半導体レーザの雑音特性を用いた物理乱数の生成
～ファブリ・ペロー型レーザと面発光型レーザの比較～
Physical-random number generation using laser diodes' noise
—Comparison between a Fabry-Perot type laser and a VCSEL—

○西村 宏樹[*1] 土井 康平[*1] 千葉 純[*1] 佐藤 孝[*2] 大平泰生[*2] 大河 正志[*2]
Hiroki Nishimura Kohei Doi Jun Chiba 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
[*1]Graduate School of Science and Technology, Niigata University [*2]Faculty of Engineering, Niigata Univasity

1. はじめに[1][2]

暗号の生成に利用される乱数には、疑似乱数と物理乱数がある。疑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のに対し、物理乱数はランダムな自然現象から生成されるため周期性を持たない。それにより物理乱数を用いた暗号は解読が不可能となる。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。

半導体レーザは固有の雑音として量子雑音と発振モードに起因する雑音を持ち、またレーザ光が外部で反射され半導体レーザに戻ることでも雑音が生じる。これらの雑音の影響によりレーザ光の強度及び周波数は激しく変動する。この雑音特性を利用して物理乱数を高速に生成をすることができ、より無秩序な乱数による暗号化技術の安全性の向上が期待できる。

本研究では、これまでにファブリ・ペロー型レーザ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た。そこで今回は面発光型レーザ(VCSEL)を用い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、温度コントローラーで LD の温度を±1/100K の温度変動で制御する。レーザ光を APD に入射し、出力される電気信号を AC アンプで増幅する。増幅された電気信号をオシロスコープに入力し、波高値が A/D コンバータの定格入力レンジ(-1～+1V)の範囲内になるよう調整する。サンプリング周波数 f_sは、1MHz、2MHz、10MHz、20MHz の 4 パターンとし、コンピュータでそれぞれの f_s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 12 ビットなので、20,000 桁の二進数の乱数が 12 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]の評価尺度を用いて検証する。評価法によって得られた結果から(1)式を用いて検定透過率を求め、それぞれの f_sについて評価を行う。

$$\text{検定透過率} = \frac{\text{検定を透過した回数}}{\text{実験を行った回数}} \times 100[\%] \quad (1)$$

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、f_s=20MHz 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。

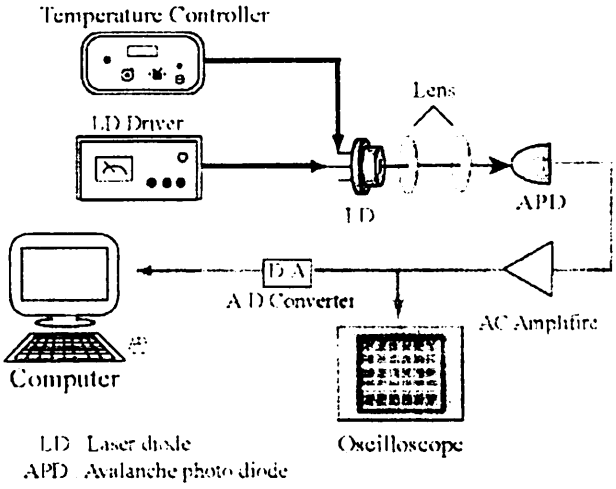

図 1 実験系

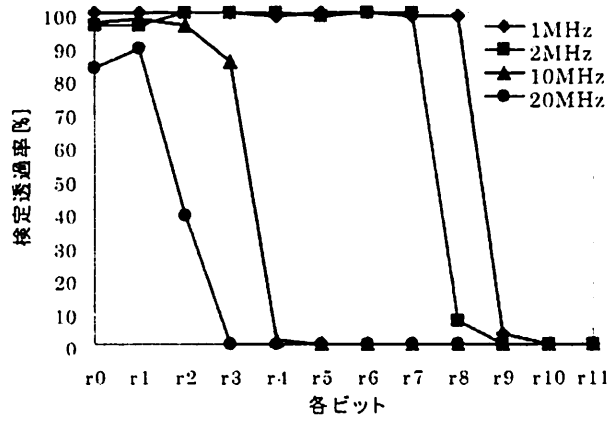

図 2 各ビットにおける検定透過率

4. 今後の課題

今回の実験より、VCSEL の雑音特性を利用して f_s=20MHz のサンプリング周波数で物理乱数の生成が可能であることが分かった。今後は周波数選択素子を用いるなどして周波数雑音を上手く取り出し、物理乱数のさらなる高速生成を目指す。

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