様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年６月８日現在

機関番号：１２４０１
研究種目：若手研究(A)
研究期間：2009～2011
課題番号：２１６８６００９
研究課題名（和文）　半導体レーザにおける量子ノイズのカオス増幅効果を用いた超高速物理乱数生成
研究課題名（英文）　Ultra-fast random number generation with chaotic amplification effect of quantum noise in semiconductor lasers
研究代表者
内田　淳史（UCHIDA ATSUSHI）
埼玉大学・大学院理工学研究科・准教授
研究者番号：５０３２７９９６

研究成果の概要（和文）：
本研究では、半導体レーザカオスを用いることで新たな超高速物理乱数生成方式の開発を行った。半導体レーザカオス信号をアナログ－デジタル変換して論理演算を行うことにより、物理乱数生成の実証実験に成功した。生成された乱数に対して国際標準の統計検定を適用したところ全検定項目に合格し、ランダム性の高い乱数が生成された。さらに物理乱数生成の高速化方式を新たに提案および実装して乱数生成を行ったところ、400 Gb/s の乱数生成速度を実現した。加えて物理乱数生成器の非再現性の理論的保証や量子暗号通信への実証実験に成功した。

研究成果の概要（英文）：
We experimentally demonstrated fast random number generation using chaotic semiconductor lasers. Chaotic fluctuation of laser output is generated and converted into binary sequences for random number generation. Statistical tests verify the randomness of bit sequences generated in the experiment. We succeeded in generating random bit sequences at rates up to 400 Gb/s. We also achieved the estimation of entropy rate and demonstrated quantum cryptography experiment with the random number generator.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	13,900,000	4,170,000	18,070,000
２０１０年度	4,600,000	1,380,000	5,980,000
２０１１年度	2,600,000	780,000	3,380,000
年度			
年度			
総　計	21,100,000	6,330,000	27,430,000

研究分野：工学
科研費の分科・細目：　分科：応用物理学・工学基礎　　細目：応用光学・量子光工学
キーワード：乱数、レーザ、カオス、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

高度情報化ネットワークにおける情報セキュリティの重要性は近年増加する一方であるが、その信頼性はランダムな信号列を生成する乱数生成器に強く依存している。例えばインターネット商取引においては、電子情報の秘匿化、本人認証、デジタル署名などに乱数が利用されており、乱数の予測不可能性、非再現性、統計的均一性が情報セキュリティ上極めて重要な特性となる。しかしながら現

在多く用いられている擬似乱数は計算機内のアルゴリズムにより決定論的に生成されるため、盗聴者がその初期値（シード）を推定することで乱数の予測が可能になるという致命的欠点を有している。これを改善するために、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、光量子効果、周期クロックの位相揺らぎ等を用いて実装されている。物理乱数は自然ノイズを用いているが故に予測不可能という非常に優れた特性を有している一方で生成速度が遅いのが欠点であり、その生成速度は毎秒あたり 1〜100 メガビット(Mb/s)程度に留まっている。高速かつ完全ランダムな乱数生成器は情報セキュリティ分野のみならず、物理、化学、生物、計算機科学分野における大規模数値計算においても必要不可欠な要素技術であり、その必要性は極めて高い。

２．研究の目的

本研究では、半導体レーザにおける量子ノイズのカオス増幅効果を用いることで新たな超高速物理乱数生成方式の開発を目的とする。本研究で提案する超高速物理乱数生成器は、カオスの有する不規則性、量子ノイズの有する予測不可能性、および半導体レーザの有する高速性の全てを最大限に利用した画期的応用である。量子ノイズをシードとして生成される数十 GHz の乱雑振動を有する半導体レーザカオスを用いることで高速かつ完全ランダムな乱数生成が実現可能となり、情報セキュリティおよび大規模数値シミュレーションにおける乱数生成器として多くの需要が見込まれる。

