平成25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242百万円（平成25年度　49百万円）

2. 研究開発の目標

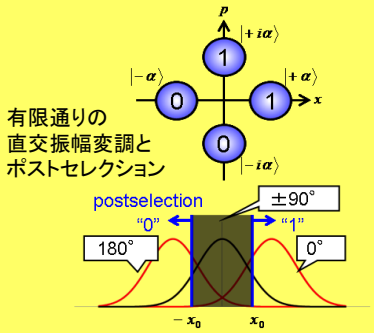
・都市圏で実用的な性能を有する連続量量子鍵配送技術と、基幹回線にも対応しうる長距離・大容量性に優れた光秘匿通信技術を開発するとともに、これらを統合する技術の研究開発を行う。

3. 研究開発の成果

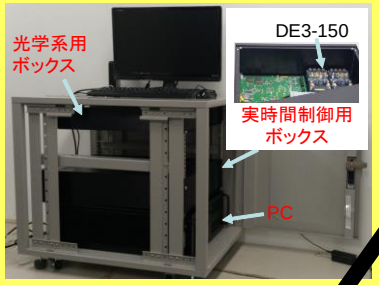
研究開発目標

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



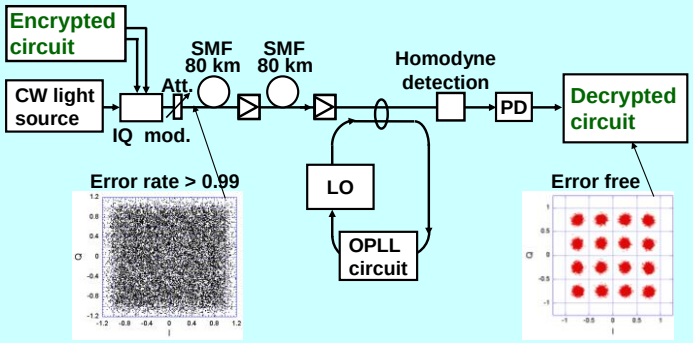
構内・アクセスネットワークで使用可能な低コスト省スペース量子鍵配送装置の開発



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　2次元暗号のコヒーレント伝送技術
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

●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。また、ソフトウェアによるポストプロセッシングを実装した。
●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。
●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。

研究開発成果：安全性評価技術の開発

●ポストセレクションと逆リコンシリエーションを行うプロトコルについて、秘密鍵を生成するプログラムを作成した。
●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。

研究開発成果：2次元暗号信号のコヒーレント伝送技術

課題Bで開発した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。
●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てエラーフリー受信を実現した。
●1024 x 1024値の2次元暗号化を図ることで、盗聴者に対して1シンボル当たり99.9 %以上の受信誤り率を達成した。

研究開発成果：リアルタイム変復調回路の開発

10 Gbps暗号化データのリアルタイムFPGA受信回路を試作。
●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、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。

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	1(0)	0(0)	1(1)	29(12)	1(0)	0(0)	0(0)

5. 研究成果発表会等の開催について

（1）課題ウの内部及び他の課題との連携を推進

課題イの研究者と定期的な会合を学習院大学で実施し、誤り訂正プログラム及び秘匿性増強プログラムの開発を行った。また、プログラムのコーディングやデバックにあたっては、SSH接続を用いて、拠点間をまたいだ共同研究を行い、研究開発を効率的に進めることができた。連続量量子鍵配送技術と光秘匿通信技術を統合する光通信システムについては、電子メールや電話等により、緊密な連携を推進した。

（2）学会等での成果報告

省スペース型連続量量子鍵配送装置を情報通信研究機構内に設置し、秘密鍵の生成の実演を実施した。また、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

・省スペース型連続量量子鍵配送装置の開発においては、自動化、高速化、安定化のための技術開発を進める。自動運転制御においては、量子鍵生成中の温度変動等により生じた装置の異常を検知し、調整する機能を実装する。また、光源の繰り返し周波数10MHzに対応する高速なデータ処理を実現するとともに、光学系の安定化を行い、NICT内で構内接続し、フィールド実証を行う。伝送距離40kmの伝送装置は、小型化と低雑音化のための研究開発を行う。

・安全性評価技術の開発については、様々な状況下におけるポストプロセッシングの研究開発を行う。

・光秘匿通信技術については、H25年度までに試作したリアルタイム送受信器の高速化を図り、最終目標である速度が40 Gbps、伝送距離が300 km以上の光秘匿伝送システムを実現する。また、H27年度にNICTにて動態展示ができるよう、送受信光源の機械的安定度の改善を図る。

・連続量量子鍵配送と光秘匿通信の統合技術については、量子鍵配送技術で配信した鍵情報をもとに生成した乱数列（基底情報）により2次元暗号化／復号化を図る機能をFPGA送受信回路内に備え、これにより両伝送技術の融合化を図る。