Theory and experiments of fast non-deterministic random bit generation using on-chip chaos lasers

Takahisa Harayama [1], Satoshi Sunada [1], Kenichi Arai [1], Jun Muramatsu [1], Kazuyuki Yoshimura [1], Peter Davis [1], Ken Tsuzuki [2], Atsushi Uchida [3]

[1] *NTT Communication Science Laboratories, NTT Corporation, 2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto, 619-0237, Japan, harayama@cslab.kecl.ntt.co.jp*

[2] *NTT Photonics Laboratories, NTT Corporation, 2-4 Hikaridai, 3-1, Morinosato-Wakamiya Atsugi, Kanagawa 243-0198, Japan*

[3] *Department of Information and Computer Sciences, Saitama University, 255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama, 338-8570, Japan*

Fast generation of non-deterministic random bit sequences is crucially important for secure communication and computation systems. Random bits can be obtained by sampling random physical phenomena, but it is generally difficult in practice to avoid correlations and statistical bias when bits are generated at high speed. It has recently been shown that random bits can be generated at multi-gigabits per second using chaotic oscillations in semiconductor lasers [1]. However, previous demonstrations of chaotic laser random bit generators used discrete fiber-optic or spatial optic components with long optical delays to achieve chaotic oscillation. In addition, The realization of random bit generation in more compact and robust photonic circuits is expected to have large impact from the point of view of commercial feasibility and range of applications. On one hand, monolithically integrated chaotic lasers with short delay have been developed for data transmission with chaotic optical carriers [2]. However, it has not been known whether chaos suitable for high-quality random bit generation can be achieved with short-cavity lasers integrated on-chip. Here, we report the monolithically integrated optical random bit generator which operates at rates up to 2.08 Gbps. This achievement demonstrates the potential for widespread use of small devices for fast optical random bit generation using chaotic lasers. We also theoretically elucidate the role of chaos for random bit generation.

Fig. 1a shows the schematic structure of the chaos laser chip. In a chaos laser chip, a distributed-feedback (DFB) laser is monolithically integrated with passive waveguides, two optical amplifiers (SOA), and a photodiode. High-reflective coating at the edge of the passive waveguide reflects the light back into the DFB laser, inducing high-frequency chaotic oscillations in the gigahertz regime. The feedback delay length is just 10mm, and the photodiodes have coupling efficiency over 70%. The strength and phase of the optical feedback is controlled with the current to the SOA. Two chaos laser chips are contained in a single module with two high-frequency connectors to output the electrical signals from the integrated photodiodes to outside as shown in Fig. 1b.

The scheme for generating random bit sequences using a module with two chaos laser chips is shown in Fig. 2a. The AC components of the electrical signals from the photodiodes are digitized at a 2.08 GHz sampling rate. The AC signals are converted to binary signals by comparing with a threshold voltage, and finally the binary bit signals are combined by a logical Exclusive-OR (XOR) operation to generate a single random bit sequence. No other digital post-processing is required.

The temporal waveforms of the electrical signals from the two photodiodes of the chaos laser chips are shown in Fig. 2b and 2c. The sequence of random bits is obtained as the output from the XOR operation.

In order to evaluate the statistical randomness of digital bit sequences, we used the standard statistical test suite for random number generators provided by National Institute of Standard Technology (NIST) and the Diehard test suite Bit sequences obtained from the experiment passed all of the NIST and Diehard tests.

We theoretically show that completely stochastic fast physical random bit generation at the rate more than 1 Giga bits per second can be realized by using lasers with optical delayed feedback which creates high-dimensional chaos of laser light outputs. A method to transform microscopic quantum noises of spontaneous emission in lasers into discrete macroscopic random states is studied based on the mixing property of chaos. Without knowing the details of microscopic noises, it is possible to design the frequencies of random macroscopic states only by using the natural invariant density of a chaotic laser dynamical system. The randomness of the obtained bit sequence can be evaluated quantitatively from the distance between the time evolving density and the natural invariant density.

