平成２４年度研究開発成果概要書
セキュアフォトニックネットワーク技術の研究開発（157 ア 0101）
課題ア　量子鍵配送ネットワーク制御技術
副題　量子鍵配送システムの実環境での信頼性向上とアプリケーションの拡張

（１）研究開発の目的

量子鍵配送ネットワークの信頼性技術開発と試験を進めるとともに、新しいネットワーク制御技術や安全性評価技術に基づいた研究開発を行う。これにより、量子暗号装置の信頼性の実証とセキュアフォトニックネットワーク構築の可能性を実証する。量子鍵配送技術のアプリケーション拡張も実現する。

（２）研究開発期間

平成２３年度から平成２７年度（５年間）

（３）委託先

三菱電機株式会社

（４）研究開発予算（百万円単位切上げ）

| | |
|---|---|
| 平成２３年度 | ３５（契約金額） |
| 平成２４年度 | ３３（　〃　） |
| 平成２５年度 | ３１（　〃　） |
| 平成２６年度 | ２９（　〃　） |
| 平成２７年度 | ２８（　〃　） |

（５）研究開発課題と担当

課題ア：量子鍵配送ネットワーク制御技術
ア-１．安定化技術（三菱電機株式会社）
ア-２．アプリケーションプラットフォームの拡張（三菱電機株式会社）
ア-４．長期運用試験（三菱電機株式会社）

（６）これまで得られた研究開発成果

（累計）１２件　（当該年度）６件

| | | | |
|---|---|---|---|
| 特許出願 | 国内出願 | 2 | 2 |
| | 外国出願 | 0 | 0 |
| 外部発表 | 研究論文 | 1 | 1 |
| | その他研究発表 | 7 | 3 |
| | プレスリリース | 0 | 0 |
| | 展示会 | 2 | 0 |
| | 標準化提案 | 0 | 0 |

具体的な成果

(1)光子検出器のノイズ解析と正弦波遅延フィルタでの同期検出の提案

光子検出器のノイズ解析を実施した。ノイズレベルを理論的下限程度に抑えることを目標として、熱雑音やアンプノイズなど各ノイズ源を定量的に解析した。アバランシェ信号の効率的抽出とノイズ低減による検出率の向上を目指した新たな方式を提案した。また新たな誤り訂正方式として、光子検出器の補助情報を用いた軟判定復号をする方式を提案した。

(2)偏波補償技術の実装により通信路特性の変動への耐性を向上

量子暗号を実運用環境へ適用するために必要な技術として、当社従来の古典光を用いた動的補償に加え、偏波無依存化による静的補償技術（偏波無依存化技術）の原理検証を行った。

(3)携帯電話ソフトウェア及び鍵配送 I/F の詳細仕様の作成

H23 年度に実施した調査結果を元に、Android OS 上で動作可能なワンタイムパッド携帯電話ソフトウェアの詳細仕様の設計を行った。さらに、異なる量子暗号装置から、様々なアプリケーションへ量子鍵の配送ができる共通 I/F を設計し、共通 I/F の内容をワンタイムパッド携帯電話ソフトウェアの仕様に適用した。

（７）研究開発イメージ図

別添のイメージ図の通り。

# 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」の研究開発目標・成果と今後の研究計画

## 1. 実施機関・研究開発期間・研究開発費

◆実施機関　　三菱電機株式会社
◆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155百万円（平成24年度　33百万円）

## 2. 研究開発の目標（平成28年3月末）

量子鍵配送ネットワークの信頼性技術開発と試験を進めるとともに、新しいネットワーク制御技術や安全性評価技術に基づいた研究開発を行う。これにより、量子暗号装置の信頼性の実証とセキュアフォトニックネットワーク構築の可能性を実証する。量子鍵配送技術のアプリケーション拡張も実現する。

## 3. 研究開発の成果

最終目標

### ア-1. 安定化技術、ア-4. 長期運用試験

・敷設ファイバ25kmでQBER 3%以下で安定に100kbps鍵生成
・実環境において数ヶ月程度の連続運転により長期間運用

**ア-1. 安定化技術**

検出タイミングのずれ


偏波の揺らぎ

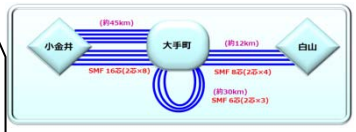
・自動補償
・モニタ・リカバリ
・鍵蒸留処理の効率化

量子暗号装置

・能動的安定化技術
・フィードバック制御
・長期フィールド検証

**ア-4. 長期運用試験**

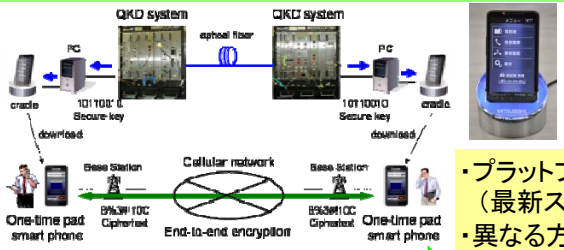
敷設光ファイバ設備（JGNX）




・通信路での短長期変動の解析
・装置性能への影響解析
・隣接ファイバの漏れ光解析

### ア-2. アプリケーションプラットフォームの拡張

・量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェアを、スマートフォンOSとしてシェアが最も高いAndroid上で実現し、フィールドで検証






