様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 １３ 日現在

機関番号：１２４０１
研究種目：若手研究(A)
研究期間：2012～2015
課題番号：２４６８６０１０

研究課題名（和文）レーザのカオス現象を用いた物理乱数生成器の高速化と小型化

研究課題名（英文）Development of ultrafast and miniature random number generators using chaotic lasers

研究代表者
内田　淳史（UCHIDA, Atsushi）

埼玉大学・理工学研究科・教授

研究者番号：５０３２７９９６

交付決定額（研究期間全体）：（直接経費）　　20,100,000円

研究成果の概要（和文）：本研究では、レーザの高速性とカオスの不規則性を利用した超高速物理乱数生成器の開発を行い、高速化および小型化を達成した。乱数生成速度を向上させるために、半導体レーザを一方向に結合することで帯域拡大カオスの生成実験を行った。その結果カオスの周波数帯域を拡大することに成功した。さらに帯域拡大カオスを用いて高速物理乱数生成を行い、乱数のランダム性を評価したところ統計検定に合格した。この時の乱数生成速度は、最大で１秒間に1兆２０００億個（毎秒１．２テラビット）であり、高速物理乱数生成に成功した。加えて、レーザカオス発生用光集積回路を用いた物理乱数生成実験の実証を行った。

研究成果の概要（英文）：We demonstrate ultra-fast random number generation based on chaotic dynamics in semiconductor lasers. We generate bandwidth-enhanced chaos with unidirectionally-coupled semiconductor lasers and use it for ultra-fast random number generation. The generated random numbers pass statistical tests of randomness. We succeed in generating random numbers at the maximum generation rate of 1.2 Tb/s. We also demonstrate random number generation using photonic integrated circuits for miniaturization.

研究分野：レーザ工学

キーワード：乱数　応用光学・量子光工学　先端機能デバイス　セキュア・ネットワーク　情報通信工学

１．研究開始当初の背景

高度情報化社会における情報セキュリティには、乱数と呼ばれるランダムな数列が必要不可欠である。コンピュータにより決定論的に生成される擬似乱数が現在多く用いられているが、盗聴者が擬似乱数の初期値を推定することで乱数の予測が可能になるという安全性の脅威が存在する。また、天気予報や地震予測などの自然災害予測のための大規模数値シミュレーション分野や、流体力学に基づく設計工学分野においても、ランダム性の高い大量の乱数が必要とされている。しかしながら並列計算機で複数の擬似乱数を用いた場合、予測結果の重大な誤りが存在することが指摘されており、擬似乱数の大きな問題点となっている。

上述の問題を改善するために、物理乱数と呼ばれる自然現象を利用した乱数生成方式が近年注目を浴びており、電子回路の熱雑音等を用いて実装されている。物理乱数は雑音を用いているが故にランダム性が高いという優れた特性を有しているものの、従来の方式では生成速度が遅いのが欠点であり、その生成速度は 1 秒間に 1 億個（毎秒 0.1 ギガビット）程度に留まっている。このように情報セキュリティ分野、自然災害予測分野、および設計分野において、ランダム性が高くかつ高速な物理乱数生成器の必要性が近年非常に高まっている。

２．研究の目的

本研究では、レーザの高速性とカオスの不規則性を利用した超高速物理乱数生成器の開発を行い、高速化および小型化を達成することを目的とする。特に世界最速となる１秒間に１兆個（毎秒１テラビット）の生成速度を有する超高速物理乱数生成器の開発を行う。さらには小型化のために、光集積回路を用いた超高速物理乱数生成の実証実験を行う。

３．研究の方法

【高速化】

(1-a) 周波数帯域拡大カオスの生成実験

乱数生成速度を向上させるためには、カオスの有する周波数成分を広帯域化することが重要である。そこで、カオス生成用半導体レーザと帯域拡大用半導体レーザを準備する。帯域拡大用レーザの光出力をカオス発生用レーザへと注入することで、カオスの周波数帯域拡大を実験的に達成する。

