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 ウ 01
個別課題名 ：課題ウ　連続量量子鍵配送技術とその応用
副　　題 ：QAM 光伝送技術を用いた量子鍵配送と光秘匿通信技術の開発

（1）研究開発の目的

都市圏で実用的な性能を有する連続量量子鍵配送技術と、基幹回線にも対応しうる長距離・大容量性に優れた光秘匿通信技術を開発するとともに、これらを統合する技術の研究開発を行う。連続量量子鍵配送技術においては、50km の伝送距離で 10kbps の安全鍵生成が可能な送受信装置を開発する。光秘匿通信技術の研究に関しては、直交振幅変調（QAM: Quadrature Amplitude Modulation）光伝送技術とストリーム暗号技術を組み合わせ、量子雑音を利用した安全性の高い 40 Gbps 級の光ファイバ伝送技術による２次元暗号伝送を世界に先駆けて開発する。また、これらの技術を統合し、連続量量子鍵配送と光秘匿通信の両方に対応したプロトタイプ伝送装置のフィールド実証実験を行う。

（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

学校法人学習院大学（実施責任者　教授　平野琢也）、国立大学法人東北大学

（4）研究開発予算（契約額）

総額　２４２百万円（平成 27 年度　４３百万円）
※百万円未満切り上げ

（5）研究開発課題と担当

課題ウ-1： 連続量量子鍵配送技術の研究開発
課題ウ-1-1…　連続量量子鍵配送装置の開発（学習院大学）
課題ウ-1-2…　安全性評価技術の開発　（学習院大学）
課題ウ-2　光秘匿通信技術の研究開発
課題ウ-2-１…　２次元暗号のコヒーレント光伝送技術の開発（東北大学）
課題ウ-2-２…　暗号化および復号化回路の開発　（東北大学）
課題ウ-3　連続量量子鍵配送と光秘匿通信の統合技術の開発
課題ウ-3-１…　統合光暗号装置の高速化　（東北大学）
課題ウ-3-２…　統合光暗号装置の低雑音化　（学習院大学）
課題ウ-3-３…　統合化技術の開発と評価　（学習院大学）

（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	2	1
	外国出願	0	0
外部発表	研究論文	20	5
	その他研究発表	50	10
	プレスリリース・報道	3	0
	展示会	1	1
	標準化提案	0	0

（7）具体的な実施内容と成果

課題ウ-1　連続量量子鍵配送技術の研究開発

- 連続量量子鍵配送装置の自動制御運転技術については、送受信者間で共有する暗号鍵が不一致とならないようにする機能、通信パラメータの変動に対する動作パラメータの自動補正の機能などを装置に実装し、動作の検証を実施した。連続量量子鍵配送において最も重要な量子通信路のパラメータは、通信路の透過率と過剰雑音であり、これらを常にモニターし、その値に応じて秘匿性増幅パラメータをリアルタイムに適切な値に設定する技術を実装した。これらの開発により、実利用可能な暗号鍵をリアルタイムに生成することができた。
- 連続量量子鍵配送装置の高速化技術については、受信データのPCへの転送速度を10倍以上高速化した場合でも量子雑音限界のホモダイン検出が可能となるよう、光学系や制御系の最適化を実施した。これにより、検出器自身の雑音に比べて、光の量子雑音が１５倍以上大きくなる量子雑音限界の動作を実現した。光学系については、送受信者の光学部品を密閉度の高い断熱ボックスに収め、小型化と安定化を図った。これにより、送受信者間の位相のずれを補正するプログラムの最適化と合わせ、安定した長時間の暗号鍵生成が可能となった。
- 安全性評価技術については、盗聴者の能力を制限した仮定の下での暗号鍵の生成率の計算などを実施した。また、エンタングリング・クローナ攻撃についても、受信者の装置に対する攻撃に現実的な仮定を置いた際の鍵生成率を様々な条件下で数値的に計算し、この結果を用いて、実機の動作パラメータ近傍で秘匿性増強パラメータを一次関数式で近似し、この近似式を用いるリアルタイムの制御を実現した。

課題ウ-2　光秘匿通信技術の研究開発

- 伝送速度が20～60 Gbit/s、伝送距離が320 kmのリアルタイム光秘匿伝送に成功し、本課題の最終目標を達成した。また、送信部と受信部をそれぞれ一台ずつの19インチラックへ収納する形でそれら装置をNICTへ移設し、ラボツアーにおいて動態展示を実施した。さらに、本課題における研究成果を国際会議ECOCおよびAsilomar conferenceにて発表した。
- H26年度に開発したFPGA回路において、暗号化に用いるランダム信号の生成アルゴリズムを見直し、盗聴者に対する符号誤り率が増大するよう改良した。また、光伝送路内の非線形光学効果（自己変調効果）による光位相回転に対する補償回路を新たに導入した。

課題ウ-3　連続量量子鍵配送と光秘匿通信の統合技術の開発

- NICT（ラボツアー時）においてQKDシステムで配信した秘密鍵を元に光秘匿通信システムを正常に駆動できることを確認し、提案する統合システムの原理実証に成功した。さらに、東北大学において同一の光ファイバ伝送路（長さ10 km）を用いた秘密鍵とデータの同時配信試験を実施し、共通の光伝送路を用いても双方のシステムを正常に動作できることを実証した。