2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Fast physical random bit generation by chaotic lasers with delayed feedback using extremely short external cavities

Shin Suzuki[1], Satoshi Sunada[2], Susumu Shinohara[3], Takehiro Fukushima[4], and Takahisa Harayama[1]

[1] Department of Applied Physics, School of Advanced Science and Engineering, Waseda University,
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, Japan
[2] Faculty of Mechanical Engineering, Institute of Science and Engineering, Kanazawa University,
Kakuma-machi, Kanazawa, Ishikawa 920-1192, Japan
[3] NTT Communication Science Laboratories, NTT Corporation,
2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan
[4] Department of Information and Communication Engineering, Okayama Prefectural University,
111 Kuboki, Soja, Okayama 719-1197, Japan
Email: sin-yougaku@akane.waseda.jp

Physical (true) random bits play an essential role in secure communications and data encryptions. As a device for physical random bit generation, chaotic lasers with delayed optical feedback have attracted considerable attention, because they make possible fast (gigabits/second) physical random bit generation. Such a chaotic laser has recently been realized by a photonic integrated circuit on a chip [1]. The laser chaos chip consists of a photodiode, a semiconductor distributed feedback laser, semiconductor optical amplifiers, and a passive waveguide for delayed optical feedback. The length of the passive waveguide is 1 cm, which is almost equal to the whole system size, since the sizes of all the other optical components are much less than 1 mm. Although a shorter passive waveguide is desirable for device size reduction, it is not clear how short we can make it, while maintaining the capability of generating good quality of random bit at the fast rate of gigabits/second.

In this work, we numerically studied random bit generation in cases of short passive waveguides by using the Lang-Kobayashi equations. The generated random bit sequences were evaluated by the statistical tests of randomness provided by NIST [2]. We found that by controlling the injection current and the amount of the optical feedback, we can obtain highly chaotic oscillations, even when the lengths of the passive waveguides are much shorter than 1cm. Using these chaotic oscillations, we were able to generate random bits at the rate of gigabits/second that pass all of the NIST tests.

[1] T. Harayama, S. Sunada, K. Yoshimura, J. Muramatsu, K. Arai, A. Uchida, and P. Davis “Theory of fast nondeterministic physical random-bit generation with chaotic lasers,” Phys. Rev. E. **85**, 046215 (2012).

[2] A. Rukhin et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” National Institute of Standards and Technology, Special Publication 800-22 Revision 1a (2010).