平成27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
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。

（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

日本電気株式会社＜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27年度　６９百万円）
※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
課題エ-1　ベースラインモデルの研究（日本電気(株)）
課題エ-2　周辺関連技術の適用研究（日本電気(株)）
課題エ-3　量子暗号技術の適用研究（北海道大学）
課題エ-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	2	0
	その他研究発表	36	14
	プレスリリース・報道	9	7
	展示会	4	3
	標準化提案	0	0

（7）具体的な実施内容と成果

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

課題エ-1　ベースラインモデルの研究

社会インフラを構成する典型的通信環境として、「1対1の通信モデル」を「データバックアップセンタとの長距離大容量（100km/1Gbps）通信」、「1対多の通信モデル」を「複数拠点（4拠点）からなる秘匿電話網」と定義し、その技術課題として、①one-time pad 暗号や現代暗号を利用する多様なアプリケーションへの鍵供給、②実装方式の異なる多様な QKD 装置で構成される任意拠点間の鍵共有、③ネットワーク冗長性の確保と光子伝送路での盗聴/障害への対応、を抽出した。

また上記技術課題の解決のため、階層アーキテクチャと層間インタフェースを定義した。量子層ー鍵管理層間のインタフェースには、鍵生成状況等の統計情報収集を加え、光子伝送路における盗聴/障害の検知と鍵リレー経路の切り替え(迂回)を可能とした。

アプリケーション層より下位の層は、アプリケーション層に QKD を意識させずに安全な暗号鍵を供給するインフラとして、アプリケーション層と明確に区分し、「QKD プラットフォーム」と定義した。

課題エ-2　周辺関連技術の適用研究

認証、鍵の効率的な伝送と共有、鍵の管理といった典型的なベースラインモデルにおける問題を解決するための既存技術を周辺関連技術として抽出し、選択・実装した。具体的には、QKD プラットフォーム内の鍵伝送におけるノード間の認証方式として、複数の認証方式を周辺関連技術として抽出し、Wegman-Carter 認証方式を選択・実装した。またアプリケーション層への鍵供給方式として、様々なアプリケーション端末に対応できるように、物理インタフェース方式を周辺関連技術として複数抽出し、有線 LAN、無線 LAN、USB、FLAP（FeliCa）を選択・実装した。

さらに、1 対 1 の通信モデル実証のための現代暗号を利用するレイヤ2回線暗号装置連携アプリケーションと、1 対多の通信モデル実証のための現代暗号と one-time pad を併用するスマートフォン秘匿通信アプリケーションを開発した。いずれも開発においては段階的なカスタマイズを行った。

課題エ-3　量子暗号技術の適用研究

典型的なベースラインモデルにおける認証、（論理）鍵の複数拠点間における効率的な伝送と共有、鍵の有効性管理といった問題を解決するために活用可能な量子暗号技術・量子通信技術を抽出・評価した。具体的には、量子リレーにおける課題を解決するために、量子グループ秘密分散技術と分散コンピューティング技術を用いた量子リレーのプロトコルを提案した。また初期鍵共有の問題を解決するために、PSMT（Perfectly Secure Message Transfer）プロトコルに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安全な経路を確立するためのラウンド数が低減できることを明らかにした。さらに、束縛量子もつれのアクティベーションを利用したもつれ回復を検討すると共に、束縛量子もつれ生成に必要な高次元量子もつれ光子対発生装置を設計製作した。またダブルバランスドミクサを用いた調整不要型の低価格 APD 光子検出回路の開発を行った。

実際の装置のパルス毎の強度を記録するシステムを開発して強度変動の評価を行い、変動要因を解析すると共に、変動の影響を抑えるソフト的な手法を提案した。また実機において必要な光子検出器の検出効率と暗計数の等化法を提案した。

課題エ-4　環境構築／動作検証

課題エ-1 で定義した 1 対 1 の通信モデル及び1対多の通信モデルにおいて、課題エ-2 及び課題エ-3 で特定した課題解決方式の妥当性を評価するために、検証環境 5 拠点から成る動作検証環境「Tokyo QKD Network」を構築した。QKD 層には課題ア、ウで開発された QKD 装置（東芝、学習院、NTT/NICT、NEC）を接続し、またアプリケーション層に、エ-2 で開発したアプリケーション、三菱電機㈱の成果であるス

マートフォンアプリケーション、NICT 自主研究の成果であるL3 スイッチアプリケーション、TV 会議アプリケーション、電子カルテシステムを接続し、各 QKD 装置、各アプリケーションの動作を検証した。また、鍵生成状況・気象・温度などをモニタするための鍵生成状況監視システム（公開 Web サイト）を構築し、Tokyo QKD Network の状態モニタとして、平成 24 年度から運用し続けた。さらに、エ-1 で策定した盗聴検知機能を拡張し、盗聴/障害検知時に鍵管理層において鍵リレーの最適経路を自動選択して切換え、盗聴/障害の位置を推定する機能を実装・動作検証した。その中で、4 拠点間（3 スパン、距離合計約 114ｋm、伝送ロス合計約 41dB）の鍵リレーを検証した。

研究開発成果については、2015 年 9 月 28 日～10 月 2 日に開催された UQCC2015 および QCrypt2015 において、演発表・デモンストレーションを実施した。