・プラットフォーム拡張
（最新スマートフォンOSAndroidで実現）
・異なる方式やメーカーの量子暗号装置で使用可能な鍵出力インターフェース

量子暗号のスマートフォン応用

H24年度研究開発成果

**研究開発成果：光子検出器のノイズ解析と正弦波遅延filterでの同期検出**

量子鍵配送システムにおいて安定して鍵生成を実現するためには、光子検出器における信号とノイズの厳密な評価と特性向上が不可欠である。

●本研究開発では、光子検出器のノイズ解析を実施した。具体的には、ノイズレベルを理論的下限程度に抑えることを目標として、熱雑音やアンプノイズなど各ノイズ源を定量的に解析した。また正弦波遅延filterでの同期検出方式を提案した。
●いわゆる「有限長効果」を考慮した安全性証明を与え、従来より厳密な安全性を保証しつつも通信測度を向上させた。また軟判定復号と光子検出器の補助情報を用いた、新たな誤り訂正方式を提案した。

**研究開発成果：偏波補償技術実装による通信路特性変動への耐性向上**

実運用環境へ適用するために通信路での変動がある場合の安定化が課題である。

●本研究開発では、当社従来の古典光を用いた動的補償に加え、偏波無依存化による静的補償技術（偏波無依存化技術）の原理検証を行った。
●今後、周辺温度の影響の検証とその制御方式の改良、さらに安定性試験行う。

**研究開発成果：携帯電話ソフトウェア及び鍵配送I/Fの詳細仕様の作成**

配送した鍵の使い道となるキラーアプリケーションの開発は重要である。スマートフォンの音声通話の盗聴を防止するため、量子鍵配送により共有した鍵を用いて携帯端末間のEnd-to-Endで通話内容を暗号化する機能を開発する。

●異なる量子暗号装置から、様々なアプリケーションへ量子鍵の配送ができる共通I/Fを検討し、Java及びC言語用の仕様を作成した。
●H23年度に実施した調査結果を元に、Android OS上で動作可能なワンタイムパッド携帯電話ソフトウェアの詳細仕様を設計し、上記の共通I/Fを仕様に適用した。
●今後、今年度作成した仕様に従い、他社の量子暗号装置から共通I/Fにより量子鍵が受けられる携帯電話ソフトウェアの開発を行う。

## 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 | 国際会議予稿 | 収録論文 | その他研究発表 | プレスリリース | 展示会 | 標準化提案 |
|---|---|---|---|---|---|---|---|---|---|
| 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 | 2（2） | 0（0） | 1（1） | 0（0） | 0（0） | 7（3） | 0（0） | 2（0） | 0（0） |

## 5. 研究成果発表会等の開催について

### （1）NICT委託研究「セキュアフォトニックネットワーク技術の研究開発」の各課題関係者が年 数回開催される全体会議で議論を行い連携を強化

NICT 量子ICTグループ関係者、「セキュアフォトニックネットワーク技術の研究開発」受託機関 （課題ア：NEC、東芝、三菱電機、課題イ：NTT、三菱電機、東工大、東北大、北大、課題ウ：学習院大、東北大、課題エ：NEC、北大）が一同に会し、最新の研究進捗を紹介や今後の計画説明、国内外の研究開発動向分析と今後の連携や分担など開発戦略立案を議論している。特に、成果紹介は守秘義務対象とし、学会等ではできない議論を展開し、連携を密に進めている。

## 6. 今後の研究開発計画

国プロ受託機関などにより敷設ファイバ上の長期安定性試験データが蓄積され、その解析が進むにつれ、装置を構成する各コンポーネントの特性変動や新たな故障、障害事例などが明らかになりつつある。一方、量子暗号の実利用に関する研究により、具体的な要求仕様が明らかになりつつあり、新たな保全技術の開発が必要になることが分かってきた。

このような動向を踏まえ、平成25年度は、単なる鍵配送速度や誤り率の数値的改善ではなく、故障や障害要因をより明確に特定できるようにするため、光子検出部や信号変調部など重要コンポーネントの評価系を構築し、故障率を定量化するとともに効果的な信頼性向上策を導出することを目標とする。具体的には、光子検出器の信頼性評価系の構築と信頼性向上策の導出と、偏波補償技術開発を行う計画である。前者は、光子検出器の評価系を構築し、環境変動と光子検出器の特性の相関を明らかにして、信頼性や故障原因に関する知見を蓄積することを目指す。また、後者は、光源や位相変調器の特性変動を詳細に評価し、これらのコンポーネントの不完全性が量子誤り率に与える影響を評価するものである。

アプリケーションプラットフォームの拡張においては、「鍵蒸留アルゴリズムの効率化」を引き続き行う。また「携帯電話ソフトウェア」を行い、Android上で動作するワンタイムパッド携帯電話ソフトウェアのデモ試作を行う計画である。