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　田島　章雄

審査担当者　主　査　教　授　本村　真人
副　査　教　授　髙橋 庸夫
副　査　准教授　岡本 淳

学位論文題名

量子セキュアネットワークの研究
（Study on Quantum Secure Network）

重要な情報の安全性を保つ方法として暗号技術が知られているが, 現代の暗号技術は解読に膨大な時間がかかるという, いわゆる計算量的安全性を与えるものである. そのため, 技術の進歩によって暗号が危殆化し, 世代交代の必要がある. また, 暗号通信を傍受して解読が可能になるまで保管しておくことができるため, 世代交代の時間を越えて長期に安全性を担保するのは極めて難しい.
一方, 量子暗号鍵配送 (QKD) 技術は量子力学的状態を測定することによって生じる擾乱を検知することによって盗聴のおそれのない暗号鍵を離れた 2 者間で共有する技術である. 安全性の根拠を計算量ではなく, 量子力学の原理に置いているため, いかなる盗聴技術, 暗号解読技術の進歩に対しても安全性が失われないという特質を持っている. このため,QKD で共有した鍵を用いた One-time-pad 暗号によって行った通信は情報理論的安全性を持つ. このことから, 安全保障, 金融, 医療など長期に渡って高度な秘匿性を要求される分野への QKD 技術の適用が期待されている.

最初の QKD プロトコルは 1984 年に発表され,1992 年に原理実証実験が報告されている. しかしながら, 実用的な装置の開発が始まったのは 2000 年ごろからであり, 長期間の連続自動運転が実証されたのは 2010 年以降のことである. 実際の装置・システムに対する安全性保証, ネットワークにおける鍵管理, アプリケーション開発など実社会で用いるための研究開発は未だ不十分である.

本論文では QKD 装置及びシステムを実用的なものとするために著者が行ってきた技術開発の内容が述べられている. 本論文の内容は以下のとおりである:
第 1 章では研究背景として重要な情報を盗聴・解読から保護する量子鍵配送/量子暗号技術の実用化が求められていることを述べ, 量子鍵配送ネットワークの実現に向けた研究動向が紹介されている. 続く第 2 章では QKD の概要を説明し,QKD の実証と実用化に向けて行われてきた研究開発の歴史を概観している.
第 3 章では QKD システム技術の詳細を述べている, 従来,QKD 技術は実験室内で光子伝送・受信を行い, オフラインで鍵抽出処理を行っていたためシステムとしての実現性は不透明であった. そこで本研究ではシステム構成に不可欠な要素を考察している. その結果をうけて, 光子伝送と鍵抽出処理を連続で行うために必要不可欠な量子 bit/frame 同期と同期復旧技術を考案・実装した. また, 実使用環境での温度変動などの変動の影響を受けない Alternative shift phase modulation (ASPM) と呼ぶ安定な光子変調技術を提案・実証した. これらの技術をもとに実用的なペルチェ冷却による光子検出器を一体化した QKD システムを開発し,2005 年には商用光ファイバでの 14 日間連続リアルタイム量子鍵生成を世界で初めて達成することに成功したことを述べている.

第 4 章では QKD システムの高速化について論述している. 鍵生成の高速化に必要な技術を考察した結果, 方向付けを行った単一方向・偏波無依存型波長多重技術, 高速光子検出技術, リアルタイム量子鍵抽出 (基底照合, 誤り訂正, 秘匿増強) ハードウェアの開発が論述されている. 新たな設計による QKD システムを開発し, 世界最高レベルの鍵生成速度 100 kbps 以上かつ世界最小の誤り率 1.7 % 以下を損失 13 dB のフィールド光ファイバ伝送路を用いた 30 日連続動作試験において達成したことが述べられている. また, 実使用環境においても 21 週間の長期連続安定動作試験中の鍵生成レート変動が 10 % 以下であったことが述べられている.
第 5 章では、QKD ネットワークのアーキテクチャ提案と構築, アプリケーションの実証が論述されている. 量子レイヤ, 鍵管理レイヤ, 鍵供給レイヤの 3 レイヤからなる QKD ネットワークアーキテクチャ, 鍵フォーマットと鍵管理方法を提案し, フィールド光ファイバ上における QKD ネットワーク (東京 QKD ネットワーク) の構築が述べられている.
第 6 章はまとめとして, 上記の成果を基盤とした量子鍵配送ネットワークが今後ユーザによる実証を経て, さらに機能・使い勝手向上、信頼性・安全性保証が行われるとの展望を明らかにしている.

これを要するに著者は QKD 装置・システム要素技術の提案と実証を行い, システム実装, さらに QKD ネットワークのアーキテクチャ提案と構築, アプリケーションの実証を行うことで世界的にもトップレベルの性能を実現し, 実用的な QKD 技術の確立に必要な多くの知見を与えたと言える.

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あるものと認める.