(1-b) 帯域拡大カオスを用いた高速物理乱数生成実験

帯域拡大カオスを用いた物理乱数生成の実証実験を行う。帯域拡大カオスを光検出器にて検出・増幅し、電気信号へと変換する。さらに電子回路によりアナログ－デジタル変換を行い 0 または 1 へと変換し、論理演算を行って 2 値乱数列を生成する。特に、生成速度を向上させるために、取得された時間波形から乱数を生成する際の後処理方式の開発を行う。一つのサンプリング点から複数のビットを抽出するマルチビット生成方式を適用し、後処理としてビット反転処理を実現する。さらに複数のレーザカオス光源を用いて並列化し、時間遅延信号と組み合わせることで高速な乱数生成を実現する。

【小型化】

(2-a) 光集積回路の設計・製作とカオスダイナミクスの調査

半導体レーザから受光素子までを一体化した乱数生成用光集積回路の設計を行う。特に、カオス発生用の外部共振器と戻り光用の光増幅器を備えた半導体レーザ光集積回路を製作する。また異なる外部共振器長を有する光集積回路の製作も行う。これらの光集積回路におけるレーザ出力強度の時間ダイナミクスの調査を行う。

(2-b) 光集積回路を用いた物理乱数生成実験

光集積回路を用いた物理乱数生成の実証実験を行う。小型化によりレーザカオスの性質も変化しているため、自己相関関数を計測することで、物理乱数生成速度の最適化を行う。また、異なる外部共振器長を有する光集積回路を用いて生成された乱数のランダム性の評価を行う。

４．研究成果

【高速化】

(1-a) 周波数帯域拡大カオスの生成実験

帯域拡大カオス生成の実験装置図を図１に示す。本研究では 3 つの半導体レーザ(レーザ 1，2，3 と呼ぶ)を一方向に結合した実験装置を用いて周波数帯域拡大カオスを生成する。レーザ 1 は戻り光を加えることでカオスを発生させる。レーザ 2 はレーザ 1 のカオス光を注入することで帯域拡大を行う。さらにレーザ 3 はレーザ 2 の帯域拡大カオス光を注入することで、より広帯域な帯域拡大を行う。

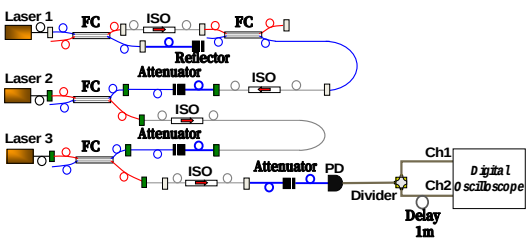

図１ 帯域拡大カオスの実験装置図

ここで周波数帯域は最大の周波数成分からパワーを加算して全体の周波数成分の 80 % になる周波数範囲と定義する。また、RF (Radio Frequency)スペクトルの平坦さの指標として、周波数帯域内における周波数パワーの最大と最小パワーの差を平坦度として

用いる。平坦度は値が小さいほど平坦な RF スペクトルであることを示す。

周波数帯域拡大は、レーザカオスを他のレーザに注入することにより生じた光周波数の差（数十 GHz）とレーザカオスの周波数（数 GHz）の非線形相互作用によりスペクトル幅が広がり、周波数帯域が向上する現象である。実験で得られたレーザ出力強度の時間波形と RF スペクトルを図 2 に示す。ここでレーザ 1-2 間の光周波数差をΔf_{12} = 16.5 GHz とし、レーザ 2-3 間の光周波数差を Δf_{23} = 28.0 GHz と設定した。図 2(左)の時間波形から、レーザ 1，2，3 の順に振動成分が増加し、高速に振動していることが分かる。また図 2(右)の RF スペクトルから、レーザ 1，2，3 の順にスペクトル幅が広がり、帯域拡大カオスが得られていることが分かる。この時、レーザ 1 は緩和発振周波数により周波数帯域が 9.6 GHz と低くなっているが、レーザ 2 では帯域拡大により周波数帯域が 13.8 GHz となり、さらにレーザ 3 では 26.0 GHz の周波数帯域が得られた。またこの時の平坦度は 5.6 dB となり、平坦な RF スペクトルが得られた。

