# 08 Genuine physical random bit generator

## - Stably preserving unpredictability originated in entropy sources -


## Abstract

Unpredictable Physical Random Bits (PRBs) are required to implement ultimately secure, or intrinsically indecipherable, cryptographic systems. It is believed that PRBs can be generated by appropriately designed physical devices. However, in order to certify the unpredictability of PRBs, it is necessary to clarify the mechanism of a Physical Random Bit Generator (PRBG). To this end, we have introduced a concept of the genuine PRBG by constructing an end-to-end entropy source model. In our model, uncertainty of the entropy source is converted into the final random bits through multiple steps, such as observation, digitalization, and post processing, i.e. changing the appearance (from analogue to digital), but with the essence of the uncertainty (unpredictability) preserved. Based on the proposed concept, we have implemented a physical random number streaming system comprising a chaos laser device, a fast AD converter, real-time bit manipulation systems, and a computer application interface.


### End-to-end entropy source model

Chaos laser
Photo detector
RF amplifier
AD converter
Bit manipulator
PC interface
User memory
Laser control

transmit the uncertainty of entropy source to random bits through the steps preserving the essence and changing the appearance of the uncertainty

Confirmed PRBG's abilities as total system

### Chaos laser device

chaotic photonic integrated circuit (2011)

Generates irregular signals based on micro noises in laser

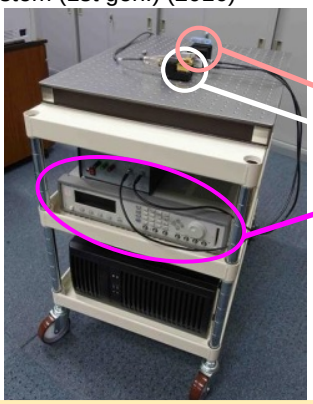
A small device, with a potential ability to generate fast and unpredictable PRBs

### Newly implemented random bit generator (prototype)

The end-to-end entropy source model is implemented.

Supplies PC memory with ready-to-use PRBs at a throughput of more than 1 Gbps

Physical random bit streaming system (1st gen.) (2016)



Small physical random bit streaming system (2017)

Downsized laser controller, photodetector, and RF amplifier

Applications:
- Ultimately secure secret sharing
- Fast Monte Carlo simulation

## References


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

[2] S. Shinohara, K. Arai, P. Davis, S. Sunada, T. Harayama, "Chaotic laser based physical random bit streaming system with a computer application interface", *Optics Express*, Vol. 25, pp.6461-6474, 2017.


## Contact


**Kenichi Arai** Signal processing Research Group, Media Information Laboratory
Email : arai.k(at)lab.ntt.co.jp