別紙３

「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）研究予算（百万円）

平成１８年度	１７９．９（契約金額）
平成１９年度	１８９．９（契約金額）
平成２０年度	２０９．９（契約金額）

（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）主な研究成果

特許出願：　　３５件
外部発表：　　１２１件

● 具体的な成果

課題イ：量子暗号ネットワーク技術の研究開発

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）

①暗号鍵高速伝送・生成技術

- 平成１９年度に試作した量子光基板各部の改造を行い、本基板への乱数/電源供給を行う制御基板の試作、および基本動作を確認した。
- 暗号鍵蒸留過程のハードウェア処理による高速化に関して、平成１９年度に引き続き、フレーム同期処理の設計を行い、シミュレーションによるパフォーマンス評価を完了し、さらに鍵蒸留基板の設計／試作／評価を行い、外部光 IF、対サーバ IF、FPGA 間 10Gbps パス、メモリの基本動作を確認した。
- 東京大学ナノエレクトロニクス研究機構ならびに関係諸機関と連携して、1.5 um 帯単一光子光源を用いた量子鍵配付実証実験の企画ならびに実験系の設計／試作／評価を行った。

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

- 同期基板の試作、評価を行い、155MHz クロック、およびフレーム周期情報を極低光強度で伝送できることを確認した。
- 鍵の使い捨てを想定し、暗号鍵の生成と消費に追従する鍵管理方式を提唱し、実験の結果、複数ノードからなる量子暗号ネットワークにおいて、鍵の消費量に応じて共有暗号鍵を最適配分できることを実証した。

③エンタングル光子対量子暗号システム

- 平成１９年度までの研究成果用いて 2 波長光子対量子鍵配付の時間基底における動作を確認し、光子検出レート、およびエラー率を評価した。
- さらに、光子対量子鍵配付システムにおいて、800nm 帯 PLC 干渉計の設計／試作／評価を行い、充分に使用可能な特性を持つことを確認した。

イ－１－２都市圏量子セキュリティ技術（三菱電機株式会社）

①量子暗号システム技術

- 古典信号と量子信号を 100dB の強度差を持って波長多重分離す

る MUX・DEMUX を開発、動作検証に成功した。
- 日本大学の開発した信号抽出方式を改良し、周波数フリーな光子検出器を開発、100-330MHz で動作検証に成功した

②鍵管理プロトコル技術
- 実用的な量子鍵基盤構築を目標に、鍵管理センタの機能分析を行い、量子通信路から分離された鍵管理センタの形態が柔軟なネットワーク構成を低コストで実現できることを示した。

③安全性解析と新プロトコル提案
- デコイ方式の安全性を左右するパラメタ「イールド」の最適化問題を厳密に解くことに成功した。
- これまで存在した閾値検出器による光子検出器の不完全さと、量子暗号の安全性証明のギャップについて、squash operator と呼ぶ量子演算子を導入することにより、厳密な意味での安全性証明が成り立つことを示した。

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)

①長距離 DPS-QKD 方式
- クロック周波数 1GHz の DPS-QKD のプロトタイプ実験システムを実装し、初期動作を確認。高速/大容量な信号処理が要求される箇所のみハードウェア（Field Programmable Gate Array: FPGA）とし、その他は柔軟性を高めるためにソフトウェアにより実装した。
- 短ジッタ特性を持つ Hybrid photon detector (HPD) を 980 nm ポンプの周波数上方変換型単一光子検出器に適用し，これを用いてクロック周波数 2 GHz の DPS-QKD 実験を実施した。10 km の光ファイバ伝送距離において 1.3 Mbit/s ビットレートで一般的個別攻撃に対して安全な鍵を生成する事に成功した。
- スタンフォード大との共同研究により、DPS-QKD において送信側に偏波変調を加えることで偏波依存性のある光子検出器を用いても安定に動作させることのできる方式を提案した。特に、周波数上方変換型の単一光子検出器を用いたデモンストレーションに成功した。
- レーザーカオスを用いたギガヘルツクラスの高速物理乱数発生器を DPS-QKD システム量子鍵配送に適用し、25ｋｍの光ファイバを伝送し、量子ビットエラー3.2%、シフト鍵生成率 9.0kbps という結果を得た。

②低暗計数単一光子アバランシェ検出器

Sb 系 APD に関して、専用に利用してきた結晶成長装置の老朽化、Sb を含む層の偶発的なクラック発生と不確定な要素が多数発生

し制御が困難になってきた。そのため周波数変換による光子検出の進展を考慮し集中的な取組みのためAPD開発は終結させた。

③周波数上方変換型単一光子検出システム

波長 1810nm 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、毎秒 100 カウント以下の DC レベルで量子効率 5%程度での 1500nm 帯単一光子検出を確認できた。

