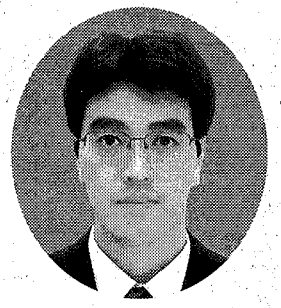
サイ・テクこらむ

知と技の発信【5】

埼玉大学・理工学研究の現場

レーザーカオスで高速乱数

内田　淳史　埼玉大学大学院 理工学研究科准教授



■情報セキュリティ技術

高度情報化社会において、情報を安全にやりとりするための情報セキュリティ技術の重要性は年々高まりつつある。

情報セキュリティ技術や暗号技術の信頼性は、ランダムな信号列を生成する「乱数生成器」に強く依存している。「乱数」とは、何の秩序も無いランダムな数字を並べたものである。現在多く用いられている乱数生成器はコンピュータで生成されるため（擬似乱数と呼ばれる）、その初期値を推定することで乱数の予測が可能になるという大きな欠点を有している。

これを改善するために、「物理乱数」と呼ばれる自然現象を利用した乱数生成方式が近年注目を浴びており、電子回路の熱雑音などを用いて実装されている。物理乱数は、自然ノイズを用いているために予測不可能という非常に優れた特性を有しているが、一方で生成速度が遅いのが欠点であった。

■世界初

そこで本研究室では、物理乱数の問題点であった低生成速度を飛躍的に向上させるために、半導体レーザーにおけるカオス現象を用いた物理乱数生成方式を世界に先駆けて提案し、1秒間に17億個（1・7ギガビット）の「高速物理乱数」の実時間生成実験に成功した。

レーザーの有する高速性および不規則なカオス現象を積極的に利用することで、従来技術の10倍以上の生成速度を有する「超高速物理乱数生成器」を、世界で初めて実現した。

2つの半導体レーザーのカオス的出力振動を光検出器で電気信号へと変換し、これを「しきい値処理」（1と0に変換）して論理演算を行うことで物理乱数を生成した。この乱数列に対してランダム性の統計的評価を行い、ランダム性の高い乱数であることを示した。

本研究成果は英科学誌「ネイチャー・フォトニクス」に発表された。

◇　◇　◇

■脆弱性の改善

本成果を応用することで、情報セキュリティ技術や暗号技術の多大なる発展が期待されている。レーザーから受光素子までを一体化した光集積回路の実装を行うことで、コンピュータに超高速物理乱数生成器を搭載でき、従来よりも、はるかに安全な電子商取引や情報ネットワーク社会の実現が可能となる。

加えて乱数の高速性を生かすことにより、従来の暗号方式とは本質的に異なる新しい情報セキュリティ方式や量子暗号通信の実現が可能となり、現在のインターネットの脆弱（ぜいじゃく）性を大幅に改善できる可能性を秘めている。

超高速物理乱数生成器の実現により、既成概念を超えた新たな情報セキュリティ技術が、実用化へ向けて一気に進展する可能性が高く、高度情報化社会における安全性の飛躍的な向上が期待されている。

◇　◇　◇

内田　淳史氏（うちだ・あつし）72年埼玉県生まれ。浦和高校卒。慶応大学・大学院卒。博士（工学）取得。08年から現職。専門は情報通信工学、レーザー工学、非線形力学。

埼玉経済