

「量子暗号の実用化のための研究開発」の開発成果について

～イ 量子暗号ネットワーク技術の研究～

1. 施策の目標

- 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。

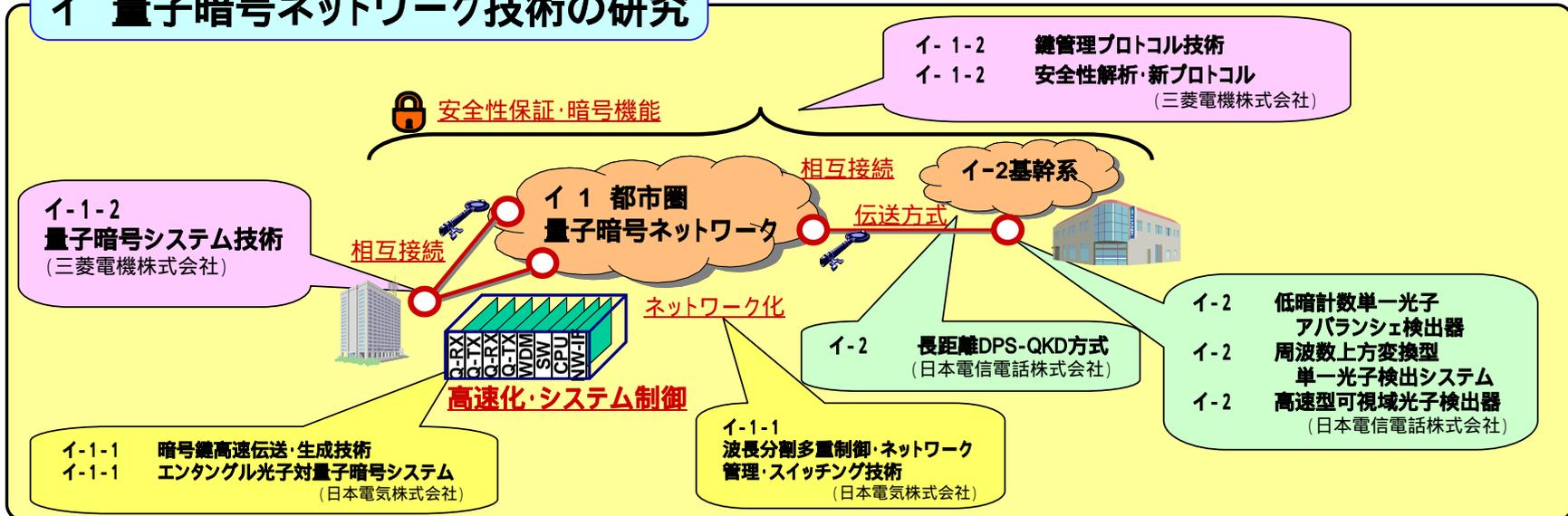
2. 研究開発の背景

- 安心・安全な社会を実現するためのインフラストラクチャーとして、ネットワークは、ユーザが盗聴・改ざん・成りすましなどのさまざまな危険から解放され、通信の安全性が保証されたサービスなどを利用できることが求められている。

3. 研究開発の概要と期待される効果

- 都市圏ネットワークに対応した高速な量子鍵配送技術と、基幹回線ネットワークに対応した量子鍵配送技術、さらに両ネットワーク間の接続技術を開発することにより、都市圏ネットワークから基幹回線ネットワークまでのシームレスな量子鍵配送が実現できる。

イ 量子暗号ネットワーク技術の研究



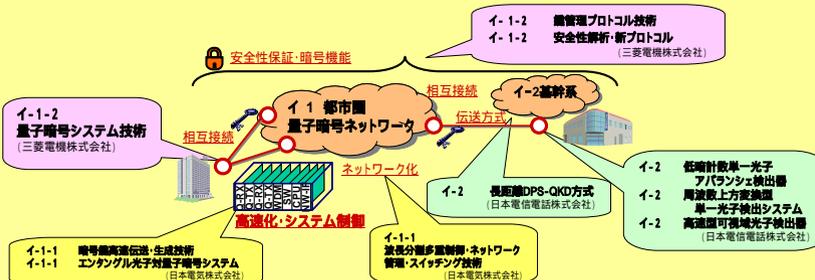
4. 研究開発の期間及び体制

- 平成18年度～平成22年度(5年間)
- NICT委託研究(日本電気株式会社、三菱電機株式会社、日本電信電話株式会社)

イ 量子暗号ネットワーク技術の研究の主な成果

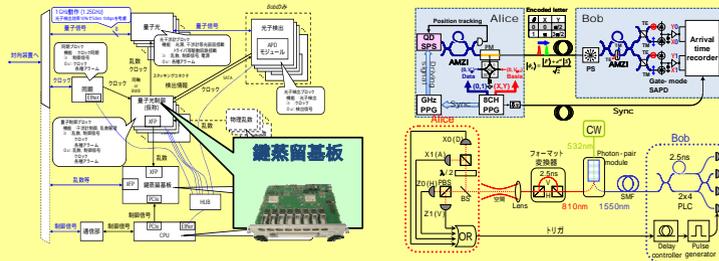
イ 量子暗号ネットワーク技術の研究

- 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)
 - イ 1 2: 都市圏量子セキュリティ技術 (三菱電機株式会社)
- 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)



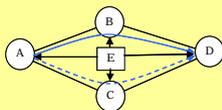
イ 1 1: 都市圏量子暗号ネットワーク技術 (日本電気 株)

