プロジェクト名：**半導体レーザを用いた超高速物理乱数生成方式に関する研究**

プロジェクト代表者：内田　淳史（理工学研究科 数理電子情報部門・准教授）

1　研究の目的

近年の高度情報化社会における情報セキュリティ技術において、乱数は非常に重要な役割を演じている。乱数は生成方法により擬似乱数と物理乱数に分類される。擬似乱数は一つの初期値と決定論的アルゴリズムにより生成されるために、再現性および周期性が存在する。一方で物理乱数はサイコロ等のように物理現象から生成されるために再現性は無く、周期性も無い。しかし、既存の物理乱数の生成速度は擬似乱数と比べて遅く、最大で数百 Mbps (Megabit per second)程度に留まっている[1]。ここで新たな物理乱数生成方式として GHz オーダで不規則振動する半導体レーザカオスを用いる方式が近年提案されており、1.7 Gbps (Gigabit per second)の生成速度での物理乱数生成が達成されている[2]。しかしながら量子暗号通信や情報理論的セキュリティの新たな情報セキュリティ方式では、超高速な物理乱数生成器が不可欠であり、更なる生成速度の向上が望まれる。

そこで本研究では、半導体レーザを用いた物理乱数生成方式の実験的実現を目的とする。特に本研究では物理乱数生成器の生成速度の向上を行う。乱数生成速度の高速化のために、レーザカオスの周波数帯域拡大を実験的に実現する。さらに、１つのサンプリング点から複数の２値乱数を生成するマルチビット生成方式を実装し、その有効性について検証を行う[3]。

2　研究方法と成果

乱数生成速度の高速化の手法として周波数帯域を拡大させたカオスを用いて、1 サンプリングで複数ビット列(マルチビット)を生成する乱数生成方式を提案する。はじめにカオスの周波数帯域の拡大を行なった。実験装置図を図１に示す。まず２つの半導体レーザを用意し、それぞれレーザ１およびレーザ２と呼ぶ。レーザ１に外部鏡を設け、戻り光を付加してカオスを発生させる。レーザ１のカオス光をレーザ２に一方向に注入することで、２つのレーザ周波数差がレーザ２の緩和発振周波数と非線形相互作用することにより、レーザ２の出力が帯域拡大されたカオスとなる。

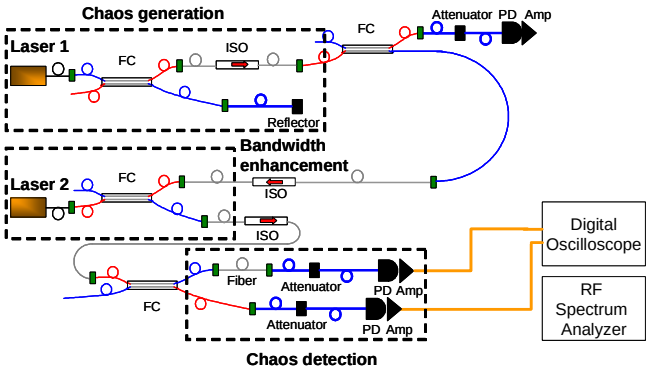

図１ 実験装置図

この時のレーザ１で発生させたカオスと、光注入により帯域が拡大されたレーザ２のカオスの RF スペクトルを図２に示す。図 2(a)と 2(b)に示すように 9.53 GHz から 15.36 GHz に周波数帯域が拡大されているのが分かる。また、図 2(a)の RF スペクトル

