平成 26 年度研究開発成果概要書

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
採択番号　：157 エ 01
個別課題名：課題エ　セキュアフォトニックネットワークアーキテクチャ
副題　　：量子暗号技術を活用した安全な通信網の構築技術の研究

（1）研究開発の目的

情報の安全な共有を実現するための基盤としてのセキュアフォトニックネットワークを構築するにあたっては、安全な通信網の構築技術として、量子鍵配送ネットワーク制御技術、量子暗号安全性評価論、連続量量子鍵配送技術及びその他、最新のネットワーク理論、認証技術等の周辺関連技術を有機的に融合させ、高度化、多様化している盗聴攻撃や撹乱法に対抗可能なセキュアなネットワークアーキテクチャの研究開発を実施する必要がある。このため、量子暗号技術の安定化等の研究を進めるとともに、実際の環境における周辺関連技術との融合、動作検証等を実施し、各種研究成果を有機的に融合させセキュアなネットワークアーキテクチャとして確立する必要がある。

（2）研究開発期間

平成 23 年度から平成 27 年度（5 年間）

（3）実施機関

日本電気（株）＜代表研究者＞、国立大学法人北海道大学

（4）研究開発予算（契約額）

総額 211 百万円（平成 26 年度 58 百万円）
※百万円未満切り上げ

（5）研究開発課題と担当

課題エ：セキュアフォトニックネットワークアーキテクチャ
1. ベースラインモデルの研究（日本電気（株））
2. 周辺関連技術の適用研究（日本電気（株））
3. 量子暗号技術の適用研究（国立大学法人北海道大学）
4. 環境構築／動作検証（日本電気（株））

（6）これまで得られた成果（特許出願や論文発表等）

		累計（件）	当該年度（件）
特許出願	国内出願	1	0
	外国出願	0	0
外部発表	研究論文	1	0
	その他研究発表	22	7
	プレスリリース・報道	2	1
	展示会	1	1
	標準化提案	0	0

（７）具体的な実施内容と成果

⑴ 日本電気（株）

・（ベースラインモデルの改善）

QKD レイヤーで生成された量子鍵を受け取り、量子鍵を管理・配送するキーマネージメントレイヤーに、QKD レイヤーから鍵生成の情報、盗聴による鍵生成ができなくなる（盗聴検知）のインタフェースの機能を追加することにより効率的な安全鍵の管理・運用をできるようにした。また、エー２で開発するセキュアフォトニックネットワークで利用されるアプリケーションとして現代暗号を利用した回線暗号装置、スマートフォンとの融合を図るために必要となるインタフェースを開発し、課題エー４の実証環境を構築できるようにした。

・（連携アプリケーションの開発）

量子鍵配送と融合した現代暗号を利用したアプリケーションとして、スマートフォンによる秘匿通信アプリケーション（以下、「ＡＰ１」）、および回線暗号装置連携アプリケーション（以下、「ＡＰ２」）の２つを開発した。ＡＰ１は、キーサプライレイヤーからの鍵供給については、ＦＡＬＰインタフェースを実装しスマートフォンへ量子鍵を供給する。スマートフォンへ供給された量子鍵は、ＳＩＰサーバー～スマートフォン間の端末認証に用いる。量子鍵を用いた端末認証を行った上で、暗号通信で使用する暗号鍵をＳＩＰサーバーからスマートフォンに配布する。ＡＰ２は、キーサプライレイヤーからの鍵供給については、有線ＬＡＮインタフェースを実装し回線暗号装置へ量子鍵を供給する。回線暗号装置に供給された量子鍵をワークキーとして通信データをＡＥＳ暗号する。この２つのアプリケーションをセキュアフォトニックネットワークに取り込んだ。

・（実証環境の構築／動作検証）

セキュアフォトニックネットワークの安全情報伝送の実証を行うために、課題エー１で実装した盗聴検知機能と鍵管理システムのカプセル化リレー機能を用いたセキュアフォトニックネットワークの自動切り替えを可能とする実証環境を構築した。まず、課題アで新たに開発したＮＥＣの量子鍵配送装置１式をＱＫＤレイヤーに取り込み、トポロジーを変更した。また、アプリケーションレイヤーに、課題エー２で開発したスマートフォンによる秘匿通信アプリケーションと回線暗号装置連携アプリケーションを取り込んだ。さらに、平成２５年度に取り込んだ課題アで開発した NEC の量子鍵配送装置に対し盗聴を仕掛けて検知させた際に、あらかじめ設定した迂回路に自動切り替えを行い、継続して量子鍵リレーできることを確認した。

⑵ 国立大学法人北海道大学

・（量子暗号方式の適合化）

QKD 装置の送信部における強度揺らぎの評価を行った。その結果、半導体レーザに注入するDCバイアス電流は閾値の0.9倍程度が最適であるという知見を得た。また、強度変調器に起因する強度の変化は変調器に入力する電圧波形によることが分かり、タイミング調整によって強度揺らぎが改善されることを示した。

・（量子情報技術の活用提案）

ダブルバランスドミクサを用いた調整不要型の APD 光子検出回路の開発を行った。フィルタによる参照信号の高純度化が信号対雑音比の向上に有効であるという知見を得た。