レーザカオスを用いた超高速物理乱数生成器の高機能化

内田　淳史（理工学研究科・准教授）

1　研究の目的

ランダムな数列を生成する乱数生成器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、盗聴者による乱数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、従来の熱雑音を用いた方式では生成速度が遅いのが欠点であり、その生成速度は毎秒０.１ギガビット（0.1 Gb/s）程度に留まっている。また天気予報や地震予測などの自然災害予測および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の必要性が急速に高まっている。

そこで本研究では、レーザカオスを用いた新たな超高速物理乱数生成器の開発およびその高機能化を目的とする。特に半導体レーザの周波数帯域拡大効果を用いることで、物理乱数生成速度の高速化を目標とする。

2　研究方法と成果

提案する超高速物理乱数生成方式の概念図を図1(a)に、その方式を図 1(b)に示す。戻り光により出力がカオス状態であるレーザ光を用意して別のレーザへ光注入することで、16 GHz まで帯域拡大されたレーザカオス信号を得る。次にそのカオス波形を二つに分岐し、一方に時間遅延を加える。カオス波形とその時間遅延波形を 50 GS/s でサンプリングし、8 ビット AD 変換を行う(図 1(b)の Step 1)。ここで時間遅延波形の 8 ビット信号の各ビットを逆順に並べ替える(Step 2)。元の波形とビット順を反転した時間遅延波形の 8 ビット信号に対して、ビットごとに排他的論理和演算を行うことで乱数を生成する(Step 3)。このとき、乱数生成速度は等価的に 8 bit × 50 GS/s = 400 Gb/s となる。

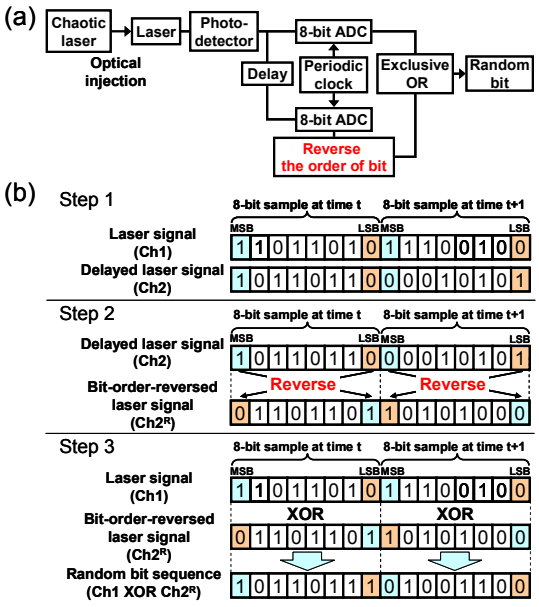

図１　超高速物理乱数生成方式

本方式で生成された乱数に対して国際標準の統計検定を行うために、NIST Special Publication (SP) 800-22 を使用した。その結果、各検定項目において P-value、Proportion 共に合格基準を満たしているため、全 15 項目に合格していることが分かった。

本方式ではビット順反転処理(図 1(b)の Step 2)を付加することにより、下位ビット切り出しを行う必要が無く、8 ビットを全て乱数生成に使用できる点が優れている。そこでビット順反転処理の効果を調査するために、カオス波形および生成された乱数の確率密度分布を調査した。8 ビットカオス信号(Ch1 と呼ぶ)およびビット順反転したカオス信号(Ch2^{R} と呼ぶ)の確率密度分布を図 2(a)に示す。元のカオス信号(Ch1)はガウス分布に近い確率密度分布となっているがビット順反転を適用することで、離散的な確率密度分布に変化することが分かる(Ch2^{R})。またビット順反転無し(Ch1 XOR Ch2 と呼ぶ)およびビ

ット順反転あり(Ch1 XOR Ch2^{R}と呼ぶ)の後処理により生成された乱数(8 ビットごとに 10 進数で表示)の確率密度分布を図 2(b)に示す。ビット順反転が無い場合には、元のカオス波形がガウス分布に近いために、生成された乱数も中心の出現頻度が大きい確率密度分布となっている。一方でビット順反転がある場合には、生成された乱数の確率密度分布はほぼ一様となっている。このようにビット順反転処理によりマルチビット乱数列の出現頻度を一様にすることが可能となり、ランダム性の高い乱数が生成できる。

