平成２５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）委託先

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 165 百万円（平成 25 年度 27 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）これまで得られた研究開発成果

		（累計）件	（当該年度）件
特許出願	国内出願	1	1
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	15	9
	プレスリリース	1	1
	展示会	0	0
	標準化提案	0	0

（７）具体的な成果実施内容と成果

(1) 日本電気（株）

・(アプリケーションレイヤーへの鍵供給方式の考案)

セキュアフォトニックネットワークのベースラインモデルにおいて、キーマネジメントレイヤーからアプリケーションレイヤーに鍵を供給する部分をキーサプライレイヤーとして分離し、現代暗号と連携できる仕組みを取り込んだ。さらに、キーサプライレイヤーに汎用性の高いインターフェイスを実装することで、課題アで開発した三菱電機のスマートフォンアプリケーションへ鍵供給できるようにし、相互接続試験を実施できるようにした。

・(実証環境の構築)

課題ア、ウ、NICT 協同研究、自主研究の各量子鍵配送装置をクァンタムレイヤーに取り込み、三菱電機のスマートフォンアプリケーション、NICT 自主研究の L3 スイッチ＋TV 会議、電子カルテシステムをアプリケーションレイヤーに取り込んで、セキュアフォトニックネットワークの実証検証環境を構築した。また、キーマネジメントレイヤーにおける各量子鍵配送装置の鍵生成状況を公開サイトに反映するようにした。

(2) 国立大学法人北海道大学

・(量子暗号方式の適合化)

量子暗号鍵配送プロトコルでは初期乱数を共有する必要がある。この初期乱数共有も通信によって安全に行うことができれば量子暗号鍵配送の適用範囲が拡大するものと期待される。古典的には、盗聴者に仮定を設けることで情報理論的に安全な通信ができることが知られている。今年度はこのようなプロトコルの一つである、PSMT（Perfectly Secure Message Transfer）に関して、量子アルゴリズムの一つであるグローバーアルゴリズムを用いることによって初期鍵共有のための安全な経路探索のラウンド数が低減できることを示した。

・(量子情報技術の活用提案)

現行の光子検出器は高価な APD を用い、さらに不要信号の除去に高性能のフィルタが必要であり、また製作後の調整も必要である。

今年度、ダブルバランスドミクサを用いる不要信号除去回路を提案した。この回路では高性能なフィルタや作成後の調整が不要になる。本回路に基づく光子検出器を容易に入手可能な国産 APD を用いて試作し、初期的な結果としてゲート周波数 1GHz において、温度 193 K で量子効率 4.1%かつダークカウント率 0.001 [counts/pulse]を得た。ここで得られた特性は同種の APD を用いたゲート周波数 62.5MHz のバランス型光子検出器のものとほぼ同等である。