平成27年度研究開発成果概要図 （目標・成果と今後の成果展開）

採択番号：157ア0101

1. 研究課題・実施機関・研究開発期間・研究開発予算

◆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）
◆研究開発予算：総額１１７百万円（平成２７年度６百万円）

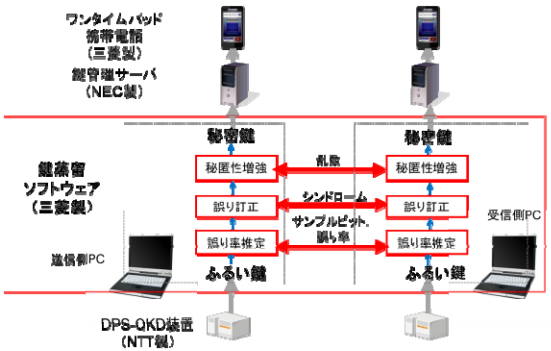
2. 研究開発の目標

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

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。

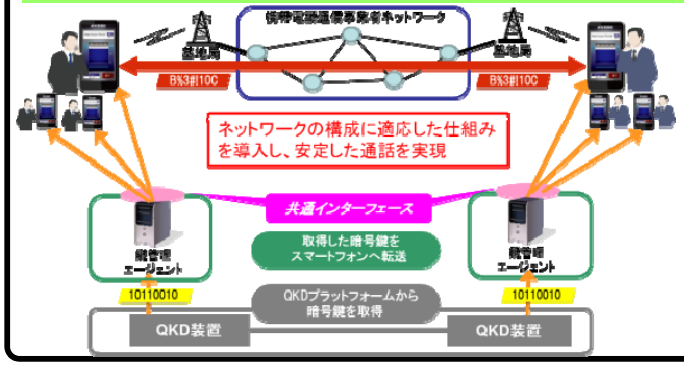
鍵蒸留ソフトウェアの開発

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が、この処理には専用のハードウェアが必要だと考えられていた。これに対し我々は、課題イの成果を有効活用してアルゴリズムの見直しを行い、鍵蒸留処理を完全ソフトウェア化することに成功した。

そして昨年度には、その鍵蒸留ソフトウェアをNTT製量子暗号通信装置（DPS-QKD装置）と接続し、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。さらに今年度は同じ構成における連続動作試験を実施し、長時間安定動作を実現するための改良を行った。

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による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



- フィールド環境下での動作検証と通話品質調査
- 携帯電話網の接続に問題ないエリアで、安定した通話ができることを確認
- 通信遅延量の解析を行い、通信パケットの損失は発生しているが通話品質への影響は軽微であると確認

ワンタイムパッド携帯電話ソフトウェアのフィールドでの通話品質調査

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した。今年度は、以下の成果を達成した。

- 三菱電機居室での通話品質を基準とし、送受信者が数百km以上離れた環境、高層階や地下、通信回線が混雑している環境、ハンドオーバー発生時、といった各環境で通話品質を調査した。結果、携帯電話網への接続に問題のないエリアでは、良好な通話品質であることを確認した。
- 各環境での通信遅延量の解析から、パケット損失は通話者が知覚できない頻度でしか発生していないと結論した。

4. これまで得られた成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース報道	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（0）	2（1）	2（0）	11（0）	4（0）	6（2）	0（0）

※成果数は累計件数、（ ）内は当該年度の件数です。

（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、最新の研究進捗の紹介や、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た。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た。

（2）UQCC2015 / Qcrypt2015にて量子携帯電話の通話デモンストレーションとポスター展示を実施し量子暗号アプリケーションを国内外にアピール

UQCCとは、NICT主催による量子暗号と量子通信を対象とした国際会議である。UQCC2015は、量子暗号の国際会議であるQcrypt2015と合同で開催された。両会議にて量子暗号のアプリケーションであるワンタイムパッド携帯電話の展示及び公衆網を用いた通話のデモンストレーションを実施した。本委託研究成果により量子暗号の実用化に大きく近づいたことを、国内外の量子暗号・量子通信研究者やマスメディアに対して大々的にアピールした。

UQCC2015 : Updating Quantum Cryptography and Communications 2015
Qcrypt2015 : 5th International Conference on Quantum Cryptography

5. 研究開発成果の展開・普及等に向けた計画・展望

鍵蒸留ソフトウェアについては今後も、連続動作試験を継続するとともに、年単位での安定動作を実現するための改良を続けていきたい。また開発したソフトウェアを、他の研究機関も活用できるよう、オープンソース化にむけて努力したい。

ワンタイムパッド携帯電話アプリケーションについては、本課題の成果や検討内容を他のアプリケーション開発に活用することを想定している。例えば、量子鍵配送装置からアプリケーションに鍵を供給するための共通インタフェースについては、他の研究機関がアプリケーションを開発する際に活用することが可能である。また、ワンタイムパッド携帯電話アプリケーションは、暗号鍵の取得手段を量子鍵配送装置に限定するものではなく、量子鍵配送以外の鍵取得方法との組み合わせが可能である。そこで、量子鍵配送以外の鍵取得方法との組み合わせにより、新たな応用を検討していきたいと考えている。