

周波数安定化半導体レーザーによる物理乱数生成システムの構築

Construction of the physical random number generation system using the frequency stabilized semiconductor laser

新潟大¹ ○^①新井秀明¹, 前原進也¹, 土井康平¹, 佐藤孝¹, 大平泰生¹, 坂本秀一¹, 大河正志¹Niigata Univ.¹, ○H. Arai¹, S. Maehara¹, K. Doi¹, T. Sato¹, Y. Ohdaira¹, S. Sakamoto¹, M. Ohkawa¹

E-mail: f10l005g@mail.cc.niigata-u.ac.jp, tsato@eng.niigata-u.ac.jp

はじめに

半導体レーザーには、定常発振しているレーザー光の中に、自然放出によるランダムな光が混入することで生じるAM雑音やFM雑音といった量子雑音がある。また、外部反射器から半導体レーザーの活性領域に光が再入射すると、レーザー周波数や光出力が不安定になりやすい性質を持っている。それゆえ、これらの雑音特性を十分に把握し改善することは、精密光計測や超高速光通信の性能向上にとって非常に重要である。

一方で、このような雑音は積極的に応用される場合もある。量子雑音を用いた高分解能分光法では^[1]、半導体レーザー、光周波数弁別器（原子の吸収線）、光検出器、スペクトラムアナライザを用いたシンプルなシステムで分光実験が行われており、レーザー光が原子の吸収線付近をゆっくりと掃引されるとき、透過光強度に大きな揺らぎが見られることが指摘されている。

我々はこの光周波数の揺らぎを光強度の変化に変換する原理を利用し、物理乱数の新しい生成方法を提案してきた^[2]。しかし、半導体レーザーは雰囲気温度や注入電流の変化によって発振周波数が大きく変化するため、より品質の安定した乱数生成器の実現には半導体レーザーの発振周波数安定化が必要である。

乱数の生成

我々は、半導体レーザーの周波数揺らぎを光強度の変化に変換するための周波数弁別器に Rb-D₂ 吸収線を用い、その利得が最大のところで乱数生成を行うため、試料半導体レーザーの発振周波数を Rb-D₂ 吸収線に安定化された Stabilized Laser の発振周波数に対して PLL 技術を利用して調整できるようにした^[3]。

今回の実験では Fig.1 の RNG section で検出された光周波数雑音は、8bit AD コンバーター (A/D) でサンプリングされた 8 桁の 2 進数出力（下位から順に r0、r1、・・・）各々に対して乱数を生成することで物理乱数の並列生成を行っている。A/D のサンプリング速度は 500MS/s で行い、生成された物理乱数は NIST の SP800-22 によって評価した。

評価結果を Fig.2 に示す。実験結果は r2bit を除き r0bit から r5bit まで SP800-22 のすべての項目にパスした。r2bit の評価が悪い理由は、まだ不明であるが、AD コンバーター自身のノイズレベルが大きく、その影響を特に強く受けたのが r2bit ではないかと予想している。

本実験で周波数安定化半導体レーザーから 500MS/s × 5bit (2.5Gbps) の生成速度で物理乱数生成に成功した。

参考文献

- [1] T. Yabuzaki, T. Mitsui, and U. Tanaka, "New Type of High-Resolution Spectroscopy with a Diode Laser", Phys. Rev. Lett., **67**, 2453-2456 (1991).

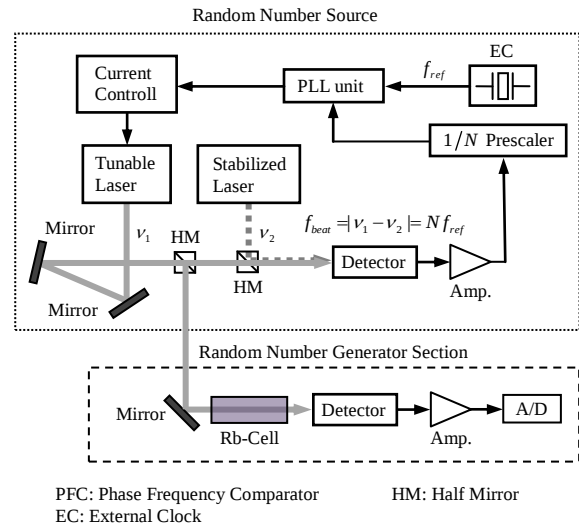


Fig1. Experiment setup of Random Number Generator (RNG)

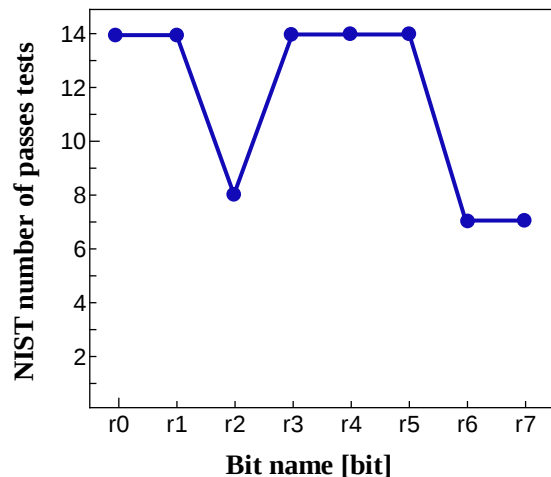


Fig2. Evaluation result of Random Number by NIST SP800-22

- [2] S. Maehara, K. Kawakami, H. Arai, K. Nakano, K. Doi, T. Sato, Y. Ohdaira, S. Sakamoto, M. Ohkawa, "Frequency noise characteristics of a diode laser and its application to physical random number generation", Opt. Eng. **52** (1), 014302; doi: 10.1117/1.OE.52.1.014302 (7pp) (2013).
- [3] K. Kuboki, M. Ohtsu, "Frequency Offset Locking of AlGaAs Semiconductor Lasers", IEEE J. Quantum Electron., **QE-23**, pp. 388-393 (1987).