氏名	本庄利守（ほんじょうとしもり）
博士の専攻分野の名称	博士（工学）
学位記番号	第 21221 号
学位授与年月日	平成 19 年 3 月 23 日
学位授与の要件	学位規則第４条第１項該当 工学研究科電気電子情報工学専攻
学位論文名	**通信波長帯における量子鍵配送に関する研究**
論文審査委員	（主査） 教授 井上 恭 （副査） 教授 滝根 哲哉　教授 北山 研一　教授 小牧 省三 教授 馬場口 登　教授 三瓶 政一　教授 河崎善一郎 教授 鷲尾 隆　教授 溝口理一郎

論文内容の要旨

本論文では、究極的に安全な暗号通信の実現に向けた量子暗号の研究、特に光ファイバー伝送に適した量子暗号（量子鍵配送）の実験的研究について述べた。

第１章では、本研究の背景として量子鍵配送の現状と問題点を述べ、本研究の位置付けを明らかにした。

第２章では、量子鍵配送の原理について述べた。

第３章では、従来方式である Plug&Play 量子鍵配送方式の改善について述べた。信号光に変調側波帯を利用することにより、Plug&Play 量子鍵配送システムの高速化が可能であることを示した。

第４章では、差動位相シフト量子鍵配送について述べた。本方式は、微弱なコヒーレントパルスの間の位相差が確率的にしか読み出せないことを巧みに利用した、光ファイバー伝送に適した新しい量子鍵配送方式である。原理実証実験などを通じて、本方式の有用性および実現性を示した。

第５章では、差動位相シフト量子秘密共有について述べた。量子秘密共有が差動位相シフト量子鍵配送方式の拡張により実現可能であることを示した。

第６章では、もつれ光子対列を用いた差動位相シフト量子鍵配送について述べた。周期分極反転 $LiNbO_3$ 内の自然放出パラメトリック下方変換を用いた方式、および分散シフトファイバー内の自然放出四光波混合を用いた方式の双方による通信波長帯における時間位置もつれ光子対の発生について述べた。そして、後者の方法による時間位置もつれ光子対光源を用いて差動位相量子鍵配送の実現性を示した。

第７章では、結論として本研究の内容、意義を総括し、また、この分野の将来展望について述べた。

論文審査の結果の要旨

本論文は、通信波長帯における量子鍵配送に関する研究成果をまとめたものであり、以下に示す７章より構成されている。

第１章では、本研究の背景となる研究分野についての現状と課題を述べ、本研究の位置付けを明らかにしている。

第２章では、量子鍵配送の基本原理について述べている。具体的には、量子鍵配送が拠り所とする量子力学の公理・定理を述べた後、従来のプロトコル（BB84、BBM92)、及び、最終秘密鍵を得るためのあと処理過程であるエラー訂正・プライバシー増幅、について述べている。

第３章では、従来の BB84 プロトコルの実装上の課題を解決する手段を提案し、実証実験を行なっている。具体的には、プラグ＆プレイ折り返し構成におけるレーリ散乱雑音の影響を、信号光の光周波数を位相変調側帯波発生によりシフトさせることによって回避する方法を提案・実証している。

第４章では、新しい量子鍵配送プロトコルである差動位相シフト（DPS）方式に関する実験的研究を行なっている。動作原理や鍵の安全性について説明した後、本方式に関して行なった様々な実験について述べている。具体的には、基本原理確認実験、観測自由度を拡張して安全度を高める改良システムの実験、正常なシステム動作のための送信光源への要求条件の明確化、周波数上方変換型光子検出器を用いた高速鍵配送実験（世界トップデータ達成)、システム応用を目指した量子鍵配送スイッチング実験、敷設ファイバを用いた現場環境下実験、などである。

第５章では、秘密鍵を分割して共有する量子秘密共有に関し、差動位相シフト方式を応用する新方式の提案及び実証実験を行なっている。

第６章では、システムの長距離化を可能とする量子もつれ光子鍵配送に関して述べている。従来、通信波長帯での量子もつれ光子の発生は困難であったが、光ファイバ及び PPLN 導波路の光非線形性を利用してこれを実現し、さらには、発生させたもつれ光子による鍵配送の原理確認実験を行なっている。

第７章は、本論文の結論であり、本研究で得られた結果の総括を行なっている。

以上のように、本論文は、通信波長帯における量子鍵配送、特に新しいプロトコルである DPS 方式に関して、様々な実証実験を行なった。これらの成果は、通信波長帯量子鍵配送システムに関して多くの知見を与えており、通信工学の発展に寄与するところが大きい。よって本論文は博士論文として価値あるものと認める。