平成 27 年 3 月 31 日

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 26 年度

研究開発課題名：

新世代量子セキュリティ技術の研究開発

研究開発機関名：

東京大学

研究開発責任者
小芦 雅斗

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

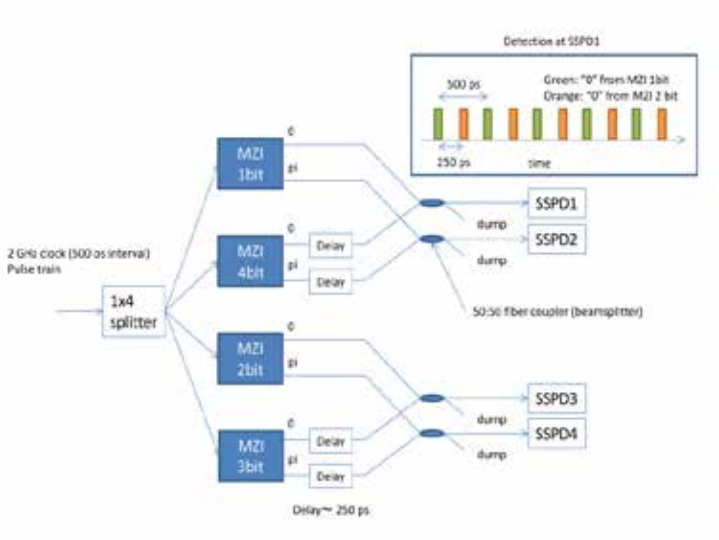
量子セキュアネットワークのグローバルネットワーク化に向けて、多様な形態を持つネットワークに適用するために様々な条件で動作する新世代技術が求められる。本研究開発課題では、雑音の監視によって盗聴の多寡を検知する従来の量子鍵配送とは異なる動作原理に基づく RR-DPS（総当たり式差動位相変調）量子鍵配送プロトコルについて、現実的な実装を想定したセキュリティ理論を確立することで、高い雑音耐性を持ち、短いセッションでの効率的な動作が可能な量子鍵配送方式の設計を行う。

計画の最初にあたる平成２６・２７年度は、理想モデルと実際の装置との解離がもっとも顕著な光子検出器について、実用的な装置モデルのもとでのセキュリティ理論を確立する。光子の個数を完全に見分ける検出器は現在存在せず、低コストで使用できる検出器は、光子の有無だけを検出する閾値型の検出器となる。この場合、現状のセキュリティ理論には直接当てはまらなくなるため、複数光子の入力が少ないことを監視する仕組みの導入や、セキュリティ理論の拡張により対応する手法を開発する。可変遅延回路を能動的に切り替える実施形態と、受動的に光経路を分岐する実施形態では、複数光子が測定装置に入力された場合の振る舞いが異なるため、両者の場合についてそれぞれ解析が必要である。平成２６年度は、受動的に光経路を分岐する実施形態について、閾値型検出器を使用する場合のセキュリティ理論の確立を目標とする。

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

現実的な装置を用いた場合のセキュリティ理論の構築にあたっては、RR-DPS プロトコルを実際に実装することで得られる知見が有用であることは言うまでもない。この点で、RR-DPS プロトコルは、まだ理論的提唱の段階に留まっていた。そこで、本プログラム参画機関である NTT（日本電信電話株式会社）との研究協力により、RR-DPS プロトコルの原理実証実験に着手した。RR-DPS プロトコルは、連続したパルスを１つのブロックとして、検出側で可変遅延を持つ干渉計により相対位相を総当たり的に読み出すものであり、ブロックを構成するパルスの数 L というパラメーターを持つ。性能という点では、L は大きいことが望ましいが、その分干渉計の構成が複雑になる。今回は、最初の原理実証実験として、L が 5 パルスの場合の RR-DPS プロトコルを、受動的に光経路を分岐することで干渉計の遅延を可変とした実施形態を選択した(右図)。L が 5 パルスであっても、雑音の監視に依らずに



鍵配送を行うという RR-DPS プロトコルの最大の特長は実証可能である。

この原理実証実験では、閾値型の検出器を用いているため、この実験により確かに鍵配送が実行できることを実証するには、今年度の目標である閾値型検出器を使用する場合のセキュリティ理論の構築が必要となる。RR-DPS プロトコルの動作原理の中で重要な点として、ブロック中の L 個のパルスの中で、どのパルス対の相対位相がビットとして採用されるかが十分にランダムであり、盗聴者が作為的に制御できないという性質がある。当初のセキュリティ理論においては、この性質は、受信者に届く L 個の光パルスの中に含まれる光子の総数がたかだか 1 個であるという仮定のもとに証明されていた。この議論は、光子数 1 個と 2 個を見分ける能力をもつ検出器を用いて、光子の総数が 1 である場合のみのデータを抽出する実施形態の場合にしか適用できない。検出器が閾値型の場合、複数光子が検出器に入力したデータが混入することが避けられないため、その上でセキュリティをどう確保するかが課題であった。

今回の原理実証実験では、盗聴者による意図的な攻撃がない場合には、複数光子の入力が起こる頻度は非常に少ないことが想定された。そのため、セキュリティ対策としては、複数光子入力の頻度が確かに少ないことを、複数の検出器で同時に検出が起こるイベントの頻度を手がかりとして推定する方針を選択した。

2-2 成果

受動的に光経路を分岐する RR-DPS プロトコルの実施形態について、閾値型検出器を使用する場合のセキュリティ理論を構築した。複数の検出器で同時に検出が起こるイベントの回数をもとに、複数光子の入力が起こる頻度を推定し、秘匿性増幅の度合いに反映させることで、セキュリティを保証するものである。この推定のために、実施上特別な装置を追加する必要はない。総通信時間が長い極限における漸近的な鍵生成レートだけでなく、総通信時間が限られた場合に、与えられたセキュリティパラメータを満足する最終鍵を生成する手続き（有限長解析）も与えた。

原理実証実験に適用するにあたっては、上記の一般論に加えて、時分割多重化に伴う検出器の不感時間の影響が無視できないことが判明したが、これについても、同時検出が起こるイベントの種類を精査することで、影響が回避できることを見出し、解決した。実際に実験で得られたデータで解析を行い、現実的な通信時間で鍵生成に成功していることが確かめられ、原理実証実験としての目的が達せられたと考えている。

2-3 新たな課題など

今回は、複数光子の入力が起こる頻度の推定によりセキュリティを確保する手法を開発したが、一般には、推定を伴う手法は通信時間が短い場合に推定精度が落ちる欠点がある。そこで、今回の手法と相補的な手法として、複数光子の入力が起こる頻度に依らずに成立するセキュリティ確保の手法を検討している。また、パルス数 L を大きくするためには能動的な可変光遅延回路が望ましいが、その可変の速度に関する制約を大幅に低減する可能性が浮上し、検討を開始した。

3．アウトリーチ活動報告

今年度はとくに該当なし。