レーザカオスを用いた超高速物理乱数生成器の高速化

Enhancement of generation speed for physical random number generator with chaotic lasers

山﨑　泰基[1]、森勝　進一朗[1]、奥村　悠[1]、会田　裕貴[1]、内田　淳史[1*]
吉村　和之[2]、原山　卓久[2]、ディビス　ピーター[2]
Taiki Yamazaki[1], Shinichiro Morikatsu[1], Haruka Okumura[1], Hiroki Aida[1], Atsushi Uchida[1],
Kazuyuki Yoshimura[2], Takahisa Harayama[2], Peter Davis[2]

[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] 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

We experimentally demonstrate random bit generation using multi-bit samples of bandwidth-enhanced chaos in semiconductor lasers. Chaotic fluctuation of laser output is generated in a semiconductor laser with optical feedback and the chaotic output is injected into a second semiconductor laser to obtain a chaotic intensity signal with bandwidth enhanced up to 16 GHz. The chaotic signal is converted to an 8-bit digital signal by sampling with a digital oscilloscope at 12.5 Giga samples per second (GS/s). Random bits are generated by bitwise exclusive-OR operation on corresponding bits in samples of the chaotic signal and its time-delayed signal. Statistical tests verify the randomness of bit sequences obtained using 1 to 6 bits per sample, corresponding to fast random bit generation rates from 12.5 to 75 Gigabit per second (Gb/s) (= 6 bit × 12.5 GS/s).

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

1. はじめに

乱数はインターネット上での暗号・認証技術や数値計算におけるモンテカルロ法など様々な分野で用いられている。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[1,2]。一方で近年、量子暗号通信等の分野において超高速物理乱数生成器が望まれている。

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いる[3]。2 つの半導体レーザカオスを用いた物理乱数を生成方式で、1.7 Gbps (Gigabit per second)の生成速度

* 〒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

での物理乱数の実時間生成が可能であることが実験的に示されている[3,4]。また Reidler らにより、サンプリング点間で差信号を取りマルチビットを使用した乱数生成方式も提案されている[5]。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高速化を目的とする。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[6]。

2．帯域拡大カオスを用いたマルチビット乱数生成

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[7]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 Fig. 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。

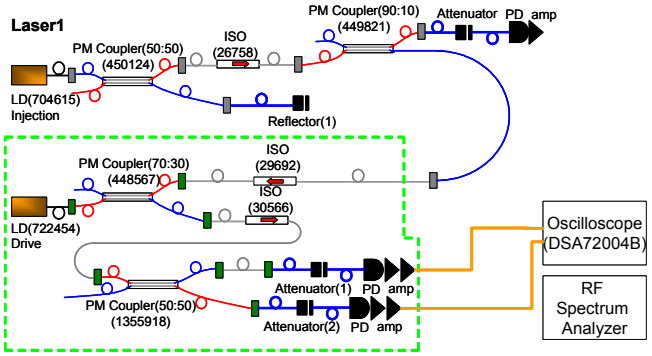
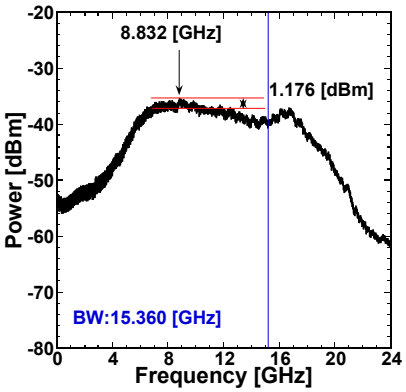


Fig. 1　Experimental setup for random bit generation with chaotic lasers. Amp, electronic amplifier; ISO, optical isolator; LD, laser diode; PD, photodetector.

(a)



(b)

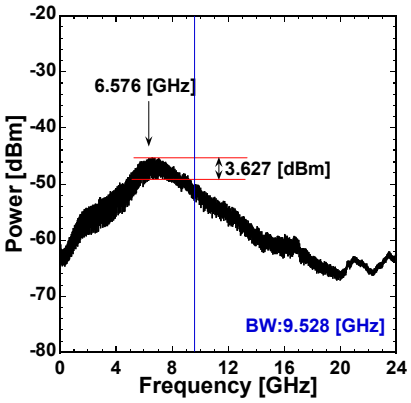


Fig. 2　(a) RF spectra of Laser 1 and (b) Laser 2. BW: bandwidth.

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。

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 Fig. 2 に示す。Fig. 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、Fig. 2(a)の RF スペクトルと比較して、Fig. 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 Table 1 にまとめる。NIST SP 800-22 では有意水準がα = 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。

Table 1 Result of NIST Special Publication 800-22. All the 15 tests are passed.

