

物理乱数源としての半導体レーザカオス時系列のエントロピー評価実験 Entropy evaluation of chaotic waveform in semiconductor lasers as a random number generator

埼玉大, °川口 佑, 菅野 円隆, 内田 淳史

Saitama Univ., °Yu Kawaguchi, Kazutaka Kanno, and Atsushi Uchida
E-mails: y.kawaguchi.678@ms.saitama-u.ac.jp, auchida@mail.saitama-u.ac.jp

はじめに:

近年、情報化社会の進展に伴い情報セキュリティの重要性が高まっている。特に暗号等の分野においては予測不可能な乱数を用いる必要がある。現在はアルゴリズムにより生成される擬似乱数が主流であるが、再現性や周期性を完全に排除することは困難である。そこで物理現象から生成される物理乱数の利用が提案されている。特に半導体レーザのカオス時系列を物理乱数源とすることで Gb/s を越える高速な物理乱数生成が報告されている[1]。

しかしながら物理乱数の評価においては課題が存在する。従来は、取得時系列に対してアルゴリズムによる後処理を行い、生成した乱数列に対して統計的な検定を行っていた。この手法では後処理による効果を含むために、物理源の非再現性を越える速度での乱数生成をした場合でも、検定を通過することが可能であると指摘されている[2]。したがって物理乱数としての予測不可能性を保障するためには、後処理前の時系列自体の非再現性(エントロピー)を評価する必要がある。

予測不可能性の指標として (ϵ, τ) エントロピー [3, 4] が提案されている。この手法では、振幅の量子化分解能 ϵ とサンプリング間隔 τ により離散化されたデータのエントロピー生成率を算出する。そのため、実験データおよびノイズの時系列に直接適用することが可能である。

そこで本研究では、光注入された半導体レーザから生成されたカオス時系列に対して (ϵ, τ) エントロピーを算出し、物理乱数源としての評価を行うことを目的とする。

実験方法:

Fig. 1 に実験装置図を示す。半導体レーザ 1 (Laser 1) の出力を一方方向に半導体レーザ 2 (Laser 2) に注入する。このとき、レーザ間の初期光周波数差および注入光強度に依存してレーザ 2 のダイナミクスが変化する。レーザ 2 の出力はアイソレータ (Isolator) とアッテネータ (Attenuator) を介して各計測器により取得される。本研究では注入光強度を 100 nW から 400 nW まで変化

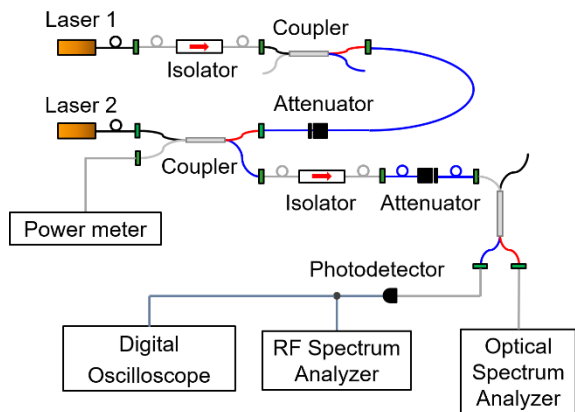


Fig. 1 Experimental setup for generation of chaos using a semiconductor laser with optical injection

させて、取得した各出力強度のカオスの時間波形に対して (ϵ, τ) エントロピーの算出を行う。

結果:

注入光強度を変化させたときの (ϵ, τ) エントロピー生成率の実験結果を Fig. 2(a) に示す。ここでは ϵ を各時間波形の標準偏差に設定し、 τ を 0.02 ns (50 GS/s) に設定している。エントロピー生成率は注入光強度の増加に伴い増加し、300 nW のときに最大値 6.2 Gb/s となった。また、さらに注入光強度が増加するとエントロピー生成率は減少することが分かった。

Fig. 2(b) にサンプリング速度に対する 1 サンプル当たりのエントロピーを示す。なお物理乱数源としての評価のために、 ϵ はオシロスコープの量子化分解能 (8 ビット) に対応するように設定している。MSB n は上位 n ビットを使用することを意味する。ここでは、エントロピー生成率が最大となる注入強度 300 nW における算出結果を示している。1 サンプル当たりのエントロピーは、サンプリング速度が減少するにつれて増加することが分かる。また MSB が大きいほどエントロピーは増加する。MSB 2 および MSB 3 では低いサンプリングレートにおいて 1 サンプルあたり 1 ビットを越えていることが分かった。したがって、これらの分解能で取得した時間波形を用いることで、各サンプル点において 1 ビット以上のエントロピーが保証された物理乱数生成を行うことが可能であると考えられる。

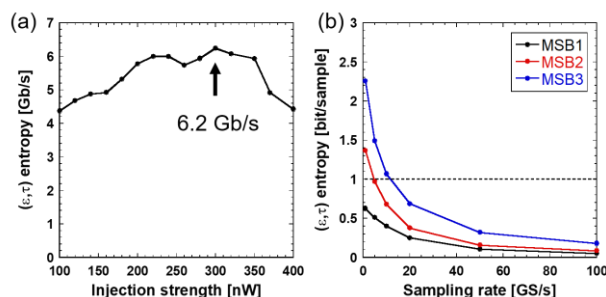


Fig. 2 (a) Entropy rate as the injection strength is changed. (b) Entropy per sample from MSB 1 to MSB 3 as the sampling rate is changed.

まとめ:

本研究では、レーザカオス時系列に対して (ϵ, τ) エントロピーを算出し、物理乱数源としての評価を行った。 (ϵ, τ) エントロピーの評価により、各サンプル点において 1 ビット以上のエントロピーが保証された物理乱数生成が可能であることを示した。

参考文献

- [1] A. Uchida, et al., Nat. Photon. **2**, 728 (2008).
- [2] J. D. Hart, et al., APL Photonics **2**, 090901 (2017).
- [3] P. Gaspard and X. -J. Wang, Phys. Rep. **6**, 291 (1993).
- [4] A. Cohen and I. Procaccia, Phys. Rev. A **31**, 1872 (1985).