Physical-random number generation using laser diodes' inherent frequency noises

◎Hiroki Nishimura†, Kohei Doi†, Tetsuro Ushiki†,
Yasuo Odaira‡, Takashi Sato‡, and Masashi Ohkawa‡
†C/O Sato Lab., Graduate School of Science and Technology, Niigata University,
Ikarashi 2-no-cho, Niigata 950-2181, Japan
‡Faculty of Engineering, Niigata University, Ikarashi 2-no-cho, Niigata 950-2181, Japan

1. Introduction

Random numbers can be classified as either pseudo- or physical-random in character. Pseudo-random numbers' periodicity renders them inappropriate for use in cryptographic applications, in an age of ultra high-speed data-processing, but naturally-generated, physical-random numbers have no calculable periodicity, thereby making them ideally-suited to the task. Laser diodes (LD) naturally produce a wideband "noise" signal that is believed to have tremendous capacity and great promise, for the rapid generation of physical-random numbers for use in cryptographic applications.

This work demonstrates how laser diodes' inherent noises can be exploited for use in generating physical-random numbers in the field of cryptography. In the initial stages of the experiment, we measured a laser diode's output, at a fast photo detector and generated physical-random numbers using laser diode's intensity noises. We then identified and evaluated the binary-number-line's statistical properties.

2. Experiment

Because the character and shape of the laser diode's oscillation exert tremendous influence on the intensity and frequency noises, we need to determine which noise is best suited for the generation of fast physical-random numbers. To do this, we worked to identify the frequency noises by observing the transmitted light intensity through the frequency reference, such as the Rb absorption line or Fabry-Perot etalon, and generated the physical-random numbers using an analog-digital (A/D) converter that produces, for example, 8-digits binary numbers from the detected laser intensity.

Figure 1 illustrates the experimental setup. We set an injection current to an LD just above the LD's threshold current. We introduced the laser beam to an Avalanche Photo Diode (APD) through a Fabry-Perot etalon and then its output electrical signal to a digital oscilloscope.

The sampling frequencies (fs) of an A/D converter in the digital oscilloscope were set at 250MHz. We also show the data obtained in our experiment using the intensity noises at 10MHz for comparing the frequency and intensity noises.

We then divided the data of each experiment into 20,000 bits set. These sample random numbers are produced by collecting, for example, the lowest digit of 20,000 8-digits binary numbers. We have 100 sets of 20,000 random numbers for each of three experiments.

The data was verified, in accordance with NIST's (National Institute of Standard Technology) FIPS140-2 evaluation standard [3, 4], consisting of the "monobit-", the "poker-", the "runs-" and the "long-run-" test; -considered to be the most stringent evaluation of statistic randomness for figures of this type. And the data, which satisfies all four tests, is considered as the safe and correct random numbers.

3. Experimental Result

Figure 2 presents the results obtained, using the test setup shown in Fig. 1. The horizontal axis means digit numbers in the observed 8-digits intensity; r0 means the lowest digit, r1 -the second lowest, and so on. The vertical axis shows the examination pass rate. We evaluated the examination pass rate for the 100 sets of 20,000 binary numbers, each of which is a group of the lowest-digit, i.e., r0, r1, and so on.

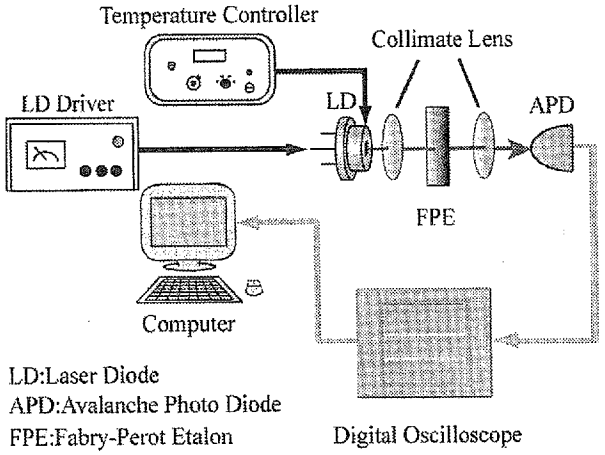

Fig. 1 Experimental setup

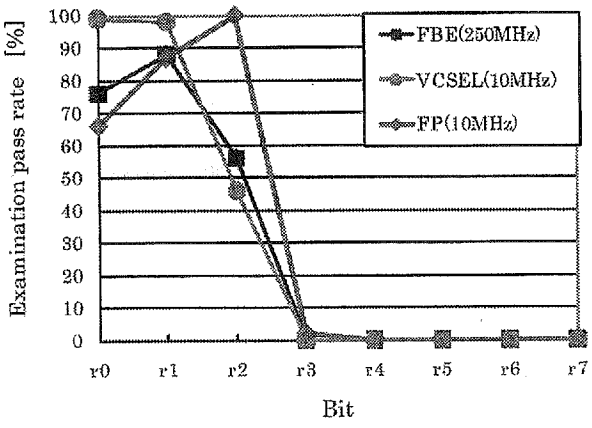

Fig. 2 Examination pass rate

4. Discussion and Conclusion

We produced random numbers with high sampling frequency, using the noise of a laser diode driven at slightly above its threshold current. The resulting noise-profile demonstrates the device's applicability to the generation of physical-random numbers. However, the rate at which the physical-random numbers were generated in our experiment is not fast enough for our goal, yet. Because laser diodes have very fast instinct noise characteristics, we are investigating a few other methods, such as mode competition, multi-mode operation, and optical feedback.

Because the frequency noise has higher frequency components than the intensity noise has, our preliminary result shows that fast physical-random numbers are obtainable, using the laser diode's frequency noise characteristic.