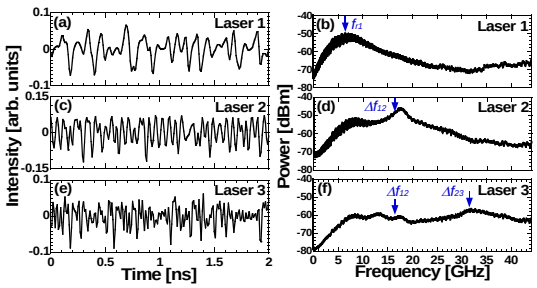

図 2　レーザ 1，2，3 の出力強度の（左)時間波形と(右)RF スペクトル

(1-b) 帯域拡大カオスを用いた高速物理乱数生成実験

続いて帯域拡大カオスを用いて、シングルビット乱数生成方式とマルチビット乱数生成方式により物理乱数生成を行う。

(i) シングルビット乱数生成

はじめに、乱数生成に適したカオス状態を判別するために、簡潔な後処理方式としてシングルビット乱数生成方式を用いる。帯域拡大カオスとその時間遅延波形をオシロスコープで同時刻にサンプリングし、シングルビット AD 変換により得られたビットに対して排他的論理和演算（XOR）を行うことで、2 値の乱数列を生成する。本方式ではサンプリング速度が乱数生成速度に等しくなる。生成された乱数は国際標準の乱数検定である米国国立標準技術研究所(NIST)の統計的乱数検定 NIST Special Publication 800-22 を用いて検定を行った。NIST 検定は 15 個の検定項目からなり、1 ギガビットの 2 値乱数列を用いる。全項目に合格することで、真性乱数と統計的に区別不可能となることを意味する。

乱数生成速度を変化させたときの NIST 検定の合格項目数を図 3 に示す。下の横軸は乱数生成のサンプリング時間を示し、上の横軸はサンプリング時間の逆数である乱数生成速度を示している。縦軸は生成された乱数に対する NIST 検定の合格項目数を示しており、15 が全項目に合格することを意味している。乱数生成速度を変化させて生成された乱数は、最大生成速度 20.0 Gb/s において NIST 検定の全項目に合格し、十分なランダム性を有していることが分かった。

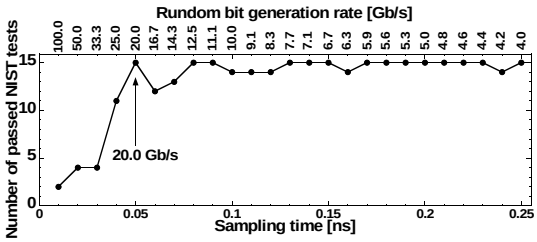

図 3 乱数生成速度（サンプリング時間）の変化に対する NIST 検定合格項目数。縦軸の 15 が全項目合格を意味する。

(ii) マルチビット乱数生成

次に複雑な後処理を用いて高速な乱数生成を実現するために、マルチビット乱数生成方式を適用する。その方式を図 4 に示す。帯域拡大カオスとその時間遅延波形をオシロスコープにより同時刻に 100 GS/s でサンプリングし、8 ビットデジタル信号として記録する。この時、物理的な時間遅延が加えられていない 8 ビット信号を A とし、遅延が加えられている 8 ビット信号を B とする。A，B の各々に対してソフトウェアによる処理を用いて新たな時間遅延信号 A'および B'を生成する（1.59 ns の時間遅延)。生成した時間遅延信号は最上位ビットから最下位ビットまでを逆順に並び替える処理を行い、これらを A'^{R} および B'^{R} とする。次に A と A'^{R}、また B と B'^{R} においてビットごとの排他的論理和演算（XOR）を行う。XOR 演算により得られた 8 ビット列 X と Y の上位ビットを切り捨てた後に、残りの下位ビットを順に出力することで 2 値乱数を生成する。

