半導体レーザの雑音特性を用いた物理乱数の生成
～面発光型レーザの偏光雑音特性を利用した乱数生成～
Physical-random number generation using laser diodes' noise
—Polarization noise characteristics of a VCSEL—

○牛木 哲郎*1　土井 康平*1　西村 宏樹*1　佐藤 孝*2　大平泰生*2　大河 正志*2
Tetsuro Ushiki　Kohei Doi　Hiroki Nishimura　Takashi Sato　Yasuo Ohdaira　Masashi Ohkawa
*1 新潟大学自然科学研究科　*2 新潟大学工学部
*1Graduate School of Science and Technology, Niigata University　*2Faculty of Engineering, Niigata Univasity

1. はじめに[1][2]

乱数には、擬似乱数と物理乱数がある。擬似乱数は確定的アルゴリズムから生成されるため周期性を持つ。それに対して、物理乱数はランダムな自然現象を用いて生成されるため周期性を持たず、信頼性の高い暗号生成が可能である。しかし、一般に物理乱数は高速生成が困難であるとされている。

半導体レーザには固有の雑音として量子雑音と縦モードに起因する雑音があり、その他にもレーザ光が外部で反射され半導体レーザに戻ったときに生じる戻り光に起因する雑音がある。これらの半導体レーザ雑音特性は高速であることが知られている。そこで、半導体レーザを利用して物理乱数を高速に生成することが可能ではないかと考えた。

本研究では、これまでにファブリ・ペロー型半導体レーザ及び面発光型半導体レーザ(VCSEL)のしきい値電流付近で生じる光強度雑音を用いて、物理乱数の生成を行ってきた。そこで今回は VCSEL が持つ偏光雑音特性を利用して同様の実験を行い、結果の比較を行った。

2. 実験方法

図 1 に実験系を示す。LD(Laser Diode)にしきい値付近の電流を流し、レーザを発振させる。そのレーザ光を偏光板に通し APD に入射し、出力された電気信号をデジタルオシロスコープに入力し、波高値が入力レンジの範囲内になるよう調節する。データ取得のサンプリング周波数 fs は、デジタルオシロスコープに内蔵されている A/D converter で設定可能な 10MHz、25MHz の 2 パターンとし、コンピュータでそれぞれの fs についてデータを取得し、20,000 データずつに分ける。

今回用いた A/D converter の分解能は 8 ビットなので、20,000 桁の乱数が 8 個生成された。

こうして得られた乱数を暗号用乱数の統計的乱数性評価法として用いられている NIST の FIPS140-2[3]の評価法を用いて検証する。評価法によって得られた結果から検定透過率を求め、それぞれの fs について評価を行う。

3. 実験結果

図 2 に実験結果を示す。グラフの横軸は、実験によって得られたデータを下位ビットから順に r0,r1,r2…として表し、縦軸は各ビットについて 100 回測定を行った際の検定透過率を表している。図 2 から、サンプリング周波数が高くなると、上位ビットでの検定透過率が低くなっていることが分かる。しかし、fs=25MHz といった高いサンプリング周波数でも、乱数が生成されていることが確認できる。この結果は VCSEL に偏光板を加えずに行った同様の実験よりも高い検定透過率を示している。

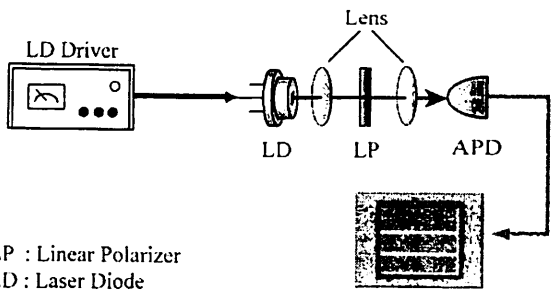

図 1　実験系

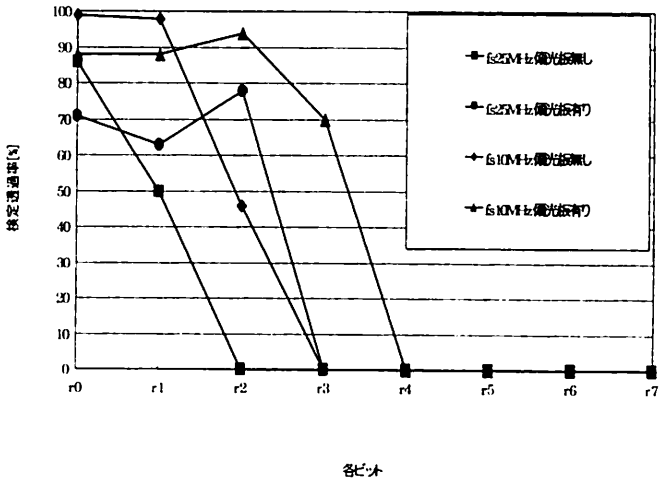

図 2　各ビットにおける検定透過率

4. 今後の課題

今回の実験から、VCSEL の偏光雑音特性を利用することで、より高速に物理乱数が生成できることが分かった。これは偏光方向がばらばらであるという特徴を VCSEL が持つためであると考えられる。今後は目標である生成速度を達成するために、周波数選択素子を用いて周波数雑音を利用することで、物理乱数のさらなる超高速生成を目指す。

5. 参考文献

[1] 宅間宏、応用物理学会編、半導体レーザーの基礎、オーム社、1987.
[2] 沼居貴陽、半導体レーザー工学の基礎、丸善、1996.
[3] National Institute of Standards and Technology, "Security requirements for cryptographic modules," FIPS 140-2, 2002