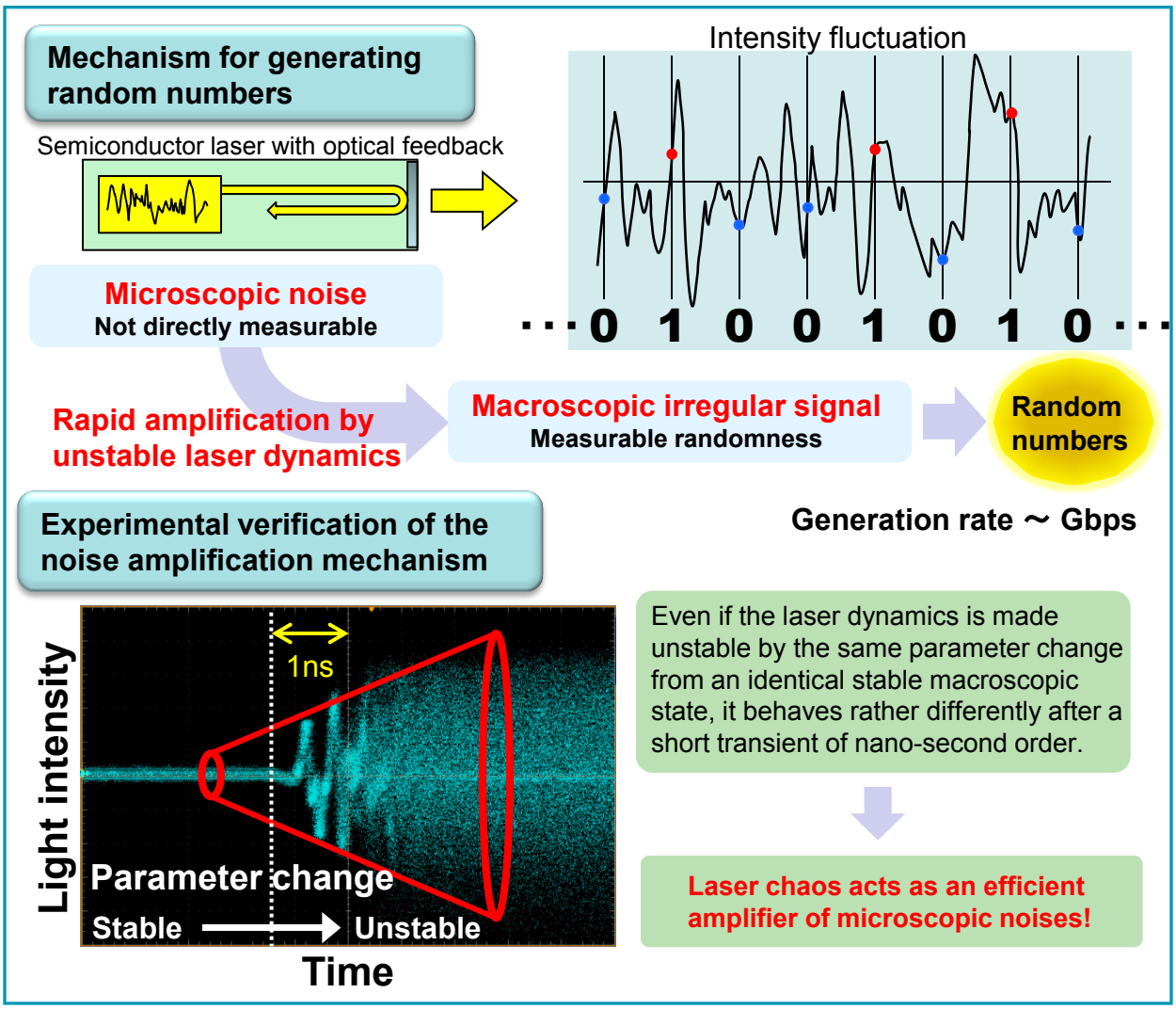
10

Making proper randomness

Physical random numbers generated by laser light

***Abstract*— Random number generation is an indispensable technology for secure communications. We developed a random number generator that utilizes the irregular fluctuations of a semiconductor laser output as the randomness source, thus achieving a gigabit per second generation rate. In addition to their lack of bias, the *unpredictability* of generated random numbers is of crucial importance for ultimate security. We therefore verify experimentally that our random number generator work in accordance with the theory explaining the origin of its unpredictability. Our research aims to extend the applicability of our system in a secure information and communication service environment by establishing a solid basis guaranteeing the quality of generated random numbers.**



Related works

[1] S. Sunada, T. Harayama, P. Davis, K. Tsuzuki, K. Arai, K. Yoshimura, A. Uchida, "Noise amplification by chaotic dynamics in a delayed feedback laser system and its application to nondeterministic random bit generation," *Chaos* 22, 047513, 2012.
[2] K. Arai, T. Harayama, S. Sunada, P. Davis, "Randomness in a Galton board from the viewpoint of predictability: Sensitivity and statistical bias of output states, " *Physical Review E* 86, 056216, 2012.

Contact

Kenichi Arai Signal Processing Research Group, Media Information Laboratory
E-mail : arai.k{at}lab.ntt.co.jp (Please replace {at} with @)