平成23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23年度　55百万円）

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。

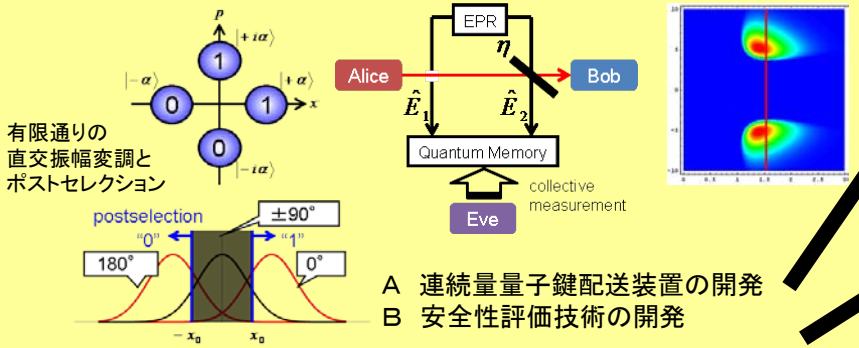
3. 研究開発の成果

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

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。

●本研究開発では、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て、過剰雑音や安定性を検証。
●長さ40kmの光ファイバーを用いた低雑音動作に成功 。

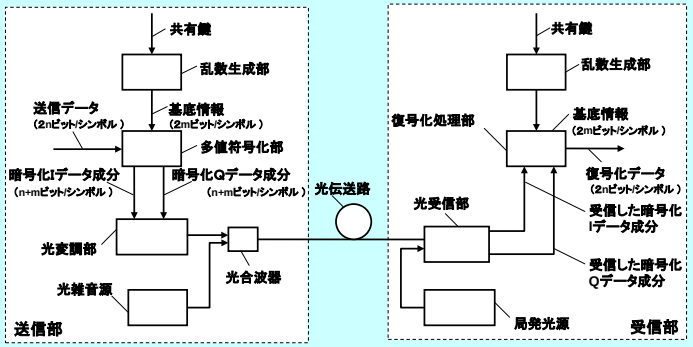
研究開発成果：安全性評価技術の開発

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は他の課題と共通な鍵蒸留技術を用いることが可能。
●実用的な環境下においてエンタングリングクローナ攻撃を行う盗聴者の得る情報量を評価し、鍵生成率を蒸気方式に対して初めて明らかにした。

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：オフライン伝送による2次元暗号の原理実証

オフライン伝送系の構築および2次元暗号化データの変復調特性評価

- 2次元暗号化QAMデータ信号のコヒーレント受信系を構築
- 原理実証実験として、1 Gsymbol/s, QPSK信号（2 Gbit/s）を8ビットの基底情報で暗号化した1024 QAM信号の復調特性を評価した結果、正規受信者が誤りなく復調できる条件のもとで94 %の盗聴者の誤り率を得た。

研究開発成果：リアルタイム変復調回路の開発

リアルタイム回路の構築に必要なハードウェアの情報収集

- 変復調回路を構築するために必要な高速FPGA, 高速ADC, 高速DACに関する情報を収集した。その結果、所望の仕様を満たす高速DACはまだ市販されておらず、変調器と復調器の開発の順序を入れ替える必要があることがわかった。

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	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	0 (0)	0 (0)	0 (0)	5 (5)	0 (0)	0 (0)	0 (0)

5. 研究成果発表会等の開催について

（1）課題ウのなかの連携を推進

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ほか、2011年10月11日に東北大学において合同ミーティングを開催した。

（2）他の課題との連携推進

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、2011年12月1日および2012年2月1日に学習院大学で打ち合わせを行ったほか、電子メールや電話会議でも情報交換を行った。

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。高速化については、光源の繰り返し周波数を10MHzとするための変復調技術、特に、高速低雑音のホモダイン検出器の開発を行う。低雑音化については、伝送距離50km圏で過剰雑音が0.01以下を実現するために、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。
- 安全性評価技術の開発については、鍵生成率の評価に用いる前提条件の厳密化、サイドチャンネル攻撃の評価、より優れた鍵蒸留方式などについて研究を行う。
- 光秘匿通信技術については、伝送データを2.5 Gsymbol/s, 16 QAM信号（10 Gbit/s）に拡張し、また暗号化の多値度を16~20ビットに拡大した条件のもとで2次元暗号化信号のオフライン伝送実験を行い、暗号の安全性の評価ならび暗号化アルゴリズムの最適化を図る。また、デジタル信号処理に造詣の深い通信機器メーカの協力のもと、FPGAを用いた10 Gbit/s暗号化データ信号のリアルタイム暗号化／復号化回路を試作する。
- さらに、連続量量子鍵配送と光秘匿通信技術の統合技術の開発、他の研究課題との連携、統合についても研究開発を進める。