平成26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・研究開発予算

◆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26年度　13百万円）

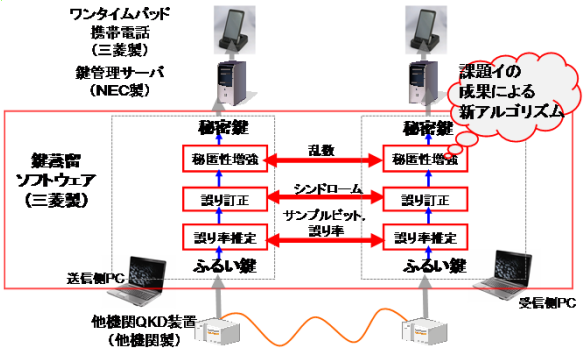
2. 研究開発の目標

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する
・得られた成果を他機関製の量子暗号装置に適用する



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

完全ソフトウェア化による低コスト化、汎用化の実現
・秘匿性増強アルゴリズム改良（課題イの成果を活用）
・マルチコアCPUによる並列化
汎用性を生かし、他機関量子暗号装置への適用を検討する

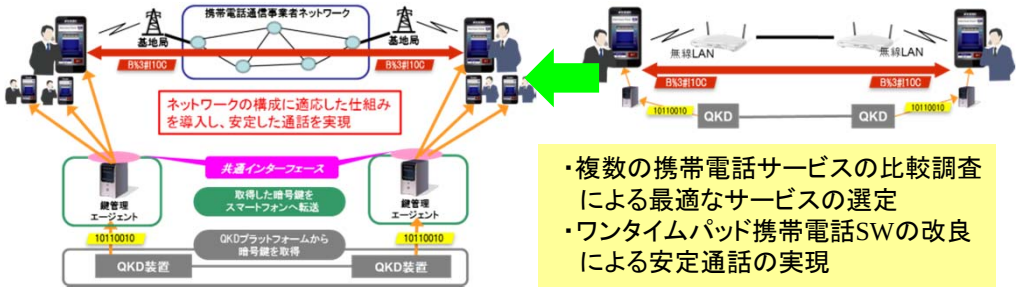
研究開発成果：
鍵蒸留ソフトウェアの開発、およびNTT製量子暗号装置との連係動作

鍵蒸留処理を、専用ハードウェアに頼らずソフトウェアのみで実装することにより、量子暗号システムの低コスト化が期待できる。この目標のため、本研究課題では今年度、以下の研究開発を実施した。

- 鍵蒸留アルゴリズムの高速化のための理論検討を実施し、その成果を踏まえた鍵蒸留ソフトウェアを開発した。
  ここで課題イで得られた理論的成果を活用することにより、現状で最適のアルゴリズムを選定することに成功した。
- 上記で開発したソフトウェアを、NTT製量子暗号装置（DPS-QKD装置）と接続し、鍵蒸留処理の動作検証を実施した。結果として、DPS-QKD装置のふるい鍵を、完全ソフトウェア処理により、リアルタイムで鍵蒸留できることが確認できた。

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による安定通話を実現可能な携帯電話サービスを調査。サービスの選定とSW改良による安定通話の実現。



・複数の携帯電話サービスの比較調査による最適なサービスの選定
・ワンタイムパッド携帯電話SWの改良による安定通話の実現

研究開発成果：
携帯電話ソフトウェアに適したサービス選択による通話安定化検討

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。

- 本研究では、H25年度にAndroid上への移植を実施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、以下を実施した。
  ①複数の携帯電話サービスの比較調査によりワンタイムパッド携帯電話ソフトウェアの安定通話に最適なサービスの選択、また②ワンタイムパッド携帯電話ソフトウェアを選択したサービスに改良して、安定した通話の実現。
- 今後は携帯電話ソフトウェアの、より現実的な環境での通話安定化を目指す。具体的には、通話を行う場所や周囲の環境（屋内、屋外）など、Android端末の通信状態に影響があると思われる状況下で正しく通話できることを確認する。

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（1）	0（0）	2（0）	11（0）	4（1）	4（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。

5. 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27年度は、まず課題アで開発中の量子暗号装置に対する有限長解析、および課題ア、ウの装置むけの秘匿性増強アルゴリズムの最適化を実施することにより、実環境における安全性の向上を目指す。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、課題アで開発中の量子暗号装置に対し、有限長効果を考慮した安全性解析を実施する。また課題ア、ウで開発中の量子暗号装置における使用を想定して、秘匿性増強アルゴリズムを最適化する。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通信安定化を目指す。具体的には、通話を行う場所や周囲の環境（屋内、屋外）など、Android端末の通信状態に影響があると思われる状況下で通話の確認を行い、正しく通話できることを確認する。通話状態が良好でない状態については、対策を検討する計画である。