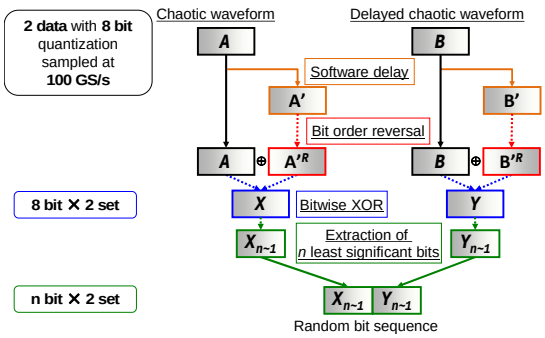

図 4 マルチビット乱数生成方式

ここで、乱数生成に用いる下位ビット数を変化させた場合の NIST 検定の合格項目数を

調査した。8 ビットのうち下位 7 ビットまでを用いた乱数では NIST 検定の全項目に合格することが分かった。この時の乱数生成速度は、1.4 Tb/s (= 2 data × 7 bit × 100 GS/s)となり、高速乱数生成実験に成功した。さらに、より多くの 44 ギガビットの乱数列に対して、TestU01 の Crush 検定を適用した。その結果、8 ビットのうち下位 6 ビットまでを用いた乱数では Crush 検定に合格し、最大で 1.2 Tb/s (= 2 data × 6 bit × 100 GS/s)での乱数生成に成功した。(毎秒 1.2 テラビット。1 秒間に 1 兆 2000 億個の乱数。)

以上まとめると、本研究では、一方向結合された 3 つの半導体レーザを用いて周波数帯域拡大を実験的に達成した。周波数帯域が 26.0 GHz、平坦度が 5.6 dB の帯域拡大レーザカオス波形を得ることができた。また、得られた帯域拡大レーザカオスを用いて乱数生成を行った。シングルビット乱数生成方式を用いた場合に 20.0 Gb/s の乱数生成速度を達成した。また、マルチビット乱数生成方式を用いた場合には、最大で 1.2 Tb/s での乱数生成速度を実験的に達成した。(1 秒間に 1 兆 2000 億個の乱数。)

【小型化】

(2-a)光集積回路の設計・製作とカオスダイナミクスの調査

本研究にて製作したレーザカオス発生用光集積回路の構成を図 5(a)に示す。光集積回路は、光検出器(PD)、DFB レーザ(DFB)、2 個の光増幅器(SOA1,2)、導波路(PW)、外部鏡(M)から構成される。DFB レーザから発振した光が導波路を通り外部鏡で反射され、戻り光として再び DFB レーザに注入されることによりカオスが発生する。この時、光増幅器への注入電流を変化させると戻り光量が変化する。レーザ端面から外部鏡までの距離は 1～10 mm であり、これが外部共振器長に対応する。DFB レーザへの注入電流と戻り光量を変化させると時間ダイナミクスが変化する。

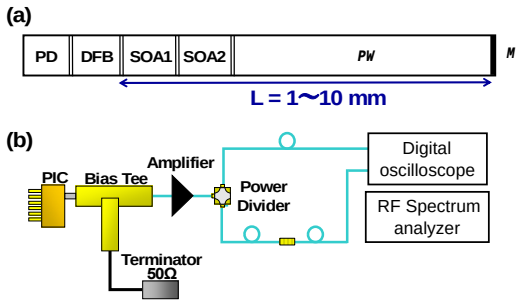

図 5 (a)光集積回路の構成図。(b)実験装置図。

また実験装置の全体図を図 5(b)に示す。光集積回路から出力された電気信号はバイアスティ(Bias Tee)により直流信号(DC)と交流信号(AC)に分離される。AC 成分を電気増幅器(Amp)により増幅し、その後パワーディバイダ(Power Divider)により分岐する。分岐した一方にのみ 1 m のケーブルを 1 本追加することで時間遅延を発生させ、オシロスコープで 2 つの波形を取得する。取得した 2 つの時間波形に対して乱数生成処理を施し、乱数を生成する。

はじめに、5 mm の外部共振器長を有する光集積回路を用いる。レーザ出力のカオス時間波形および RF スペクトルを図 6 に示す。図 6(a)に示す時間波形は不規則に振動している。また、図 6(b)に示す RF スペクトルは広帯域でなだらかなスペクトルであり、周波数帯域は 7.7 GHz である。

