平成２４年度研究開発成果概要書
セキュアフォトニックネットワーク技術の研究開発（157ヴ01）
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（百万円単位切上げ）
平成２３年度　５５（契約金額）
平成２４年度　５２（　〃　）
平成２５年度　４９（　〃　）
平成２６年度　４６（　〃　）
平成２７年度　４３（　〃　）

（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	１
	外国出願		
外部発表	研究論文		
	その他研究発表	１７	１２
	プレスリリース		
	展示会		
	標準化提案		

具体的な成果

(1)繰り返し周波数 10MHz で動作する連続量量子鍵配送装置を開発

(2)エンタングリングクローナー攻撃に対して安全な鍵生成率の計算

(3)10 Gbps 暗号化データのオフライン伝送実験

(4)10 Gbps 暗号化データのリアルタイム送信器の試作

（７）研究開発イメージ図

平成24年度「セキュアフォトニックネットワーク技術の研究開発」の研究開発目標・成果と今後の研究計画

1. 実施機関・研究開発期間・研究開発費

◆実施機関　　学習院大学（幹事）、東北大学
◆研究開発期間　平成23年度から平成27年度（5年間）
◆研究開発費　　総額243百万円（平成24年度　52百万円）

2. 研究開発の目標

・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。

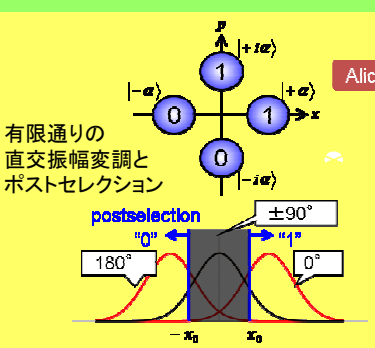
3. 研究開発の成果

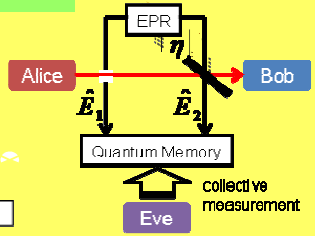
研究開発目標

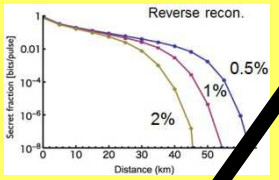
①連続量量子鍵配送技術

光の直交振幅の量子ゆらぎを利用した暗号技術

ガウス通信路の場合に最適なエンタングリングクローナー攻撃に対して安全な鍵の生成率



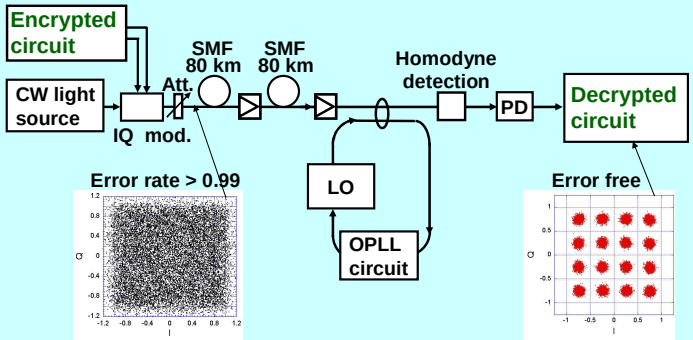




A　連続量量子鍵配送装置の開発
B　安全性評価技術の開発

②光秘匿通信技術

量子ストリーム暗号を用いた高速かつ安全な光秘匿通信システムの開発



A　オフライン伝送による2次元暗号の原理実証

B　リアルタイム変復調回路の開発

研究開発成果

研究開発成果：連続量量子鍵配送装置の開発

送信者がレーザー光を直交振幅変調し、受信者がホモダイン検出器を行う量子鍵配送技術は、コヒーレント光通信と親和性が高く、実装面で有利。量子雑音限界に近い動作を実現することが必要。