- 昨年度までに試作した量子光基板/同期基板/制御基板の結合評価、課題(ア)の成果である光子検出基板との結合評価、鍵蒸留基板との結合評価を完了した。
- 平成22年度の相互接続実験に際してNW全体を管理する鍵管理システムを検討、暗号鍵管理とサイト管理を別サーバで管理する構成を採用し、制御用GUI開発を完了。
- 1.5μm帯単一光子による安全な量子鍵の50kmファイバ伝送に成功した。
- 偏光 - 位相間のハイブリッドエンタングルメントを利用した空間 - ファイバ統合型QKDの原理実証実験を行い、ファイバ伝送距離20kmを達成した。



イ 1 2: 都市圏量子セキュリティ技術 (三菱電機 株)

- 平成20年度までに開発した量子暗号装置 (光学系と電気系) を制御するATCA準拠のシステム制御基板を開発した。この基板を装置と接続しシステム試験とデバッグを実施した。
- 篩い鍵生成S/Wを開発し、H/Wと接続して試験を行い鍵生成の動作を確認した。
- 最終年度に予定されているNEC, NTT他との相互接続デモの準備検討を実施した。
- 安全性証明について、squash operatorと呼ぶ量子演算子を導入することで、厳密な意味での安全性証明が成り立つことを示した。また、鍵蒸留S/Wの高速な新方式の基礎検討を実施し、その高速性をPC上で評価した。

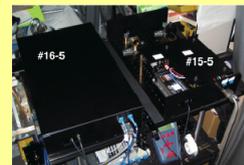


イ 2: 基幹回線対応型量子鍵配送技術の研究開発 (日本電信電話 株)

- H/WとS/Wを組み合わせたDPS-QKDプロトタイプ実験システムの開発を進め、大手町-小金井間の往復敷設ファイバ(JGN2)を用いて、SSPDを用いたDPS-QKDの安全鍵配送に成功し、来年度のデモンストレーションに向けた見通しを立てた。
- ビット誤りの小さいシフト鍵を得るためのデータ処理方法を特許提案 (三菱と共同)
- 1810nm励起によるラックマウントタイプ周波数上方変換型(UCD)検出装置を作製。電子冷却装置を一体化したHPDのモジュール化を完了し、周波数上方変換器と結合して、数GHz程度の高速度クロックのQKDシステムに適用する見通しを得た。

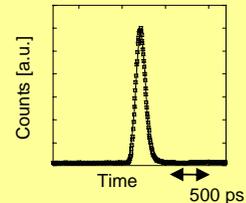


高速大規模信号処理が可能なプロトタイプ実験システム



長波長ポンプUCDモジュール化、ラックマウント

FWHM: 126 ps (before de-convolution)



カウント率 1 McpsでのHPDヒストグラム波形

5. これまで得られた成果(特許出願、論文発表等)

	国内出願	外国出願	研究論文	その他研究発表	報道発表	展示会	標準化提案
量子暗号の実用化のための研究開発 課題イ	43 (15)	8 (0)	48 (7)	72 (6)	10 (2)	2 (0)	0 (0)

累計件数を記載。括弧内は、平成21年度の件数。特許は、取得予定を含む。

6. 研究成果発表会などの参加について

■ 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)

ECOC2009(ウィーン)にて2件、OFC(サンディエゴ)にて1件発表など

- ECOCにて、WDMによる量子暗号の大容量化に関して講演を行うと共に、量子暗号の将来展望についてワークショップで講演を行い、先端的な鍵配付ネットワークに向けた日本の研究開発をアピールした。
- OFCでもスペシャルシンポジウムで量子暗号装置の高速化について招待講演を行い、日本の技術水準の高さを示した。
- 公開シンポジウム「ナノ、量子、IT融合によるイノベーション創出～エレクトロニクス研究拠点の新展開～」にてPLCを用いた単一光子量子暗号伝送に向けた発表を行った。
- International Symposium on Quantum Nanophotonics and NanoelectronicsにおいてもPLC単一光子量子暗号伝送装置に関する成果をアピールした。
- その他、応用物理学会、電子情報通信学会に参加し、成果をアピールした。
- また、応用物理学会量子エレクトロニクス研究会「量子情報の最前線と今後10年の展開」に講師として参加し、委託研究の成果を紹介すると共に、量子暗号研究の将来について若手研究者に講演した。

■ イ 1 2: 都市圏量子セキュリティ技術(三菱電機株式会社)

研究論文2件、学術解説3件、取材掲載1件など

- 電子情報通信学会(SCIS, QITなど)、日本航空宇宙学会などに参加し、成果をアピールした。
- 日本経済新聞に三菱電機の量子暗号のこれまでの取り組みおよびNICT委託研究に関する取材を受け、掲載され技術アピールを行った。
- 応用物理学会「量子情報の最前線と今後10年の展開の小特集で量子暗号に関する解説紹介を行った。
- 日本光学会「光学」において、量子暗号通信と光が果たす役割という題目で解説紹介を行った。
- Physical Review A誌に、量子暗号の安全性に関する論文を掲載した。(T. Tsurumaru, PRA 81, 012328 (2010)).

■ 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)

ECOC2009(ウィーン)、LPHYS'09(バルセロナ)にて発表

- ECOCにてFPGAを用いたギガヘルツクロックでの量子暗号実験システムに関して報告した。
- LPHYS'09にてレーザーのカオスを利用した高速物理乱数を用いた量子鍵配送実験について報告した。