研究開発成果概要図 （目標・成果）

1. 研究課題・実施機関・研究開発期間

◆課題名　　：セキュアフォトニックネットワーク技術の研究開発
◆個別課題名　：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
◆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）

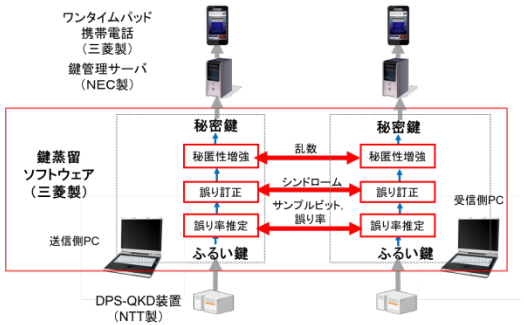
2. 研究開発の目標

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

ア-1. 安定化技術

・処理速度と安全性を保ちつつ、鍵蒸留処理を完全ソフトウェア化
・他機関製の量子暗号装置に適用し、鍵蒸留処理が正常実行されることを確認



従来、鍵蒸留処理には専用ハードウェアが必須とされていた

課題イの成果を活用することにより
・秘匿性増強アルゴリズムの改良
・処理フローの見直し
を実施し、鍵蒸留処理を完全ソフトウェア化した。これにより量子暗号システムの低コスト化、汎用化が実現できる。

鍵蒸留ソフトウェアの開発

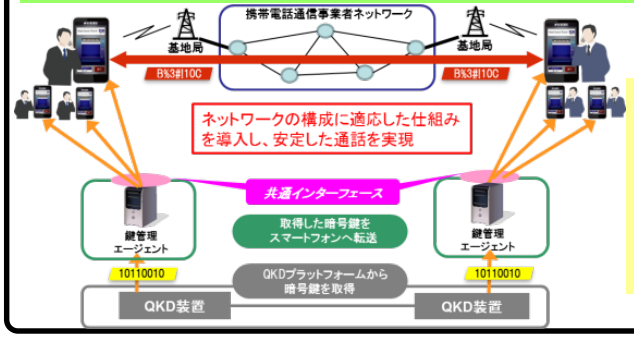
量子暗号通信を成立させ、無条件安全性を保証するためには「鍵蒸留処理」と呼ばれるデータ処理が不可欠である。我々はこの鍵蒸留処理を、全てPC上で実行できる「鍵蒸留ソフトウェア」を開発した。

2010年以前の量子暗号システムでは、鍵蒸留処理のために専用のハードウェアを開発することが一般的だった。これに対し我々は、処理フローの見直しを行い、課題イ－２－2による新アルゴリズムを採用することにより、鍵蒸留処理にかかる計算量を大幅に削減させた。その結果、従来の専用ハードウェアは不要となり、鍵蒸留処理をすべてPC上のソフトウェアで実行できることとなった。

また、現実の装置によって検証するために、実際の量子暗号システムに本ソフトウェアを組み込み、鍵蒸留処理がリアルタイムで正しく実行できることを確認した。これは、量子暗号システムの低価格化と小型化につながる成果である。

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向けに改良し、鍵供給IFを共通化
・フィールドでの通話品質調査を行い、安定して通話できることを確認



- ワンタイムパッド携帯電話SWをAndroid向けに改良
- 量子鍵配送装置からアプリケーションへの鍵供給インタフェースの共通化
- フィールド環境下での動作検証と通話品質調査

ワンタイムパッド携帯電話ソフトウェアの拡張開発及び安定通話の検証

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。本課題においては、以下の成果を達成した。

- Windows Mobile向けであったワンタイムパッド携帯電話ソフトウェアをAndroid向けに改良した。
- 量子鍵配送装置からアプリケーションに鍵を供給する際に利用するための共通インタフェースの仕様をNEC殿と共に検討した。検討したインタフェースをワンタイムパッド携帯電話アプリケーションに適用した。
- 現実的な環境下における通話安定化を目的として、ワンタイムパッド携帯電話の試作ソフトウェアの通話品質を調査した。その結果、携帯電話網への接続に問題のないエリアにおいては、問題なく通話可能であることを確認した。