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ア0301
個別課題名　：課題ア　量子鍵配送ネットワーク制御技術
副　　題　：安全な通信網の構築に向けた量子鍵配送技術の研究開発

（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理論、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＞

（4）研究開発予算（契約額）

総額　４２６百万円（平成27年度　６２百万円）
※百万円未満切り上げ

（5）研究開発課題と担当

課題ア：量子鍵配送ネットワーク制御技術
課題ア-1　安定化技術（日本電気(株)）
課題ア-2　アプリケーションプラットフォームの拡張（日本電気(株)）
課題ア-3　次世代量子鍵配送システム技術（日本電気(株)）
課題ア-4　長期運用試験（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	8	1
	外国出願	3	1
外部発表	研究論文	1	0
	その他研究発表	14	2
	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

課題ア：量子鍵配送ネットワーク制御技術

課題ア-1　安定化技術

微弱コヒーレント光を用いた波長多重量子鍵配送システムの安定化技術と、障害発生時に通常動作モードに復旧するための技術の確立を目的に研究開発を行った。量子鍵配送システムの安定化技術として、変調器のバイアス電圧、PLC 干渉計の温度、検出器のゲートパルス位相、検出器のデータ遅延補正量といった各種パラメータの自動調整機能を開発した。またデコイパルス強度の安定化技術を確立し、変調器の能動的制御により暗号鍵生成速度の揺らぎを 1/2 以下に抑制した。小金井―府中間のフィールド環境における長期運転試験（2 波長 WDM）では、伝送損失が 13dB の場合には量子ビット誤り率 1.70%、安全鍵生成速度 229.8kbps、伝送損失が 15dB の場合に 8 波 WDM 換算で 574.5kbps を達成した。また NEC のサイバーセキュリティ対策の中核拠点であるサイバーセキュリティ・ファクトリーにおける長期運転試験（1 波長）では、デコイ法を実装したシステムにより、鍵生成速度変動の標準偏差が±8.6%での連続動作を達成した。本試験により、安全性証明を伴った条件下での高安定な鍵共有を実証した。

また障害復旧技術として、初期設定やパラメータ自動調整機能を統合すると共に、システム起動を一括で実行する GUI を開発した。また Web ブラウザ上での 3 ステップのクリック操作を確立した。

課題ア-2　アプリケーションプラットフォームの拡張

量子鍵配送技術のアプリケーションプラットフォームの拡張を目的に研究開発を行い、「遠隔拠点に属するスマートフォンの安全な鍵設定手法」を、アプリケーションインタフェースとして実現するためのアプリケーションプラットフォームアーキテクチャを設計した。具体的には、遠隔拠点間の量子鍵配送レイヤーと、鍵管理レイヤー、ならびに鍵供給レイヤーの 3 つからなるアーキテクチャを考案し、鍵共有レイヤーとアプリケーション間の鍵供給・鍵設定インタフェースを定義した。鍵供給レイヤーを導入することにより、近地拠点間も遠隔拠点間もトランスペアレントに鍵供給・鍵設定が可能になった。また本成果は、課題エに組み込んで動作を検証している。

課題ア-3　次世代量子鍵配送システム技術

次世代量子鍵配送システムのコンパクト化と安定化を目的に、小型光子検出器の研究開発を行った。具体的には、APD 冷却用筐体や温度コントローラ、電源などの外部機器を検出回路と一体化して 8 波長多重時でもラック 2 本以下に小型化した光子検出器を開発した。ATCA シャーシに収容可能（2 スロット幅）な大きさで、活線挿抜（電源系のみ）も可能にした。装置の体積、消費電力を従来の 1/3 以下に抑えながら、安定性、可用性、操作性も大幅に向上し、検出速度はディスクリート型と同等以上を実現した。さらに単体の鍵生成速度については 62.5kbps(8 波多重時 500kbps)を達成した。

小金井―府中間、サイバーセキュリティ・ファクトリー内の二か所のフィールド環境における長期運転試験では、課題ア-1 の成果を利用した装置の安定化によって量子ビット誤り率 3%以下での長期間連続運転の達成を確認すると共に、適宜 SSPD、APD の性能比較を行った。

また光学的非対称基底選択方式の採用により、従来の対称基底選択方式から鍵生成功率が 30%向上した。

課題ア-4　長期運用試験

量子鍵配送システムの長期運転実績の確立のために、デモ用システムを開発して長期

運用試験を行った。具体的には、課題ア-1 で確立した安定化技術を、課題ア-3 で開発した次世代量子鍵配送システムに活用したデモ用システム（WDM QKD システム、1 波長 QKD デモシステム）にて、小金井-府中間、サイバーセキュリティ・ファクトリー内の二か所のフィールド環境において長期連続運転による運転試験を行った。2 波長 WDM 構成によるフィールドファイバ伝送 30 日間連続運転、1 波長装置による 21 週間連続動作を実証した。

また長期運転実績の公開のために、気象・装置温度・鍵生成状況などの暗号鍵生成状況を監視して Web に公開するシステムを開発し、動作検証環境として構築した「The Tokyo QKD Network」の状態モニタとして稼働させた。The Project UQCC HP から随時状態をモニタすることが可能である。