A new concept toward reliable physical random bit generation

15 でたらめを保証する

～物理乱数生成の信頼性を評価する新概念：ノイズロバスト性～

どんな研究

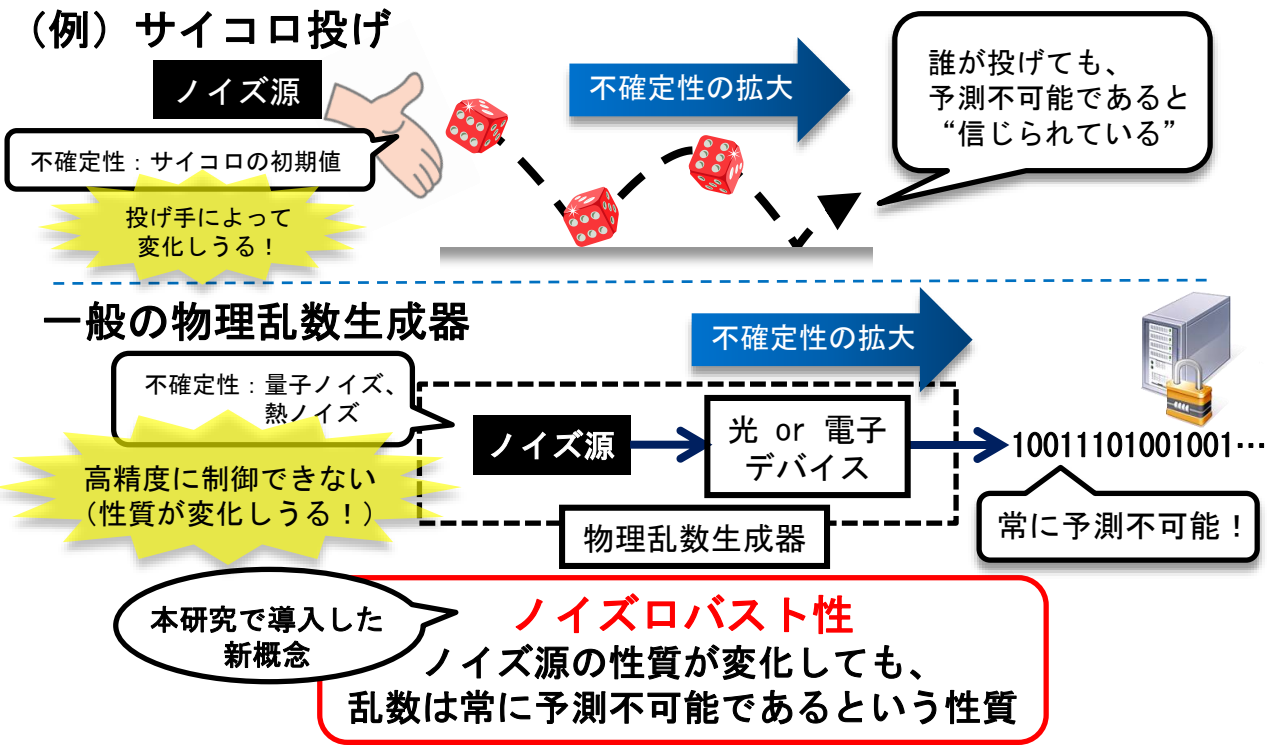
ランダムな物理現象を用いて作られる乱数は**物理乱数**と呼ばれ、近年研究が盛んに行われています。しかし物理乱数が**真にでたらめ（予測不可能）**であることを保証する研究はほとんどありません。本研究では予測不可能性を実現する物理乱数生成器が備えるべき条件を解明しました。

どこが凄い

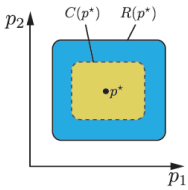
物理乱数が安心して情報セキュリティ技術に用いられるために、備えているべき必要不可欠な性質とは何か？その答えとして**新概念“ノイズロバスト性”を創出し、数理的に定式化**しました。さらに**NTTが提案している物理乱数生成器がノイズロバスト性を持つことを保証**しました。

目指す未来

今後益々発展が期待されるネットワーク社会において情報セキュリティ技術の重要性は増し、**品質の保証された物理乱数生成技術**は必要不可欠なものとなります。我々の物理乱数生成器の信頼性保証の研究により、安心安全な通信が実現することを目指します。



◆ 数理的定式化

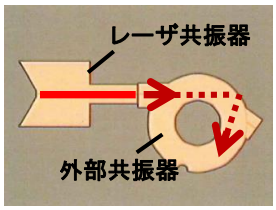


定義：物理乱数生成器が

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

を満たすとき、ノイズロバスト性を持つという。
ここでp^*はノイズパラメタの設計値、$C(p^*)$はノイズ制御可能領域、$R(p^*)$はノイズロバスト領域。

◆ NTT方式のノイズロバスト性保証



NTTは半導体レーザーを用いた方式の物理乱数生成器を提案しています。我々はこのNTT方式の物理乱数生成器がノイズロバスト性を持つことを数値的に保証しました。

関連文献

[1] M. Inubushi, K. Yoshimura, P. Davis, “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, K. Arai, P. 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.

連 絡 先

犬伏正信 (Masanobu Inubushi)　メディア情報研究部 情報基礎理論研究グループ
Email: inubushi.masanobu(at)lab.ntt.co.jp