学　位　論　文　内　容　の　要　旨

博士の専攻分野の名称　　博士（工学）　　氏名　田島　章雄

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）

情報通信技術の進展によりインターネットが社会インフラとなった現在、金融情報をはじめとする重要個人情報がネットワーク上を流れている。さらに近い将来、遺伝子情報など絶対に漏洩してはならない情報がネットワーク上でやりとりされる可能性があるため、このような重要な通信情報を盗聴・解読から守る秘匿通信技術の重要性が増している。情報を秘匿する技術として暗号技術が知られているが、数学を利用した従来の暗号はコンピュータや解読アルゴリズムの発展によりいずれ解読される危険性がある。そこで、上記危険性から重要情報を秘匿する技術として、物理法則によって安全性が保証されている量子暗号技術が注目されている。

本論文では、量子暗号技術の課題であった実使用環境下でのリアルタイム量子鍵生成と、実使用で要求される仕様レベルの達成にむけた量子鍵配送 (Quantum Key Distribution, QKD) システム技術の高性能化を述べる。本研究では、光子伝送から鍵抽出まで一気通貫のリアルタイム処理を行うシステムの研究開発を行った。さらに, 動作速度、鍵生成効率の向上のため, 平面光回路 (Planar Lightwave Circuit, PLC) を用いた新しいシステムを開発し、実使用環境における長期間連続運転試験により高安定・高信頼な QKD システムの構成技術を確立した。本論文では、装置開発にとどまらず、多様なアプリケーションへ量子鍵を配送する量子鍵配送ネットワークのアーキテクチャを提案し、提案したネットワークの構築と秘匿通信アプリケーションの実証を行った。

以下に本論文の構成を示す。

第 1 章では研究背景として、重要な情報を盗聴・解読から保護する技術として量子鍵配送/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を紹介する。

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する。

第 3 章では、本研究で提案・実証した QKD システム技術の詳細を述べる。従来、QKD 技術は光子伝送・受信結果を用いたオフライン鍵抽出処理によって実現していたため実システムとしての実現性は不透明であった。そこで本論文では、以下の技術開発を行った。

(ア) リアルタイム量子鍵生成技術: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、復旧技術を考案した。

(イ) 実使用環境下での安定化技術:実使用環境での温度変動などの変動の影響を受けない安定化技術として、Alternative shift phase modulation (ASPM) と呼ぶ安定な光子変調技術を提案した。

これらの技術と、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、商用光ファイバでの 14 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。

第 4 章では QKD システムの高速化について述べる。第 3 章で述べたシステムは、往復型とよばれる構成を用いたため、損失 8 dB の伝送路を用いたときの鍵生成レートは 13.0 kbps と、One Time

Pad 暗号化の鍵として用いることができるアプリケーションがテキスト主体の E-mail や Voice over IP などに限定されてしまうという問題があった。そこで、鍵生成速度の向上を目的に、動作速度・鍵生成効率の向上、波長多重技術の研究開発を行った。

(ア) 単一方向・偏波無依存型波長多重技術:動作速度と鍵生成効率の向上のために、往復型のような動作速度制限がなくかつ干渉計の明瞭度が高い単一方向型を採用した。特に、PLC を用いた偏波無依存型システムを採用することで高速・高効率に加え高安定、低誤り、高信頼性を実現した。さらに複数波長の信号を多重化することで全体の鍵生成速度を向上させる波長多重技術に関しては、光学干渉計を複数波長で共用する方式を提案し、波長多重時のシステムのコスト・サイズ増大を抑えることに成功した。

(イ) 高速光子検出技術:動作速度を制限している要因の一つである光子検出器に関しては、高速 (GHz) 動作だけでなく低雑音化を同時に実現しなくてはならない。そこで、新たに検出信号を A/D 変換し信号処理技術を用いて、ノイズ特性をセルフトレーニングによってキャンセルするセルフトレーニング型検出回路を考案し GHz 動作と低雑音特性を両立した。

(ウ) リアルタイム量子鍵抽出 H/W 技術:上記の技術によって光子伝送の速度が向上した際、最終鍵抽出のための信号処理の高速化・高効率化も重要課題となる。鍵生成速度 1Mbps を目標とした場合、動作速度 1.25 Gbps、8 波長多重のシステムが想定される。その場合、乱数、基底など合計 5 Gbps のデータ処理を行わなければならない。そこで、複数の FPGA を用いた鍵抽出速度 1 Mbps のリアルタイム量子鍵抽出 (基底照合、誤り訂正、秘匿増強) ハードウェアを新規に開発した。

以上の技術を組み合わせた 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。また、実使用環境において 21 週間の長期連続安定動作試験を行い、鍵生成レート変動 10 % 以下を達成した。

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について述べる。量子暗号技術は複数の秘匿通信アプリケーションに対して安全に鍵を供給する鍵配送ネットワークとして用いられることが考えられる。

(ア) レイヤ構成と機能: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を提案した。また、各レイヤの機能をサポートする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 QKD ネットワーク (東京 QKD ネットワーク) を構築した。

(イ) 鍵配送ネットワークにおいて動作する秘匿通信アプリケーションとして、QKD によって共有した鍵を advanced encryption standard (AES) 暗号化の seed 鍵として用いる QKD-AES ハイブリッドシステムと、複数携帯端末間の通信をサポートする秘匿スマートフォンシステムの開発を行った。これらアプリケーションを実際に鍵配送ネットワーク上で動作させ、有用性を実証した。

第 6 章はまとめであり、上記の成果を基盤とした量子鍵配送ネットワークがユーザによる実証を経て、機能・使い勝手向上、信頼性・安全性保証が行われ、実システムとしての導入が期待されることを述べる。