

半導体レーザを有する光集積回路とビットシフト回転法を用いた物理乱数生成

Physical random number generation with a photonic integrated circuit and bit-shift rotation method

埼玉大¹, NTT CS 基礎研², 早稲田大³,
 °宇賀神 上総¹, 寺島 悠太¹, 内田 淳史¹, 原山 卓久^{2,3}, 吉村 和之²
 Saitama Univ.¹, NTT CS Lab.², Waseda Univ.³,
 °K. Ugajin¹, Y. Terashima¹, A. Uchida¹, T. Harayama^{2,3}, and K. Yoshimura²
 E-mails: {s14mm305, auchida}@mail.saitama-u.ac.jp

はじめに: 近年、高速な不規則振動を生じるレーザカオスを物理乱数源として用いた物理乱数生成の研究が報告されている[1]。従来の研究において、レーザカオスを有する物理乱数生成装置は光学定盤上に設置されており、実用化のためには小型化が必要となる。これまでに、光集積回路を用いたレーザカオス発生部の小型化が報告されている[2]。また、乱数生成処理部において、レーザカオスを電気信号に変換する AD 変換器の量子化誤差によるランダム性の低下を軽減する必要がある。これまでに、量子化誤差の影響を軽減する手法として差分法[3]が提案されている。また、乱数のランダム性を向上させる手法としてビットシフト回転法[4]が提案されている。しかしながら、二つの手法を組み合わせるレーザカオスに適用した研究は未だ報告されていない。

そこで本研究では、光集積回路で生成されたレーザカオス波形に対して差分法とビットシフト回転法を組み合わせた乱数生成方式を適用して物理乱数生成を行うことを目的とする。

実験方法と結果: 本研究で用いるレーザカオス発生用光集積回路は、半導体レーザ、二つの光増幅器、長さが 10.3 mm の導波路、外部鏡、および光検出器により構成されている。レーザから出力された光は外部鏡により反射され、戻り光として再びレーザに注入される。これにより Fig.1(a)に示すようなレーザカオス波形が生じる。レーザカオスは光集積回路内の光検出器により電気信号として出力される。また、本光集積回路から得られたレーザカオスの振幅の出現確率のヒストグラムを Fig.1(b)に示す。ヒストグラムは正規分布に似た形状を示している。しかしながら、レーザカオスの振幅の出現頻度のヒストグラムは、AD 変換器の量子化誤差により特定の振幅の出現頻度が高く、不連続的である。そこで差分法を用いることにより、ヒストグラムの平坦化を行う。

ここで乱数生成処理について説明する。レーザカオス波形からそれぞれ異なる遅延時間を有する三つの遅延波形を生成する。レーザカオス波形と一つ目の遅延波形間および二つ目と三つ

目の遅延波形間で差分を行うことで二つの差分信号を得る。次に一つ目の差分信号に対し、8 ビットごとに n ビットシフト回転を行う ($n = 1, 2, 4$) [4]。以上により、二つの差分信号と 1 ビット、2 ビット、4 ビットシフト回転信号が得られる。最後に五つの信号の個別ビット間で排他的論理和を行うことで乱数列を生成する。

生成した乱数のランダム性を NIST 検定[5]および Test U01 検定[6]を用いて評価した。全ての検定項目に合格した乱数は真性乱数と統計的に区別不可能とされる。本手法で生成した乱数は全ての検定項目に合格することができた。

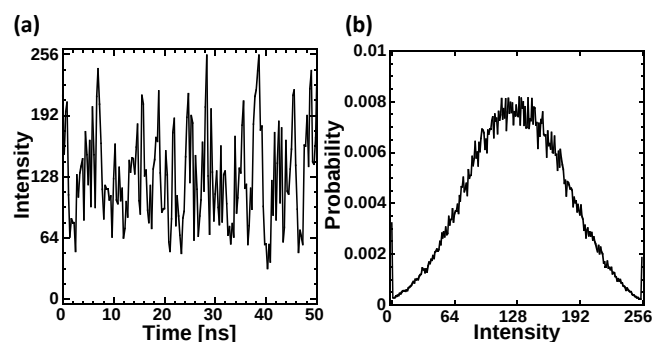


Fig.1 (a) Chaotic temporal waveform of photonic integrated circuit. (b) Probability distribution of chaotic temporal waveform.

まとめ: 本研究では、光集積回路で生成されたレーザカオス波形に対して、差分法とビットシフト回転法を組み合わせた乱数生成方式を適用することで乱数を生成した。生成した乱数のランダム性をNIST検定とTest U01検定を用いて評価したところ、全ての検定項目に合格できた。

参考文献

- [1] A. Uchida, et al., Nat. Photonics, **2**, 728 (2008).
- [2] R. Takahashi, et al., Opt. Express, **22**, 11727(2014).
- [3] I. Reidler, et al., Phys. Rev. Lett, **103**, 024102 (2009).
- [4] M. Dichtl, Lect. Not. Comput. Sci, **4593**, 137 (2007).
- [5] A. Rukhin et al., NIST. Special Publication 800-22, Revision 1a (2010).
- [6] P. L'Ecuyer et al., ACM Trans. Math. Soft, **33**, 22 (2007)