平成25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）
◆研究開発予算　　総額156百万円（平成25年度　31百万円）

2. 研究開発の目標

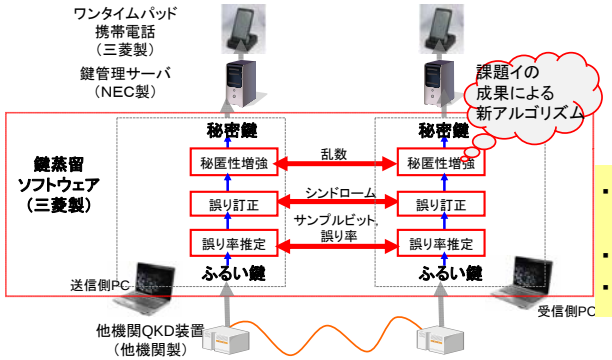
量子鍵配送ネットワークの信頼性技術開発と試験を進めるとともに、新しいネットワーク制御技術や安全性評価技術に基づいた研究開発を行う。これにより、量子暗号装置の信頼性の実証とセキュアフォトニックネットワーク構築の可能性を実証する。量子鍵配送技術のアプリケーション拡張も実現する。

3. 研究開発の成果

最終目標

ア-1. 安定化技術

・鍵蒸留処理を完全ソフトウェア(SW)化、および委託研究各機関のQKD装置に共通して適用可能な汎用SW開発

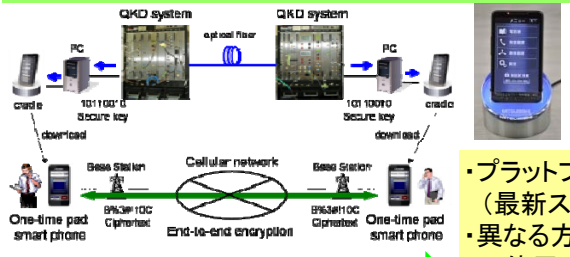


・高速化
（アルゴリズム改良）
・汎用ソフトウェア
・各QKD装置への適用検討

鍵蒸留アルゴリズムの改良と汎用ソフトウェアの開発

ア-2. アプリケーションプラットフォームの拡張

・ワンタイムパッド携帯電話SWを、Android上への移植し、携帯キャリアネットワークでの安定動作検証。任意QKD装置からの共通I/F開発検証



・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

H25年度研究開発成果

研究開発成果：鍵蒸留汎用ソフトウェア開発と他機関装置への適用検討

量子鍵配送システムにおいて、鍵蒸留処理を、専用ハードウェアを用いずにソフトウェアのみで低コストかつ高速に実現することは必須である。

●本研究開発では、最新の安全性証明の知見による不要な処理の削減や秘匿性増強の高速アルゴリズムなど課題イ（理論）の成果によるアルゴリズム改良や、マルチコアCPUによる並列化を行い、QKD装置に共通して適用可能な汎用ソフトウェアを開発した。またH25年度はDPS-QKD装置適用のための開発を実施した。

研究開発成果：光源と伝送路の偏波変動が与える影響調査と対策の検証

実運用環境適用のために通信路や光源での変動下での安定化が課題である。

●本研究では、光源と伝送路の偏波変動がQKD装置へ与える影響を調査し、偏波無依存化技術を送信側干渉計にも適用すると改善することを実験で検証した。
●今後、測定データを増やし、詳細な解析評価を行う。

研究開発成果：携帯電話ソフトウェア試作とキャリアネットワーク上の検証

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。

●本研究では、H24年度に実施した詳細仕様の設計のもとに、ワンタイムパッド携帯電話ソフトウェアのAndroid上への移植（試作）を実施した。また、携帯キャリアネットワークでの基本的な動作検証を実施した。
●また、異なるQKD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、携帯電話ソフトウェアの仕様に適用し、開発と動作検証を実施した。
●今後は携帯電話ソフトウェアの、より現実的な環境での活用を目指す。具体的には、①複数の携帯電話サービスの比較調査により安定通話に最適なサービスの選択、また②携帯電話ソフトウェアを改良して、安定した通話の実現。

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の研究開発　課題ア	5（3）	0（0）	2（1）	11（3）	3（0）	2（0）	0（0）

5. 研究成果発表等について

（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

各課題ア、イ、ウ、エの受託チームやNICTとの連携により、敷設ファイバ上での長期安定性試験のデータが蓄積され、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、NICTが中心になって行った量子鍵配送ネットワーク技術の実利用に関する調査研究によって、より具体的な要求仕様が明らかになりつつあり、より現実のシステムに即したかたちで、かつ、安定して動作する装置の開発が早期に望まれる状況となっている。

このような動向を踏まえ、平成26年度は、鍵蒸留方式の最適化を進めると共に、課題受託チーム間の研究成果を共有することで開発の加速を推し進めるべく、鍵蒸留ソフトウェアの汎用化と他チームQKD装置での実証動作を目標とする。さらに、秘匿携帯電話のより現実的な環境での活用を目指して、移動体通信に特有のハンドオーバーや通信品質の劣化などを克服し、公衆網においての安定動作を目標とする。

具体的には、鍵蒸留アルゴリズムの効率化においては、課題イの理論的成果をふまえ、秘匿性増強と誤り訂正のアルゴリズムを見直し、最適な鍵蒸留方式を提案する。そして課題ア、ウの量子暗号装置と接続して動作させることを想定して、ソフトウェア実装を行う計画である。また、携帯電話ソフトウェアに関しては、Android端末へ移殖したワンタイムパッド携帯電話の試作ソフトウェアに関して、より現実的な環境での活用を目指す。より詳細な内容は次の通り。①複数の携帯電話サービスの比較調査を行い、ワンタイムパッド携帯電話の安定通話に最適なサービスを選択する。②選択したサービスに合わせてワンタイムパッド携帯電話ソフトウェアを改良して、安定した通話を実現する計画である。