半導体レーザを用いた小型・高速乱数生成器

NTTコミュニケーション科学基礎研究所

概　　要

絶対に予測不可能な乱数列は、情報セキュリティに必要不可欠です。そのため、物理現象に基づいた小型かつ高速の乱数生成器が望まれています。本研究では、半導体レーザから出力される光の強さが、ランダムに高速時間変化する現象に着目しました。最先端の光集積回路技術と高周波パッケージング技術を用いて、小型かつ高速なランダム信号発生モジュールを実現しました。本モジュールのランダム出力信号をデジタル化することにより、予測不可能な乱数列の高速生成が可能となります。

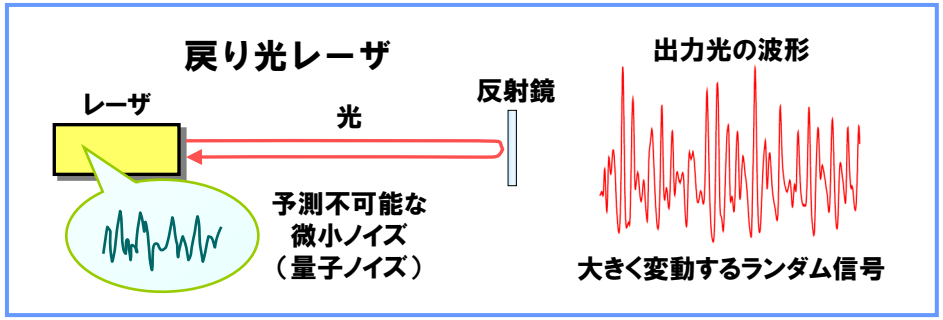
特　　徴

- 光集積回路技術の利用による装置の集積化・小型化
- 毎秒2.08ギガビットの高速乱数生成
- 生成される乱数列の予測不可能性を理論的に保証

利用シーン

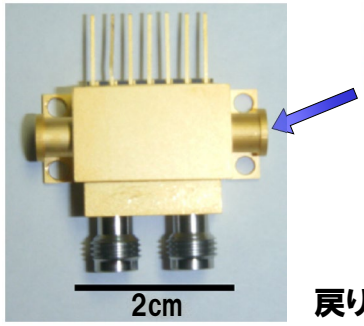
- パスワードの生成、暗号鍵の生成
- 秘密分散法による秘密情報の分割処理に必要な乱数の生成
- 量子暗号における鍵系列の生成
- 乱数を利用する科学技術数値計算にも利用可能

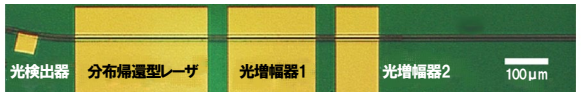
予測不可能なランダム信号生成のしくみ



ランダム性の起源は、原理的に予測不可能な量子ノイズです。戻り光レーザの不安定性により、量子ノイズによる揺らぎは20億分の1秒以下の時間で急速に拡大され、観測しやすく予測不可能なランダム出力光に変換されます。

小型・高速ランダム信号発生モジュール





戻り光レーザ集積回路の写真
（1cm×300μm）

戻り光レーザ集積回路2個を内蔵