レーザのランダム現象に基づく超高速物理乱数生成器の開発

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、情報セキュリティ分野や自然災害予測のための大規模数値シミュレーション分野に必要不可欠な基盤技術である。しかしながらコンピュータで生成される擬似乱数を用いた場合、安全性の脅威や予測精度の低下が近年大きな問題となっている。一方で自然現象を利用する物理乱数はランダム性が高いという優れた特性を有しているものの、従来の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 1 秒間に 1 億個（0.1 Gb/s）程度に留まっている。

そこで近年、再現性と周期性の無い物理乱数の乱数源として GHz オーダで不規則的に振動する半導体レーザカオスが注目されており、市販のレーザ装置を用いた様々な物理乱数生成方式が実証されている。しかしながら、市販のレーザ装置や光検出器は光学定盤上に設置されるため 300 mm × 1000 mm 程度と大きく、コンピュータ等への搭載は困難であることが問題となっている。そのため、レーザカオス発生部を 10 mm × 20 mm に集積化した光集積回路を用いた高速物理乱数生成がこれまでに報告されている[1,2]。しかしながら、従来の光集積回路は外部共振器長が 10 mm に固定されており、さらに時間ダイナミクスの詳細な調査が行われていない。外部共振器長を短くすることで外部共振周波数の高速化が可能となり、カオスの周波数帯域拡大と乱数生成速度の高速化が期待される。また、光集積回路の小型化や製造過程における歩留まりの改善も期待される。

そこで本研究では、5 mm の外部共振器長を有する高速カオス発生用光集積回路において、時間ダイナミクスの詳細な調査を行うことを目的とする。また、レーザへの注入電流と戻り光比率を同時に変化させたときの二次元分岐図を実験的に作成する。さらに、光集積回路を用いた物理乱数生成実験を行う。

2　研究方法と成果

本研究で用いた高速カオス発生用光集積回路は、半導体レーザ、光増幅器、外部共振器、光検出器により構成されている。本光集積回路は、NTT コミュニケーション科学基礎研究所および NTT フォトニクス研究所との共同研究により作製された[2]。本研究では外部共振器長が既存の光集積回路の 10 mm よりも短い 5 mm の光集積回路を用いる。レーザの出力光は光増幅器により増幅された後、外部共振器で反射されレーザ自身に戻り光として注入される。これにより、レーザ出力はカオス的不規則振動を生ずる。レーザカオス光は光集積回路内部の光検出器により検出され、電気信号として出力される。実験では、パラメータとして発振しきい値により規格化されたレーザへの注入電流 J/J_{th} と、光増幅器へのバイアス電流に依存して決まる戻り光比率 P_f を変化させて時間ダイナミクスの観測を行った。

はじめに実験にて観測された時間波形を図 1 に示す。図 1(a) ~ 1(f)はそれぞれ、安定状態、周期、準周期、カオス、間欠性、パルスパッケージの時間波形を示している。本実験では中心周波数 6.6 GHz の高速なカオス(図 1(d))が観測された。また、振幅の大きなバースト部と小さなラミナー部が混在した間欠性の時間波形(図 1(e))が観測された。

次に、規格化された注入電流 J/J_{th} と戻り光比率 P_f を同時に変化させたときの二次元分岐図を図 2 に示す。図 2 の色は観測された時間波形の種類を示している。また、図 2 の記号(a)~(f)は図 1 で示した時間波形が観測されたパラメータを示している。図 2 から、二次元分岐図には大きく分けて準周期(QP)、カオス(C)、パルスパッケージ(PP)のパラメータ領域が存在している。準周期(QP)はレーザへの注入電流

