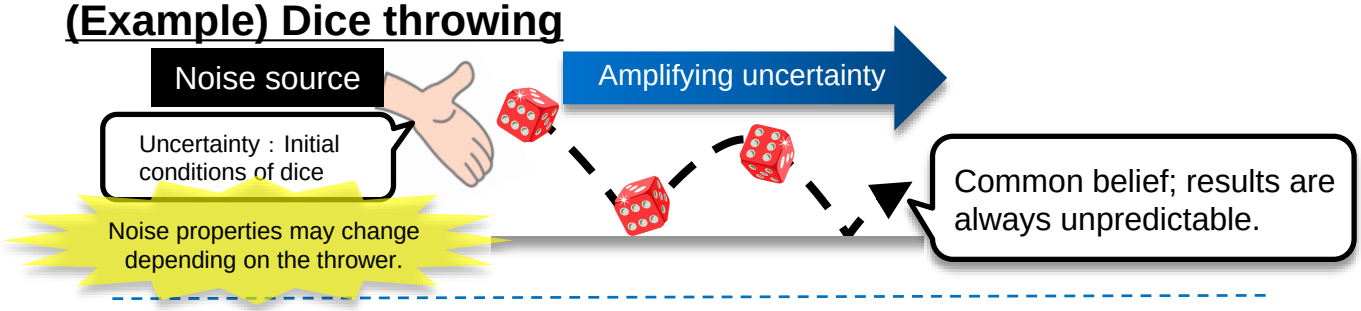
15 Guaranteeing Randomness

～A new concept toward reliable physical random bit generation～

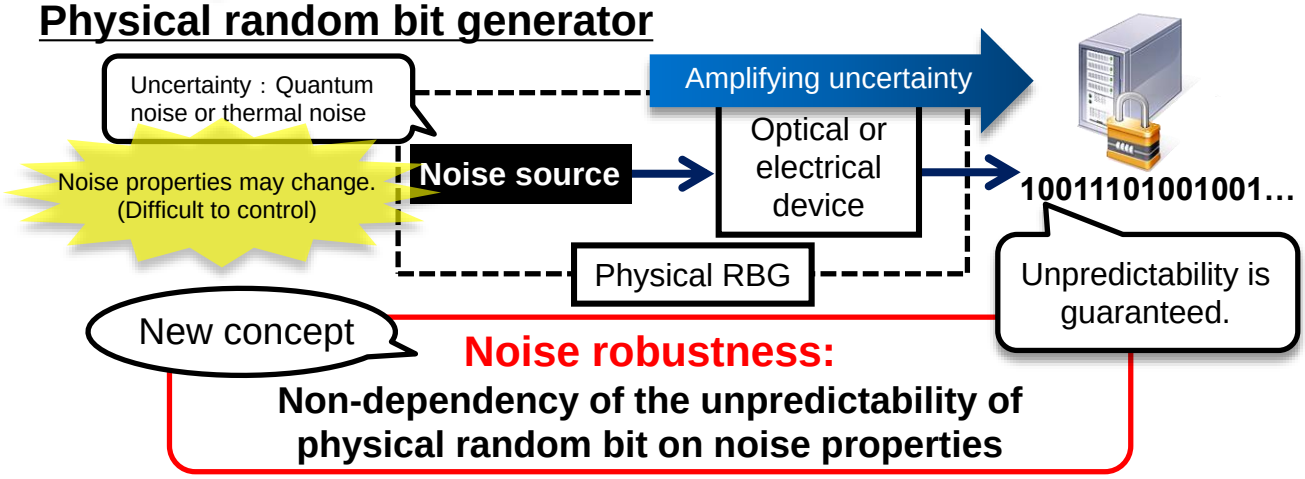
Abstract

We are all familiar with throwing dice to get random numbers. How can we be sure that they are truly random and unpredictable? Our study shows how to handle this fundamental problem. The ability to create random and unpredictable bits from random physical processes in electronic devices (physical random bit generators (RBGs)) is essential to security and privacy in modern IT systems. However, little is known about how to evaluate and guarantee the reliability of the unpredictability of such devices. We have introduced a new property of physical RBGs, called "noise robustness", and formulated it. Furthermore, we have shown that a semiconductor laser RBG developed by NTT is an example of promising physical RBG that has noise-robustness.

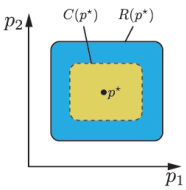
(Example) Dice throwing



Physical random bit generator



◆ Mathematical definition

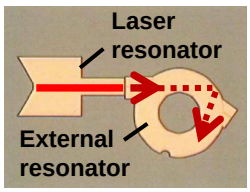


Def. We say a physical RBG has noise robustness if

$$C(p^*) \subset R(p^*),$$

where $p^*$is noise target parameter, $C(p^*)$is noise controllable region, and $R(p^*)$ is noise robust region.

◆ Noise robustness of laser RBGs



NTT is developing physical RBG using a semiconductor laser with delayed feedback. We have shown theoretically that this physical RBG has a particular type of noise-robustness.

Related works

[1] M. Inubushi, K. Yoshimura, P. Daivs, "Noise robustness of unpredictability in a chaotic laser system: Toward reliable physical random bit generation," *Phys. Rev. E*, Vol. 91, 022918, 2015.
[2] M. Inubushi, K. Yoshimura, Kenichi Arai, Peter Davis, "Physical random bit generators and their reliability: focusing on chaotic laser systems," *Nonlinear Theory and Its Applications (NOLTA), IEICE*, Vol. 6, no. 2, 2015.

Contact

Masanobu Inubushi Computing Theory Research Group, Media Information Laboratory
E-mail : inubushi.masanobu(at)lab.ntt.co.jp