３．研究の方法

(1) 半導体レーザにおける超高速物理乱数生成の実験的実証と物理乱数の統計的評価

半導体レーザに内在する量子ノイズをカオスにより増幅することで、超高速物理乱数生成の実証実験を行う。半導体レーザは戻り光により数 GHz〜数十 GHz のカオス的出力振動を引き起こすことが可能である。本手法では半導体レーザに戻り光を加えてカオスを発生させ、レーザ内部の量子ノイズを増幅してレーザ出力強度のエントロピーを増大させる。これを光検出器にて検出し、電気信号へと変換する。さらに電子回路によりアナログーデジタル(AD)変換を行い、0 または 1 のランダムビット列へと変換して 2 値乱数列を生成する。加えて、高いランダム性を有する 2 値乱数列を再現性良く実現するために、カオスを生成するためのレーザパラメータの最適化を行う。さらに国際標準の乱数検定方式を用いて、生成された乱数列のランダム性の統計的評価を行う。

(2) 高周波数帯域を有する半導体レーザカオス生成と乱数生成速度の高速化

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。そこで半導体レーザの注入同期現象を利用した広帯域化実験を行う予定である。カオス生成用レーザと帯域拡大用レーザを準備し、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。レーザの波長を高精度に制御することで、最適な帯域拡大幅の調査を行う。本方式によりカオスの帯域を 10〜20 GHz まで向上させることが可能となる。さらに乱数生成速度の高速化を目的として新たな乱数生成方式の提案・実証を行う。

(3) 量子ノイズのカオス的増幅過程でのエントロピー生成率の算出と予測不可能性の理論的検証

本乱数生成器の予測不可能性を証明することは非常に重要な課題であり、これは量子ノイズのランダム性およびカオス増幅過程におけるエントロピー生成率により保障することが可能となる。本研究では、数値計算を駆使して理論的評価を行う予定である。量子ノイズを含むレーザのレート方程式を数値計算し、２つの異なる初期値の誤差が増幅される速度を定量化し、エントロピー生成率を計算する。エントロピー生成率が AD 変換による乱数生成速度よりも十分に速ければ、乱数の予測不可能性を理論的に保障することが可能となる。エントロピー生成率を向上させることで、乱数生成速度の向上が可能になると期待される。

(4) 物理乱数生成器の量子暗号通信への応用

超高速物理乱数生成器の一つの工学応用として、量子鍵配送方式への適用が有用である。位相差シフト量子鍵配送方式において、光パルスの位相差をランダムに高速変調することで量子鍵配送を行う手法が提案されている。本方式では送信側において高速なランダム変調信号が必要とされている。そこで、レーザカオスを用いた高速物理乱数生成器を量子鍵配送方式に適用し、量子鍵配送の実証実験を行う。

４．研究成果

(1) 半導体レーザカオスを用いた超高速物理乱数の実時間生成

本研究ではレーザカオスを用いた超高速物理乱数の実時間生成を行った。2 つの独立した分布帰還型(DFB)半導体レーザにそれぞれ外部鏡を設置して戻り光を付加することで、中心周波数が 3 GHz 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

波形を光検出器で検出し、電気信号増幅器を通して高速1ビットアナログーデジタル(AD)変換器へ入力する。1 ビット AD 変換器では入力され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してデジタルビット列に変換する。ここでは 1.7 Gb/s の生成速度で実時間での物理乱数生成を行った。

物理乱数生成時に観測された 2 つのレーザのカオス波形、クロック信号、および実時間生成された 2 値乱数列 (Non Return to Zero, NRZ 形式) の時間波形を図 1(a)に示す。クロック信号の立ち上がり時に 2 つのレーザのカオス波形を周期サンプリングしている（図 1(a)の黒点）。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演算して、NRZ 形式の 2 値乱数列を最終的な乱数として出力する。また生成された 2 値乱数列に対して、0 を黒、1 を白に変換して 500×500 ビットの二次元平面上に表した結果を図 1(b)に示す。図 1(b)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。

