



2008年11月20日

世界最高速！半導体レーザのランダム現象による 高速物理乱数生成に成功

～ 量子暗号分野等に活用可能な物理乱数を毎秒1.7ギガビットで生成 ～

日本電信電話株式会社（以下、NTT：東京都千代田区、代表取締役社長：三浦愷）は、拓殖大学（東京都文京区 理事長：藤渡辰信）との共同研究において、半導体レーザ※1から出力される光の強度（明暗）がランダムに変動する物理現象を利用し、物理乱数※2を毎秒1.7ギガビット（ギガビットは10億ビット）で生成することに成功しました。物理現象を利用して乱数を生成する技術としては、既存技術の乱数生成レート（1秒間に生成される乱数の数）を大幅に上回り世界最速となるものです。

今回の成果は、＜1＞量子暗号といった次世代の暗号分野、＜2＞金融工学や自然科学などの大規模シミュレーション分野などにおける乱数生成技術として応用されることが期待できます。

なお本成果は、英国の学術雑誌『Nature Photonics』（電子版、英国時間2008年11月23日18:00）に学術論文※3として掲載される予定です。

1. 開発の背景

ネットワークで伝送される情報を第3者が簡単に知ることができないようにするために、パスワードや暗号鍵が使われていますが、これらの生成には乱数が必要です。また、次世代技術である量子暗号においても、乱数は不可欠です。現状ではコンピュータで生成される擬似乱数※4が主に用いられていますが、擬似乱数は、シードと呼ばれる情報（初期値）とアルゴリズムが判明してしまうと、原理的には出力乱数を予測することが可能と言われています。理想的には、セキュリティ用途の乱数には、過去の乱数から将来の乱数が予測できないという性質が必要とされており、ランダムな物理現象を用いて生成された物理乱数が適しています。しかし、既存の物理乱数生成技術は、乱数の生成レートの低さが課題として挙げられており、生成レートの向上が必要とされています。

2. 技術のポイント

半導体レーザーにおいて出力光を再びレーザーに戻すと、レーザーから出力される光の強度が時間的にランダム変動する現象が生じます。このランダムに変動する出力光強度のアナログ信号を、0と1にデジタル化して2値乱数系列※5を高速に生成する技術を開発しました。

(1) 半導体レーザーの高速性と内部ノイズのカオス増幅効果を利用

半導体レーザー内部には、自然放出※6や熱雑音※7などの予測不可能な微小なノイズが存在します。半導体レーザーは、出力された光を反射鏡で戻すループを付加する(図1)と、カオス※8と呼ばれる現象のため本質的に不安定となり、微小ノイズが増幅されます。これにより、半導体レーザーから出力される光信号は、ランダムに変動します。また、半導体レーザーの光信号のランダムな変動は高速であり、約2~5ギガヘルツ(GHz:ギガヘルツは、毎秒10億回の振動)という速い周波数帯の振動成分を有しています(図2)。今回の成果である物理乱数生成技術では、高い乱数生成レートを実現するために、この高速性を積極的に利用しました。

(2) 2つの半導体レーザーの組み合わせにより乱数のランダム性を向上

高い乱数生成レートと高ランダム性を得るために、2つの半導体レーザーを用いて装置を構成しました(図3)。レーザー1個の場合には、レーザー出力光に内在する振動の周期性の影響により、生成される乱数列のランダム性が不十分となります。この点について、2個のレーザーを用い、さらに、各レーザー部分のパラメータを適切に異なった設定にすることで、ランダム性の向上に成功しました。生成される乱数列が十分なランダム性を備えていることは、NISTの検定※9を全項目合格したことから確認されています。

上記のポイントにより、十分なランダム性を実現しつつ、同時に、1秒間に17億個の0または1のビット列(1.7Gbps)という高い乱数生成レートを達成しました(図4, 図5)。

3. 今後の展開

今後は、装置の小型化や集積化および、さらなる生成レートの高速化の実現を目指します。また、量子暗号への応用を含め、さまざまなセキュリティ技術への応用の検討も進めて参ります。

〈用語解説〉

※1 半導体レーザー:

半導体結晶中の電子と正孔の再結合による発光現象を利用したレーザー。小型で消費電力が少なく安価に製造出来るため、情報機器や光フ

アイバ通信などで広く用いられている。

※2物理乱数：

物理乱数とは、サイコロ振って出る目など、結果を予測できないランダムな物理現象の観測値を用いて生成される乱数のこと。電子回路の熱雑音や、不確定な量子現象を利用した物理乱数生成装置が市販されている。乱数の生成レートは低く、複数の乱数生成素子を並列に組み合わせ、毎秒数百メガビット（メガビットは、100万ビット）程度。

※3論文タイトル：Fast physical random bit generation with chaotic semiconductor lasers （カオス半導体レーザを用いた高速物理乱数生成）
著者：

拓殖大学 内田 淳史（現：埼玉大学 准教授）

拓殖大学

天野 和也，井上 真樹，平野 邦仁，内藤 直，染谷 弘行，
大和田 功，倉重 隆行，志岐 優，吉森 茂

N T Tコミュニケーション科学基礎研究所

吉村 和之，Peter Davis

※4擬似乱数：

シードと呼ばれる情報を入力して決められた手続き（アルゴリズム）に従って生成され、一見乱数のように見える数列。擬似乱数は計算によって作られるので、シードとアルゴリズムが分かれば、原理的には出力系列を予測可能である。

※5乱数系列

何回もサイコロを振って出る目の数列など、規則性の無い数列。特に、0と1がランダムに現れる数列のことを、2値乱数系列と呼ぶ。

※6自然放出：

電子が高いエネルギー準位から低いエネルギー準位に遷移して、光子を放出する機構の一つ。レーザ中の電磁場には無関係に、確率的に起こる現象。

※7熱雑音：

半導体レーザ結晶を構成する原子や、結晶中の電子の熱振動によって生じる雑音。

※8カオス：

システムが乱雑な時間的変化を示し、ほんのわずかな初期状態の違い

が、予想が難しい大きく違った結果を生む現象。

※9 N I S T 検定：

正式名称は、NIST Special Publication 800-22と呼ばれている。米国国立標準技術研究所（National Institute of Standards and Technology）が推奨している世界標準のランダム性検定テストであり、例えば、0と1が同じ頻度で現れるかなど、数列に統計的な偏りが無いことを判定する。

- ・ [図1：レーザモジュールの説明図](#)
- ・ [図2：出力信号のスペクトル](#)
- ・ [図3：装置の全体構成](#)
- ・ [図4：レーザの出力信号と乱数系列](#)
- ・ [図5：生成された乱数のランダムパターン](#)

＜本件問い合わせ先＞
N T T 先端技術総合研究所
企画部 広報担当
飯塚
TEL：046-240-5157
<http://www.ntt.co.jp/sclab/contact>

NTT ニュースリリース 