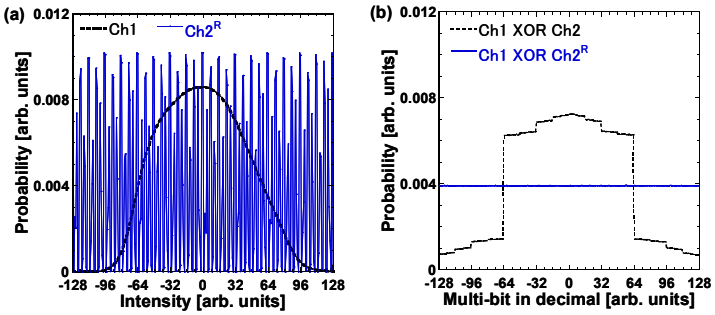

図 2　(a) 8 ビットカオス信号(Ch1)およびビット順反転したカオス信号(Ch2^{R})の確率密度分布。(b) ビット順反転無し(Ch1 XOR Ch2)およびビット順反転あり(Ch1 XOR Ch2^{R})の後処理により生成された乱数(8 ビットごとに 10 進数で表示)の確率密度分布。

さらにビット順反転処理によるランダム性向上の理由を調査するために、1 の出現頻度から 0.5 を引いた絶対値であるバイアスの調査を行った。その結果を図 3 に示す。バイアスが小さいほどランダム性の高い乱数であると言える。ビット順反転処理が無い場合(図 3(a))、8 ビット量子化後のカオス波形(Ch1, Ch2)は上位ビットほどバイアスが大きくなっていることが分かる。したがって生成される乱数のバイアスも上位ビットが大きく、非一様なバイアス分布となっている(図 3(a)の Ch1 XOR Ch2)。一方でビット順反転処理がある場合(図 3(b))、8 ビット量子化後のカオス波形(Ch1)に対して、8 ビットを逆順にした波形(Ch2^{R})の個別ビットのバイアス分布が反転していることが分かる。この 2 つの分布を持つ波形から、バイアスが高い個別ビットと低い個別ビットで排他的論理和演算を行うことで、生成された乱数の個別ビットのバイアスが低減されていることが分かる(図 3(b)の Ch1 XOR Ch2^{R})。さらに乱数の個別ビットのバイアスはほぼ一様に分布しており、そのバイアス値は 10^{-5} 程度まで低減させることに成功している。これは NIST SP 800-22 の 1 頻度の偏り検定の基準以下(図 3 の点鎖線)となっており、ランダム性の高い乱数が生成可能であることが分かる。

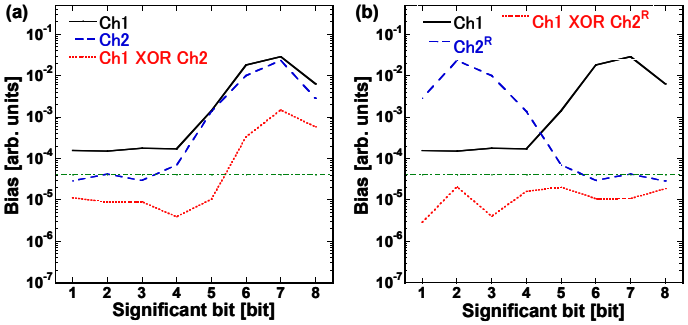

図 3　8 ビット AD 変換されたカオス波形(Ch1, Ch2)と後処理により生成された 8 ビット乱数列に対する各ビットのバイアス(1 頻度の出現確率の偏り)。最下位ビットが 1、最上位ビットが 8 に対応する。(a) ビット順反転無し(Ch1 XOR Ch2)および、(b)ビット順反転あり(Ch1 XOR Ch2^{R})の後処理により生成された乱数の各ビットのバイアス。

3　まとめ

本研究では半導体レーザカオスを用いた物理乱数生成の高速化手法を提案した。帯域拡大されたカオス波形とその時間遅延信号を 8 ビット量子化し、一方のビット列を逆順に並べ替えて排他的論理和演算を行うことにより乱数を生成した。この時、等価的に 8 bit × 50 GS/s = 400 Gb/s での物理乱数生成速度を達成した。また個別ビットのバイアスに対する後処理の効果を調査し、個別ビットのバイアスを一様に低減可能であることが明らかとなった。