

戻り光を有する半導体レーザーにおける位相ダイナミクスと高速物理乱数生成

Extraction of phase dynamics and physical random number generation in a semiconductor laser with optical feedback

埼玉大、[○]舟橋 遼、工藤 翔太、菅野 円隆、内田 淳史

Saitama University

[○]Ryo Funabashi, Syota Kudo, Kazutaka Kanno, and Atsushi Uchida

E-mails: r.funabashi.728@ms.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の重要な要素技術であり、ランダム性の高い乱数が必要とされている。しかしながら、現在広く利用されている擬似乱数は、再現性と周期性を有している。そこで、非再現性と非周期性を有している物理乱数を生成するために、戻り光を有する半導体レーザーの光強度ダイナミクスを用いた Gb/s を超える高速物理乱数生成が報告されている[1]。

戻り光を付加した半導体レーザーから出力される光強度ダイナミクスは、カオスと呼ばれる GHz オーダの高速不規則な振動を生じる。一方で戻り光を有する半導体レーザーは、光強度だけでなく、周波数や位相も同様にカオス振動する。これまでに、MHz オーダで低速振動する低周波不規則振動の周波数ダイナミクスを光ヘテロダイン検波により抽出した報告例がある[2]。しかしながら、GHz オーダのカオス振動における位相の抽出は報告されていない。このような高速振動する位相ダイナミクスの抽出には、コヒーレント光通信に用いられる光コヒーレント検波技術が有用であると考えられる[3]。

そこで本研究では、光コヒーレント検波を用いることにより、GHz オーダで高速振動する半導体レーザーカオスの位相の抽出ダイナミクスを数値計算により行い、高速物理乱数へ応用することを目的とする。

方法: 光コヒーレント検波による位相の抽出方法を以下に示す。Fig. 1 に本研究における数値計算のモデル図を示す。戻り光を有する半導体レーザー (Laser 1) と戻り光を有していない参照レーザー (LO) は、90° 光ハイブリッドで干渉させる。そして、光強度はバランスフォトリセーバにより検出される。また、バランスフォトリセーバの出力である $I_I(t)$ と $I_Q(t)$ を用いることで、以下のように Laser 1 の複素電界を復元できる。

$$I_e(t) = I_I(t) + iI_Q(t) = A_c(t)A_l \exp[i2\pi\Delta f t + \theta_c(t) + \theta_n(t)] \quad (1)$$

ここで、 Δf は初期光周波数差を表し、 $\theta_c(t)$ と $\theta_n(t)$ はそれぞれ、Laser 1 の位相とノイズの位相を表している。初期光周波数差を $\Delta f = 0$ とすることで、以下の式により位相を抽出できる。

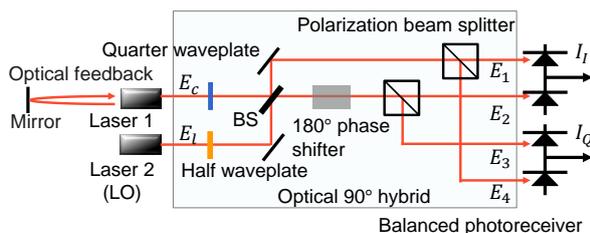


Fig. 1. Model for optical coherent detection using 90-degree optical hybrid.

$$\theta_e(t) = \arg(I_e(t)) \quad (2)$$

結果: 本研究により、式(2)を用いて抽出された戻り光を有する半導体レーザーの光強度ダイナミクスと位相ダイナミクスの数値計算結果を Fig. 2(a) の黒線と赤線にそれぞれ示す。Laser 1 の光強度と位相ダイナミクス $\theta_e(t)$ は、GHz オーダの高速カオス振動をしていることが分かる。また、位相ダイナミクスは $0 \leq \theta_e(t) < 2\pi$ の範囲で振動している。次に、光強度ダイナミクスと位相ダイナミクスを 8 ビット量子化することにより物理乱数を生成する。そして、8 ビットを個別ビットに分割して連結した乱数を、国際的な乱数統計検定である NIST Special Publication 800-22 [4] を用いて、生成された乱数のランダム性を統計的に評価する。NIST 検定は全 15 項目から構成され、全 15 項目に合格した乱数は統計的に真性乱数と区別不可能である。8 ビット量子化された光強度ダイナミクスと位相ダイナミクスの各個別ビットを切り取り並べた乱数の NIST 検定結果を Fig. 2(b) の黒線と赤線にそれぞれ示す。Fig. 2(b) より、光強度ダイナミクスはどの個別ビットも NIST 検定に合格していないが、位相ダイナミクスは、下位 1, 2 ビットで NIST 検定に合格していることが分かる。以上より、物理乱数生成に位相を用いることで、従来の光強度ダイナミクスを用いた物理乱数生成方式より、ランダム性の高い乱数を生成できることが分かった。

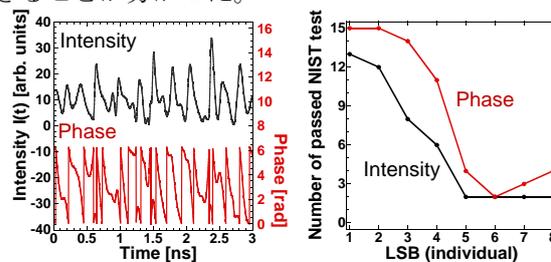


Fig. 2. (a) Intensity (black) and phase dynamics (red) of Laser 1. (b) Number of passed NIST tests of intensity (black) and phase dynamics (red) as a function of extracted individual least significant bit (LSB).

まとめ: 本研究では、光コヒーレント検波を用いて、GHz オーダで高速振動する半導体レーザーカオスの位相ダイナミクスの抽出を行い、位相ダイナミクスを用いた物理乱数生成を行った。位相ダイナミクスを用いた乱数生成は、従来の光強度ダイナミクスを用いた従来の手法よりもランダム性の高い乱数を生成できることが分かった。

参考文献

- [1] A. Uchida, et al., Nat. Photon., **2**, 728 (2008).
- [2] D. Brunner, et al., Sci. Rep., **2**, 732 (2012).
- [3] K. Kikuchi, IEICE Electronics Express, **8**, 20 (2011).
- [4] A. Rukhin, et al, NIST SP 800-22, Revision 1 a (2010).