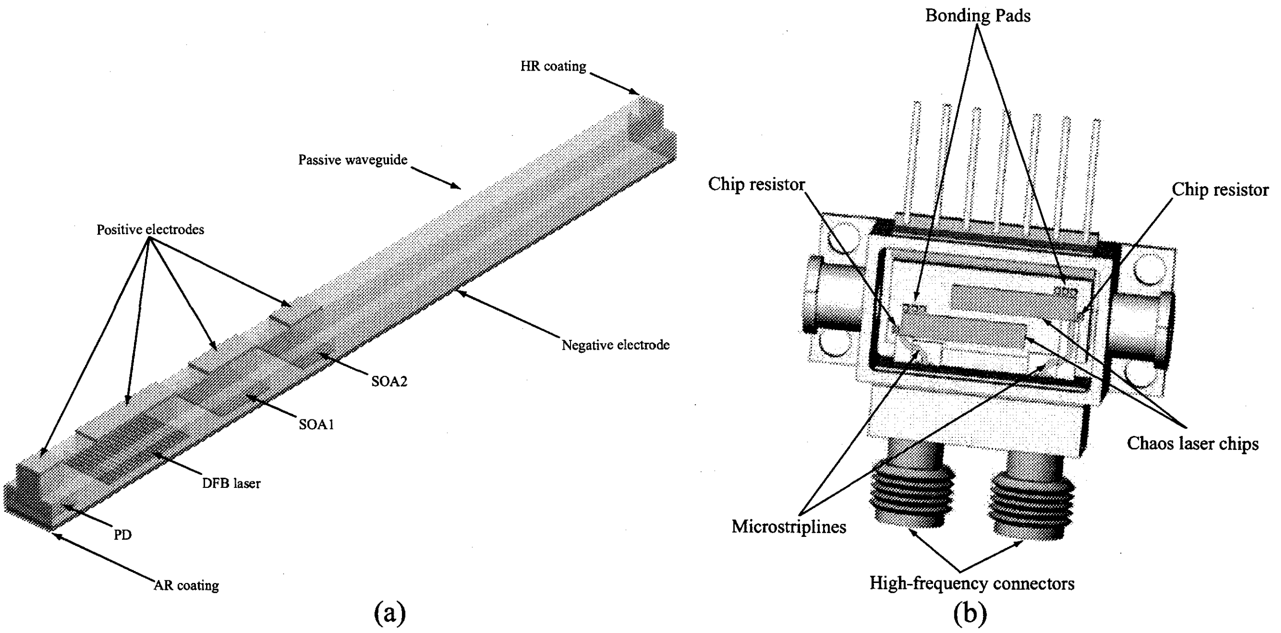

Figure 1: Structure of chaos laser chips and random signal generation module. Schematics of (a) a chaos laser chip. (b) random signal generator module consisting of two chaos laser chips.

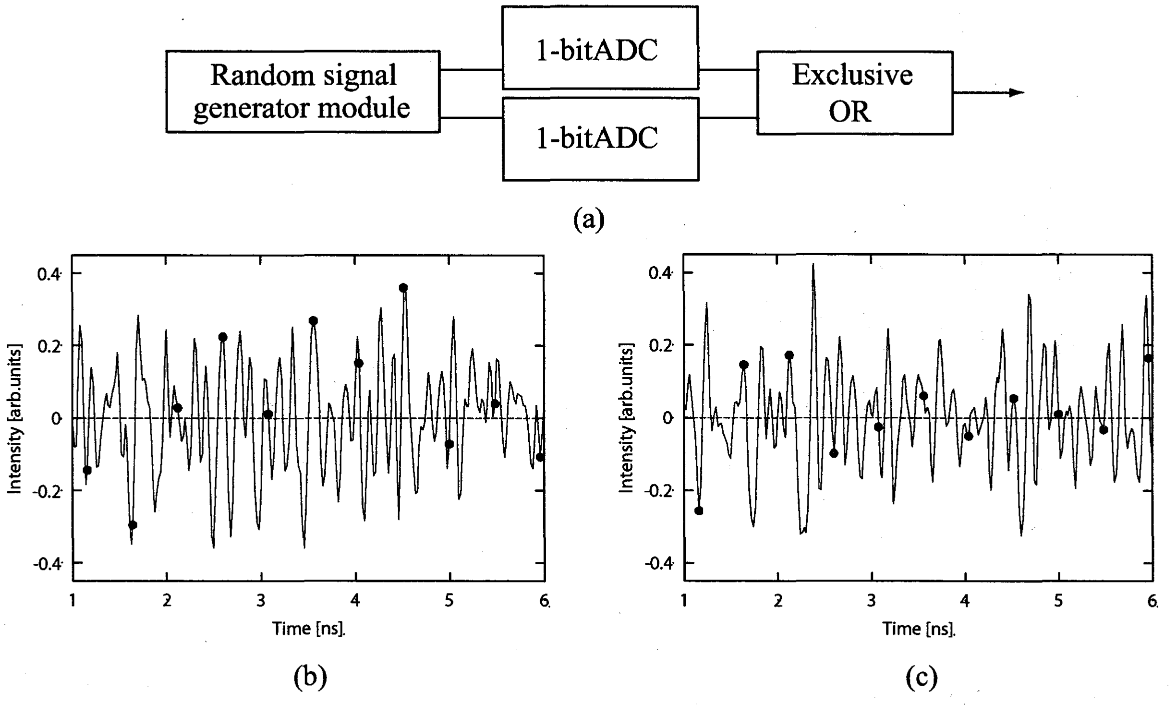

Figure 2: Random bit generation using the random signal generator module. (a) Schematic diagram. ADC, 1-bit analog-digital converter. (b) Temporal waveforms of the signals from one of the outputs of the module. Solid dots mark points sampled with 2.08 GHz sampling rates. The threshold value for the ADC is zero shown as solid lines. The digitized data is 00111111010. (c) Temporal waveforms of the signals from the other output of the module. The digitized data is 01100101101. The finally obtained random bit sequence is 01011010111 after the exclusive OR process.

References

[1] 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. *Nature Photon.* 2, pp. 728–732 , 2008.

[2] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, Photonic Integrated Device for Chaos Applications in Communications, *Phys. Rev. Lett.* 100, 194101, 2008.