戻り光を有する半導体レーザカオスのサンプルエントロピー評価と物理乱数生成

Sample entropy evaluation and physical random number generation in a semiconductor laser with optical feedback

埼玉大，○大熊 智彦，澤山 太一，菅野 円隆，内田 淳史
Saitama University
○Tomohiko Okuma, Taichi Sawayama, Kazutaka Kanno, and Atsushi Uchida
E-mails: t.okuma.675@ms.saitama-u.ac.jp, auchida@mail.saitama-u.ac.jp

はじめに: 近年の情報化社会では，情報セキュリティにおける暗号化や大規模数値シミュレーション等の幅広い場面で乱数が利用されている．一般的には擬似乱数が利用されているが，周期性や再現性が存在するため，安全面の脆弱性が指摘されている．そこで近年，半導体レーザカオスを物理乱数源とした高速物理乱数生成方式が報告されている [1]．この方式の提案以降，様々な生成方式が提案され，現在に至るまでに Tb/s を超える乱数生成速度を実現している [2]．しかしながら乱数生成の高速化に伴い，物理乱数源が持つエントロピーを超えた乱数生成を行っているという問題点が指摘されている．そのため，物理乱数を生成する際は，物理乱数源である時間波形のエントロピーの評価が重要である [3]．

時間波形のエントロピー評価手法として Kolmogorov-Sinai (KS) エントロピーが知られているが，KS エントロピーが算出できるのは数値計算が主であり，実験データから直接算出することは難しい．そこで，実験データから直接エントロピーを算出する手法としてサンプルエントロピーが提案されている [4]．しかしながら，物理乱数源のエントロピー評価としてのサンプルエントロピーの有用性は未だ報告されていない．

そこで本研究では，戻り光を有する半導体レーザカオスを実験で取得し，サンプルエントロピー評価を行うことを目的とする．特に，エントロピー評価をしたレーザカオスを乱数源として乱数生成を行い，サンプルエントロピーの算出結果と乱数生成結果の関係性を調査する．

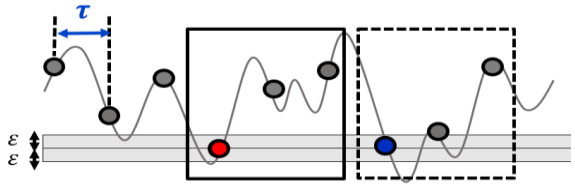

Fig. 1. Concept of the calculation of entropy from temporal waveforms.

方法: 時間波形からエントロピーを算出する方法の概念図を Fig.1 に示す．はじめに，取得した時間波形をサンプリング間隔 τ により量子化を行い，時系列データを取得する．次に，時系列データ上からランダムに 1 点を選び，この点を基準に長さ d の基準ベクトルを生成する．そしてこの基準ベクトルと各成分との差が ε 以内であるベクトルが時系列データ上に存在する確率 A_i^d を算出する．この操作を R 回繰り返す．そして以下の式のように，確率 A_i^d の平均値を先に計算した後に対数を算出する．

$$A^d = -\log_2\left(\frac{1}{R}\sum_{i=1}^{R} A_i^d\right) \qquad (1)$$

最後にベクトル長が $d+1$ と d の場合における A^{d+1} と A^d の差をとり，サンプリング速度 $1/\tau$ を乗算した値がエントロピー値 h となる．

$$h = \frac{1}{\tau}(A^{d+1} - A^d) \qquad (2)$$

結果: 実験で取得した戻り光を有する半導体レーザカオスに対するサンプルエントロピーの算出結果を Fig. 2(a) に示す．横軸の MSB n は 8 ビットに量子化されるレーザカオスの上位 n ビットを示す．時間波形の振幅のサンプリング間隔 τ は 100 ps と設定し，分解能 ε はオシロスコープの量子化分解能を基準に設定する．例えば $\varepsilon = 128$ である場合のエントロピー算出結果は 8 ビット のデータ (-128 から 128 の振幅) のうち上位 1 ビットのエントロピーに対応している．算出結果より，MSB 4 以上でサンプルエントロピーの値が 1 bit/sample を超えることが分かった．

次に，サンプルエントロピー評価に用いたレーザカオスを乱数源として，時間波形とその遅延波形を個別ビットごとに排他的論理和演算 (XOR) することで物理乱数生成を行った．そして，8 ビットを個別ビットに分割してサンプリング点ごとに連結し 2 値で乱数を生成した．乱数列を国際的な乱数統計検定である NIST Special Publication 800-22 [5]により評価した結果を Fig. 2(b) に示す．サンプルエントロピーの算出値が 1 bit/sample を超えるビットである MSB4 以上で NIST 検定の全ての検定項目 (15 項目) に合格することが分かった．

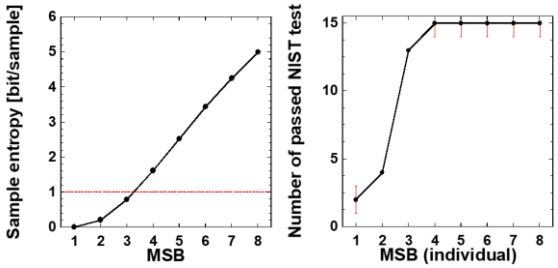

Fig. 2. (a) Result of sample entropy as a function of extracted individual most significant bit (MSB). (b) Number of passed NIST tests as a function of extracted individual MSB.

まとめ: 本研究では，戻り光を有する半導体レーザカオスを実験で取得し，サンプルエントロピー評価と物理乱数生成を行った．また，国際的な統計検定を用いて生成した乱数列を評価した．高いサンプルエントロピーを有する乱数列は統計検定に合格することが分かった．

参考文献

[1] A. Uchida, et al., Nat. Photon., **2**, 728 (2008).
[2] R. Sakuraba, et al., Opt. Express., **23**, 1470 (2015).
[3] J. D. Hart, et al., APL Photonics, **2**, 090901 (2017).
[4] J. S. Richman, et al, Am. J. Physiology **6,** 2039 (2000).
[5] A. Rukhin, et at, NIST SP 800-22, Revision 1 a (2010).