学位論文審査の要旨

博士の専攻分野の名称　博士 (情報科学)　氏名　葛　皓波

審査担当者　主　査　准教授　岡本 淳
副　査　教　授　池辺 将之
副　査　教　授　富田 章久

学位論文題名

測定装置に依存しない量子鍵配送における時間同期に関する研究
（Study on measurement-device-independent quantum key distribution with time synchronization）

暗号は通信の安全性を確保するために必須のものであるが, 計算機の能力向上, 計算理論の進歩によってその安全性は常に脅かされている. 特に, 量子コンピュータに代表される量子情報技術の急速な発展により計算能力が飛躍的に向上し安全性が著しく脅かされる可能性が指摘されている. 将来にわたる情報セキュリティの脅威に対処するため, 安全性の基盤を物理法則におく量子暗号が提案され世界的に広く研究・応用されている. 量子暗号鍵配送 (QKD) を用いることで鍵共有における第三者の盗聴を検知することができる.QKD と絶対安全であることが証明されているワンタイムパッド暗号方式と組み合わせることで, 無条件に安全な通信システムを構築することができる.

QKD システムは理論的には無条件安全性が保証されている. しかし、実際の QKD システムには装置の不完全性のため, 様々なセキュリティホールが存在する可能性がある. 例えば, 検出器の不完全性を利用した efficiency mismatching attack や time-shift attack が知られている. これらの盗聴法は現在の技術でも実行可能であり,QKD システムに対する脅威となりうる. 一般に QKD システムの受信機においては入力される光の状態は盗聴者が自由に選べるものとするため, 装置の不完全性を利用した攻撃に対しては脆弱である.

この問題に対して,2012 年に Lo らは MDI-QKD(Measurement-Device Independent QKD) を提案した. この方式では正規ユーザであるアリスとボブは単一光子パルスを第三者 (チャーリー) に送信する. チャーリーは 2 光子に対してベル状態測定 (BSM) を行って結果をアリスとボブに報告する. チャーリーは BSM を行うため,2 光子間の量子相関のみを知り得, アリスとボブが送った個々の光子状態については情報が得られない. このため, 検出器の不完全性による攻撃は無効化される. MDI-QKD システムはレーザを光源としても実装することができるが, そのためには 2 つの独立したレーザから発せられる光子が識別不可能であることが必要である. これは MDI-QKD プロトコルにおける BSM は 2 つの識別できない光子の HOM(Hong-Ou-Mandel) 干渉に基づいているためである. 光子が識別不能であるときは明瞭な HOM 干渉が得られる. しかし, 現実のファイバー伝送路では外乱の影響を受けるため, 特に長距離伝送では光子の識別可能性が現れる. 実用的な MDI-QKD システムの構築にあたっては,HOM 干渉の明瞭度と最終的な鍵レートの関係を明らかにし, 明瞭度を改善する方法を確立することが必要である.

本研究の目的は 2 光子の識別不可能性を保証する実用的なスキームを提供することである. このため, 本論文ではまず 2 光子の HOM 干渉の明瞭度が MDI-QKD の鍵生成率に与える影響を調べた. 有限鍵長での統計的揺らぎを考慮した解析によって鍵生成率を計算し,2 光子の到達時刻のずれ

の許容される範囲をガウシアンパルスを仮定することで求めている. 次に, 本論文では到達時刻のずれを補償する新しい同期方式を提案した. 本方式は周波数光コム (OFC) を利用して同期した信号光と参照光を同時に伝送し, チャーリーが参照光の到達時刻のずれを測定し, その結果を元に信号光の時間差を補償する. 本論文では原理実証実験により, 本方式の実現可能性と時間制御の精度を実証した.

第 1 章では研究背景と本研究の目的を述べている.

第 2 章では主に QKD の一般的なプロトコルの原理を述べた後, 現実の QKD システムにある脆弱性とそれに対する対策を述べている.

第 3 章では測定装置非依存量子鍵配送 (MDI-QKD) プロトコルの原理を詳細に述べた後, 実装法を論じている.

第 4 章では MDI-QKD においてこれまで見過ごされてきた,2 つの光子から放出される光子の識別不可能性に関わる問題を検討している. 特に,MDI-QKD プロトコルにおける時間的な識別性の影響について詳細に分析し, 本プロトコルにおける時間遅延の許容範囲を導出した.

第 5 章では MDI-QKD システムのための新しい同期方式を提案した. このアプローチは, 光周波数コム (OFC) 技術を活用し, 同期システムのコンポーネントを BSM 側に集めるものであり, 実装が容易になることが期待される. さらに原理実証実験を行い, 本方式の実現可能性を示した..

第 6 章では本論文を総括し, 今後の展望について述べている.

これを要するに, 著者は装置の不完全性の影響を受けにくい MDI-QKD システムの実装における光子の識別不可能性に関する要件を解析し, システムの実現に必要な時間制御の精度を具体的に与えた. さらに, 時間制御を実現するための新しい時間同期方式を考案し, 実証実験を行うことで, 量子鍵配送技術における多くの有益な知見を得ており, 量子情報技術の分野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 (情報科学) の学位を授与される資格あるものと認める.