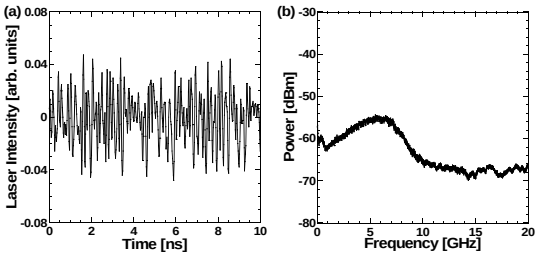

図 6 光集積回路の出力強度の(a)時間波形と(b)RF スペクトル

(2-b)光集積回路を用いた物理乱数生成実験

外部共振器長が 5 mm の光集積回路から出力されたカオス時間波形を用いて、シングルビット乱数生成を行った。乱数生成速度を変化させた時の NIST 検定の合格項目数を図 7(a)に示す。横軸はシングルビット乱数生成のサンプリング時間を示し、逆数にすると乱数生成速度に相当する。縦軸は、生成した乱数に対する NIST 検定の合格項目数を示している (15 が全項目合格)。その結果、外部共振器長が 5 mm の光集積回路では 4.6 Gb/s (サンプリング時間 0.22 ns に対応)が最大乱数生成速度となることが分かった。

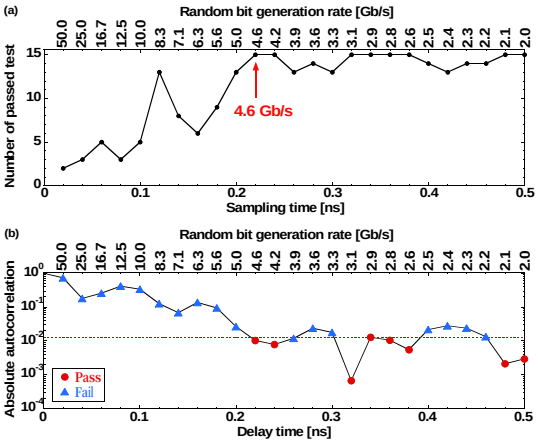

図 7 (a) 乱数生成速度を変化させた時の NIST 検定の合格項目数。縦軸の 15 が全項目合格を意味する。(b) 自己相関の対数プロットと NIST 検定結果。赤丸が全項目合格を示し、青三角が 1 項目以上不合格を示す。

次に、乱数生成速度を変化させて乱数を生成した時の、カオス波形の自己相関と乱数のランダム性の関係性を調査した。自己相関関

数と NIST 検定の検定結果の関係性を図 7(b)に示す。自己相関は絶対値で対数プロットし、遅延時間を変化させている。また、自己相関の遅延時間を乱数生成のサンプリング時間に対応させて、乱数生成結果を自己相関上にプロットした。NIST 検定の全 15 項目に合格している生成速度は赤い丸で示し、1 項目でも不合格の場合は青い三角で示す。その結果、自己相関が低い遅延時間に対応するサンプリング時間では、ランダム性の高い乱数が生成できる傾向があることが分かる。図 7(b)の点線は 10^{-2} を示しており、自己相関が 10^{-2} を境として NIST 検定の合否が分かれることが分かった。つまり、自己相関が 10^{-2} よりも低いサンプリング時間で生成された乱数はランダム性が高いことが明らかとなった。

次に異なる外部共振器長(1,2,3,4,5,および 10 ㎜)を有する光集積回路を用いて乱数生成を行った。外部共振器長が 5 ㎜ の光集積回路と同様に、乱数生成速度を変化させて乱数を生成し、NIST 検定を用いて評価を行った。異なる外部共振器長を用いて乱数生成を行った結果を図 8 に示す。NIST 検定の全 15 項目に合格する生成速度を赤い丸で示し、1 項目でも不合格の場合は青い三角で示す。乱数生成速度は、1 Gb/s 以上に設定し、自己相関の極小値と極大値を中心に選択して生成しているため、離散的に変化させている。図 8 に示すように外部共振器長 2 ㎜ 以下の光集積回路では、生成した全ての速度においてランダム性の高い乱数を生成することができなかった。これは RF スペクトルが平坦でないため、周期性が乱数に出現するためであると考えられる。一方で、外部共振器長が 3 ㎜ 以上の光集積回路ではいずれもランダム性の高い乱数生成に成功した。特に、外部共振器長が 4 ㎜ の場合、最大生成速度が 5.6 Gb/s での乱数生成に成功した。