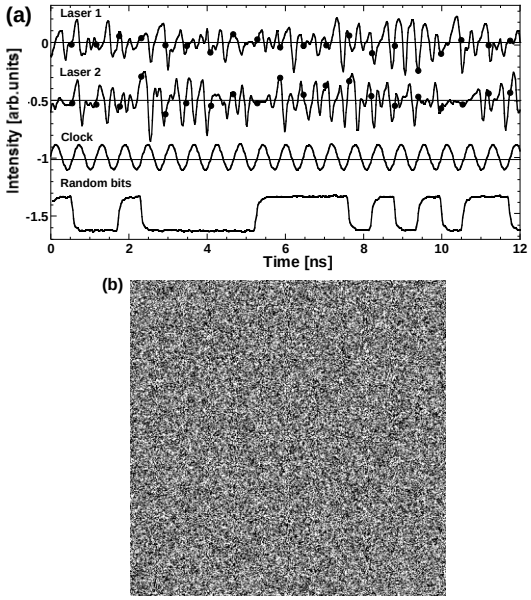

図 1　(a) レーザ出力のカオス時間波形、クロック信号、および実時間生成された 2 値乱数列の時間波形の実験結果。 (b) 生成された 2 値乱数列の二次元表示図。

レーザカオスから生成されたビット列が乱数であることを示すために、ビット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 Standards and Technology, NIST)が発行する NIST Special Publication 800-22 (NIST SP 800-22)を使用した。NIST SP 800-22 は 15 種類の検定項目で構成され、国際的に用いられている統計的乱数検定方式であり、全ての検定項目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。検定の結果、全ての検定項目が合格条件を満たしており、全 15 項目に合格していることが分かった。以上より、レーザカオスを用いて生成された物理乱数は、高いランダム性を有していることが明らかとなった。

(2)物理乱数生成器の高速化

(2-a) カオス信号の周波数帯域拡大

物理乱数生成器の高速化のために、周波数帯域を拡大させたカオス信号を用いて、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の提案・実証を行う。はじめに、カオスの周波数帯域の拡大実験を行なった。2 つの半導体レーザ（レーザ 1、レーザ 2 と呼ぶ）を用意し、レーザ 1 のみに外部鏡を設置して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 に一方向に注入し、インジェクションロッキングレンジの僅かに外側になるようにレーザ 2 の光波長を調整する。このとき 2 つのレーザ波長は一致せず、対応する光波長差（光周波数差）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 の光出力が帯域拡大されたカオスとなる。

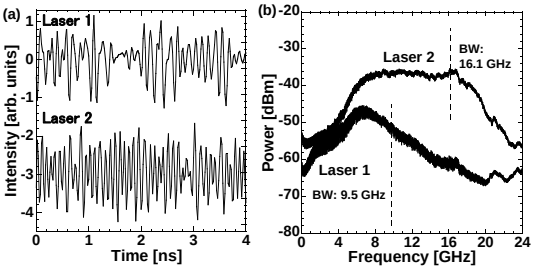

図 2　レーザ 1 のカオス信号と帯域拡大されたレーザ 2 のカオス信号の (a) 時間波形と、(b) RF スペクトルの実験結果。

この時のレーザ 1 のカオス信号と、帯域拡大されたレーザ 2 のカオス信号の、時間波形と RF スペクトルを図 2(a)、図 2(b)にそれぞれ示す。図 2(a)より、レーザ 1 のカオス振動に比べてレーザ 2 のカオス振動の方が高速であることが分かる。さらに図 2(b)に示すように、周波数帯域（スペクトル強度全体の 80%を含む最大周波数と定義）は、レーザ 1 の 9.5 GHz からレーザ 2 の 16.1 GHz へと拡大されている。また、帯域拡大前(レーザ 1)の RF スペクトルと比較して、帯域拡大後(レーザ 2)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ることが分かり、本特性は物理乱数生成に適していると言える。

(2-b) マルチビット乱数生成方式

次に高速化のための乱数生成方式の提

案・実証を行った。帯域拡大されたカオス信号とその時間遅延信号(5 ns の遅延)を用いて乱数生成を行った。提案するマルチビット乱数生成方式を図 3 に示す。マルチビット乱数生成では、帯域拡大されたカオス信号とその時間遅延信号を、1 つのサンプリング点に対してそれぞれ 8 ビット AD 変換し、各ビットごとに排他的論理和演算を行なう。さらに生成された 8 ビットから下位 m 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生成を行った。この時の生成速度は 75 Gb/s (＝ 12.5 GS/s × 6 ビット)となる。