STATISTICAL TEST	P-VALUE	PROPORTION	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. 下位ビット数によるランダム性の変化

次にマルチビット乱数生成において、選択する下位ビット数を変化させることで、どのように乱数のランダム性が変化するかを NIST の合格項目数を用いて調査した。その結果を Fig. 3 に示す。選択した下位ビット数を横軸に、NIST の合格項目数を縦軸にプロットした。結果を見ると、下位 1 ビットから 6 ビットまでの乱数では NIST で全 15 項目合格している。よって最高の生成速度は 75 Gbps (12.5GS/s×6 ビット)であることが分かった。また、下位 7 ビット以上では合格項目数が低下していることが明らかとなった。

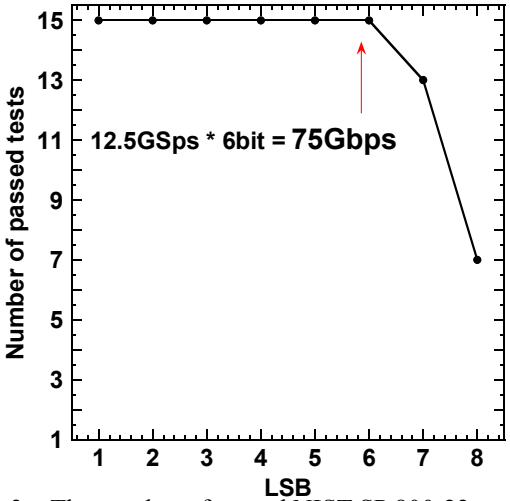


Fig. 3 The number of passed NIST SP 800-22 tests as a function of the number of least significant bits (LSBs) used to generate the bit sequence. “15” indicates that all the tests are passed.

4. 使用ビット数によるビットパターンの出現頻度の分布

続いてマルチビットにおける出現頻度の偏りについて調査した。マルチビット乱数生成の際の下位ビット数の変化に対するマルチビットの出現確率を調べた。下位 8 ビットから下位 5 ビットまでの確率密度分布を Fig. 4 に示す。マルチビットの値を 10 進数に変換した値を横軸に、出現確率を縦軸ににプロットした。Fig. 4 の 2 ビットの数字は表示範囲のマルチビット(2 進数表示)の先頭 2 ビットを示している。まず Fig. 4(a)の下位 8 ビットでの分布を見ると、大

きな偏りが見える。Fig. 4(b)の下位 7 ビットの分布を見ると、Fig. 4(a)よりも小さいが、若干偏りが見える。しかしながら Fig. 4(c), (d)の下位 6 ビット、5 ビットの分布を見ると、ほぼ一様に分布していることが分かる。つまり、下位ビット数を減らすことにより分布が平坦になり、ビットパターンの出現確率が一様になることが分かる。以上の結果から、最大で下位 6 ビットの選択により一様分布を有する乱数の生成が可能となることが分かった。

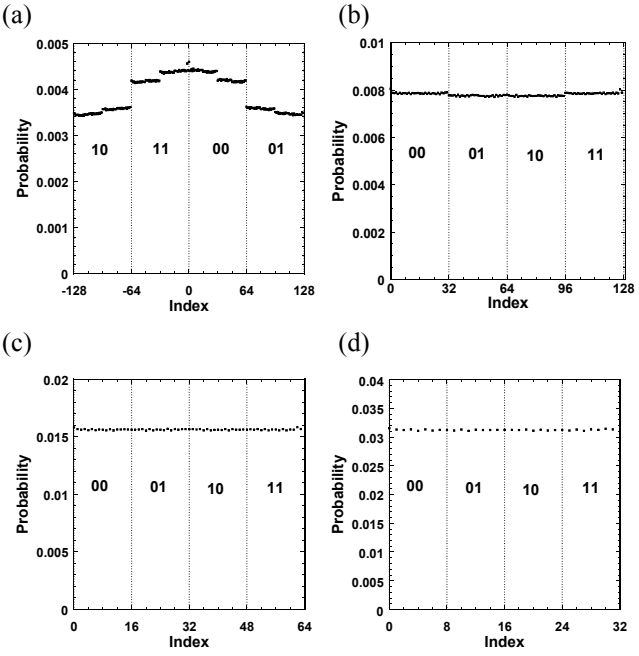


Fig. 4 Probability density functions for (a) 8-bit random bits after bitwise Exclusive-OR (XOR) operation is applied to the two 8-bit digitized chaotic waveforms, (b) 7 least significant bits (LSBs) selected from the 8-bit XOR data, (c) 6 LSBs selected from the 8-bit data, and (d) 5 LSBs selected from the 8-bit data.

５．おわりに

本研究では、半導体レーザカオスを用いることで物理乱数生成方式の高速化を行った。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。また選択ビット数を変化させたときの乱数列のランダム性について調査したところ、最大で下位 6 ビットを選択することで、一様分布を有するランダム性の高い乱数の生成に成功した。

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

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

[3] 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).

[4] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, IEEE Journal of Quantum Electronics, vol.45, no.11, pp.1367-1379 (2009).

[5] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, Physical Review Letters, vol. 103, pp. 024102-1--024102-4 (2009).

[6] 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).

[7] H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, Optics Express, vol. 17, no. 22, pp. 19536-19543 (2009).

[8] 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).