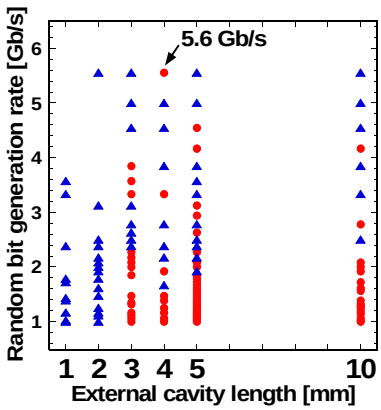

図 8　外部共振器長と乱数生成速度の関係性。赤丸が全項目合格を示し、青三角が 1 項目以上不合格を示す。

以上まとめると、本研究ではカオス発生用光集積回路を用いて乱数生成を行った。外部共振器長が 5 ㎜ の光集積回路を用いてシングルビット乱数生成を行い、乱数生成速度を変化させた。その結果、低い自己相関に相当する生成速度で乱数を行った場合に、ランダム性が高くなる傾向があることが分かった。次に、異なる外部共振器長(1,2,3,4,5, および 10 ㎜)を有する光集積回路を用いて乱数生成を行った。その結果、外部共振器長が 3 ㎜ 以上の光集積回路において乱数生成に成功した。特に外部共振器長が 4 ㎜ の場合に、最大生成速度 5.6 Gb/s を達成した。

５．主な発表論文等

〔雑誌論文〕（計２５件）

(1) K. Kanno, A. Uchida, and M. Bunsen, "Complexity and bandwidth enhancement in unidirectionally coupled semiconductor lasers with time-delayed optical feedback," ***Physical Review E,*** Vol. 93, pp. 032206-1－032206-11 (2016).

(2) R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," ***Optics Express,*** Vol. 23, No. 2, pp. 1470-1490 (2015).

(3) M. Arahata and A. Uchida, "Inphase and antiphase dynamics of spatially-resolved light intensities emitted by a chaotic broad-area semiconductor laser," ***IEEE Selected Topics in Quantum Electronics,*** Vol. 21, No. 6, pp. 1800609-1－1800609-9 (2015).

(4) J. Muramatsu, K. Yoshimura, P. Davis, A. Uchida, and T. Harayama, "Secret-key distribution based on bounded observability," ***Proceedings of the IEEE,*** Vol. 103, No. 10, pp. 1762-1780 (2015). **(invited paper)**

(5) A. Karsaklian Dal Bosco, K. Kanno, A. Uchida, M. Sciamanna, T. Harayama, and K. Yoshimura, "Cycles of self-pulsations in a photonic integrated circuit," ***Physical Review E,*** Vol. 92, pp. 062905-1－062905-9 (2015).

(6) K. Kanno and A. Uchida, "Finite-time Lyapunov exponents in time-delayed nonlinear dynamical systems," ***Physical Review E,*** Vol. 89, pp. 032918-1－032918-8 (2014).

(7) R. Takahashi, Y. Akizawa, A. Uchida, T. Harayama, K. Tsuzuki, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation," ***Optics Express,*** Vol. 22, No. 10, pp. 11727-11740 (2014).

