Super fast physical-random number generation using laser diode frequency noises

Tetsuro Ushiki†, Kohei Doi†, Shinya Maehara†,
Takashi Sato‡, Yasuo Odaira‡, 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.

Some researchers used diode laser's intensity noises and generated physical-random numbers faster than Gbps. They are using optical feedback techniques to create chaotic oscillation and using the diode laser's intensity noises.

The diode laser's frequency noise spectrum depends on its bias current and it spreads higher than GHz, so we tried to generate the super fast physical-random numbers using its frequency noises.

We worked to identify the frequency noises by observing the transmitted light intensity at a fast photo detector through the frequency reference, and generated the physical-random numbers using a fast analog-digital (A/D) converter at 10GSps. 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 noises are 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 operation current. We introduced the laser beam to an Avalanche Photo Diode (APD) through the Rb cell and then its electrical output signal to a digital oscilloscope.

The sampling frequencies (fs) of an A/D converter in the digital oscilloscope were set at 10GHz.

We then divided the data of each experiment into eight 20,000-bit sets. We produced the sample random numbers 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 one of the most stringent evaluations 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 the digit number in observed 8-digits; 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, the second lowest, i.e., r1, and so on.

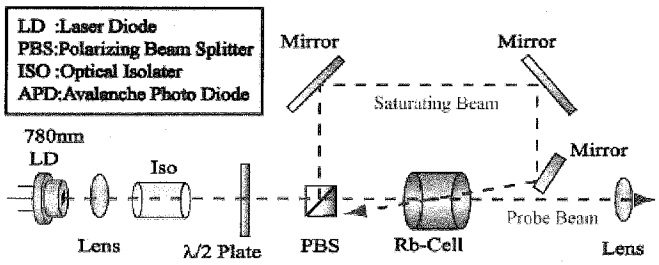

Fig. 1 Experimental setup

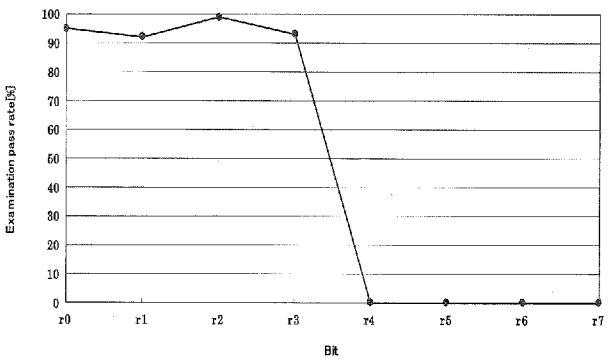

Fig. 2 Examination pass rate

4. Discussion and Conclusion

We completed the generation of ultra-fast physical-random numbers using the original parallel binary random number generating system and multiplied the generation speed of physical-random numbers. We then identified and evaluated the binary-number-line's statistical properties. Our result showed that fast physical-random number generation, as fast as 40Gbps, was obtained, and it would be faster than a few 100Gbps, using the diode laser's frequency noise characteristic.

References

1. Hiroki Nishimura et al., " Physical-random number generation using laser diodes' inherent noises " , Proc.SPIE,7597-22,2010