学位論文審査の要旨

博士の専攻分野の名称　博士 (工学)　氏名　張　維楊

審査担当者　主　査　准教授　岡本　淳
副　査　教　授　浅井 哲也
副　査　教　授　池辺 将之

学位論文題名

Study on improved implementation of a transmitter in BB84 quantum key distribution system
（BB84 量子鍵配送システムの送信機実装の改善に関する研究）

近年ゲノムデータや製薬情報など長期間にわたって秘匿性を保つ必要のある情報が電子的に伝送、保管、処理されるようになった。そこで、将来いかに技術が進歩しても安全性が保たれる暗号方式の開発が必要となる。情報理論的安全な暗号プロトコルはこの条件を満たすが、利用者間での安全な鍵共有が課題となる。量子暗号鍵配送 (QKD) は離れた 2 者間で情報理論的に安全な暗号鍵の共有を可能にする。QKD とワンタイムパッド暗号を組み合わせた暗号通信は量子暗号ともよばれ、高秘匿通信を実現する。

1984 年に最初の QKD プロトコル (BB84 プロトコル) が提案されて以来、QKD は理論的にも実験的にも大きな進歩を遂げているが、QKD システムの社会的実装はまだ不十分である。その理由の一つは現実の装置に対する安全性保証がなされていないことである。QKD プロトコルの安全性は理論的に証明されている。しかし、不完全性を持つ現実の装置において証明に必要な仮定が満たされていることは明らかではなく、実際の装置について安全性を定量的に示すこと、即ち実装安全性の保証が必要である。また、別の理由として装置の製作コストが高いこともあげられる。コストを上昇させている要因の一つは、QKD プロトコルでは大量の真性乱数を必要とすることである。このため、高速な物理乱数発生器が必要になり、装置が複雑化する。

そこで、本研究はこれらの問題に対してハードウェアの面から解決策を示すことを目的とした。本研究は現在実用試作機に広く用いられている、位相コーディングによって BB84 プロトコルを実装する高速 QKD 装置を取り上げ、特に送信機の改良を行った。QKD の安全性証明の重要な仮定の一つに送信状態がプロトコルで規定されているものに合致していることがある。本研究では高速変調時でも正しい状態が作られる方法を提案し、動作を実験的に検証した。また、乱数発生器を送信機に統合することで製作コストを下げる方法を提案し、有効性を実証している。

本論文は第 1 章から第 8 章までで構成されている。第 1 章では現在の暗号システムの課題を解決するものとして量子暗号鍵配送 (QKD) を導入し、社会実装に向けた課題として QKD 装置の実装安全性保証、特に高速 QKD 装置における問題点を指摘している。また、高速な物理乱数発生器の必要性も述べている。第 2 章では QKD プロトコルの基礎として、BB84 プロトコルと同プロトコルにおける安全な最終鍵レートの表式を説明したのち、BB84 プロトコルの実装方法を述べている。第 3 章では送信される光子状態の理想からのずれが State preparation flaw として定式化できることを説明している。続いて, 高速 QKD 装置における State preparation flaw の要因が帯域制限によって変調器に印加される電気信号の波形が歪むことであることを論じ、その対策と

して従来の Double Drive Modulator(DDM) と呼ばれる構造の位相変調器に変えて、Dual Parallel Modulator(DPM) を用いることを提案している。さらに、実際の高速 QKD 装置で観測された最大 20% の信号電圧の誤差に対しても DPM が有効であることを理論的に示している。第 4 章では DPM の State preparation flaw 抑圧の効果を実験的に検証している。量子トモグラフィを導入し、送信状態の密度行列の再構成を行って、State preparation flaw を定量化している。実験で得られた結果を元に安全鍵の生成レートを計算し、信号電圧の誤差が 25% あってもほとんど影響を受けずに鍵生成ができることを示している。第 5 章は乱数生成について基本的な事項を説明している。第 6 章では量子雑音に起源をもつ物理乱数発生器を少数の追加部品で構成する方法を提案している。ここで重要になるのは光源となる利得スイッチ半導体レーザのパルスが位相相関を持たないことであるが、動作条件を最適化することでこの条件が満たされることを示している。第 7 章では提案した構成を用いた実験で得られたデータから乱数性が保証されたビット列を得るための乱数蒸留法を論じ、蒸留アルゴリズムを実装して乱数列を生成している。さらに、得られたビット列の乱数性を NIST の SP-800 で規定されている乱数テストおよび自己相関関数によって評価し、良質の乱数が生成されたことを確かめている。本研究では蒸留における計算速度で乱数の生成レートが制限されているが、理論的には 4.9Gb/s の速度で乱数生成が可能であり、本提案の有効性を示している。第 8 章は以上の研究成果をまとめている。

これを要するに、著者は量子暗号鍵配送装置の社会実装の障害となる課題を分析し、解決法を新たに提案し、有効性を実証したものであり、量子情報通信技術の実用化に向けた新たな知見を得たものである。これは量子暗号鍵配送技術、さらには量子情報通信分野の発展に貢献するところ大なるものがある。よって著者は、北海道大学博士 (工学) の学位を授与される資格があるものと認める。