④高速型可視域光子検出器

- バイアルカリフォトカソードから出力された光電子を APD で増倍する Hybrid photon detector により、1 MHz のカウントレートにおいてジッタ FWHM <80 ps, FWTM<150 ps を達成し、これを 980nm ポンプ周波数上方変換系と組み合わせることにより、実効量子効率約 4%、暗計数約 100kHz を得た。

● 連携について

量子暗号全体会議を四半期に一度の割合で開催し、事務連絡、進捗報告、目標達成度の確認だけではなく、技術課題に関する討論を実施した。

鍵蒸留処理に関しては、処理の切り分け、最大符号長、インタフェースについての議論を行い、それぞれ以下の合意の基、設計/製造/評価を行った。

処理の切り分け

- 秘匿性増強までハード化
- 動作監視、ネットワーク制御、鍵管理はソフト

最大符号長

- 1Mbit

インタフェース

- 主信号:XFP による光接続
- その他：10/100/1000 Ether x4 本、PCI-Express(～8 レーン)、および 1Gbps の疑似乱数発生のための SMA コネクタ

想定使用法

- 乱数（～6Gbps x 8 本）若しくはシフト鍵（1Mbit 単位：～50Mbps）を入力、処理後、最終鍵を取り出す
- 干渉計、検出器周りの調整の為の情報（温度制御情報、位相情報等）は本基板からは出力されない

