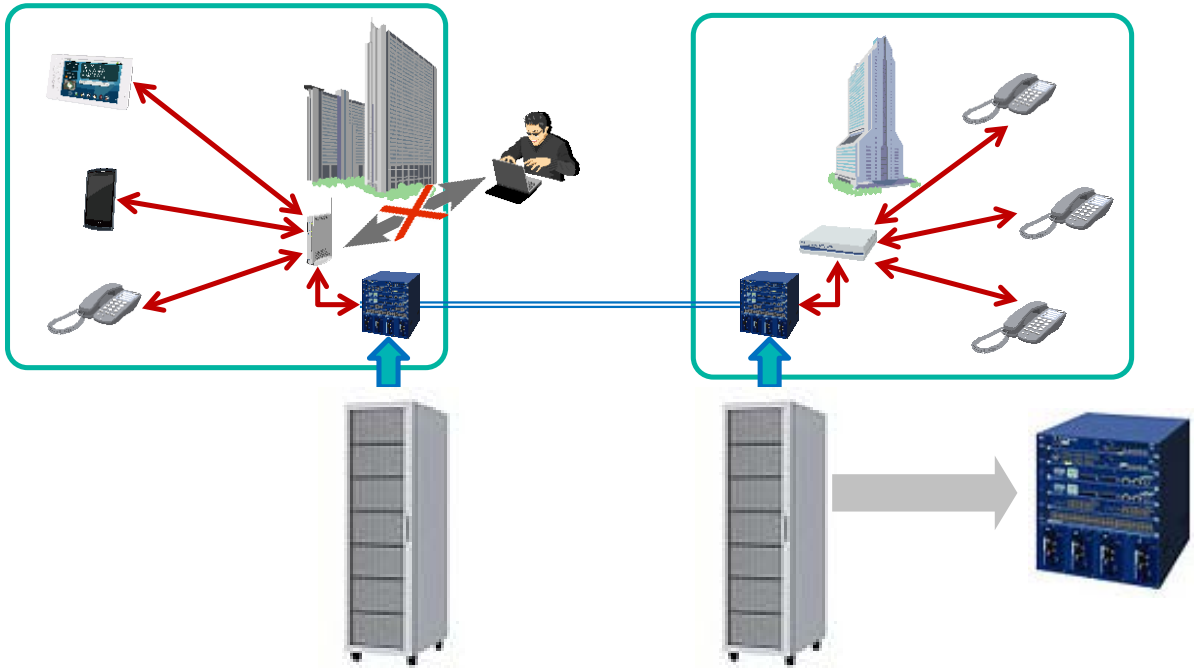
平成24年度「セキュアフォトニックネットワーク技術の研究開発」
課題ア　量子鍵配送ネットワーク制御技術
安全な通信網の構築に向けた量子鍵配送技術

1．実施機関・研究開発期間・研究開発費

■実施機関　　日本電気株式会社（幹事者）
■研究開発期間　　平成23年度から平成27年度（5年間）
■研究開発費　　総額 441百万円（平成24年度94百万円）

2．研究開発の目標

研究開発課題全体の目標としては、物理的安全性が理論的に保証された量子鍵配送技術をベースとして50km圏内の都市圏ファイバネットワーク上に量子鍵配送ネットワークを構築し、500kbps以上の速度で半年以上にわたって鍵を生成し続け長期運転実績を積むと共に信頼性の確立を行う。
そのため、量子鍵配送ネットワーク制御技術を実現する要件より課題ア「（1）安定化技術　（2）アプリケーションプラットフォームの拡張　（3）次世代量子鍵配送システム技術　（4）長期運用試験」の4つの技術課題を抽出し、研究開発を遂行する。
前年度は、量子鍵配送装置の安定化・小型化に向け、現状装置の課題、対策を明らかにし、さらに長期運転性能のWeb公開に備えて、暗号鍵生成状況公開システムの概要設計を行った。これを基に平成24年度は、安定・小型量子鍵配送装置の設計および試作を行う。また、前年度の設計に基づいて暗号鍵生成状況監視システムを開発し、量子鍵配送装置との連携試験まで完了する。