(8) 内田 淳史, 吉村 和之, 村松 純, デイビス ピーター, 原山 卓久, 砂田 哲, "半導体レーザーのランダム現象を用いた超高速物理乱数生成と相関乱数秘密鍵配送," ***光学,***

Vol.43, No. 5, pp. 194-201 (2014). **(解説論文)**
(9) T. Yamazaki and A. Uchida, "Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers," ***IEEE Journal of Selected Topics in Quantum Electronics,*** Vol. 19, No. 4, pp. 0600309-1－0600309-9 (2013). **(invited paper)**
(10) H. Koizumi, S. Morikatsu, H. Aida, T. Nozawa, I. Kakesu, A. Uchida, K. Yoshimura, J. Muramatsu, and P. Davis, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," ***Optics Express,*** Vol. 21, No. 15, pp. 17869-17893 (2013).
(11) T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Estimation of entropy rate in a fast physical random-bit generator using a chaotic semiconductor laser with intrinsic noise," ***Physical Review E,*** Vol. 85, pp. 016211-1－016211-7 (2012).
(12) K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," ***Physical Review Letters,*** Vol. 108, pp. 070602-1－070602-5 (2012).
(13) Y. Akizawa, T. Yamazaki, A. Uchida, T. Harayama, S. Sunada, K. Arai, K. Yoshimura, and P. Davis, "Fast random number generation with bandwidth-enhanced chaotic semiconductor lasers at 8 × 50 Gb/s," ***IEEE Photonics Technology Letters,*** Vol. 24, No. 12, pp. 1042-1044 (2012).

その他12件

〔学会発表〕(計87件)
(1) A. Uchida, "Recent advances in ultra-fast random number generation with chaotic lasers," Dynamics Days Europe 2015, Exeter, UK, September 6-10, 2015.
(2) A. Karsaklian Dal Bosco, K. Kanno, A. Uchida, M. Sciamanna, T. Harayama, and K. Yoshimura, "High-frequency self-pulsations in a semiconductor laser with optical feedback in a photonic integrated circuit," Proceedings of 2015 International Symposium on Nonlinear Theory and its Applications (NOLTA 2015), Vol. 1, pp. 149-152 (2015), Kowloon, Hong Kong, China, December 1-4, 2015.
(3) J. Nakayama, K. Kanno, and A. Uchida, "Reservoir computing using consistency of semiconductor lasers with optical feedback and injection," Proceedings of 2014 International Symposium on Nonlinear Theory and its Applications (NOLTA 2014), Vol. 1, pp. 557-560 (2014), Luzern, Switzerland, September 14-18, 2014.
(4) R. Sakuraba, K. Kanno, K. Iwakawa, and A. Uchida, "Bandwidth enhancement of chaos in three cascaded semiconductor lasers," Frontiers in Optics 2013 Technical Digest, Orlando, Florida, USA, October 6-10, 2013.
(5) 宇賀神 上総, 寺島 悠太, 内田 淳史, 原山 卓久, 吉村 和之, "半導体レーザを有する光集積回路とビットシフト回転法を用いた物理乱数生成," 2016 年 第 63 回応用物理学会春季学術講演会,東京工業大学, 東京, 2016 年 3 月 19～22 日.
(6) 寺島 悠太, 岩川 健人, 宇賀神 上総, 櫻庭 良佑, 内田 淳史, "帯域拡大カオスを用いた差分法による超高速物理乱数生成方式," 電子情報通信学会 2015 年ソサイエティ大会, 東北大学, 仙台, 2015 年 9 月 8～11 日.

その他81件
(国際会議30件、国内学会51件)

〔図書〕(計2件)
(1) 内田 淳史, "複雑系フォトニクス -レーザカオスの同期と光情報通信への応用-," 共立出版, 単著, 314 ページ (2016).
(2) A. Uchida, "Optical Communication with Chaotic Lasers, -Applications of Nonlinear Dynamics and Synchronization-," Wiley-VCH, Weinheim, Germany, 640 pages (2012).

〔産業財産権〕
○出願状況（計0件）
無し

○取得状況（計0件）
無し

〔その他〕
ホームページ
http://www.au.ics.saitama-u.ac.jp/

6．研究組織

(1)研究代表者
内田 淳史（UCHIDA, Atsushi）
埼玉大学・大学院理工学研究科・教授
研究者番号：５０３２７９９６

(2)研究分担者
無し

(3)連携研究者
無し