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 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

（1）研究開発の目的

無条件安全性が理論的に保証された高速な量子鍵配送技術を利用したセキュアフォトニックネットワークの構築に向けた、量子鍵配送技術の高性能化、安定性向上を目的とする。さらに、複数の携帯端末間での量子暗号鍵共有のためのインターフェイスを開発することにより、セキュアなネットワーク領域を拡大することを目的とする。

（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）＜代表研究者＞

（4）研究開発予算（契約額）

総額 426 百万円（平成 26 年度 83 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
1. 安定化技術
2. アプリケーションプラットフォームの拡張
3. 次世代量子鍵配送システム技術
4. 長期運用試験

（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	7	3
	外国出願	2	0
外部発表	研究論文	1	0
	その他研究発表	13	4
	プレスリリース・報道	2	1
	展示会	0	0
	標準化提案	0	0

（７）具体的な実施内容と成果

(1) 量子鍵配送システムを長期間にわたって運用する場合には各種パラメータの能動的安定化制御が必要であり、H25 年度までに誤り率の最小化や光子検出数の最大化といった自動制御機能を開発してきた。しかし、これらの制御のみではデコイ BB84 プロトコルによる暗号鍵生成速度が大きく揺らぐことが課題であった。暗号鍵生成速度が揺らぐ原因について調査した結果、揺らぎはデコイパルスの強度と強い相関を持つことが判明した。デコイパルスを生成するための変調器の出力強度をモニタし、それを元に変調器に印加するバイアス電圧を能動的に制御することでデコイパルスの強度を安定化することができ、暗号鍵生成速度の揺らぎを 1/2 以下に抑制することができた。

(2) H25 年度にシステム起動時に各種パラメータを最適値に自動調整する機能を開発したが、ユーザが調整順序を考慮した上でパラメータ毎に実行する必要があり、システムを熟知していないユーザには負担が大きいという課題があった。これを解決するため、量子鍵配送システムの初期設定やパラメータ自動調整機能を統合し、システム起動を一括で実行する GUI を開発した。Web ブラウザ上での３ステップのクリック操作により安定運用状態に到達可能とした。

(3) オリジナルの BB84 プロトコルでは２種類の基底を各々50%の確率で選択し、送受信者間で選択が一致したデータのみを利用する。鍵生成速度を向上するためには基底選択を各々50%ではなく一方に偏らせた非対称基底選択方式として、利用できるデータ数を増加させることが有効である。送受信者間の選択基底が一致する確率を高めるため、２種類の基底選択の割合を 50%以外にも $1/2^n$ の割合に設定可能な鍵蒸留用 FPGA を開発した。また、各基底における誤り率を個別に評価し、一方を誤り訂正に、他方を秘匿増強に用いる方式とし、鍵蒸留効率が向上した最新の安全性理論を適用可能とした。

(4) 近年懸念されているサイドチャネル攻撃の１つとして、受信機に強い光を入射する明光攻撃がある。この攻撃により攻撃者は正規受信者の受信データを操作できてしまう可能性があるため、明光攻撃を検知する必要があった。攻撃者が受信機に強い光を入射した場合には、複数の光子検出器から同時に検出信号が出力される。この同時検出の発生を監視して明光攻撃を検知する機能を実装した。3 台以上の光子検出器で同時検出があった場合には明光攻撃の可能性が高いとしてアラームを表示する。

(5) 量子鍵配送システムの信頼性を確立するためには、実運用に近い環境で長期間にわたる特性評価試験を行う必要がある。H25 年度に 1 ヶ月間の連続運転試験を行った波長多重対応の試作システムに加え、同年度に開発したコンパクトなデモシステムを用いて 1 ヶ月程度の連続運転を行った。両システムに（１）で開発した安定化制御を導入し、試作システムでは送受信機を 50km のファイバスプールを介して接続し、1 ヶ月間の連続運転試験を行った。また、デモシステムでは NICT 小金井～NEC 府中事業場間の光ファイバ（往復 22km、損失 13dB＝理想的なファイバでは 65km に相当）を用いた 3 週間のフィールド試験を行った。その結果、両システムとも誤り率 3%以下の長期間連続安定運転を達成した。

(6) 複数の量子鍵配送システムによる冗長化試験や潜在ユーザへのデモンストレーションを行うため、1 チャンネルに限定したコンパクトなデモシステムを追加構築し、既存システムと同等の特性を得た。デモシステムには量子鍵配送のアプリケーションとして、現代暗号（AES）による暗号化通信で実績のあるレイヤー２回線暗号装置を組み込み、現代暗号への鍵供給による双方向 100Mbps の高速な暗号化通信を実現した（課題エと連携）。