半導体レーザカオスを用いた超高速物理乱数の生成実験

Experiment on fast physical random number generation with chaotic semiconductor lasers

内田　淳史[1*]、天野　和也[2]、平野　邦仁[2]、吉森　茂[2]、吉村　和之[3]、
ディビス　ピーター[3]

Atsushi Uchida[1], Kazuya Amano[2], Kunihito Hirano[2], Shigeru Yoshimori[2], Kazuyuki Yoshimura[3], Peter Davis[3]

[1] 埼玉大学　大学院理工学研究科　数理電子情報部門
Department of Information and Computer Sciences, Saitama University
[2] 拓殖大学　工学部電子システム工学科
Department of Electronics and Computer Systems, Takushoku University
[3] 日本電信電話株式会社　NTT コミュニケーション科学基礎研究所
NTT Communication Science Laboratories, NTT Corporation

Abstract

Random number generators in digital information systems exploit physical entropy sources, such as electronic and photonic noise, to add unpredictability to deterministically generated pseudo-random sequences. However, there is a large gap between the generation rates achieved with existing physical sources and the high data rates of many computation and communication systems, which is a fundamental weakness in these systems. Here we show that good-quality random bit sequences can be generated at very fast bit rates using physical chaos in semiconductor lasers. Streams of bits which pass standard statistical tests for randomness have been generated at rates of up to 1.7 gigabit per second by sampling the fluctuating optical output of two chaotic lasers. This rate is an order of magnitude faster than that of previously reported devices for physical random bit generators with verified randomness.

Key Words: Chaos, Laser, Noise, Random number generator, Security, Information technology

1.　はじめに

近年のインターネットに代表される高度情報化社会において、通信時における情報の安全性の確保は必要不可欠である。その手段として暗号化技術や認証技術が挙げられるが、これらの暗号技術には乱数が使用されている。また、乱数はモンテカルロ法に代表される数値計算には不可欠であり、多くの計算機シミュレーションで用いられている[1]。

一般に乱数とは等確率性と無規則性の 2 つの性質を併せ持つ数列のことであり、生成方法により疑似乱数と物理乱数に分類される。疑似乱数はコンピュータのアルゴリズムにより生成され[2]、線形合同法や M 系列、メルセンヌ・ツイスタ法等が代表例である。疑似乱数は 1 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、再現性があり周期性も

* 〒338-8570　さいたま市桜区下大久保２５５
電話：048-858-3490 FAX：048-858-3716
Email：auchida@mail.saitama-u.ac.jp

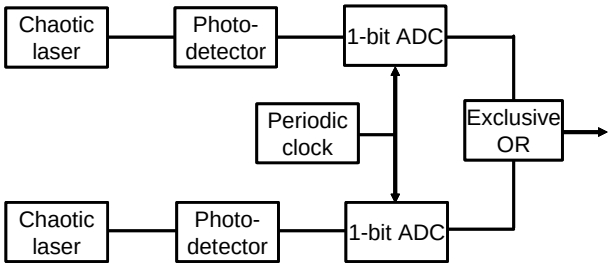

Fig. 1　Schematic diagram for physical random bit generation using two chaotic lasers.

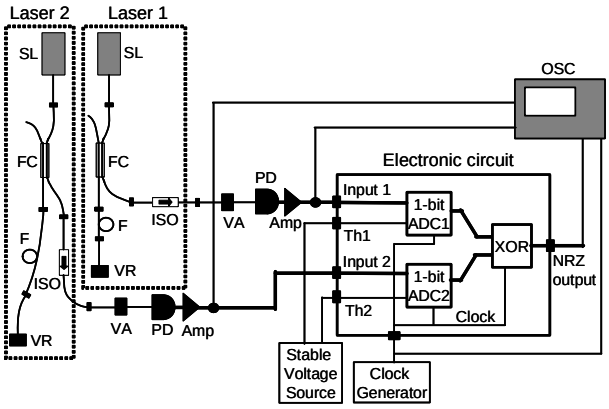

Fig. 2　Experimental setup for physical random bit generation using two chaotic lasers.

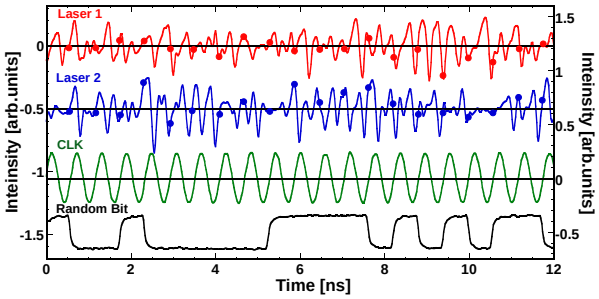

Fig. 3　Temporal waveform of chaos, clock, and random bits.

