平成 27 年 1 月 30 日

高速な物理乱数生成に成功
－1 秒間に 1 兆 2000 億個の乱数生成－

概要

国立大学法人　埼玉大学[学長　山口宏樹]大学院理工学研究科　内田淳史准教授らの研究グループは、情報セキュリティ分野や大規模数値シミュレーション分野に必要不可欠な物理乱数生成の高速化に関する研究を行い、結合された半導体レーザのカオス現象を用いることで、1秒間に1兆 2000 億個（毎秒1.2 テラビット）の生成速度での高速な物理乱数生成の実証実験に成功した。

1. 研究の背景

ランダムな数列である乱数は情報セキュリティに必要不可欠な基盤技術であるが、コンピュータを用いて生成される擬似乱数を用いた場合、盗聴者による暗号鍵の予測が可能になるという安全性の脅威が存在する。そこで自然現象を用いて生成された物理乱数が情報セキュリティに必要とされているが、半導体の熱雑音を用いた従来の方式では生成速度が遅いのが欠点であった。また天気予報や地震予測などの自然災害予測分野や、設計工学のための大規模数値シミュレーション分野においてもランダム性の高い大量の乱数が用いられているが、予測精度や設計精度の向上のために、高速な物理乱数生成方式の開発の必要性が急速に高まっている。

2. 研究の成果

本研究では、半導体レーザの高速性およびカオスの不規則性を利用することで、1 秒間に 1 兆 2000 億個（毎秒 1.2 テラビット）の生成速度を有する物理乱数生成の実証実験に成功した。3 つの半導体レーザを一方向に結合することで、半導体レーザから出力されるカオスの不規則振動を高速化する技術を開発した。また複数の論理演算を組み合わせたマルチビット乱数生成方式を新たに開発し、生成されたカオス信号へ適用することで、高速乱数の生成を行った。本手法で得られた乱数は国際標準の統計検定に合格し、十分なランダム性が保障された。本研究における物理乱数の生成速度は、従来法と比べて約 3 倍向上しており、1 秒間に 1 兆個（毎秒 1 テラビット）の生成速度の壁を初めて突破した。

図1　一方向に結合された 3 つの半導体レーザから発生されたカオス信号の時間波形（左図）と周波数スペクトル（右図）を示す。レーザ 1，2 よりもレーザ 3（下図）の時間波形の方が高速で振動しており、周波数も広がっていることが分かる。

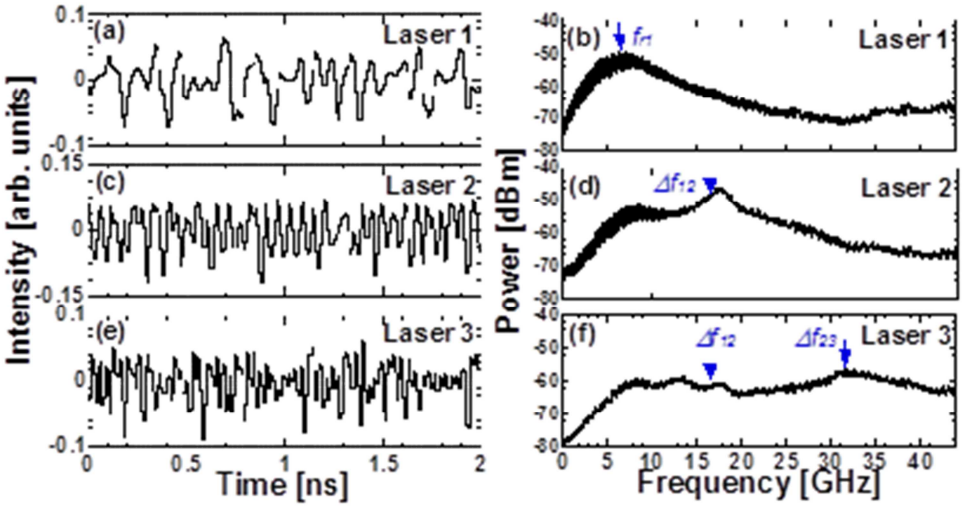
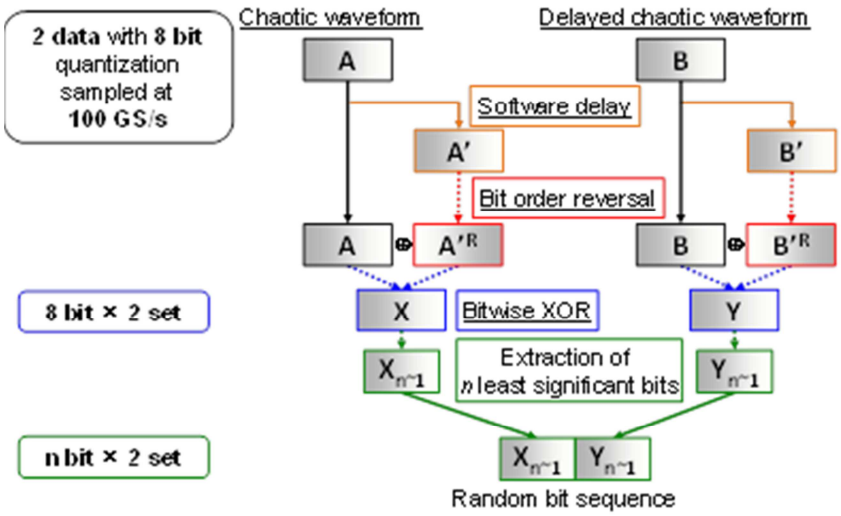


