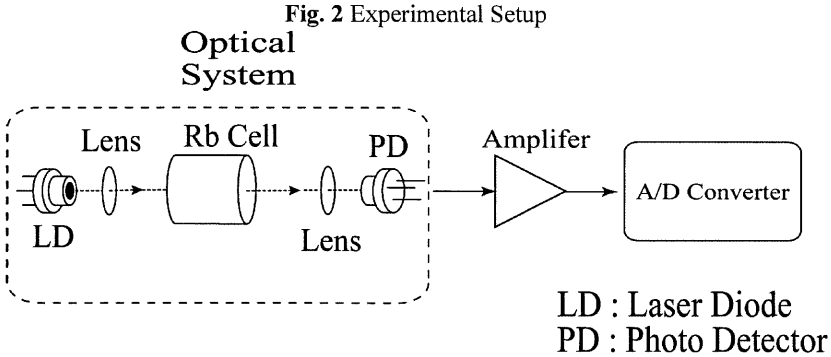

Fig. 3 Optical Setup

/From that information, we generated a series of physical-random numbers, using an ADC that produces, for example, 8-digit binary numbers from the detected laser intensity, so that, when we group; the lowest digits of successive 8-digit binary numbers; the second lowest digits; -and so on, we obtain 8 series of binary numbers, as shown in Fig. 4. These binary numbers are expected to have no cyclic period, and be physically-random, in character, thus allowing for the possibility of obtaining 8 physical-random numbers at once. But, because higher digits correlate with digits of the same value, in each successive 8-digit binary number, we need to verify whether each binary number thus acquired is, in fact, random.

In this undertaking, we sampled the ac signal of the intensity noise at 10 GS/s; -our standard digitization-rate, for 8-digit A-D conversion. This means that our ADC sends input signals from an encoder circuit, every 10^{-10} sec, to eight output ports, as binary data; -information that is usually handled as 8-digit data. But we noted that 8 ports output binary data, at 10^{-10} sec intervals; i.e., our system is capable of producing multiple streams of binary data, simultaneously. As physical-random numbers are produced at each port, we determine the final generating speed of the system, by simply multiplying the binary data generating-speed by the number of ports. And instead of using all of the 8-digit binary data obtained from our ADC to generating just one random-number series, we generate a total of 8, from the 8 ports' stored binary data, anticipating a lack of randomness, at higher digits in 8-digit binary data-stream. This is all verified in accordance with NIST's (National Institute of Standard Technology) FIPS140-2 evaluation standard, consisting of the "monobit"-, the "poker"-, the "run"- and the "long-run"- test; -considered to be among the most stringent evaluations of statistical randomness, for figures of this type. The random-number data that satisfies all four tests is assumed to be safe and correct. We collected 100 data-sets of 20,000 bits, from 8 ADC ports, according to NIST's 140-2 standard evaluation procedure. Finally, we evaluated all data sets, according to NIST 140-2 standards, and obtained the examination pass rates.

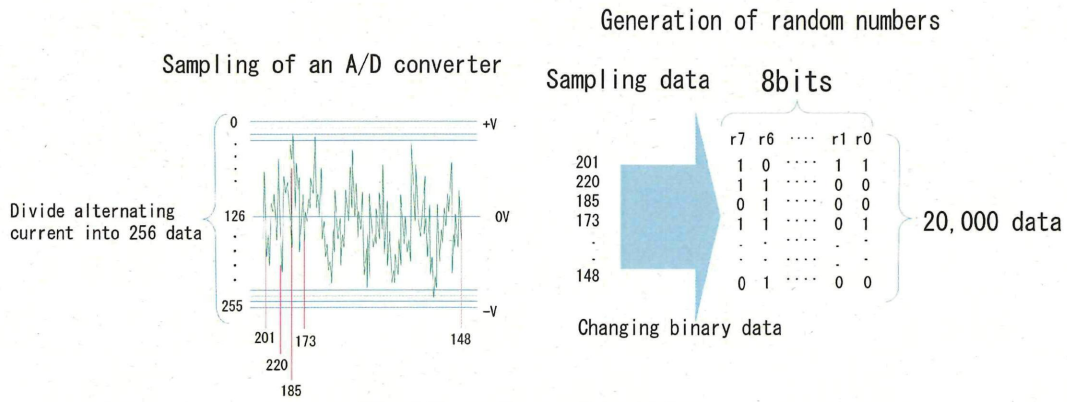

Fig. 4 Generation random numbers

4. RESULTS

Fig. 5 illustrates the ac voltage signal of the intensity noise converted from the laser diode's frequency noise and the sampled points at 10 GS/s, -our digitizing rate using the 8-digit ADC. This figure shows the 50 ns trace of the intensity noise. The 10 GS/s sampling points are indicated by circles.

Table 1 outlines the results we obtained using a VCSEL and a Fabry-Perot diode laser. "r0" means the "lowest digit", "r1", -the second lowest digit, and so on. We evaluated the 100 sets of 20,000 binary numbers and also the examination pass rates at every digit. The examination pass rate shows the number of times the physical-random numbers passed the NIST's FIPS140-2 test.

Experimental results indicated a lower 5-digit data's examination pass rates were of over 90% when we used a VCSEL & PIN Photo Diode. It is considered that the higher 3-digit data couldn't pass the test, because the intensity of the high-frequency noise components of a VCSEL was larger than that of a Fabry-Perot laser.

In this research, we used an 8-digit ADC at a sampling rate of 10 GS/s. This allowed us to obtain 80 GS/s at full speed, when every digit binary number passes the examination. We generated physical-random numbers at a rate of 50 GS/s, using VCSELs' frequency noise & PIN Photo diode. By comparison, our previous Fabry-Perot type laser & APD-based attempts generated the desired numbers, at only 40 GS/s. So, we succeeded in increasing generating speed 10 GS/s.

