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 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）委託先

学校法人学習院大学＜幹事者＞、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 25 年度 49 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）これまで得られた研究開発成果

		（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	1	1
	その他研究発表	29	12
	プレスリリース	1	0
	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

課題ウ-1　連続量量子鍵配送技術の研究開発

- 省スペース型の連続量量子鍵配送装置の構築については、小型サーバーボックスに収納可能な連続量量子鍵配送装置を開発した。動作周波数は 500KHz 及び 10MHz で、500KHz の動作については物理乱数による変調を実現した。光学系は、平成 24 年度に開発した一方向分離光学系であり、自動調整のための光スイッチや可変光減衰器は、FPGA ボードから制御可能である。
- ポストセレクションと逆リコンシリエーションを行う連続量量子鍵配送プロトコルについて、秘密鍵を生成するプログラムを開発した。ポストプロセッシングのプログラムは主に３つの機能ブロックからなり、全て Linux 上で動作するソフトウェアである。
- 通信距離 10km で連続量量子鍵配送装置の動作検証を行い、4QAM とポストセレクションを行って得たデータに対して誤り訂正と秘匿性増強を実行し、秘密鍵をプログラム動作により生成した。
- メトロネットワークに対応可能な低雑音の連続量量子鍵配送装置については、繰り返し周波数 100KHz のパルス光源を用いて通信距離 40km の量子鍵配送実験を行い、0.01 以下の過剰雑音を実現した。
- 受信者の装置の不完全性を考慮した個別攻撃及びコレクティブ攻撃に対する秘密鍵生成率の理論的な導出を行った。

課題ウ-2　光秘匿通信技術の研究開発

- H25 年度は、H24 年度に作製した 10 Gbps 暗号化データの送信回路（暗号化回路）に整合のとれた受信回路（復号化回路）を試作した。サンプリング速度 10 GSample/s、垂直分解能 8 bit の高速 ADC と FPGA 回路を用いて、受信した暗号化データをリアルタイムで復号化し、符号誤り率の測定が on-line で可能な受信回路を実現した。
- H24、H25 年度に試作した FPGA 送受信回路を用いて、2.5 Gsymbol/s, 16 QAM（10 Gbps)信号のリアルタイム 160 km 伝送実験を実施した。光位相同期(OPLL)回路を用いてコヒーレント検波系内の光電界の位相揺らぎを 2 deg.以内に抑制し、160 km 伝送時に正規受信者に対しエラーフリー受信を実現した。一方、盗聴者に対しては、1024 x 1024 値の 2 次元暗号化を図ることで、1 シンボル当たり 99.9 %以上の受信誤り率を達成した。

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

- 連続量量子鍵配送と光秘匿通信を統合するセキュアネットワークの設計を行い、連続量量子鍵配送装置は KSA に秘密鍵を渡す機能について、光秘匿通信装置は KSA から秘密鍵を受け取る機能について、詳細な検討を行った。連続量量子鍵配送装置については、NICT 内に設置した際に、KSA との接続試験を実施した。