

# 半導体レーザの帯域拡大カオスを用いた物理乱数生成器における エントロピー生成率の評価

Evaluation of entropy rate in physical random number generator using bandwidth-enhanced chaotic semiconductor lasers

埼玉大<sup>1</sup> 寺島 悠太<sup>1</sup>, 吉屋 圭吾<sup>1</sup>, 内田 淳史<sup>1</sup>

Saitama Univ.<sup>1</sup> Yuta Terashima, Keigo Yoshiya, and Atsushi Uchida

E-mails: s15mm318@mail.saitama-u.ac.jp, auchida@mail.saitama-u.ac.jp

**はじめに:** 乱数は情報セキュリティにおける暗号等に用いられており、周期性や再現性を持たない物理乱数が望まれている。近年、半導体レーザカオスを乱数源として用いることで、乱数生成速度が Gb/s を超える高速物理乱数生成方式が提案されている[1]。特に物理乱数生成の高速化が進められており、複数の半導体レーザを一方方向に結合して広帯域な信号を得るために、帯域拡大カオスが提案されている[2]。しかしながら、これらの研究で用いられている物理乱数生成器の評価は、生成された物理乱数に対して統計的な検定を適用する方法に限定されている。一方で近年、物理乱数生成器の評価手法として、乱数源のエントロピー生成率を測定する手法が提案されている[3]。しかしながら、帯域拡大カオス波形に対してエントロピー生成率を測定して物理乱数生成器の評価を行う研究は、これまでに報告されていない。

そこで本研究では、物理乱数生成器の乱数源の評価を行うために、帯域拡大された半導体レーザカオスのエントロピー生成率を実験的に測定することを目的とする。

**方法と結果:** 本研究では、乱数源である半導体レーザカオスを量子化したデータからエントロピー生成率を測定する(Fig. 1 参照)。エントロピー生成率は、サンプリング間隔  $\tau$  と分解能  $\epsilon$  をパラメータとする  $(\epsilon, \tau)$ -エントロピーにより測定した[4]。また、本研究ではエントロピー生成率を測定する乱数源として、3つの半導体レーザを一方方向に結合することで生成される広帯域な帯域拡大カオスを用いた[2]。3つの半導体レーザ(Laser 1, Laser 2, Laser 3 と呼ぶ)のうち、Laser 1 では外部鏡で戻り光を付加することで半導体レーザカオスを生成する。次に Laser 1 のレーザカオス光を Laser 2 へ一方方向に注入することで広帯域な帯域拡大カオスを生成する。同様に Laser 2 の出力光を Laser 3 へ一方方向に注入することでより広帯域な帯域拡大カオスの生成を行う。生成された帯域拡大カオスは光検出器により電気信号に変換され、オシロスコープによりサンプリング速度 100 GS/s かつ 8 ビットの分解能で量子化された時間波形が取得される。本研究では Laser 1, Laser 2, Laser 3 の時間波形と、光検出器のノイズ波形に対して、エントロピー生成率の測定を行った。

エントロピー生成率を測定した結果を Fig. 2 に示す。Fig. 2 のグラフの横軸はオシロスコープの量子化分解能を示している(8 ビットが上限)。Fig. 2 より、エントロピー生成率は Laser 3 が最も高く、Laser 1 が最も低いことが分かった。これは、帯域拡大によりカオス波形が広帯域化したのみならず、エントロピー生成率も向上したためだと考えられる。また光検出器のノイズ波形からもエントロピー生成率が測定できることから、レーザ波形のエントロピー生成率にはノイズの影響も含まれていることが分かった。またどのレーザにおいても、分解能が 8 ビットの場合にエントロピー生成率が最大であり、特に Laser 3 では 484 Gb/s のエントロピー生成率を達成した。

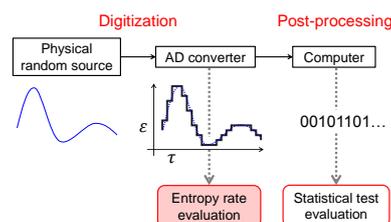


Fig. 1 Method for evaluation of entropy rate in physical random number generator.

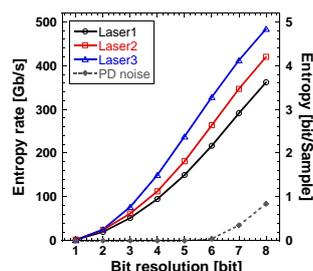


Fig. 2 Entropy rate for bandwidth-enhanced chaotic lasers and photodetector (PD) noise.

**まとめ:** 本研究では、一方方向結合された3つの半導体レーザを用いて帯域拡大カオスを生成し、各レーザ出力の時間波形からエントロピー生成率を測定した。その結果、帯域が拡大するにつれてエントロピー生成率も増大することが明らかとなった。

## 参考文献

- [1] A. Uchida, et al., *Nature Photonics* **2**, 728 (2008).
- [2] R. Sakuraba, et al., *Optics Express* **23**, 1470 (2015).
- [3] A. M. Hagerstrom, et al., *Proceedings of the National Academy of Sciences* **112**, 9258 (2015).
- [4] P. Gaspard, et al., *Physics Reports* **235**, 291 (1993).