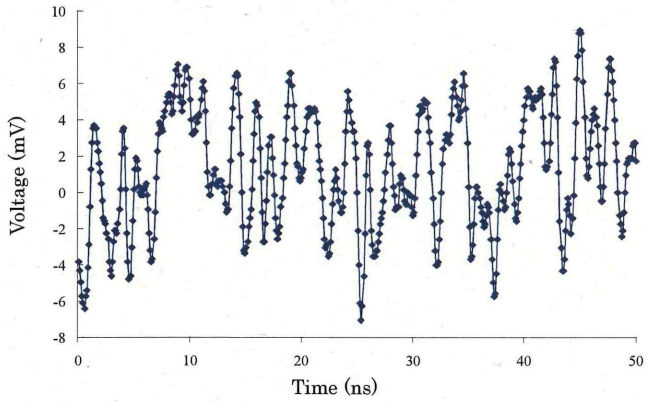

Fig. 5 A 50-ns trace of converted diode laser's frequency noise digitized at 10GS/s and sampling points (circles).

Table 1 Examination Pass Rate

	r0	r1	r2	r3	r4	r5	r6	r7
mono-bit	100	100	100	100	100	0	0	0
poker	100	100	98	100	97	0	0	0
Run	99	99	100	100	100	85	37	33
long-run	100	100	98	100	97	0	0	0
pass rate	99	99	98	100	97	0	0	0

(a) VCSEL & PIN Photo Diode

	r0	r1	r2	r3	r4	r5	r6	r7
mono-bit	100	100	99	100	55	0	0	0
poker	98	99	100	99	28	0	0	0
run	100	100	100	100	97	50	7	5
long-run	98	99	99	99	25	0	0	0
pass rate	98	99	99	99	25	0	0	0

(b) VCSEL & APD

	r0	r1	r2	r3	r4	r5	r6	r7
mono-bit	96	93	100	100	67	75	23	21
poker	100	100	100	100	0	0	0	0
run	98	98	99	93	0	0	0	0
long-run	100	100	100	100	77	0	0	0
pass rate	95	92	99	93	0	0	0	0

(C) Fabry-Perot Laser & APD

Because we were unable to increase physical-random number generating speed, by observing the same laser beam, after it had traveled farther than its coherent length, we are now repeating the experiment, with a few adjustments, to try to determine the root-cause of the failure, and will summarize our findings in a follow-up.

5. CONCLUSIONS

Through this research, we generated physical-random numbers by using VCSELs' frequency noises and an original parallel binary random number generating system. Then, we identified and evaluated the binary-number–line's statistical properties, demonstrating, in the process, that physical-random numbers were generated at speeds up to 50 GS/s. In future, we would like to generate physical-random numbers at even greater speeds, using laser diodes' frequency noise characteristics more efficiently. It will require a PD with much quicker response, and/or a high-performance ADC.

At present, we are conducting tests using "coherent collapse" -that may produce physical-random numbers in doubled speed.

ACKNOWLEDGEMENTS

This work is supported in part by a Grant-in-Aid for Scientific Research (No. 22560035) from Japan Society for the Promotion of Science.

REFERENCES

[1] T. Moro, Y. Saitoh, J. Hori, and T. Kiryu, IEICE Trans. Commun., (Japanese Edition), Vol. J88-A, No.6, pp.714-721, 2005.
[2] Y. Yamamoto, IEEE J. Quantum Electron., QE-19, 34 (1983).
[3] Y. Yamamoto, S. Saito, and T. Mukai, IEEE J. Quantum Electron., QE-19, 47 (1983).
[4] T. Numai: Handoutai Laser kogaku no Kiso (Base of Semiconductor Laser Engineering) (Maruzen, 1996) [in Japanese].
[5] Atsushi Uchida et al., "Fast physical random bit generation with chaotic semiconductor lasers", Nat. Photon. 2(12) (2008) 728.
[6] I. Reidler et al., "Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser", Phys. Rev. Lett. 103 (2009) 024102.
[7] Kunihito Hirano et al., "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers", Opt. Express. Vol.18 No.6 (2010) 5512.
[8] I. Kanter, Y. Aviad, I. Reidler, et al., Nature Phtonics., 4, 58 (2010).
[9] K. Hirano, T. Yamazaki, S. Morikatsu et al., Optical Express., 18, 5512 (2010)
[10] T. Yabuzaki, T. Mitsui, and U. Tanaka, "New type of high-resolution spectroscopy with a diode laser, " Phys. Rev. Lett., vol.67, pp.2453-2456, 1991.
[11] Y. Ohdaira, H. Hori, IEICE TRANS ELECTRON., E85-C, 12(Page) (2002).
[12] T. Yabuzaki, T. Mitsui, and U. Tanaka, Phys. Rev. Lett., 67, 2453 (1991).
[13] Hiroki Nishimura et al., "Physical-random number generation using laser diodes' inherent noises", Proc. SPIE, 7597-22, 2010.
[14] T.Nimonji et al., "New Frequency Stabilization Method of a Semiconductor Laser Using the Faraday Effect of the Rb-D2 Absorption Line", Jpn. J. Appl. Phys., Vol. 43, pp. 2504-2509, 2004.
[15] S. Maehara et al., "Frequency stabilization of laser diode light-sources in satellite-to-satellite laser interferometers", Proc. SPIE, 6115-79, 2006.
[16] Tomoyuki Uehara et al., "Comparison of three semiconductor laser systems for gravitational wave detection", Opt. Eng. Vol.48(3), 034302, March 2009.
[17] National Institute of Standards and Technology, "Security requirements for cryptographic modules, " FIPS 140-2, 2002.