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）

（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：　　２件
外部発表：　　２４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

- 高速化・長距離化を実現するための伝送技術について、100km までの伝送を実現し、PLC による変調器を用いない新方式の有効性実証。
- 鍵生成段階での安全性を保証するため、伝送路・送受信器の特性ばらつきを補償することで鍵の NIST SP800-22 乱数検定合格を達成。

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

- 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。

③エンタングル光量子暗号技術

- ２波長光子対光源に必要となる PPLN 非線形光学デバイスの設計、試作、モジュール化および二光子干渉実証デモンストレーションを実施。

(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

- 単一光子源量子暗号システムで世界最長の 80km の原理検証実験に成功。

⑤鍵管理プロトコル技術

- U2 関数を用いたメッセージ認証プログラムを作成。

⑥安全性解析と新プロトコル提案

- DPS-QKD の安全性に関する新たな結果を示した。

(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)

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。

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 10^4Hz 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。

（7）研究開発イメージ図

『量子暗号の実用化のための研究開発』（課題イ）平成18年度成果

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伝送技術について、100kmまでの伝送を実現し、PLCによる変調器を用いない新方式の有効性実証。 •鍵生成段階での安全性を保証するため、伝送路・送受信器の特性ばらつきを補償することで鍵のNIST SP800-22乱数検定合格を達成。 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。 ③エンタングル光量子暗号技術： •2波長光子対光源に必要となるPPLN非線形光学デバイスの設計、試作、モジュール化および二光子干渉実証デモンストレーションを実施。
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：単一光子源量子暗号システムで世界最長の80kmの原理検証実験に成功。 ⑤鍵管理プロトコル技術：U2関数を用いたメッセージ認証プログラムを作成。 ⑥安全性解析と新プロトコル：DPS-QKDの安全性に関する新たな結果を示した。
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。 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 10^4Hz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。