課題ア-1　安定化技術

課題ア-2　アプリケーションプラットフォームの拡張

課題ア-3　次世代量子鍵配送システム技術

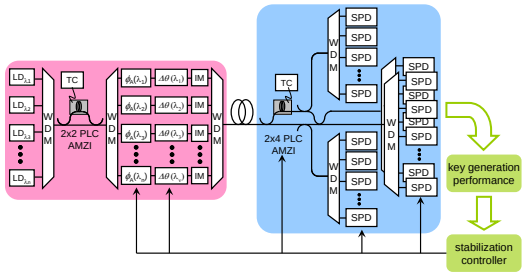
課題ア-4　長期運用試験

セキュアフォトニックネットワークの構築に向けた量子鍵配送技術の高性能化、安定性向上

3. 研究開発の成果

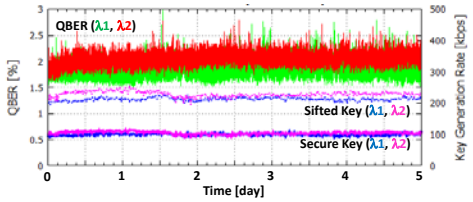
課題ア-1 安定化技術

能動的安定化機能の追加



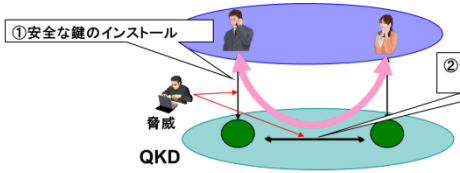
運用中の鍵生成特性を定期的に取得してフィードバック制御を行うことにより、長時間運転中に変動しやすいパラメータを能動的に最適化するソフトウェアを開発した。

安定性評価試験



上記ソフトウェアを用い、フィールドファイバによる安定性評価試験を行った。気温や湿度などが変動した場合にも各種パラメータを能動的に最適化し、安定した鍵生成特性が得られることを実証した。

課題ア-2 アプリケーションプラットフォームの拡張



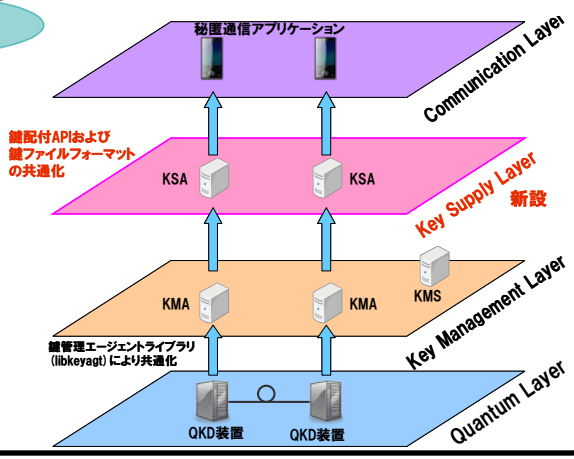
共有鍵を使用できる安全なAP基盤を確立

共有鍵のIDによる管理

アプリケーションプラットフォームのアーキテクチャ設計

鍵供給レイヤーを導入し、汎用的な鍵共有アーキテクチャを定義するとともに、アプリケーションインターフェイス定義。

KSA: Key Supply Agent
KMA: Key Management Agent
KMS: Key Management Server



研究開発成果：安定化技術

【課題】

量子鍵配送装置を長時間にわたって運用する場合、装置設置場所や敷設ファイバの環境条件が変動すると鍵生成特性も変動してしまうという課題があった。H23年度に特定した変動要因の影響を抑制するため、量子鍵配送装置および制御ソフトウェアに対して能動的安定化機能を追加する。さらに、これらの追加機能を評価するための安定性評価試験を行う。