存在する。一方で物理乱数は半導体の熱雑音等の物理現象を元に生成するため、周期性が存在せず再限性が無いという特徴を有する[3,4]。しかしながら、現在の物理乱数生成器の生成速度は最大で数十～数百 Mbps (Megabit per second) に留まっている[3,4]。これは物理乱数を生成するための乱数発生源の振動速度が遅いためである。一方で、量子暗号通信等の分野において、高速でランダム性の高い物理乱数生成器が望まれている[5]。

そこで本研究では、GHz オーダでの高速不規則振動を有する半導体レーザカオスを用いて、1 Gbps (Gigabit per second) を超える生成速度での物理乱数の実時間生成実験を行うことを目的とする。半導体レーザで発生させたカオス波形に対して、高速 AD (Analog-Digital) 変換器を用いて 2 値物理乱数列の実時間生成を行う。また、生成した乱数列に国際標準の統計検定を適用してランダム性の定量的評価を行う。

2.　半導体レーザを用いた物理乱数生成方式

半導体レーザカオスを用いた物理乱数の実時間生成の概念図を Fig. 1 に示す。また、実際に用いた実験装置図を Fig. 2 に示す[6]。2 つの独立した半導体レーザにそれぞれ外部鏡を用いて戻り光を付加することで、GHz オーダでの不規則振動出力であるカオスを発生させる。発生させたカオス波形を光検出器(PD)で検出し、電気信号増幅器(Amp)を通して高速 AD 変換器へ入力する。AD 変換器では入力したカオス波形にそれぞれ最適なしきい値を設定し、カオス波形を周期サンプリングする。サンプリングデータが設定したしきい値よりも大きければ 1、小さければ 0 としてデジタルビットに変換する。2 つのデジタルビットを排他的論理和することで、最終的な 2 値乱数列として出力する。ここでクロックの周波数を 1.7 GHz に設定して、1.7 Gbps の生成速度で物理乱数生成を行った。また半導体レーザで発生させたカオスの中心周波数は、Laser 1 では 3.07 GHz、Laser 2 では 2.86 GHz であった。

物理乱数生成時に観測した Laser 1 と Laser 2 のカオス波形、クロック信号、および 2 値乱数列 (Non Return to Zero (NRZ) 形式) の時間波形を Fig. 3 に示す。クロック信号の立ち上がり時に Laser 1 と Laser 2 のカオス波形を周期サンプリングしている。さらに、しきい値処理により得られた 2 つのデジタルビットを排他的論理和して 2 値乱数列を生成した。

生成された 2 値乱数列の 0 を黒、1 を白に変換し

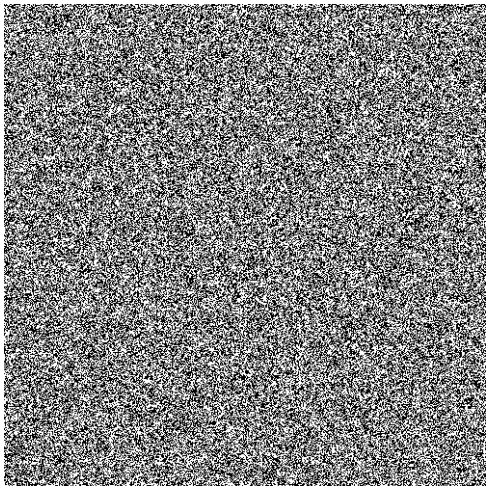

Fig. 4　Random bit patterns in a two-dimensional plane.

て 500×500 の二次元平面上に表した結果を Fig. 4 に示す。Fig. 4 のビットパターンに周期性は観測されず、0 と 1 がランダムに分布した乱数列に見えることが分かる。

3.　物理乱数の統計的評価

次に、半導体レーザカオスから生成された物理乱数列のランダム性について統計的評価を行った。本研究では米国商務省標準技術研究所(National Institute of Standard and Technology, NIST)が発行する NIST Special Publication (SP) 800-22 [7]を使用した。NIST SP 800-22 は 15 種類の検定で構成される国際標準の統計的乱数検定であり、検定項目全てに合格することで統計的にランダム性が高いと判定できる。NIST SP 800-22 の検定では 1 Mbit の乱数列を 1000 個使用して行われる。本研究にて生成された物理乱数に対する検定結果を Table 1 にまとめる。Table 1 の各検定項目における P-value と Proportion の値は、複数ある検定項目については、最も悪い値を示している。NIST SP 800-22 では有意水準 α = 0.01 の時、P-value (Uniformity of 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であると判定される。つまり、Table 1 では全ての検定項目が上述の条件を満たしており、全 15 項目合格していることが分かる。以上より、半導体レーザカオスを用いて 1.7Gbps の高速生成速度で生成された物理乱数は、国際標準の乱数検定に全項目合格することが明らかとなった。

Table 1　Result of NIST SP 800-22.

