プログラム名：量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現
PM 名：山本喜久
プロジェクト名：量子セキュアネットワーク

委 託 研 究 開 発

実 施 状 況 報 告 書（成果）

平成２９年度

研究開発課題名：

光多値変調による量子鍵配送技術の研究開発

研究開発機関名：

学習院大学

研究開発責任者
平野琢也

Ⅰ　当該年度における計画と成果

１．当該年度の担当研究開発課題の目標と計画

本研究の目的は、コヒーレント光通信と共通の技術を用いることにより、単一光子検出器に依存せず、安価な光通信機器を使って、高秘匿伝送システムを開発することである。研究内容は、量子セキュアネットワークを構成する３層構造のうち、物理層の技術として、多値変調技術を用いる量子鍵配送技術の開発を行うことである。平成２８年度までに、高速動作する量子雑音限界ホモダイン検波技術と乱数発生の技術開発を行い、これらの技術を用いる高速 CV-QKD 装置の動作実証を行った。平成２９年度は、高速 CV-QKD 装置のハードウェア機能の実装を上期までに実施するとともに、本ハードウェア用のソフトウェアの開発を進め、高速 CV-QKD 装置による鍵生成を実現する。また、東北大学中沢研究室との共同研究による多値変調秘匿伝送統合技術の開発、光通信との共存実証試験も継続して実施する。さらに、安全性評価技術の理論的な研究も進める。

２．当該年度の担当研究開発課題の進捗状況と成果

2-1 進捗状況

高速 CV-QKD 装置の研究開発については、自動運転が可能な可搬型の装置の実現のために、ハードウェアおよびソフトウェアの開発を昨年度に引き続き進めた。ハードウェアについては、平成２８年度にストリーム動作を確認した２枚の PCI-e ボードのみを用いて、送受信機ともに全ての光学部品を制御するための機器の検証、偏波コントローラの動作の検証などを進めた。計画では、平成２９年度の上期までに、ハードウェア機能の実装を実施する予定であり、順調に進捗した。ソフトウェアについては、送受信のディレイライン間の相対位相を初期化する機能、受信側のクロックを LO 光から生成する状況下で送受信者間のデータの照合を行う機能の実装などを進めた。東北大学中沢研究室との共同研究では、昨年度よりも現実的な仮定の下で 100km の鍵配送を実行する実験を進めた。東北大学との共同研究に用いていた第１世代の CV-QKD 装置は平成２９年１２月に NICT に移設し、以降の光通信との共存実証実験は、NICT との共同研究として実験を進めた。安全性評価技術の理論的な研究では、受信者の装置を盗聴者が操作できないと仮定し、盗聴者が一般的な攻撃（エンタングリングクローナ攻撃）を行う場合の鍵生成率の定量的な評価を実現した。

2-2 成果

高速 CV-QKD 装置（第２世代）の開発については、市販の PCI-e ボードのみを用いた光学部品の制御を実現するために、ハードウェアとソフトウェアの整備を行った。光スイッチ、可変光減衰器の操作は、高速 ADC ボードのオプションとして付属している DAC 出力、デジタル出力を用いて実行することができた（光スイッチは１チャンネルでは電流値が不足したので２チャンネルを用いた）。偏波コントロールについては、

外付けの高感度光検出器を用いるフィードバック動作を実装し、安定した長期間動作を実証した。光学系の改良により、第1世代と比較して1dB程度信号光の損失を改善することができた。送受信のディレイライン間の相対位相を初期化する機能については、xmlデータを送受信するプログラムを作成して実行し、相対位相のずれに関する情報が得られることを確認した。これらの機能の実装により、ソフトウェア制御により量子鍵配送動作が実行可能となり、送受信者間のデータの照合を行うための情報取得を実現できた。ハードウェア的なトリガー信号を用いることなく、送受信者間のデータの同期を実現することができれば、CV-QKD装置の簡素化とそれによる低コスト化を実現できる。

東北大学中沢研究室との共同研究として進めた100kmの鍵配送実験では、送信信号強度やポストセレクションしきい値の設定などを注意深く行い、盗聴者が0.2dB/kmの損失を持つ光ファイバーを0.15dB/kmの低損失ファイバーに置き換えたとしても安全な鍵を生成可能であることを実証することができた。NICTで実施した光通信との共存実験では、7チャンネルの12.5 Gbit/s古典信号との共存実験を行い、エラーフリーの古典信号伝送と量子鍵配送が共存可能であることを実証した。この成果は、既設ファイバー網を用いて量子鍵配送が可能であることを示すものである。

安全性評価技術の理論的な研究では、通信路の透過率と過剰雑音、受信者装置内の光の透過率と検出器によるものを含めた過剰雑音をパラメータとして扱い、受信者の装置を盗聴者が操作できないと仮定し、盗聴者が一般的な攻撃（エンタングリングクローナ攻撃）を行った場合の鍵生成率を計算し、パラメータの値が変わったときに、鍵生成率を定量的に明らかにした。また、実際の装置のパラメータを用いた鍵生成率とポストセレクションの誤り率、最適な信号光強度やしきい値の設定値などの計算を行った。これらの理論計算を用いることで、実際の装置で生成する安全性を評価することができる。

2-3 新たな課題など

高速CV-QKD装置の送受信者間のデータの同期については、xmlデータの送受信にかかる時間の変動があるため、同期を実行するための計算量を削減するという新たな課題が発生した。そのため、同期が取れたデータを見つけるためのアルゴリズムの改良を今後行う予定である。

CV-QKDと高速光通信の共存については、CV-QKDで用いる光のモードと高速光通信で使用する光のモードの重なりがあると、CV-QKDの過剰雑音が増加することが確立されつつあり、これらのモードの重なりを小さくするという課題が発生した。今後、光源や波長の構成を工夫することになり、モードの重なりが小さくなるように光学系を改良していく予定である。

3．アウトリーチ活動報告

なし