量子暗号の実用化のための研究開発

（１）研究の目的

高性能単一光子検出技術を利用して、無条件安全性が理論的に保証された高速な量子鍵配送プロトコルを都市圏ネットワークで実現するためのシステム技術の開発および量子鍵配送を基幹回線ネットワークへ適用していくための基盤技術の開発を行い、都市圏ネットワークと基幹回線ネットワークが接続したネットワーク上における量子鍵配送システムを開発して、その性能を実証することを目的とする。

（２）研究期間

平成１８年度から平成２２年度（５年間）

（３）委託先企業

日本電気（株)、三菱電機（株)、日本電信電話（株）

（４）研究予算（百万円）

平成１８年度	１８０（契約金額）
平成１９年度	２１９（契約金額）

（５）研究開発課題と担当

イ‐１：都市圏対応型量子鍵配送システム技術の研究開発

イ‐１‐１：都市圏量子暗号ネットワーク技術（日本電気株式会社）

・暗号鍵高速伝送・生成技術

・波長分割多重制御・ネットワーク管理・スイッチング技術

・エンタングル光子対量子暗号システム

イ‐１‐２：都市圏量子セキュリティ技術（三菱電機株式会社）

・量子暗号システム技術

・鍵管理プロトコル技術

・安全性解析と新プロトコル提案

イ‐２：基幹回線対応型量子鍵配送技術の研究開発（日本電信電話株式会社）

・長距離 DPS-QKD 方式

・低暗計数単一光子アバランシェ検出器

・周波数上方変換型単一光子検出システム
・高速型可視域光子検出器

（６）主な研究成果

特許出願：　　６件
外部発表：　　４６件

具体的な成果

(1)都市圏量子暗号ネットワーク技術（日本電気株式会社）

①高速伝送・生成技術

- モノリシック平面光回路を、625 MHz および 1.25GHz の高速動作仕様に最適化し、開発。
- 100 km 級のフィールドノード間において、安定かつ高速の（625 MHz 繰り返し）鍵配付実証実験に成功。

②波長分割多重制御・ネットワーク管理・スイッチング技術

- 世界初の量子信号へ影響を及ぼさない波長多重伝送を実証。

③エンタングル光量子暗号技術

- 2 波長光子対光源の開発において、量子暗号システム用光源として利用可能であることを確認。

(2)都市圏量子セキュリティ技術（三菱電機株式会社）

①量子暗号システム技術

- 量子・古典多重信号伝送系の高速化機能の備えた装置開発、および基本的特性を確認
- 単一光子検出器の再検討設計、およびモジュール開発

②鍵管理プロトコル技術

- センタ鍵管理方式の改良、機能検討、仕様化

③安全性解析と新プロトコル提案

- QBSC プロトコルについての考察結果を応用し、鍵配送以外のプロトコルの構築を実施

(3)基幹回線対応型量子鍵配送技術の研究開発(日本電信電話株式会社)

①長距離 DPS-QKD 方式

- 偏波無依存化した周波数上方変換型光子検出器(UCD)を用いたフィールド実験
- 超伝導単一光子検出器を用いた DPS-QKD 実験

②低暗計数単一光子アバランシェ検出器

- InGaAsSb/InP APD 製造における工程実施検討、およびその条件の最適化制御手法をほぼ把握。

③波長上方変換周波数上方変換型単一光子検出システム

- 波長 1800nm のポンプ下で 1500nm 帯の光子を変換するよう設計・製作したデバイスにおいて，低 DC レベルでの 1500nm のバンド単一光子検出を確認

④高速型可視域光子検出器

- 開発した PMT の量子効率，暗計数率及びタイミングジッタを評価する系を構築し，検出信号のジッタ FWHM 168.9±2.6 ps を達成

（7）研究開発イメージ図

イ-1-1：
都市圏量子暗号ネットワーク技術

日本電気株式会社

①高速伝送･生成技術：
•高速化･長距離化を実現するための一方向型量子暗号鍵配付技術について、100kmまでの伝送距離で高速伝送を実現し、PLCによる･変調器を用いない新方式の有効性を実証。
•鍵生成処理の高速化に向け、量子暗号鍵蒸留処理ハードウェア及びその制御ソフトウェアのコーディングを行い、ハードウェアのパフォーマンス評価を行った。
②ネットワーク技術：
•量子ネットワークの基本となるスイッチング技術を開発し、多者間の鍵共有と秘密通信を実現。波長配置と光フィルタ帯域、及び古典信号レベルの最適化により、暗号鍵生成特性に影響を及ぼさない100km級伝送を実証した。
③エンタングル光量子暗号技術：
•通信波長帯光子対光源を用いた、フランソン干渉をベースとした量子暗号システムの鍵配付動作実証デモを行った。

イ-1-2：
都市圏量子セキュリティ技術

三菱電機株式会社

④量子暗号システム技術：
•古典信号と量子信号の時分割による分離技術を検討し、古典信号であるクロックと偏波情報をモニタし、同期ゲート制御、フィードバック制御により、温度変化、偏波ゆらぎを補償する方式を機能分割して実装した。
⑤鍵管理プロトコル技術：
•鍵管理センタを用いた認証プロトコルの改良、複数経路を用いて、実効性能向上やDoS攻撃の耐性を向上させた。
⑥安全性解析と新プロトコル提案：
•デコイ方式におけるイールドの上限及び下限を厳密に求める方法を開発した。これにより量子暗号の通信距離及び鍵生成速度の一層の向上が可能となった。

イ-2：
基幹回線対応型量子鍵配送技術の研究開発

日本電信電話株式会社

⑦長距離伝送技術：
•長距離QKD実験：低ジッタ周波数上方変換検出器を用い新しい安全性理論に基づく100km超の伝送に成功。世界初の10GHzクロックのQKD 実験、及び超伝導単一光子検出器を用い200kmでの安全鍵配信、100kmで安全鍵配送率17kbit/s を達成。実線路において周波数上方変換型光子検出器を偏波ダイバーシティ構成を用いてDPS-QKDの安定した伝送を実現。
⑧光子検出技術：
•周波数上方変換型単一光子検出システム：暗計数率 104Hz以下、量子効率 8% のノン･ゲート単一光子検出を実現。低ジッタ Si-APD と組み合わせ、高速･低ジッタ検出を可能に。偏波ダイバシティ構成による偏波無依存化を実現。長波長ポンプによる周波数変換を開発し、暗計数率の1～2桁低減を達成。