平成２２年度研究開発成果概要書
「量子暗号の実用化のための研究開発」
（課題イ　量子暗号ネットワーク技術の研究開発）

（１）研究開発の目的

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）研究開発期間

平成１８年度から平成２２年度（5 年間）

（３）委託先企業

日本電気株式会社＜幹事＞、三菱電機株式会社、日本電信電話株式会社

（４）研究開発予算（百万円）

平成１８年度	178.8
平成１９年度	175.9
平成２０年度	192.2
平成２１年度	218.7
平成２２年度	203.9

（５）研究開発課題と担当

課題イ - １：都市圏対応型量子鍵配送システム技術の研究開発

課題イ - 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

課題イ - 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

課題イ - 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）これまで得られた研究開発成果

		（全体） 件	（当該年度）件
特許出願	国内出願	46	5
	外国出願	8	0
外部発表	研究論文	59	10
	報道発表	12	2
	その他研究発表	95	19
	展示会	7	4
	標準化提案	0	0

具体的な成果

（１）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）

- 動作速度 1GHz、日本電気オリジナル PLC による 8 波長の量子信号 WDM 状態で多重による劣化が無いことを確認した。また、本プロジェクト内、および NICT との連携により開発した高速鍵抽出と安全性を両立する鍵蒸留基板(フレーム同期、誤り訂正、秘匿増強処理)についても 8 波長分 80Gps 相当の信号処理が可能であること、リアルタイムでの 1Mbps 以上の鍵速度が可能であることを実証するとともに、NTT の DPS-QKD での動作実証についても行った。
- 本課題で試作した量子光基板/同期基板/制御基板/鍵蒸留基板、課題(ア)の成果である光子検出基板、NICT 製の SSPD を組み合わせ、高速 QKD システムを確立した。
- 小金井－大手町 14dB 損失リンクにおいて 1 波長で 80kbps の最終鍵を達成した。さらに、8 波長多重時に 10dB 損失換算で鍵速度 1Mbps 以上に相当する性能、長時間連続動作を実証した。

（２）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－１－２都市圏量子セキュリティ技術（三菱電機株式会社）

- 偏波補償機能を有する 100MHz 駆動のデコイ方式を用いた高安定な量子暗号装置を開発した。古典光を用いた微弱な量子光の偏波補償機能と、干渉計に PLC を採用することで安定化を実現した。検出器は市販 APD を用いて小型高速化を行った（検出効率 3-12%, 暗係数率 $6x10^{-6}$)。また鍵鍵蒸留処理では、Toeplitz 行列を用いた秘匿性増強用のアルゴリズムを新たに提案し、専用ハードウェアを用いずとも、ソフトウェア(PC)のみで鍵蒸留処理をすべて高速に行えることを実証

した。これらによりシステムの小型化も実現している。量子暗号のシステム性能は、Tokyo QKD Network 実証実験後さらに光子検出器と光学系を改良することにより、伝送路 10dB（50km 相当）において、最終鍵生成速度 約 15kbps を達成。開発した光子検出器は単体評価時に検出効率約 12%を実現しており、この光子検出器をシステムへ適用することで最終鍵生成速度 60kbps が実現可能。

- 本装置を大手町-白山間の往復敷設ファイバ 24km（損失 13dB）（JGN2plus）で適用し鍵配送に成功、3 日間連続安定動作を確認した（篩い鍵生成速度 10kbps, QBER 4.5%, 最終鍵生成速度 2kbps)。また、Tokyo QKD Network において、NICT, NEC, 三菱, NTT および海外研究機関と共同で鍵リレーやそれを用いた TV 会議システムなどネットワーク実験に成功した。（2011/10/14 広報発表および UQCC2010 でのライブデモ実施、JGN2plus「先端・基盤技術賞」受賞）
- 量子鍵配送装置をワンタイムパッド携帯電話ソフトウェアに適用し、音声通話を端末間の end-to-end で暗号化して通話の盗聴を防ぐセキュアモバイル通信システムを開発した。量子暗号を携帯電話という身近なアプリケーションに適用することに成功した。(2010/9/2 広報発表、および UQCC2010 でのデモ展示実施)
- 量子暗号の安全性に関する理論研究を行い、その結果を用いて鍵蒸留アルゴリズムを高速化した。これにより鍵蒸留処理のすべてをソフトウェアで行うことが可能となり、QKD 装置の高速化・低価格化に大きく寄与できた。またその成果を論文として発表した。

（３）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）

- 差動位相シフト量子鍵配送（DPS-QKD）プロトコルを用い、スタンフォード大学 NIST と共同で、10GHz クロック周波数と超伝導単一光子検出器により、200km の伝送距離において 12.1bit/s のレートで一般的個別攻撃に対して安全な鍵を生成した。105km の距離では安全鍵生成は 17bit/s のレートで目標値を達成した。また単一光子源を仮定した DPS-QKD プロトコルの無条件安全性を示すことができた。
- DPS-QKD をシステム化し、NICT が開発した超伝導単一光子検出器、NEC が開発した鍵蒸留基板と組み合わせることにより、実環境敷設光ファイバ約 90km(損失 27dB)（JGN2plus）上で安定した鍵配送が行えることを示した。また課題イ－1 の都市間ネットワーク対応のシステムとソフトウェアを共通化し、接続実証実験に成功した。

- ４時間に渡る連続最終鍵生成と８日間に渡る安定したシフト鍵生成を行い、最終安全鍵生成レート約 2kbps、シフト鍵生成レート　約 18kbps、ビット誤り率 約 2%であった。
- 暗計数雑音をさらに低減した周波数上方変換モジュール（1810nm 励起）を新たに製作. コントローラを一体化した光子検出器として最大効率で暗計数率 10^{-7} Hz/nsec 台を達成した。高速クロック(～GHz)の QKD システムに適合する。