博士論文の要旨及び審査結果の要旨

氏　　名	新井　秀明
学　　位	博士（工学）
学位記番号	新大院博（工）第 489 号
学位授与の日付	平成 31 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
博士論文名	半導体レーザの周波数雑音の無秩序性を用いた高速物理乱数生成に関する研究
論文審査委員	主査　教授・佐藤　孝
	副査　教授・鈴木　孝昌
	副査　教授・大河　正志
	副査　准教授・大平　泰生
	副査　准教授・岡　寿樹

博士論文の要旨

ネットワークを介した通信において，情報を暗号化することは，通信の安全性を確保するために必要不可欠なことである．現在，主に利用されている通信用暗号方式は，公開鍵暗号方式や公開鍵暗号と共通鍵暗号を組み合わせたハイブリット方式である．これらの方式の安全性の根拠は，公開鍵から秘密鍵を解読するために莫大な計算時間を要することであるが，ここ数年飛躍的な進歩を遂げるネットワークを使用したクラウドコンピューティングや量子コンピュータの研究の進展によって，この暗号化技術による情報セキュリティの安全性確保は困難になりつつある．

この問題を解決する一つの方法として，量子鍵配送を利用した，量子暗号通信技術がある．量子通信は通信路上での盗聴を検出できるため，秘密鍵をこの方法で送受信者双方に共有させることで完全な秘密通信を実現することができる．この技術の安全性をより確かにするために重要になってくるのは，秘密鍵すなわち暗号用乱数の無秩序性である．そのため非常に無秩序な乱数，すなわち物理乱数を高速に生成できる技術の開発が急務になっている．

本論文では物理乱数を高速に生成するために，半導体レーザの非常に高速な周波数雑音に着目し，その雑音を物理乱数生成のための源とした．本論文では，半導体レーザの高速な周波数雑音を，周波数弁別器を用いて透過光強度の変動として検出した．これは FM 通信における復調技術のスロープ検波の原理と同じものである．また半導体レーザは，波長 780nm 帯で発光するファブリ・ペロータイプのレーザを使用し，周波数弁別器にルビジウム原子の D_2 吸収線を用いた．透過光強度信号は，A/D コンバータによって 2 進数データに変換し，2 進数データから 2 進数列を抽出することで 2 進数の物理乱数列を生成した．生成された物理乱数列は，デファクト・スタンダードである暗号用乱数検定の NIST SP800-22 によって統計的に評価して，十分な品質であることを確認した．

本論文では，物理乱数列を 2 通りの方法で 2 進数データから抽出した．一つ目の方法は，垂直分解能 8 ビットの A/D コンバータから得られた 2 進数データの Least significant bits を利用して桁ごとに並列に乱数列を生成した．2 つ目の方法は，2 進数データの各桁のデータを 1 つに結合して 2 進数の乱数列を生成した．これらの方法を利用することで，物理乱数列の生成速度を A/D コンバータのサンプリング速度より速くすることが可能になる．また，物理乱数は等確率性が悪いため暗号用の乱数として使用するためには，別の乱数との間で排他的論理和（XOR）を行うなどの操作が必要である．最近の他の先行研究では，物理乱数の生成速度を更に向上させるために，この XOR 操作を発展させた Reverse XOR 方式と呼ばれる方法が提案されている．本研究で我々も，通常の XOR を用いた方法（XOR 方式）の他にこの Reverse XOR 方式を使用して物理乱数を生成した．そして本論文では，XOR 方式において 8 ビットの 2 進数データの各桁から並列的に物理乱数列を生成する方法によって物理乱数列を最大 120 Gb/s の速度で生成することに成功した．また本論文では，さらに物理乱数列の生成速度を向上させるために，通常の XOR 方式と Reverse XOR 方式を改良した Improved XOR 方式と Improved Reverse XOR 方式を提案した．その結果，本論文では最終的に物理乱数列を最大 160 Gb/s の速度で生成することに成功した．

今回提案した物理乱数生成方法では，周波数弁別器と半導体レーザの発振周波数の中心周波数の関係が，生成される物理乱数の品質に大きな影響をもたらす．これは半導体レーザの発振スペクトルの中心周波数を周波数弁別器のどの周波数に設定するかによって，検出される雑音信号の周波数特性が変化してしまうためである．そこで本論文では，この半導体レーザの発振スペクトルの中心周波数と周波数弁別器の関係を調査し，その結果から物理乱数を生成するための最適な条件を調べた．さらに，その条件において実際に半導体レーザの周波数雑音から良質な物理乱数が生成できることを確認した．

審査結果の要旨

本論文は，半導体レーザの発振周波数特性を用いた新たな高速物理乱数生成法を開発したものであり，以下のような特筆すべき成果を上げている．

(1) 通常は欠点として考えられている半導体レーザが持つ高速周波数雑音を，取り除くべき問題点としてではなく，逆に特徴としてとらえ，高速に物理乱数を生成する際の半導体レーザと周波数弁別器の関係について詳細に議論すると共に，生成される高速物理乱数の評価方法について，統計的手法を用いて精密に検討している．

(2) 提案した高速物理乱数生成法の生成速度改善に向けて，上述の評価結果を基に，半導体レーザの安定化システム並びに周波数雑音を強度雑音信号に変換する方法に更なる検討を加え，最大の乱数生成速度，160 Gb/s を実現した．

よって，本論文は博士(工学)の博士論文として十分であると認定した．