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２７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

量子セキュアネットワークの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研究開発を行う。これにより、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実現する。

平成２７年度は、多値変調技術を用いる量子鍵配送技術の高速化のために、高速動作する量子雑音限界ホモダイン検波技術の開発を行う。また、高速ホモダイン検波技術を用いて、高速化のもう一つの要素技術である高速乱数発生の技術開発を行う。ホモダイン検波を利用した乱数発生では､50Mbps 以上の乱数発生の実現を達成目標とする。さらに、これらの技術を実装する第２世代 CV-QKD 装置（第１世代の試作機に比べて安定化、高速化等の点で改善）の光学部品及び電気部品の構成、PC による制御及びデータ取得方法の詳細設計を行う。

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

量子雑音限界で動作する高速ホモダイン検出技術の開発については、従来の検出器の高速動作特性の評価、新しいバランス検出器の性能評価、PC への取り込み動作の高速化を実施した。従来の検出器の評価については、昨年度まで用いていた検出器について２つのフォトダイオードの時間差調整、高速の量子雑音限界動作の検証等を実施した。新しいバランス検出器としては、国産の製品と輸入製品の性能評価を実施した。PC への取り込み動作については、３種類の PCI-Express 接続の ADC ボードを用いて、時間分解能等による最適化の検証を実施した。

高速乱数発生の技術開発については、上記のバランス検出器と ADC ボードを用い、連続発振半導体レーザーを 50%:50%のビームスプリッタで分岐してバランス検出器に入射することにより、真空状態の量子揺らぎをエントロピー源とする物理乱数の発生を実施した。第２世代 CV-QKD 装置の開発については、光学部品及び電気部品の選定と調達、PCI-Express 接続の ADC ボードの仕様の比較と実機を用いた検証等を行った。

2-2 成果

従来の検出器の高速動作特性の評価については、２つのフォトダイオードの時間差調整により、バランス検出の実効的な同相成分除去比を改善することができた。更に、レーザー光のパルス時間幅、電圧信号をサンプリングする際の周波数特性等を調整し、市販のバランス検出器を用いて、優れた特性を持つ量子雑音限界のホモダイン検出を実現することができた。入射パルス光のパワーを増やしたとき、測定された電圧の分散は、入射パワーに対して線型に増加し、量子鍵配送の動作条件下で、ショット雑音の大きさが検出器自身の雑音よりも 16 倍大きくすることができた。また、隣り合うパルスの測定データの相関係数はほぼゼロであった。この時用いた PCI-Express 接続の

ADC ボードは高速のデータ転送が可能であり、量子鍵配送の高速化を実現することができた。送信者が 4 値の位相変調を行い、受信者がポストセレクションによりビット値を生成し、誤り訂正をリバースリコンシリエーションにより行う連続量量子鍵配送プロトコルを用いて、量子通信路が 10km の光ファイバーのとき、300 kbps の raw key rate を実現することができた。受信パルスのうち、半数は通信路のパラメーター推定に用いており、鍵の生成は、残りの半数のうち基底が一致し、かつ、測定電圧がしきい値を超えたもののみを用いた。秘匿性増幅によりエンタングリングクローナー攻撃に対して安全な鍵をリアルタイムに生成することができた。さらに、東北大学との共同研究により、フィールド動作実証、量子鍵配送と光通信との波長多重伝送実験等を実施した。ホモダイン検波は、L0 光と重なるモードの光のみを検出する原理であり、L0 光が周波数領域および時間領域のフィルターとして働くため、漏れ光に対する耐性が期待できる。実験では、光通信との波長多重による過剰雑音の増大は見られなかった。

ホモダイン検波技術を用いる量子物理乱数発生については、200 MHz の周波数帯域を持つバランス検出器の出力電圧を、14 bit の分解能で 100 MS/s の ADC でサンプリングしたデジタルデータを、32 の bin に等分割し、500 Mbps という高速の物理乱数生成を実現した。これは、真空状態の直交位相振幅の量子揺らぎを用いる物理乱数の発生として、従来よりも 2 桁程度高速であり、第 2 世代 CV-QKD 装置の乱数源として十分な速度である。次に、乱数の質を検証するため、NIST STS (NIST 800-22, sts 2-1-2)、および TestU01 (TestU01-1.2.3, Crush test)を用いて検定を実施した。TestU01 は乱数の問題点を検出する性能が優れており、標準的に用いられている乱数検証ツールである。TestU01 crush test は、31 種類 144 項目の検定からなり、1 項目最大約 4.4 Gbits の乱数を必要とする。上記の方法で生成した物理乱数を crush test により検定したところ、14 種類のテストについては全項目で合格した。不合格になる項目があるのは、例えば、レーザー光の強度揺らぎのような古典的な雑音が影響を与えていると考えられる。QKD の運用に用いる乱数に何らかの相関が存在することは望ましくないので、次に、ランダムなテープリッツ行列を用いた質の改善を試みた。テープリッツ行列の掛け算は、fft を用いることで、計算量を削減できるというメリットがある。テープリッツ行列を掛けた後の乱数を、TestU01 crush test で検定したところ、全種類全項目のテストに合格した。

2-3 新たな課題など

第 1 世代 CV-QKD 装置に用いているインターフェースボードはカスタム製品のために高価であるほか、乱数データの PC への転送が低速であるという問題点がある。予算の効率的な使用のために、入出力ボード・制御ソフトウェア・光学系と制御ハードウェアの検討、安全性証明、物理乱数の質などの研究開発を継続する。

３．アウトリーチ活動報告

出張授業、青山学院中等部、２０１６年２月２４日、中学３年生１６名