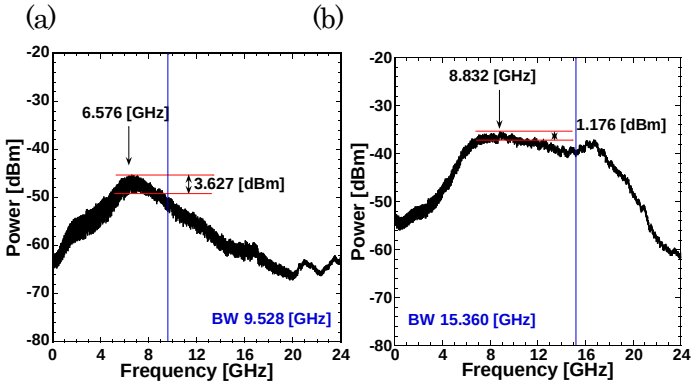

図２　(a)レーザ１および(b)レーザ２の RF スペクトル

と比較して、図 2(b)の RF スペクトルはピークの高低差が小さく平坦なスペクトルであり、物理乱数生成に適していることが分かる。

次に、マルチビット生成方式について説明する。マルチビット乱数生成では元の信号とその時間遅延信号の 2 つの波形を、1 つのサンプリング点に対して 8 ビット AD 変換し、各ビットごとに排他的論理和を行なう。さらに生成された 8 ビットから下位 n ビットを選択し、乱数列として上位ビットから下位ビットの順に出力する。ここではサンプリング速度を 12.5 GS/s に設定し、下位 6 ビットを用いて乱数の生成を行った。この時の生成速度は 75 Gbps (12.5 GS/s × 6 ビット)であった。

75 Gbps で生成した乱数列について、統計的にランダム性の評価を行った。本研究では米国国立標準技術研究所(NIST)の NIST Special Publication 800-22 [8]を使用した。NIST SP 800-22 は 15 項目の検定で構成される国際標準の統計的乱数検定であり、全検定項目に合格することで統計的にランダムであるとされる。NIST SP 800-22 の検定では 1Mbit の乱数列を 1000 個使用して行われる。生成した乱数の検定結果を表 1 にまとめる。NIST SP 800-22 では有意水準が$\alpha = 0.01$の時、P-value が 0.0001 より大きく、Proportion が 0.99 ± 0.0094392 の範囲にあるとき、その検定項目が合格とされる。Table 1 では全ての検定項目で合格条件を満たしているため、全 15 項目に合格していることが分かる。以上より、帯域拡大カオスを用いたマルチビット乱数生成方式において、75 Gbps での生成速度での高品質な乱数生成に成功した。

表 1 乱数の統計検定結果 (NIST SP 800-22)

STATISTICAL TEST	P-VALUE	PRORORTION	RESULT
frequency	0.219006	0.9880	SUCCESS
block-frequency	0.000387	0.9860	SUCCESS
cumulative-sums	0.572847	0.9870	SUCCESS
runs	0.000550	0.9860	SUCCESS
longest-run	0.917870	0.9900	SUCCESS
rank	0.440975	0.9910	SUCCESS
fft	0.933472	0.9860	SUCCESS
nonperiodic-templates	0.013856	0.9810	SUCCESS
overlapping-templates	0.777265	0.9890	SUCCESS
universal	0.518106	0.9880	SUCCESS
apen	0.087692	0.9910	SUCCESS
random-excursions	0.013411	0.9868	SUCCESS
random-excursions-variant	0.112047	0.9851	SUCCESS
serial	0.162606	0.9870	SUCCESS
linear-complexity	0.989425	0.9900	SUCCESS
Total			15

3 まとめ

本研究では、半導体レーザカオスを用いた超高速物理乱数生成方式の実験的実証を行った。特に、生成速度の高速化方法として帯域拡大カオスを用いたマルチビット乱数生成方式を提案した。その結果、最高で 75 Gbps (12.5 GS/s × 6 ビット)の生成速度の乱数生成に成功した。また生成された乱数列に対して統計的乱数検定を適用したところ、国際標準検定に合格する十分なランダム性を有する乱数の生成が達成された。

以上の成果により、半導体レーザカオスを用いた超高速物理乱数生成器の生成速度の向上が実現可能となり、情報セキュリティ分野や計算機科学分野への本技術の応用が強く期待される。

参考文献

[1] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett., vol. 93, pp. 031109-1--031109-3 (2008).

[2] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nature Photonics, vol. 2, no. 12, pp. 728-732 (2008).

[3] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, Optics Express, vol. 18, no. 6, pp. 5512-5524 (2010).