【成果】

能動的安定化機能の追加

- H23年度の研究により鍵生成特性の変動要因であることが判明した下記のパラメータについて、環境変化により最適値が変動した場合にも、運用中の鍵生成特性を定期的に取得してフィードバック制御を行うことにより、能動的にパラメータを最適化するソフトウェアを開発した。
  - 検出器のゲートパルス位相
  - 符号化用変調器のバイアス電圧
  - PLC干渉計の温度
  - 位相補償用変調器の変調振幅

安定性評価試験

- 前述のソフトウェアを用い、NICT小金井～NEC府中事業場間のフィールドファイバによる安定性評価試験を行った。気温や湿度などが変動した場合にも各種パラメータを能動的に最適化し、安定した鍵生成特性が得られることを実証した。

研究開発成果：アプリケーションプラットフォームの拡張

【課題】

量子鍵配送を用いて安全に共有できた鍵を、アプリケーションで利用する際に安全性を劣化させてはならないという課題を解決するため、共有された鍵の安全な管理と、適切な機器に鍵を安全にインストールすることを可能にするアプリケーション基盤を確立。

【成果】

アプリケーションプラットフォームのアーキテクチャ設計

課題エから提供される課題から、「遠隔拠点に属するスマートフォンの安全な鍵設定手法」を、アプリケーションインタフェースとして対応すべきと判断する課題を抽出し、これを実現するためのアプリケーションプラットフォームアーキテクチャを設計した。具体的には、遠隔拠点間の量子鍵配送レイヤーと、鍵管理レイヤー、ならびに鍵供給レイヤーの3つからなるアーキテクチャを考案し、鍵共有レイヤーとアプリケーション間の鍵供給・鍵設定インターフェイスを定義した。鍵供給レイヤーを導入することにより、近地拠点間も遠隔拠点間もトランスペアレントに鍵供給・鍵設定が可能になった。

3. 研究開発の成果

課題ア-3　次世代量子鍵配送システム技術

小型光子検出器の試作および評価

光子検出器は受光素子であるAPDを冷却するための冷却器と、信号処理のための検出回路に分けられる。冷却器は従来の2倍の素子収容効率のものを開発した。検出回路は通信装置の標準的な規格であるATCAシャーシに収容可能な体積比約1/3のものを開発し、大幅な小型化を達成した。

小型光子検出器の安定性向上

上記の試作およびその評価結果を元に、さらに小型・安定な光子検出器の設計を行った。これにより検出回路はさらに2/3に小型化されるとともに冷却器や電源も含めて主要装置は全てATCAシャーシに収納され、安定性・可用性が大幅に向上する。

ATCA
シャーシ

課題ア-4　長期運用試験

光ネットワークテストベッド上での量子鍵配送装置連続運転

NICT小金井～NEC府中事業場間のフィールドファイバ（往復22km）に量子鍵配送装置を組み込み、2週間にわたる連続運転試験を行った。その結果、誤り率が常時2.5%以下の安定した鍵生成を達成した。

暗号鍵生成状況監視ソフトウェアの開発

リモート環境からもインターネット経由により鍵生成速度や誤り率などを監視できるよう、暗号鍵生成状況監視ソフトウェアを開発した。各種気象条件も同時に表示する機能を実装し、環境変動があった場合にも安定して鍵生成を継続できることを実証した。

研究開発成果：次世代量子鍵配送システム技術

【課題】

波長多重量子鍵配送装置では光子検出器の必要数が波長数に比例して増大するため、光子検出器の小型化が課題であった。H23年度の設計に基づいて小型光子検出器の試作・評価を行い、この結果に基づいて安定性を向上させた光子検出器の設計を確立する。

【成果】

小型光子検出器の試作および評価

- 光子検出器は受光素子であるAPDを冷却するための冷却器と、信号処理のための検出回路に分けられる。冷却器は従来1台に2つのAPDを収容する設計であったが、ほぼ同サイズで1台に4つのAPDを収容可能な冷却器を開発した。
- 電源の雑音特性について詳細な評価を行うことにより電源の小型化・共用化を進めた結果、従来と比較して体積が約1/3の検出回路の開発に成功した。検出回路は通信装置の標準的な規格であるATCAシャーシに収容可能なものとした。
- 上記検出回路と冷却器を量子鍵配送装置に組込み、従来の光子検出器と同等の良好な特性を再現性良く得ることができた。

