11

Gbps streaming of physical random numbers

情報を守る真のデタラメをつくる

～物理乱数 Gbpsストリーミングの実現～

どんな研究

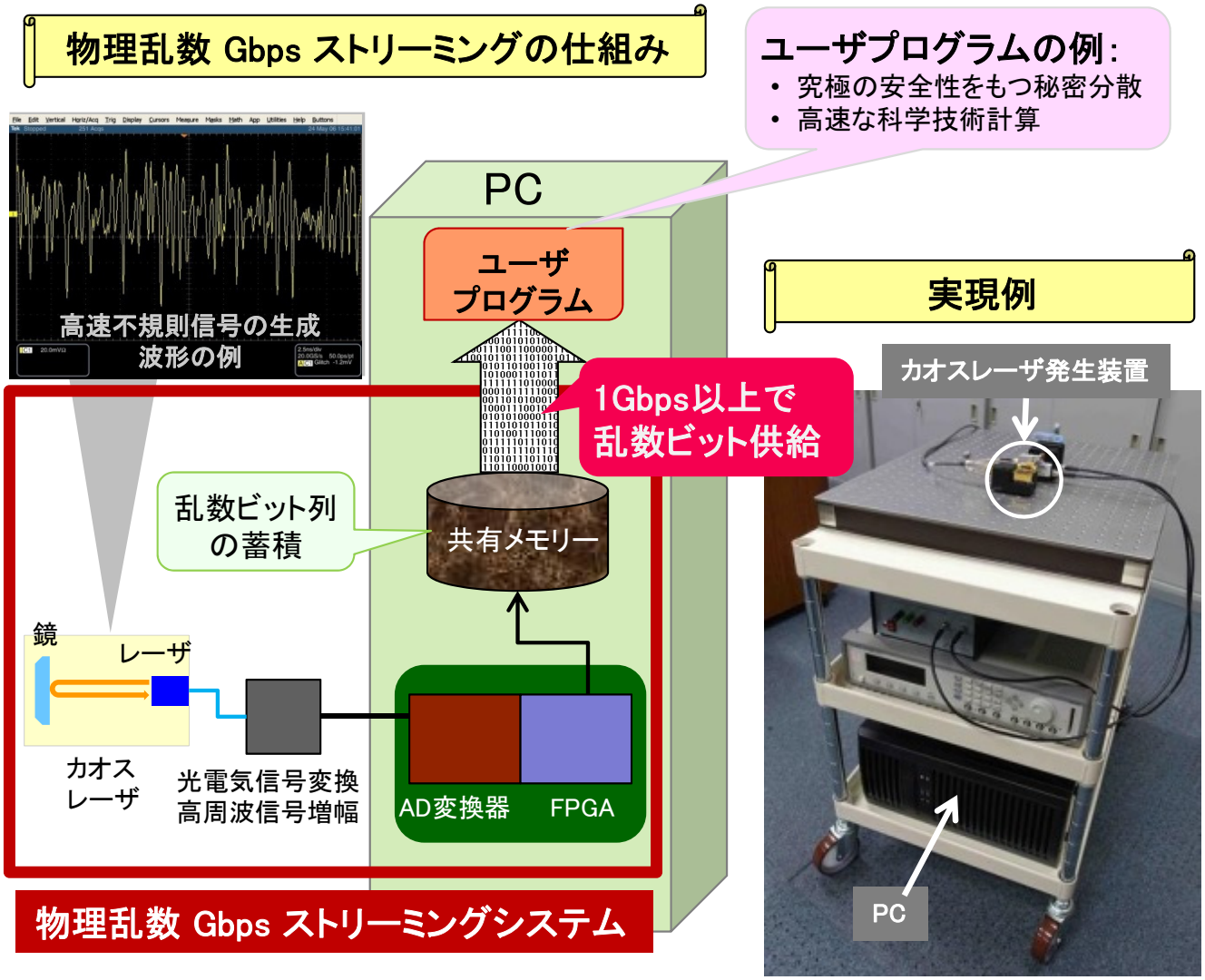
本質的に解読が不可能な究極の安全性を保証する暗号化を実現するためには物理乱数が不可欠です。私たちは、カオスレーザから生成した物理乱数列を実用的な速度で供給する研究をおこなっています。この展示では、1秒間で1Gbit(Gbps)以上の速度で直接パソコンなどへ物理乱数列を供給するシステムを紹介します。

どこが凄い

生成速度が遅いことが従来の物理乱数生成器の欠点でした。研究段階で、カオスレーザの信号を記録し乱数列に事後変換することで生成速度がGbps超になることが分かりました。高速AD変換器と高速処理システムを融合し、ユーザが高速に生成される乱数列をリアルタイムで利用できるシステムを構築しました。

目指す未来

現在一般に使われているデータの秘匿化手法は、膨大な解読時間がその安全性の根拠となっています。将来、物理乱数の高速な生成システムが実用化できれば、無限に時間をかけても解読できない究極の安全性が保証された暗号化が実現可能となり、より安心安全なデータの秘匿化ができるようになります。



【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,” *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.

【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