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）
平成 21 年度	217.3（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（平成 21 年度末までの累計）

特許出願：国内出願　43 件　　外国出願　8 件
外部発表：研究論文　48 件　　その他研究発表　72 件
報道発表　10 件　　展示会　2 件　　標準化提案　0 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

- 微弱コヒーレント光、および平面光回路技術を用いた光干渉システムをベースにした、単一方向型の受動基底選択型量子暗号システムプロトタイプを試作した。
- 平成 20 年度までに課題（イ）①で開発した量子光基板、および制御基板、鍵蒸留基板の FPGA プログラム、（イ）②で開発した同期基板、課題（ア）で開発した光子検出基板を統合し、量子暗号システムとして動作させた。
- 来年度の 8 波長を用いた 1Mbps 暗号鍵生成速度を実現するに当たり、実験 1 波長のシステムにおいて 50km（損失 10dB）を想定した暗号鍵伝送実証実験を行った。
- 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、1.5 um 帯単一光子光源を用いた量子鍵配付実証実験を行った。
- 室内 50 km 光ファイバースプールを用い、暗号鍵伝送評価を行い安全な鍵の伝送が可能であることを実証し、1.3 um 帯で行なわれた既存成果（Toshiba, 2007 年）を凌駕する成果を得た。

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

- 量子信号 8 波長を多重する際の低コスト・簡易制御構成を提案し、原理実証実験を行った。
- 平成22年度の相互接続実証実験の際に使用する鍵管理システムの制御用 GUI の開発を完了した。

③エンタングル光子対量子暗号システム

- 2 波長光子対光源、および情報通信研究機構（NICT）と開発した縺れフォーマット変換技術を用い、空間伝送された偏光状態とファイバ伝送されたTime-bin状態にわたるハイブリッドエンタングルメントを観測し、さらに受動基底選択の光学系を加え実

験室内で20㎞のファイバを用いた空間－ファイバ統合型光子対量子暗号鍵配送システム実証を行った。
- 当システムの鍵データ分析エレクトロニクスについて検討し、FPGA によるデータ収集システムを構築した。

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
- ATCA 搭載のシステム制御基板の開発と量子暗号装置の光学系、電気系との接続試験を実施した。
- 篩い鍵生成 S/W の開発、および量子暗号装置と接続させ基本動作試験を実施した。
- 平成 20 年度までに開発した 100MHz の駆動速度（波長多重の 1 波分に相当）で動作する量子暗号装置とシステム制御基板を用いてシステム試験を実施し、正常動作を確認し、システム性能値(QBER やビットレート等)を実測した。
- デコイ方式を実現するための専用の ATCA 基板製作し、デコイ光源の揺らぎの低減を実現し、安定動作を確認した。
- 量子暗号の鍵蒸留処理のための高速アルゴリズムを新たに開発し、その性能を計算機実験で検証し、PC×1 台で 1Mbps 程度の鍵蒸留処理が可能であることが確認できた。
- ネットワーク内に配置された複数の受信装置に至る経路を選択して量子信号の経路を切り替える方式の実現を目指し、古典・量子の波長多重伝送系に適した波長選択スイッチ（WSS）を基にした経路制御方式を採用し、ATCA 基板への搭載を実施した。

②認証用の鍵管理プロトコル技術
- 量子暗号の安全性を保証するための認証プロトコルを秘匿性増強プロトコルに応用し、秘匿性増強処理にかかる計算時間を大幅に短縮することに成功し、PC×1 台でも 1Mbps 以上のスループットを達成した。

③安全性解析と新プロトコル提案
- 量子暗号の安全性証明のための手法である「squash 演算子」の性質を、光検出器の対称性に着目して解析し、単一モードの検出器のみならずマルチモードの光検出器に対しても、squash 演算子の手法が適用できることを証明した。

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
- 来年度のフィールドデモンストレーションに向けて、ハードウェア(FPGA) とソフトウェアを組み合わせた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 100km の敷設ファイバ(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。

- ビットエラーシンドロームの情報も出力する仮想プロトコルのための量子回路を提案し、それが相補性に基づく証明に矛盾なく当てはめることを示すことにより、相補性に基づく証明はシンドロームを暗号化しなくても成り立つことを示した。

②周波数上方変換型単一光子検出システム

- 1810nm 励起による 1550nm→830nm 波長変換を利用するラックマウントタイプの 1.54㎜ 帯検出装置 2 セットを作製し、特性が向上したモジュールを作製することができた。

③高速型可視域光子検出器

- 電子冷却装置を一体化した HPD のモジュール化を完了し、本検出器を周波数上方変換器と結合して、数 GHz 程度の高速クロックの QKD システムに適用可能な通信波長帯光子検出器を構築する見通しを得た。

● **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下、設計/製造/評価を行った。単体動作評価を行い、XFP インタフェースを介した NEC 装置との接続動作検証、PCI-Express を介した NTT 装置との接続動作検証を完了した。

<u>処理の切り分け</u>

- 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

<u>最大符号長</u>

- 1Mbit

<u>インタフェース</u>

- 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ための情報(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、平成 22 年 10 月の量子暗号ネットワークデモンストレーションに向けて、NICT 量子 ICT グループと NP 参加 3 社とで協力して小金井‐大手町‐白山‐東大間 JGN-II の回線調査を行い、これらのファイバを利用して実験を行う際のネットワークトポロジーを検討、鍵管理・回線監視・暗号化通信等の機能を持った量子暗号ネットワークの構築方式を決定した。

また、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)の報告を受け、課題ア、イで共同して評価に当たっている。

（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。）