

1. 研究課題・実施機関・研究開発期間

- ◆課題名 : セキュアフォトリックネットワーク技術の研究開発
- ◆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
- ◆実施機関 : 学習院大学(代表研究者)、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)

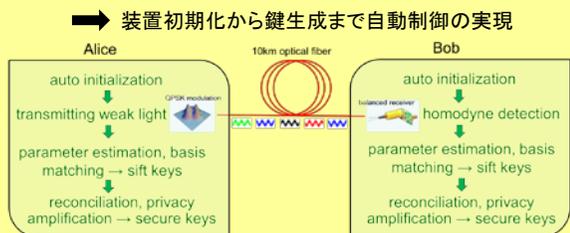
2. 研究開発の目標

- 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

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

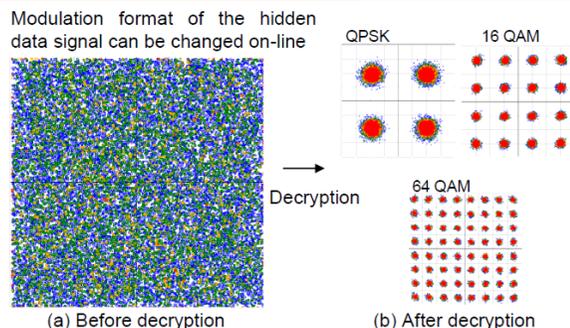


- パルス光の繰り返し周波数10 MHzで動作する連続量量子鍵配送装置を試作し、10 kmの通信距離において、300 kbpsのシフト鍵生成レート、50 kbpsの暗号鍵の生成レートを実現した。
- 誤り訂正と秘匿性増強をPCで実行するソフトウェアを開発した。
- 40 kmの通信距離で非常に小さな過剰雑音を実現する連続量量子鍵配送装置を開発した。
- 受信側の光強度の測定と偏波制御をプログラムにより自動実行し、受信者のデータ取り込みのタイミング制御と可変減衰器の減衰率の適切な設定の自動実行技術を開発した。
- 受信側のLO光強度が、予め設定した値以下になった場合は、通信路が切断されたものとして運転を中断、正常値に戻った後、秘密鍵の生成まで自動復帰できる機能を実装した。

②光秘匿通信技術



QAM/QNSCシステムの概観



4-64 QAM/QNSC信号の復調の様子

研究開発成果:光秘匿通信システムの開発

- FPGAを基盤としたリアルタイム送受信器を開発し、これを用いて偏波多重5 Gsymbol/s, 4-64 QAM/QNSC (20-60 Gbit/s) 信号の320 kmリアルタイム伝送に成功した。
- データの多値度を不規則に切り替える機構を新たに導入し、安全性の向上を図った。
- 送信部/受信部を19インチラックに収納した可搬型装置を構築した。

研究開発成果:連続量量子鍵配送との統合システムの開発

- 量子鍵配送システムにより配送された秘密鍵を外部入力できるようにFPGA送受信器を改良し、その秘密鍵をもとに生成した極めて安全性の高い乱数列をもとに暗号化/復号化動作を行う統合システムを実現した。

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、()内は当該年度の件数です。

	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 報道	展示会	標準化提案
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	3 (2)	0 (0)	20 (5)	49 (9)	3 (0)	1 (1)	0 (0)

(1) 世界最高レベルの連続量量子鍵配送装置と光秘匿通信装置を開発

課題ウー1において、光源の繰り返し周波数が従来より1桁高速な連続量量子鍵配送装置を試作し、自動運転による鍵生成を実現。暗号鍵の生成率は通信距離10 kmにおいて、50 kbpsを達成。また、40 kmの通信距離で暗号鍵生成が可能な小さな過剰雑音を実現。課題ウー2において、データの多値度を4, 16, 64, 256値の範囲で任意に切り替えることが可能な暗号化／復号化回路を開発した。そして本回路を用いて20-60 Gbit/s暗号化データの320 kmリアルタイム伝送を世界で初めて実現した。

(2) 課題ウ内、および個別課題間の連携を推進し、当初計画以上の成果を得た

課題ウー1で開発した量子鍵配送(QKD)システムにより配送した秘密鍵を外部入力できるように課題ウー2で開発した暗号化／復号化回路を改良した。そしてその秘密鍵をもとに光秘匿通信システム内の暗号化／復号化動作を行う統合動作に成功した。これによりQKDと同等の安全性をもつ乱数列をその暗号化動作に利用できるようになり、安全かつ高速な光秘匿通信システムを実現した(特許出願済)。
課題ア、イ、エとの技術情報交流、共同研究を推進し、量子鍵配送のポストプロセッシング用ソフトウェアを開発し、安価なGPUを用いた高速な誤り訂正、計算量を抑えた秘匿性増強プログラムを開発したほか、量子鍵配送から光秘匿通信への暗号鍵の供給を実現した。