

NTT持株会社ニュースリリース

(ニュースリリース)

2011年2月7日

日本電信電話株式会社
国立大学法人埼玉大学

レーザ光のランダム現象を利用、毎秒2ギガビットの物理乱数生成 ～ セキュリティ分野等への応用が期待されるランダム信号発生モジュールを開発 ～

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)と埼玉大学(埼玉県さいたま市、学長:上井喜彦)は、半導体レーザ※1光の強度(明暗)がランダムに変動する物理現象を利用し、毎秒2ギガビット(ギガビットは10億ビット)の高速物理乱数※2の生成が可能な、ランダム信号発生モジュールを開発しました。

原理的には絶対に予測不可能な物理乱数を、発生させる装置をモジュール化したことにより、機器への搭載が可能になり、より安全性が高く使いやすい暗号化装置などへの応用が期待されます。

本成果は、米国の学術雑誌『Physical Review A』に採録され学術論文として掲載されます。

開発の背景

現在、インターネットをはじめとした通信ネットワーク上で伝送される様々な情報を保護するため、乱数を用いたパスワードや暗号鍵が多く使われていますが、これらの多くはPCを用いて作成する擬似乱数※3が用いられているため、コンピュータの処理能力が向上し、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が予測されてしまう危険があるとされています。そのため、より高い安全性を確保するには、原理的に絶対に予測できない物理乱数を用いた暗号が求められています。物理乱数を使った暗号の実用化に向けては、物理乱数の生成の高速化とともに、物理乱数を生成する装置の小型化が大きな課題となっていました。

今回の成果

1. 1cm×2cmサイズのランダム信号発生モジュールを開発

従来、レーザや光ファイバなどの光学部品を組み合わせて構成されていた、大型のランダム信号発生システムの光学部品部分を、NTTが光通信デバイスの研究開発で培った半導体光集積回路技術を活用して、わずか300μm×10mmのチップにすることに成功しました。

その結果、ランダム信号発生システムを従来システムの1万分の1以下となる、1cm×2cmサイズのモジュールにすることができました(図1、図2、図3)。

これにより、機器への搭載が可能になり、実用化に向けて大きく前進しました。

2. 乱数生成速度を2.08Gbpsに向上

従来のランダム信号発生装置の光学部品部分は、数メートルの光ファイバを用いる大型のものであったため、システム内の光の伝送に時間がかかりましたが、今回チップ化し、大幅な小型化が実現できたことにより、光の伝送にかかる時間も大幅に削減でき、乱数生成速度を従来の1.7Gbps から、2.08Gbps(1秒間に20億個の0または1のビット列を生成)に向上させました(図4)。

3. レーザカオスによる物理乱数生成方法の理論を確立

半導体レーザ内部には、自然放出※4や熱雑音※5といった予測不可能な微小なノイズが存在しています。半導体レーザから出力された光を反射鏡で戻すループを付加すると、これらのノイズがカオス現象により増幅され(図5)、半導体レーザから出力される光信号がランダムに変動することは確認されていましたが、これによる物理乱数生成法の予測不可能性は保

証されていませんでした。今回、自然放出とカオス現象の持つ混合性※6という性質の組み合わせにより、予測不可能なランダムビット列が高速に生成できることを明らかにしました。

今後の展開

光集積回路および、電気信号処理部分の更なる小型化をはじめ、より高速な生成レート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る予定です。

論文名

Fast non-deterministic random bit generation using on-chip chaos lasers
(カオスレーザチップを用いた高速物理乱数生成)

用語解説

※1 半導体レーザ:

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。小型で消費電力が少なく安価に製造出来るため、情報機器や光ファ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、サイコロを振って出る目など、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て、毎秒数百メガビット(メガビットは、100万ビット)程度。

※3 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。

※4 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。

※5 熱雑音

電子の不規則な熱振動により生じる雑音。

※6 混合性

初めに持っていた情報が時間の経過と共に完全に失われるという性質。

別紙・参考資料

- ▶ [図1 レーザカオス発生光集積回路\(300μm×10mm\)](#)
- ▶ [図2 ランダム信号発生モジュール\(1cm×2cm\)](#)
- ▶ [図3 レーザモジュールの説明図](#)
- ▶ [図4 レーザの出力信号と乱数系列](#)
- ▶ [図5 出力信号のスペクトル](#)

本件に関するお問い合わせ先

■ 日本電信電話株式会社
先端技術総合研究所
企画部 広報担当 TEL:046-240-5157

ニュースリリースに記載している情報は、発表日時点のものです。現時点では、発表日時点での情報と異なる場合がありますので、あらかじめご了承くださいとともに、ご注意をお願いいたします。

[NTT持株会社ニュースリリース インデックスへ](#)

NTT持株会社 ニュースリリース

[▶ 最新ニュースリリース](#)

[▶ バックナンバー](#)

[▶ English is Here](#)

NTT持株会社 ニュースリリース内検索

1997 ▼ 年 04 ▼

月 ~

2021 ▼ 年 11 ▼ 月

検索

NTTグループの情報は
こちらからもご覧いただけます。



[▲ このページの先頭へ](#)

[▶ 更新履歴](#) [▶ サイトマップ](#) [▶ お問い合わせ](#) [▶ 著作権](#) [▶ プライバシーポリシー](#) [▶ 情報セキュリティポリシー](#) [▶ ウェブアクセシビリティポリシー](#) [▶ 個人情報保護について](#)

Copyright © 2021 日本電信電話株式会社