図 2　マルチビット乱数生成方式の概念図を示す。2 つのカオス時間波形を 8 ビットで量子化し、1 秒間に 100 ギガ点を取得して、乱数生成のために複数の論理演算を行う。最終的に下位 6 ビットを取り出すことで、1 秒間に 1 兆 2000 億個（毎秒 1.2 テラビット）の乱数生成を実現している。



3. 今後の展望

ランダム性の高い物理乱数の高速生成が可能となることで、情報セキュリティ分野における安全性の向上が見込まれる。また、高速な物理乱数を用いて新たな暗号方式を実現できるため、次世代の情報セキュリティの基盤技術となる可能性を秘めている。さらに、天気予報や地震予測などの自然災害予測分野や、設計工学などの大規模数値シミュレーション分野における計算精度の向上が期待できる。

4. 論文情報

Ryohsuke Sakuraba, Kento Iwakawa, Kazutaka Kanno, and Atsushi Uchida,"Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," Optics Express, Vol. 23, No. 2, pp. 1470-1490 (2015).

（米国光学会の電子ジャーナル）

5. 用語解説

乱数:

何回もサイコロを振って出る目の数列など、規則性の無いランダムな数列のこと。特に、コイン投げの表裏のように、0 と 1 がランダムに現れる数列のことを、2 値乱数と呼ぶ。

ランダム:

でたらめな数列の状態のこと。例えば 0 と 1 の 2 値乱数の場合、0 と 1 の出現確率が完全に 2 分の 1（または 50%）であり、どのような 0 と 1 の間にも全く関係がないような状態のこと。また過去の 0 と 1 の数列から次の値を予測できないような状態のこと。

テラビット:

テラは 10 の 12 乗のこと。ビットは 0 または 1 を表す数字の単位のこと。毎秒 1 テラビットとは、1 秒間に 10 の 12 乗個の 0 または 1 の数列を生成する速度のこと。

乱数生成方式:

乱数を生成するための方法のこと。コンピュータを用いた擬似乱数と、自然現象を用いた物理乱数に大別される。

擬似乱数:

初期値（シード）と呼ばれる情報を入力して決められた手続き（アルゴリズム）に従って生成され、一見乱数のように見えるランダムな数列のこと。擬似乱数はコンピュータによって作られるので、シードとアルゴリズムが分かれば、原理的には出力系列を予測可能である。そのため、擬似乱数を情報セキュリティ応用へ適用する場合、安全性の低下などの重大な問題点が指摘されている。

物理乱数:

サイコロを振って出る目など、結果を予測できないランダムな物理現象や自然現象の観測値を用いて生成される乱数のこと。擬似乱数に比べて高いランダム性を有している。

マルチビット乱数生成方式:

カオス波形を測定した 1 点のデータから、複数のビット列を生成する方式のこと。乱数のランダム性を向上させるために、複数の論理演算を行う手続きを含んでいる。統計検定に合格するような高いランダム性を有する乱数を高速に生成するために用いられる。

半導体レーザ：
　半導体結晶中の電子と正孔の再結合による発光現象を利用したレーザのこと。小型で消費電力が少なく安価に製造できるため、情報機器や光ファイバ通信等で広く用いられている。

カオス：
　システムが乱雑な時間的変化を示し、ほんのわずかな初期状態の違いが、予想が難しい大きく違った結果を生む不規則振動現象のこと。半導体レーザに戻り光を加えることで、レーザ出力のカオス不規則振動を生成することができる。

熱雑音：
　半導体レーザ結晶を構成する原子や、結晶中の電子の熱振動によって生じる雑音のこと。ノイズとも呼ばれている。既存の物理乱数生成方式で主に用いられている。

統計検定：
　乱数のランダム性を検証するための統計的手法のこと。例えば、2 値乱数で 0 と 1 が同じ確率で現れるかなど、数列に統計的な偏りが無いことを判定する。本研究では、米国国立標準技術研究所（National Institute of Standards and Technology）が推奨する国際的な乱数の統計検定法である NIST Special Publication 800-22 を用いている。さらに大量の乱数の統計検定を行うために、TestU01 と呼ばれる新たな統計検定方式も用いている。本研究で生成された乱数は、両方の検定方式において全ての検定項目に合格している。

問い合わせ先

埼玉大学　大学院理工学研究科　数理電子情報部門　准教授
担当教員　内田　淳史
TEL 048-858-3490
e-mail auchida@mail.saitama-u.ac.jp

〒338-8570 さいたま市桜区下大久保２５５　埼玉大学
本件発信元：総務部総務課広報担当（岡田・伊藤）
TEL :048-858-3932･3927　FAX:048-858-9057　e-mail:koho@gr.saitama-u.ac.jp