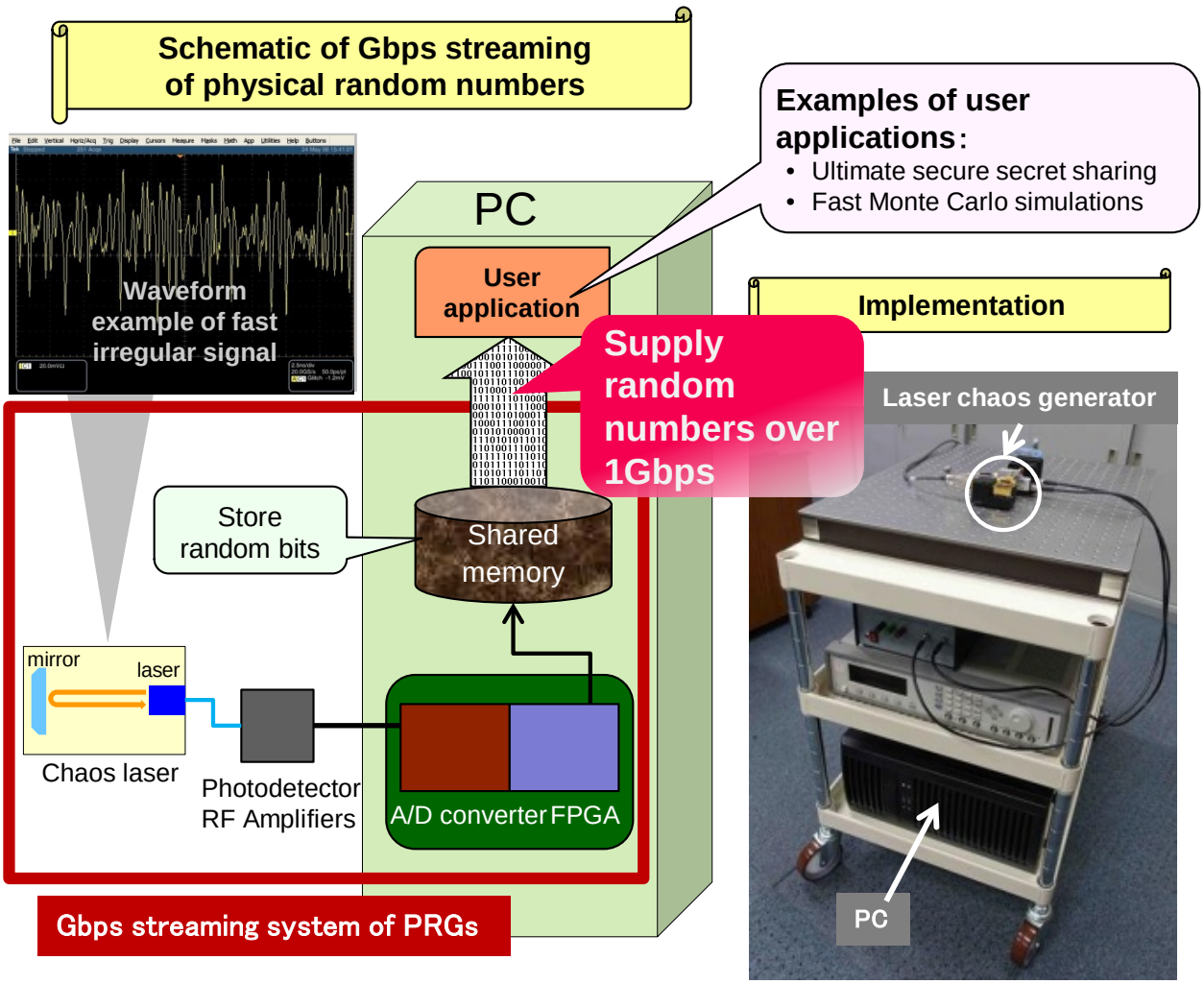
11 Generating true randomness for secure ICT

～Gbps streaming of physical random numbers～

Abstract

Physical random number generators (PRNGs) are needed to implement ultimate cryptographic systems, where decipher is intrinsically impossible. PRGNs must be fast since ciphering large data becomes more and more important these days. We have already shown that physical random numbers can be generated over several Gbps using laser chaos in experiments. However, from a viewpoint of practical utilization, a real-time transducer is required that can transform irregular analogue signal, generated from laser chaos, into physical random numbers (digital bits). We have developed a fast physical random number generation device that can supply random numbers directly to a PC at a speed of over several Gbps, by combining laser chaos, a fast AD converter, and real-time bit operation systems.



【Reference】

[1] T. Harayama, S. Sunada, K. Yoshimura, P. Davis,K. Tsuzuki, A. Uchida, “Fast nondeterministic random-bit generation using on-chip chaos lasers,” *Phys. Rev. A*, Vol. 83, 031803(R), 2011.

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

【Contact】

Kenichi Arai Signal Processing Research Group, Media Information Laboratory

E-mail : arai.k(at)lab.ntt.co.jp