# 平成23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23年度　35百万円）

## 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

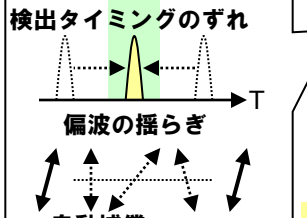
研究開発最終目標

H23年度研究開発成果

### 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**



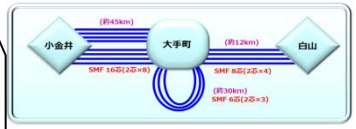

・自動補償
・モニタ・リカバリ
・鍵蒸留処理の効率化

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

**研究開発成果：性能をモニタするソフトウェア試作と自動補償の仕様検討**

量子鍵配送システムはまだ短期間での連続試験のみで、現実的な環境下での運用実績が乏しいことが課題。また、伝送路等の周辺環境に特性変動があっても、安定して鍵生成ができることや、敷設光ファイバ網での長期試験評価が不可欠。

●本研究開発では、装置の要素技術として、性能をモニタする試験環境用のソフトウェア試作を実施した。また、装置や伝送路等の周辺環境変動の影響によるタイミングずれや偏波揺らぎをモニタし自動補償する機能の仕様検討を実施した。また、特性変動の影響を受けにくい光学系の検討を実施した。

●鍵蒸留アルゴリズムの効率化では、LDPC符号を用いた再送方式をPCに実装し性能評価を実施した。また軟判定復号を適用した新しい方式を開発した。

**研究開発成果：受信側装置の小型一体化試作**

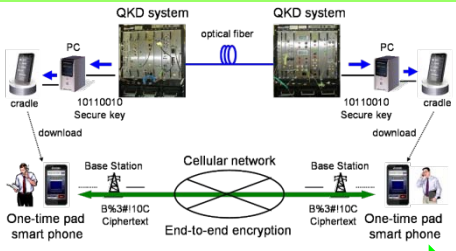
長期間連続試験での通信路・装置等の変動観測と性能への影響解析が課題。

●本研究開発では、敷設光ファイバ網での試験で測定すべき項目や装置に必要な機能の検討整理を実施した。また、フィールド試験の作業効率向上のため、受信側装置の小型一体化試作を実施した。

●今後、伝送路特性評価と試験環境の構築準備を行う。

### 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




量子暗号のスマートフォン応用

・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

**研究開発成果：Android OS上での携帯電話ソフトウェアの仕様検討**

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。

●暗号化機能のプラットフォーム拡張のため、最新の携帯電話OS Android上でのワンタイムパッド携帯電話ソフトウェア実装の予備調査と仕様検討を実施した。

具体的には、Android標準暗号フレームワーク上で動作する暗号ライブラリ、量子鍵転送機能のAndroid上とPC上ソフトウェア、Android上のスピーカなどを含む周辺装置制御方式、Android上での音声コーディングライブラリなどの要素技術に関する実装上の問題点の有無の調査と、ソフトウェアの仕様検討を実施した。

●今後、H23年度に実施した仕様検討で明らかになった問題点の解決方式や鍵転送方式、鍵の保存方法等の検討を行い、設計に反映させる。

## 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 |
|---|---|---|---|---|---|---|---|
| セキュアフォトニックネットワーク技術に関する研究開発 | 0<br>(0) | 0<br>(0) | 0<br>(0) | 4<br>(4) | 0<br>(0) | 2<br>(2) | 0<br>(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ICTG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、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

敷設ファイバにおいて安定に鍵生成ができる量子暗号装置を実現し、長期運用試験で実運用評価を行う。具体的には以下の研究開発を行う。

・安定化技術においては、①性能をモニタ管理するモジュールの開発、②伝送路等の周辺環境の特性変動による検出タイミングずれや偏波の揺らぎなどを自動補償する能動的な安定化技術装置の開発、を行う。また、鍵蒸留アルゴリズムの効率化では、誤り訂正や秘匿性増強のアルゴリズムの効率化によりデータ処理をすべてソフトウェア上で高速に実現することを目指す。

・長期運用試験においては、敷設光ファイバ網JGN-Xでの伝送路特性評価を、また量子鍵配送装置を設置して長期運用試験を行い、通信路、装置等
の特性変動の観測、装置性能への影響解析を実施する。

また、アプリケーションプラットフォームの拡張においては、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最新のAndroid OS上で開発し、フィールド環境下での検証により安定動作を確認する。