小型光子検出器の安定性向上

- 上記の試作およびその評価結果を基に、さらに小型・安定な光子検出器の設計を行った。これにより検出回路は2/3に小型化されるとともに冷却器や電源も含めて主要装置は全てATCAシャーシに収納され、安定性・可用性が大幅に向上する。来年度に試作予定。

研究開発成果：長期運用試験

【課題】

量子鍵配送の信頼性を確立するためには、実運用に近い環境で長時間にわたる特性評価試験を行う必要がある。H23年度に敷設ファイバ網に設置した量子鍵配送システムを用いて一週間程度の連続運転を行うと共に、H23年度に試作した公開用基盤ソフトウェアにより暗号鍵生成状況監視システムを構築して量子鍵配送システムとの連携試験を行う。

【成果】

光ネットワークテストベッド上での量子鍵配送装置連続運転

- NICT小金井～NEC府中事業場間のフィールドファイバ（往復22km）に量子鍵配送装置を組み込み、2週間にわたる連続運転試験を行った。課題ア-１で開発した能動的安定化ソフトウェアを使用した結果、誤り率が常時2.5%以下の安定した鍵生成を達成した。

暗号鍵生成状況監視ソフトウェアの開発

- 前年度に試作したWeb公開用基盤ソフトウェアにより暗号鍵生成状況監視ソフトウェアを開発した。量子鍵配送システムとの連携試験を行い、インターネットからも鍵生成速度や誤り率などを監視できるシステムを構築した。
- 各種気象条件も同時に表示する機能を実装し、環境変動があった場合にも安定して鍵生成を継続できることを実証した。

4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
新世代ネットワークを支えるネットワーク仮想化基盤技術の研究開発	0 (0)	0 (0)	0 (0)	7 (6)	0 (0)	0 (0)	0 (0)

5. 研究成果発表会等の開催について
（1）国際学会における発表

2012年7月6日　OECC2012 “Field Demonstration of High-speed Wavelength-division Multiplexing Quantum Key Distribution System and its Stabilized Operation” を発表
2012年8月2日　QCMC2012 “WDM quantum key distribution system using dual-mode single photon detectors”を発表
2012年9月13日　QCRYPT2012 “Real world challenges for Quantum key distribution”を発表（パネルディスカッション）

6. 今後の研究開発計画
この成果により、今後、どのような研究を行うのかを例示を上げながら、具体的、かつ簡潔に記載して下さい。

課題ア-1　安定化技術

暗号鍵生成性能の変動要因解析を元に能動的安定化技術を確立し、平成25年9月までに、例えば情報通信研究機構　本部（小金井）－NEC府中事業場間の往復22kmリンクにおいて、量子誤り率を常時3.0%以下に保持できる性能を実現する。

課題ア-2　アプリケーションプラットフォームの拡張

前年度までに本課題で検討した技術を課題エの中で具体化する。

課題ア-3　次世代量子鍵配送システム技術

前年度に試作および動作確認を完了した1波長分の小型検出器を使用し、単一波長に関しては最終目標に相当する性能を達成する。また、デバイス故障確率の低減や装置の自動初期化、保守・運用時の利便性向上のため、より小型で可用性、操作性の優れた光子検出器を試作する。これらの評価結果を元に雑音対策などについて検討し、光子検出器の設計を確立する。

課題ア-4　長期運用試験

光ネットワークテストベッドJGN-X等の敷設ファイバ網において、微弱コヒーレント光を用いた波長多重量子鍵配送システムを使用し数週間単位での連続運転を繰り返すと共に、暗号鍵生成状況監視システムの試験稼働を開始する。