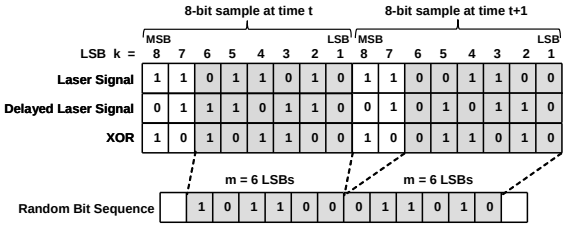

図 3　マルチビット乱数生成方式。LSB: 最下位ビット、MSB: 最上位ビット、XOR: 排他的論理和演算。

75 Gb/s で生成された乱数列について、NIST SP 800-22 の乱数統計検定を用いてランダム性の統計的評価を行った。その結果、全ての検定項目で合格条件を満たしており、全 15 項目に合格していた。つま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 Gb/s での生成速度での高品質な乱数生成に成功した。

(2-c) ビット順反転を用いたマルチビット乱数生成方式

次に物理乱数生成速度のさらなる高速化のために、新たな乱数生成方式の提案および実証を行った。提案する物理乱数生成方式の概念図を図 4(a)に、その方式を図 4(b)に示す。2 つのレーザにより帯域拡大されたカオス信号を二つに分岐し、一方に時間遅延を加える。カオス波形とその時間遅延波形を 50 GS/s でサンプリングし、8 ビット AD 変換を行う(図 4(b)の Step 1)。 ここで時間遅延波形の 8 ビット信号の各ビットを逆順に並べ替える(Step 2)。元の波形とビット順を反転した時間遅延波形の 8 ビット信号に対して、ビットごとに排他的論理和演算を行うことで乱数を生成する(Step 3)。このとき、乱数生成速度は 400 Gb/s (= 50 GS/s × 8 ビット)となる。

本方式で生成された乱数に対して統計検定を行うために、NIST SP 800-22 を使用した。その結果 NIST SP 800-22 の各検定項目において合格基準を満たしており、全 15 項目に合

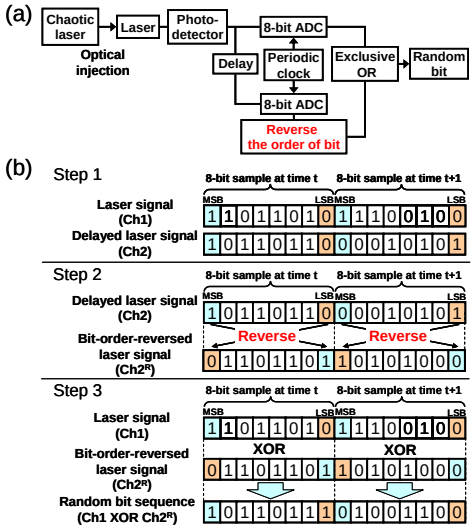

図 4　(a) ビット順反転を用いた物理乱数生成方式の概念図と、(b)その方式。

格していることが分かった。本方式ではビット順反転処理(図 4(b)の Step 2)を付加することにより、下位ビット切り出しを行う必要が無く、8 ビットを全て乱数生成に使用できる点が優れている。

以上まとめると、本研究では半導体レーザカオスを用いた物理乱数生成の高速化手法を提案・実証した。カオス波形とその時間遅延信号を 8 ビット量子化し、一方のビット列を逆順に並べ替えて排他的論理和演算を行うことにより乱数を生成した。この時、最大で 400 Gb/s での物理乱数生成速度を達成した。

(3) 物理乱数のエントロピー生成率と非再現性の評価

カオスを用いた物理乱数生成器におけるエントロピー生成率の調査は非常に重要な課題である。エントロピー生成率とは、レーザ内部のミクロな揺らぎがカオスにより非線形増幅されて、マクロなレーザ出力を予測不可能にする速度のことである。生成された物理乱数の非再現性を保障するためには、エントロピー生成率が乱数生成速度よりも大きいことが必要となる。そこで半導体レーザカオスを用いた物理乱数生成の数値解析を行い、半導体レーザカオスのエントロピー生成率の算出を行った。