●自動化に適した光学系および検出系を構築し、通信距離10kmで量子鍵配送を実行し、十分小さい過剰雑音を実現した。

●信号光と局部発振光の相対的な位相を安定化させることができる独自の光学系を用い、長さ40kmの光ファイバーを用いた低雑音動作に成功した 。

研究開発成果：安全性評価技術の開発

量子鍵配送では、盗聴者の得ることができる情報量の上限を物理法則によって決めることにより、鍵の安全性を保証することから、安全性評価技術が重要。

●有限個の直交振幅変調とポストセレクションを組み合わせる方式の鍵生成率を定量的に計算し、過剰雑音に要求されるレベルを明らかにした。

●誤り訂正および秘匿性増強のプログラム開発を進めたほか、エンタングリングクローナー攻撃以外の攻撃についての安全性についても検討を進めた。

研究開発成果：オフライン系による2次元暗号の原理実証

中間目標である2.5 Gsymbol/s, 16 QAM（10 Gbps)信号の2次元暗号伝送を、先立ってオフライン伝送系を用いて実施。

●MxM値の2次元暗号化QAMデータの160 km伝送実験において、多値度Mをパラメータとして盗聴者ならびに正規受信者の符号誤り特性（BER）を詳細に評価した。

●正規受信者がエラーフリーで受信可能な伝送条件のもと、Mを256値以上に設定することで盗聴者に対し99 %以上のBERを実現できることを明らかにした。

研究開発成果：リアルタイム変復調回路の開発

NEC通信システム社の協力のもと、10 Gbps暗号化データのリアルタイム送信器をFPGA回路を用いて試作。

●試作した送信器からの出力信号をオフラインの受信系を用いて復調解析し、所望の暗号化データが生成されていることを確認した。

4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	国際会議予稿	収録論文	その他研究発表	プレスリリース	展示会	標準化提案
セキュアフォトニックネットワーク技術の研究開発	1(1)					17(12)			

5. 研究成果発表会等の開催について

（1）課題ウの内部及び他の課題との連携を推進

課題ウとして連続量量子鍵配送技術と光秘匿通信技術の統合技術について検討を行うため、電子メール等を通じた情報の交換を行った。また、セキュアフォトニックネットワーク技術の研究開発の他の課題との連携を深め、技術の統合を進めるために、学習院大学で打ち合わせを行ったほか、電子メールでも情報交換を行った。

（2）学会等での成果報告

量子ICTフォーラムで量子鍵配送装置実機の展示およびポスター展示を行ったほか、日本物理学会、量子情報技術研究会、MITとの研究交流会などで研究成果の発表を行った。

6. 今後の研究開発計画

・連続量量子鍵配送装置の開発においては、高速化と低雑音化のための技術開発を進めるとともに、フィールド動作実験、自動化のための研究開発を行う。高速化についてはFPGA制御系とPCとのデータ転送の高速化、低雑音化については伝送距離40kmの伝送装置の過剰雑音の原因の特定とそれに対する対策を徹底的に行う。フィールド動作はNICTの構内接続試験を進める。
・安全性評価技術の開発については、量子鍵配送装置の様々な状況下の実際のデータを使用したポストプロセッシングの開発を行うほか、より優れた鍵蒸留方式についての研究、4状態ポストプロセッシング方式の無条件安全性の証明に向けた研究を行う。
・光秘匿通信技術については、H24年度に試作した暗号化回路（送信部）に対応したリアルタイム復号化回路（受信部）を試作し、中間目標である伝送速度が10 Gbpsの光秘匿伝送システムを実現する。また、最終目標である40 Gbps伝送系の実現に向け、先立ってオフライン系を用いた伝送実験を行い、暗号化フォーマットの最適条件を解析する。
・連続量量子鍵配送と光秘匿通信の統合技術については、10 Gbpsの各種回路の試作の経験を活かし、量子鍵配送とのインターフェースを備えた40 Gbps暗号化／復号化回路の設計に着手する。