

08

漏れなくデタラメです

～物理乱数源のランダムさを損なわずに乱数ビットを安定供給～

どんな研究

予測不可能な物理乱数生成は究極に安全な情報秘匿のための必須技術です。予測不可能性が担保された乱数をユーザが安心して使うには、**乱数が生成される仕組み**が明確にされていることが必要です。この展示では安心して使える物理乱数ストリーミング装置を紹介します。

どこが凄い

物理乱数の根源であるエントロピー源の不確定性から観測、量子化、事後ビット処理を経てユーザが使う乱数ビットまでをトータルで考え、**不要なノイズの影響やビットロスがないエンドツーエンドモデルの実装**としての物理乱数ストリーミング装置を実現しました。

めざす未来

今後、大量データ秘匿化のニーズがますます増大・一般化すると考えられます。本研究は、**高速に生成された物理乱数を誰でも簡単に使える**ようにし、秘密分散や暗号化などの技術とともに用いることで、膨大なデータや計算に関して**究極の安全性**を実現することを目指しています。

エンドツーエンド物理乱数生成モデル

各処理過程において物理エントロピー源の不確定性の形は変わるが本質は変えないよう次の処理へ引き渡し、最後は乱数ビットになるよう設計

トータルシステムとしての乱数生成能力を確認

カオスレーザデバイス

レーザ内の微小な不確定性をもとに不規則信号を生成

予測不可能な物理乱数を小型素子で高速に生成可能な潜在力

光集積回路製作 (2011)

物理乱数生成装置 プロトタイプシステム

エンドツーエンド物理乱数生成モデルを実装

1Gbps 以上でフルエントロピーの物理乱数をPCのユーザメモリへ供給

初代物理乱数ストリーミング装置 (2016)

小型物理乱数ストリーミング装置 (2017)

レーザ制御、光電気信号変換、高周波増幅を、実験室レベルから一般レベルの性能にして小型化

応用例:
・究極の安全性をもつ秘密分散
・高速な科学技術計算

関連文献

- [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.

連絡先

新井 賢一 (Kenichi Arai) メディア情報研究部 信号処理研究グループ
E-mail: arai.k(at)lab.ntt.co.jp