戻り光を有する半導体レーザを記述する Lang-Kobayashi 方程式に、半導体レーザに内在する量子ノイズ効果を付加して数値解析を行った。同一の初期値に対して、異なる微小ノイズを付加したときの 2 つのレーザ出力の時間波形を観測した。ノイズ付加開始時間付近では 2 つのレーザ出力は同一の振動をしているが、時間が経過するにつれて異なるカオス波形が得られた。つまり、カオスのダイナミクスにより微小ノイズが増幅されて、異

なるカオス時系列へと変化する様子が観測された。

ここでカオス波形の時間変化と乱数生成との関連付けを行うために、エントロピーの評価を行った。異なるノイズ系列を付加した1000 個のカオス時系列において、しきい値に対する大小判別を行い、0 または 1 のビット列を出力する。同時刻に生成されたビット列のエントロピーを求めることで、ノイズの影響によりカオス波形が変化する様子を定量的に評価した。

エントロピーの時間変化を図 5(a)に示す。エントロピーの値が次第に増加し、1 へと収束していることが分かる。つまり、微小なノイズがカオスにより増幅されてエントロピーが増大していることが分かる。またノイズ強度を変化させた場合のエントロピーの変化も観測した。ノイズ強度が強いほどエントロピーが 1 へと収束する時間が短くなることが分かる。

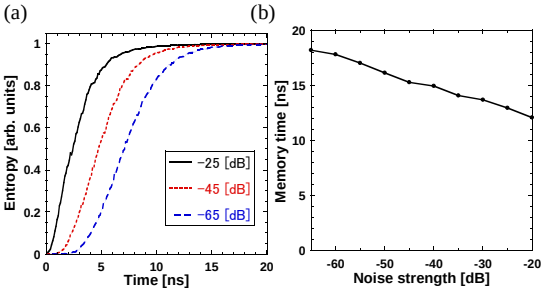

図 5　(a)エントロピーの時間変化(ノイズ強度を変化)。 (b)ノイズ強度の変化に対する初期状態記憶時間の変化。

ここでノイズ強度の変化に対する初期状態記憶時間（エントロピーが 0.995 を越えるまでの時間と定義）を図 5(b)に示す。ノイズ強度(対数表示)が増加すると、初期状態記憶時間はほぼ直線に減少していることが分かる。このように、初期状態記憶時間はノイズ強度に強く依存していることが明らかとなった。さらに図 5(b)の直線の傾きからエントロピー生成率を求めたところ、エントロピー生成率は 1.7 ns^{-1} となった。これは物理乱数生成器としての性能評価の指標となり、GHz オーダでのエントロピー生成率であることが明らかとなった。さらにエントロピー生成率は最大リアプノフ指数から算出することが可能であることが分かり、物理乱数生成器の非再現性の性能指標として非線形力学的解析手法が有用となることが明らかとなった。

(4) 物理乱数生成器の量子暗号通信への応用

本研究では、レーザカオスを用いた高速物理乱数生成器を位相差シフト量子鍵配送方式に適用し、量子暗号通信の実証実験を行った。光パルスの位相差をランダムに高速変調することで量子鍵配送を行う手法が提案されているが、鍵生成速度は光位相差の変調速度によって制限されてしまうため、高速なランダム変調信号が必要となる。本研究は NTT コミュニケーション科学基礎研究所および NTT 物性科学基礎研究所と共同で行った。

本実験において、送信側の半導体レーザ光は強度変調されて、1.0 Gb/s の光パルスが生成される。これらの光パルスの位相差を、位相変調器により 0 または π の 2 値でランダムに変調する。ランダム信号源として実時間物理乱数生成器を用いた。物理乱数生成器の乱数生成速度は 1.0 Gb/s に設定して光パルスの生成周波数と一致させた。これを 25 km の分散シフトファイバを通して光伝送を行った。

量子鍵配送実験における量子ビット誤り率はほぼ一定の値が得られており、1 時間以上にも渡り安定した量子鍵配送実験に成功した。さらに、本物理乱数生成器から生成された乱数の 1 頻度も 1 時間以上に渡って安定であった。また本実験では 9.0 kb/s のシフト鍵の生成に成功し、その時の量子ビット誤り率の平均値は 3.2 %であった。このように、レーザカオスに基づく超高速物理乱数生成器を用いた量子暗号通信に成功した。