ネットワークについては、鍵管理方式、クロック配信方式やトポロジの議論中である。装置筐体については、ATCA を用いることで三社間の共通化の合意を得ている。

課題アとの連携として、アでの開発状況(モジュール・受信基板の概要、インタフェース)の報告とイからアへの要望について議論している。

（７）研究開発イメージ図

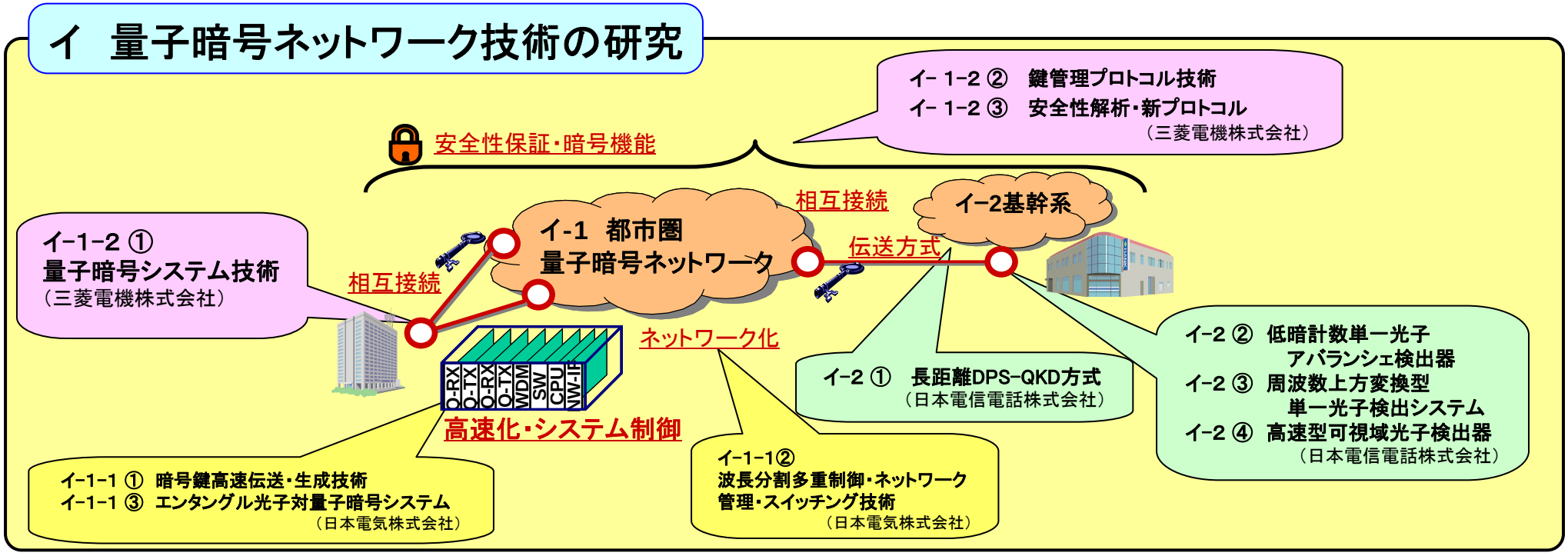
（研究開発イメージ図は添付１を参照願います。）

「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。

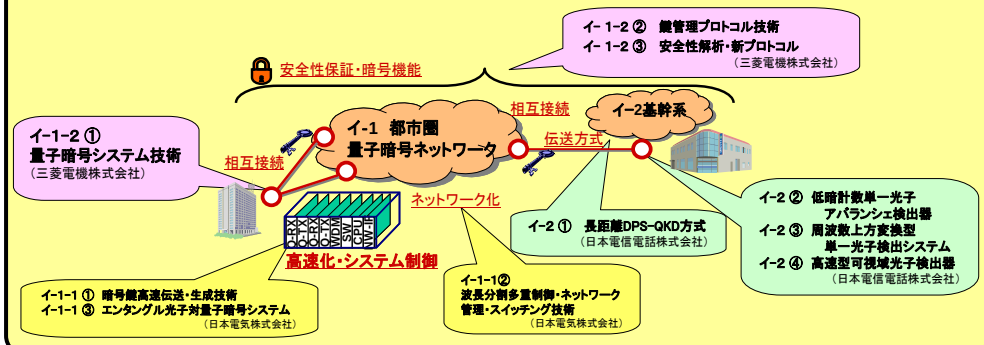


4. 研究開発の期間及び体制
– 平成18年度～平成22年度（5年間）
– NICT委託研究（日本電気株式会社、三菱電機株式会社、日本電信電話株式会社）

イ　量子暗号ネットワーク技術の研究の主な成果

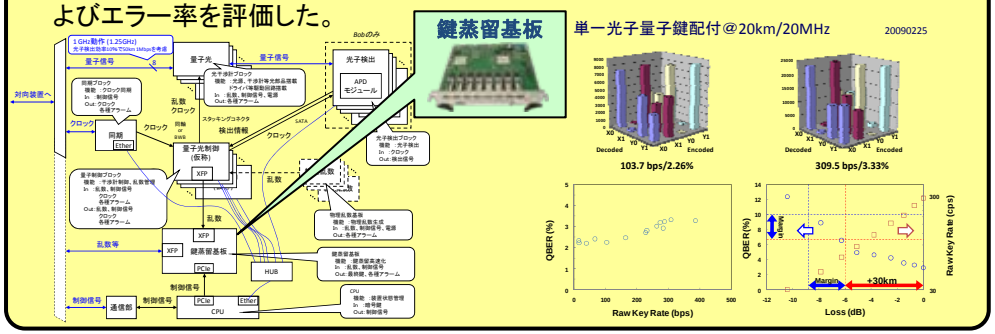
イ　量子暗号ネットワーク技術の研究

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）



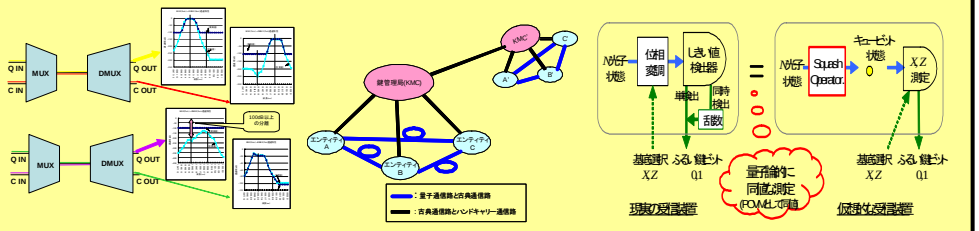
イ-1-1：都市圏量子暗号ネットワーク技術（日本電気 ㈱）

- 50 km 1Mbpsの最終鍵生成を実現する量子暗号装置の開発を進め、鍵蒸留高速化基板/同期基板/制御基板の試作を行い、各基板の基本動作評価を完了した。
- 東京大学ナノエレクトロニクス研究機構ならびに関係諸機関と連携し、世界初の1.5um帯単一光子量子鍵配付の実証に成功した。
- 鍵の使い捨てを想定し、暗号鍵の生成と消費に追従する鍵管理方式の提唱、実験を行い、実証した。
- 2波長光子対量子鍵配付の時間基底における動作を確認し、光子検出レート、およびエラー率を評価した。