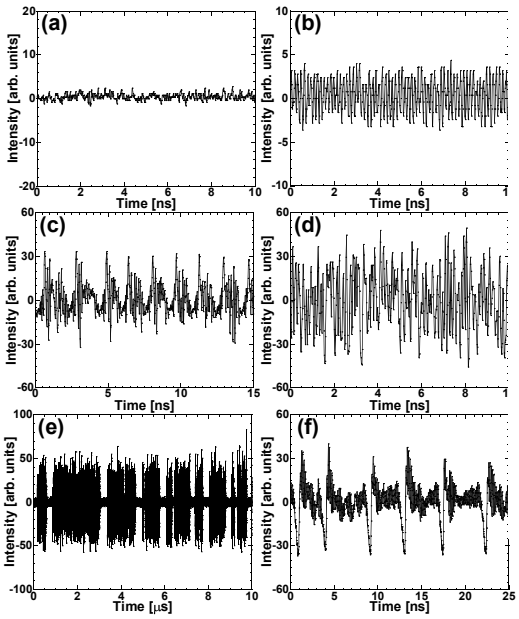

図１　光集積回路の時間波形。(a) 安定状態、(b) 周期、(c) 準周期、(d) カオス、(e)間欠性、(f)パルスパッケージ。

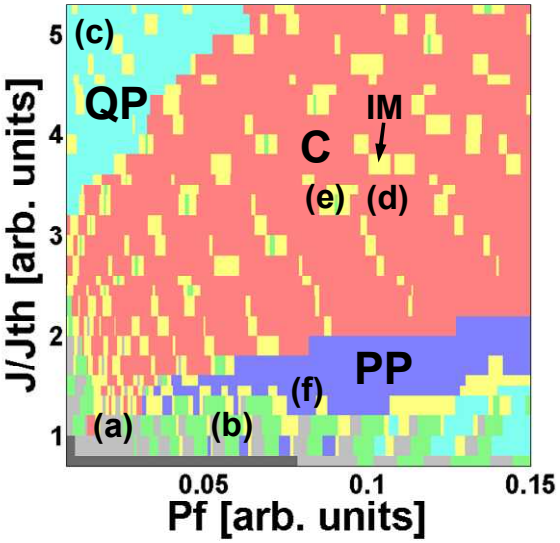

図２　外部共振器長 5 mm の光集積回路の二次元分岐図。黒: 発振なし、灰色: 安定状態、黄緑: 周期、水色: 準周期(QP)、赤: カオス(C)、黄色: 間欠性(IM)、紫: パルスパッケージ(PP)。

J/J_{th} が大きく、戻り光比率 P_f が小さい領域で観測される。またパルスパッケージ(PP)は、J/J_{th} が小さく、P_f が大きい領域で観測される。さらに、カオス(C)が広いパラメータ領域で観測されることが分かった。また図 1(e) のような間欠性の時間波形が観測される領域(黄色)は、二次元分岐図上で島状に存在していることが分かった。これは光集積回路に特有の現象であることが明らかとなった。

ここで、光集積回路から出力されたレーザカオス波形を用いて物理乱数生成を行った。レーザカオス波形とその時間遅延波形を同時刻で周期サンプリングし、しきい値を定めて 1 ビット AD 変換を行なった。得られた 2 つのビット列に対して、排他的論理和演算を施すことで 2 値乱数列として出力した。生成された乱数のランダム性について国際標準の統計検定である NIST Special Publication 800-22 [3]を用いて評価を行なった。本検定は全 15 項目から構成され、全ての検定項目に合格した乱数はランダム性が高いと言える。その結果、全 15 項目に合格する乱数の最大生成速度は、4.55 Gb/s であることが分かった。また、NIST 検定に合格する乱数生成速度とカオス波形の自己相関との関連について調査を行った。その結果、自己相関が約 2×10^{-2} 以下となる遅延時間に対応するサンプリング時間で生成された乱数において、ランダム性の高い乱数が生成できることが分かった。

3　まとめ

本研究では外部共振器長が 5 mm の高速カオス発生用光集積回路の非線形ダイナミクスを調査した。その結果、準周期、カオス、パルスパッケージの時間ダイナミクスに大別され、さらに間欠性の領域が二次元分岐図上で島状に存在することが明らかとなった。さらに光集積回路を用いた物理乱数生成を行ったところ、1 ビット AD 変換にて 4.55 Gb/s の最大生成速度での乱数生成を達成した。

参考文献

[1] A. Argyris, et al., Optics Express, Vol. 18, No. 18, pp. 18763-18768 (2010).

[2] T. Harayama, et al., Physical Review A, Vol. 83, pp. 031803(R)-1-4 (2011).

[3] A. Rukhin, et al., NIST Special Publication 800-22, Revision 1a (2010).