以上の研究成果をまとめると、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器の研究開発を行った。レーザの高速性およびカオスの不規則性を積極的に組み合わせることで、超高速物理乱数生成器という従来の価値観では得られなかった新たな学術分野および工学応用が実現可能となりつつある。今後さらなる実用化へ向けた研究の進展が重要であると期待される。

５．主な発表論文等

〔雑誌論文〕（計２３件）

(1) 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. 070602-1-5 (2012). (査読有)

(2) 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. 016211-1-7 (2012). (査読有)

(3) 内田 淳史、”セキュリティネットワークを支える物理乱数生成技術[III] -レーザカオスを用いた超高速物理乱数生成器の最新動向-、”電子情報通信学会誌、Vol. 95, No. 1, pp. 74-80 (2012).（講座、解説論文、査読有）

(4) S. Sunada, T. Harayama, K. Arai, K. Yoshimura, K. Tsuzuki, A. Uchida, and P. Davis, "Random optical pulse generation with bistable semiconductor ring lasers," Optics Express, Vol.19, No.8, pp.7439-7450 (2011). (査読有)
(5) S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Chaos laser chips with delayed optical feedback using a passive ring waveguide," Optics Express, Vol.19, No.7, pp.5713-5724 (2011). (査読有)
(6) T. Harayama, S. Sunada, K. Yoshimura, P. Davis, K. Tsuzuki, and A. Uchida, "Fast nondeterministic random-bit generation using on-chip chaos lasers," Physical Review A, Vol.83, pp.031803(R) (2011). (査読有)
(7) K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," Optics Express, Vol.18, No.6, pp.5512-5524 (2010). (査読有)
(8) K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," IEEE Journal of Quantum Electronics, Vol.45, No.11, pp.1367-1379 (2009). (査読有)
(9) H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, "Synchronization of bandwidth-enhanced chaos in semiconductor lasers with optical feedback and injection," Optics Express, Vol.17, No.22, pp.19536-19543 (2009). (査読有)
(10) I. Oowada, H. Ariizumi, M. Li, S. Yoshimori, A. Uchida, K. Yoshimura, and P. Davis, "Synchronization by injection of common chaotic signal in semiconductor lasers with optical feedback," Optics Express, Vol.17, No.12, pp.10025-10034 (2009). (査読有)
(11) T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," Optics Express, Vol.17, No.11, pp.9053-9061 (2009). (査読有)
その他 12件

〔学会発表〕（計６５件）
(1) A. Uchida, "Ultra-fast random number generation with chaotic lasers," International Symposium on Physics and Applications of Laser Dynamics 2011 (IS-PALD2011), Tainan, Taiwan, December 7-8, 2011. **(招待講演)**
(2) Y. Akizawa, T. Yamazaki, and A. Uchida, "Post-processing method for fast random number generation with chaotic semiconductor lasers," Frontiers in Optics 2011, San Jone, California, USA, October 16-20, 2011.
(3) 秋澤 康裕、山崎 泰基、内田 淳史、原山 卓久、砂田 哲、新井 賢一、吉村 和之、デイビス ピーター、”半導体レーザカオスを用いた物理乱数生成の後処理による高速化、” 電子情報通信学会 2011 年ソサイエティ大会、北海道大学、北海道、2011 年 9 月 13～16 日
(4) 内田 淳史、”レーザカオスを用いた高速物理乱数生成、” 第 57 回応用物理学関係連合講演会、東海大学、神奈川、2010 年 3 月 17～20 日 (光学論文賞受賞記念講演)
(5) A. Uchida, K. Hirano, K. Amano, M. Inoue, S. Naito, H. Someya, I. Oowada, S. Yoshimori, K. Yoshimura, and P. Davis, "Experimental evaluation of fast random bit sequence generation using chaotic semiconductor lasers," The European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference 2009 (CLEO/Europe-IQEC 2009), Munich, Germany, June 14-19, 2009. **(招待講演)**
その他 60件
（国際会議 25件、 国内学会 35件）

〔図書〕（計１件）
(1) 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〕
ホームページ等
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・准教授
研究者番号：５０３２７９９６

(2)研究分担者
無し

(3)連携研究者
無し