イ-1-2：都市圏量子セキュリティ技術（三菱電機 ㈱）

- 古典信号と量子信号を100dBの強度差を持って波長多重分離するMUX・DEMUXを開発、動作検証に成功し、さらに古典・量子波長多重伝送が可能な古典光強度限界を確認した。
- 鍵管理センタの機能分析を行い、量子通信路から分離された鍵管理センタの形態が、柔軟なネットワーク構成を低コストで実現できることを示した。
- 「デコイ方式」における重要なパラメタである「イールド」の最大値と最小値を厳密に求めることに成功し、これによってQKDの通信距離および速度を向上させた。
- BB84方式の安全性証明における新手法（squash演算子）を開発し、これによって、従来問題となっていた理論と実験とのギャップ(しきい値検出器)の解消に成功した。



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 ㈱）

- DPS-QKDが高速な鍵配送を実現できる点に着目して、短ジッタの特徴を持つハイブリット光子検出器を用い短距離での高速な鍵生成レートの確認を行うと供に高速・大容量のデータ処理を実現できるプロトタイプシステムの開発を進めた。
- レーザカオスを用いた高速物理乱数を用いたQKD実験に成功した。
- 周波数上方変換型の光子検出器（UCD）の開発をさらに進め、長波長ポンプシステムで低雑音化が可能なことを確認した。
- 単一光子光源を用いた DPS-QKD　方式の無条件安全性を示すことができた。

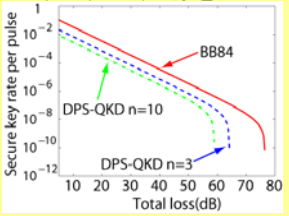


図1、単一光子を用いたDPS-QKDの鍵生成率とBB84の鍵生成率の比較

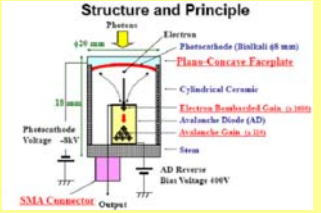


図2：Hybrid photon detectorの構造

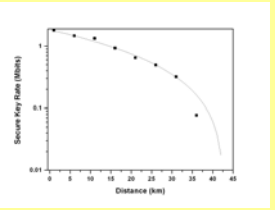


図3：HPDを用いたUCDによる安全鍵生成率と光ファイバ伝送距離

5. これまで得られた成果（特許出願、論文発表等）

	特許出願	論文	研究発表	報道発表
イ 量子暗号ネットワーク技術の研究	35件	55件	58件	8件

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）

ECOC2008（ブリュッセル）にて2件、SECOQC（ウィーン）にて1件発表、UQC2008での講演など

- ECOCにて、NICT、NISTとの連携による世界最速の長距離フィールド実験及び量子鍵の安全性に関して招待講演を行うと共に、量子鍵配付ネットワークの方式提案と実証実験について発表を行った。
- SECOQCにおいて発表を行うことで、ヨーロッパ勢に対し日本の技術力をアピール。
- ICQO08でも量子暗号装置の高速化について招待講演を行い、主にロシア・東欧圏の研究者に日本の技術水準の高さを示した。
- Photonic Westにて量子暗号装置の試験に関する招待講演で標準化に向けた考え方を示した。
- UQC2008において日本における量子鍵配付研究と標準化に向けた活動の報告を行うことで、国際連携に向けたアピールに成功。
- Information security in a quantum world（IQC，カナダ）と量子情報未来テーマ開拓研究会に講師として参加し、委託研究の成果を紹介すると共に、量子暗号研究の活性化に向けて若手研究者にアピールした。

■ イ-１-２：都市圏量子セキュリティ技術（三菱電機株式会社）

SCIS2009暗号と情報セキュリティシンポジウム（滋賀大津）にて2件発表

情報セキュリティの分野で国内で最も権威のあるシンポジウムにて，サブ課題「安全性と新プロトコル提案」の成果として，2件発表した．1件はsquash operatorに関するもので光子検出器不完全さによる安全性証明の不備を解消するもの．もう1件は擬似乱数を用いるプロトコルの脆弱性について指摘したもの．

■ 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）

The Telecommunication Standardization Sector of ITU (ITU-T) together with the Organizaing Committee of the ITU-T "Innovations in NGN" Kaleidoscope Academic Conference Geneva, 12-13 May 2008

国際電気通信連合(ITU)主催の国際会議にて、Differential Phase Shift Quantum Key Distribution と題して最近の NICTでの実験の成果をアピールし、論文賞（second best award)を受賞した。