光コヒーレント検波による半導体レーザカオスの複素電界ダイナミクスを用いた乱数生成

Random number generation using complex electric-field dynamics in a chaotic semiconductor laser with optical coherent detection

埼玉大、○工藤 翔大、舟橋 遼、菅野 円隆、内田 淳史
Saitama University
○Shota Kudo, Ryo Funabashi, Kazutaka Kanno, and Atsushi Uchida
E-mails: s.kudo.278@ms.saitama-u.ac.jp, auchida@mail.saitama-u.ac.jp

はじめに: 乱数生成は情報セキュリティや大規模数値シミュレーションへの応用に必要不可欠な技術である。乱数には擬似乱数と物理乱数があり、物理乱数は再現性や周期性がない特性を有している。数 Gb/s の高速物理乱数生成手法として戻り光を有する半導体レーザの光強度ダイナミクスを用いた物理乱数生成が報告されている[1]。

半導体レーザに戻り光を注入することにより光強度は周期性のない不規則なカオス振動を生じる。ここでカオス振動を生じるダイナミクスは光強度のみではなく、周波数や位相にも存在する。これまでにヘテロダイン検波を用いた MHz オーダーの低速な周波数ダイナミクスの抽出が報告されている[2]。また、コヒーレント光通信において光コヒーレント検波を用いた位相の抽出が行われている[3]。光コヒーレント検波は複素電界を復元し位相ダイナミクスを抽出する手法である。しかしながら、複素電界を用いた乱数生成の報告はされていない。

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、半導体レーザカオスにおける複素電界の実部と虚部のダイナミクス抽出を数値計算にて行い、高速物理乱数生成を行うことを目的とする。

方法: 光コヒーレント検波による複素電界の抽出の方法を Fig. 1 に示す。半導体レーザに戻り光を注入させてカオスを生成し参照レーザと 90° 光ハイブリッドで干渉させる。その後バランスフォトレシーバで差分の光強度を検出している。検出した光強度は複素電界における実部$I_I(t)$と虚部$I_Q(t)$に対応しており以下の式で表される。

$$I_I(t) = I_1(t) - I_2(t) = A_s(t)A_l cos\{(\omega_s - \omega_l)t\} \quad (1)$$

$$I_Q(t) = I_3(t) - I_4(t) = A_s(t)A_l sin\{(\omega_s - \omega_l)t\} \quad (2)$$

ここで参照レーザに対してI_1は 0° 、I_2は 180° 、I_3は 90° 、I_4は 270° の位相回転させて半導体レーザカオスと干渉させた光強度信号を表している。

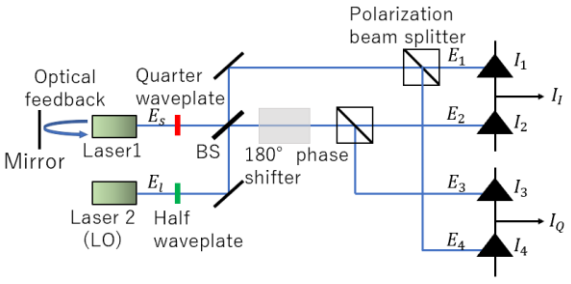

Fig. 1. Model for optical coherent detection using 90-degree optical hybrid.

結果: 本研究により、式(1)(2)を用いて抽出された戻り光を有する半導体レーザの複素電界の実部・虚部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。実部、虚部のダイナミクスはそれぞれ GHz オーダでの高速な不規則振動が観測できる。次に、複素電界ダイナミクスを 50GS/s で 8 ビット量子化することにより物理乱数を生成する。8 ビットから個別ビットに分割して生成した乱数を国際的乱数統計検定方式の NIST SP 800-22[4]を用いて評価を行った。NIST 検定は検定項目が 15 個あり、その全てに合格した乱数は真にランダムな乱数と区別がつかないとされている。8 ビット量子化されたレーザの複素電界の実部・虚部ダイナミクスの個別ビットごとの NIST 検定合格項目数を Fig. 2(b)の黒線と赤線にそれぞれ示す。また比較のために、光強度から生成した乱数の統計検定結果を青線に示す。Fig. 2(b)より、光強度はどの個別ビットでも全ての項目に合格することができなかった。一方で複素電界の実部・虚部は下位 3 ビットまでを用いて生成した乱数は全ての項目に合格したことが分かった。以上のことから複素電界の実部と虚部を用いて生成した乱数は光強度から生成した乱数よりもランダム性が高いことが分かった。

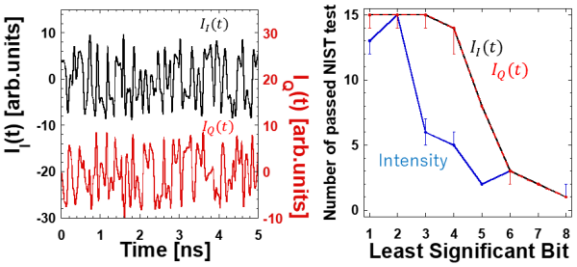

Fig. 2. (a) (black) real part and (red)imaginary part of electric field dynamics of Laser 1. (b) Number of passed NIST tests for random bits generated from (black) real part and (red) imaginary part and (blue) intensity as a function of extracted number of least significant bits (LSBs).

まとめ: 本研究では、光コヒーレント検波を用いて GHz オーダの半導体レーザにおける複素電界ダイナミクスの抽出を行い、物理乱数生成を行った。複素電界ダイナミクスを用いた乱数生成は光強度ダイナミクスを用いた場合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).