STATISTICAL TEST	P-VALUE	PROPORTION	RESULT
frequency	0.366918	0.9920	SUCCESS
block-frequency	0.639202	0.9900	SUCCESS
cumulative-sums	0.101311	0.9920	SUCCESS
runs	0.223648	0.9920	SUCCESS
longest-run	0.603841	0.9890	SUCCESS
rank	0.031012	0.9900	SUCCESS
fft	0.274341	0.9910	SUCCESS
nonperiodic-templates	0.013760	0.9810	SUCCESS
overlapping-templates	0.893482	0.9910	SUCCESS
universal	0.903338	0.9920	SUCCESS
apen	0.880145	0.9920	SUCCESS
random-excursions	0.142248	0.9836	SUCCESS
random-excursions-variant	0.067964	0.9869	SUCCESS
serial	0.440975	0.9860	SUCCESS
linear-complexity	0.291091	0.9970	SUCCESS
Total			15

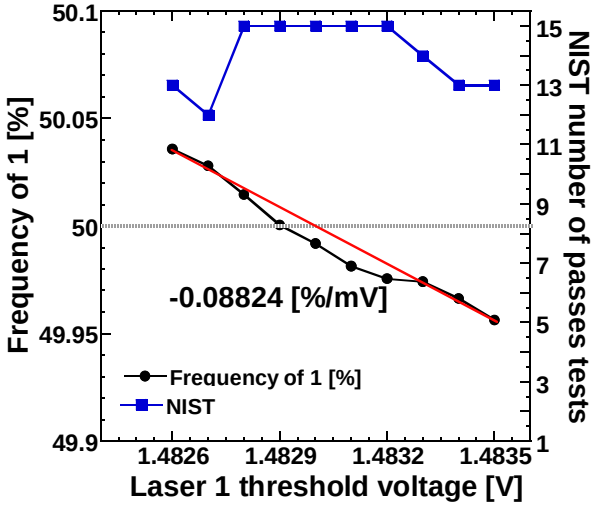

Fig. 5　Frequency of one and the number of passed NIST tests as a function of the Laser 1 threshold voltage.

4.　しきい値と 1 の出現頻度の関係

本物理乱数生成方式では、AD 変換におけるしきい値電圧の設定が物理乱数のランダム性を決定する重要なパラメータである。しきい値電圧を最適にすることで、ランダム性の高い物理乱数の生成が可能となる。そこで、AD 変換器のしきい値電圧と 2 値乱数の 1 の出現頻度の関係について調査を行った。Laser 2 のしきい値電圧を固定し、Laser 1 のしきい

値電圧を変化させて調査を行った。さらに、これらのしきい値設定にて生成された乱数列を NIST SP 800-22 で検定し、しきい値電圧に対するランダム性（NIST 検定における合格項目数）の調査も行った。その結果を Fig. 5 に示す。しきい値電圧を変化させると乱数の 1 頻度がほぼ線形に変化することが分かる。また、NIST SP 800-22 の検定合格項目数に着目すると、乱数の 1 頻度が 50%に近づくほど検定合格項目数が向上し、乱数性が高くなる。したがって、乱数の 1 頻度を 50%に近づけるように AD 変換器のしきい値電圧を調整することで、ランダム性の高い乱数生成が実現可能であることが分かる。

５．おわりに

本研究では半導体レーザカオスを用いて、生成速度が 1 Gbps を超える高速物理乱数の実時間生成実験を行った。2 つの半導体レーザカオスに対して高速 AD 変換器で周期サンプリングし、得られたデジタルビットを排他的論理和することで、最高で 1.7 Gbps の高速生成速度での 2 値物理乱数生成に成功した。生成した物理乱数列に対して国際標準の乱数統計検定を適用したところ、全検定項目に合格することが分かった。また AD 変換器のしきい値電圧を変化させた場合、2 値乱数の 1 の出現頻度が 50%に近づくほど検定合格項目数が向上し、乱数のランダム性が高くなることが明らかとなった。

レーザカオスを用いた物理乱数生成は、GHz オーダでの超高速物理乱数生成方式として非常に有用であると考えられ、今後の応用が期待される。

参考文献

[1] N. Metropolis, and S. Ulam, Journal of the American Statistical Association, **44,** pp. 335-341 (1949).

[2] D. Knuth, The Art of Computer Programming: Volume 2: Seminumerical Algorithms (3rd Edition), Addison-Wesley Professional (1996).

[3] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, IEEE Transactions on Computers, **52,** pp. 403-409 (2003).

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

[5] N. Gisin, G. Robordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics, **74,** pp. 145-195 (2002).

[6] 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, **2,** pp. 728-732 (2008).

[7] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, and M. Levenson, National Institute of Standards and Technology, Special Publication 800-22, (2001).