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：

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

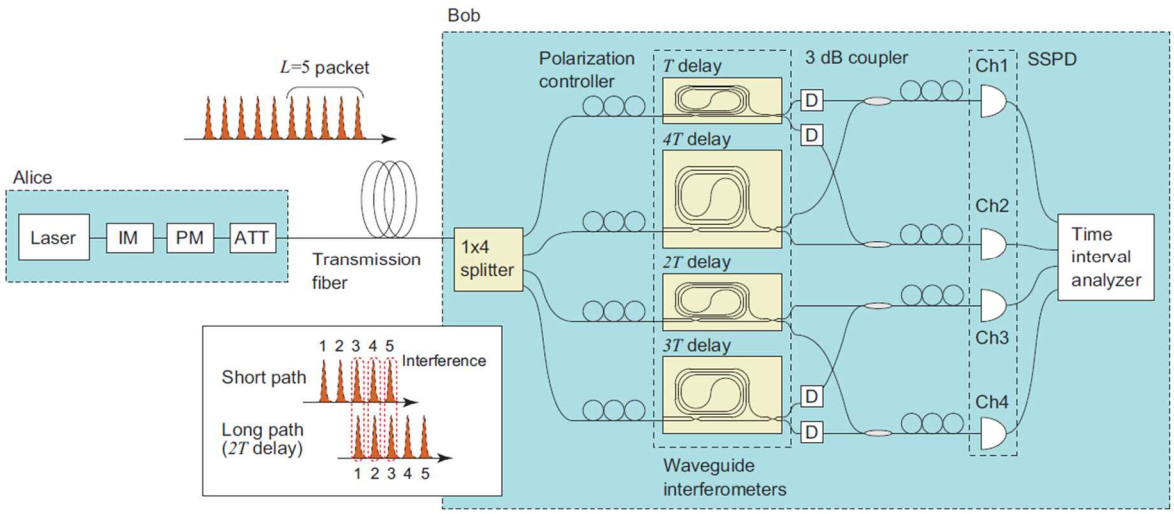
量子セキュアネットワークのグローバルネットワーク化に向けて、多様な形態を持つネットワークに適用するために様々な条件で動作する新世代技術が求められる。本研究開発課題では、雑音の監視によって盗聴の多寡を検知する従来の量子鍵配送とは異なる動作原理に基づく RR-DPS（総当たり式差動位相変調）量子鍵配送プロトコルについて、現実的な実装を想定したセキュリティ理論を確立することで、高い雑音耐性を持ち、短いセッションでの効率的な動作が可能な量子鍵配送方式の設計を行う。

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。

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

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昨年度より着手し、本年度に完了した。



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。実験は、L が 5 パルスの場合に相当し、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受信装置を用いた(上図)。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。

検出器の現実的なモデルに関しては昨年度に構築した基本理論を用い、最終的に得られる鍵長を決定した。それとは別に、送信器に関する RR-DPS プロトコルの特長として、送信者から送出される光子数の分布についての仮定が少なくて済むという点が挙げられる。レーザー光を用いた量子鍵配送で、鍵生成率が伝送距離依存性に優れている（通信路透過率に鍵生成率が比例する）ものとしては、デコイ BB84 方式があるが、光子数の分布がポアソン分布であるなどの厳しい仮定が用いられることが多く、その仮定を光源の較正実験によって確認することは容易でない。これに対して、RR-DPS プロトコルでは、所定の閾値を越える光子数が送出される確率の上限値のみを必要とする。そこで、この点を今回の原理実証実験においても確認するため、光源に対してオフラインで光子の相関測定を行うことで、この上限値を理論的仮定ではなく実験的に決定することを試みた。

遅延を能動的に切り替える場合については、昨年度に、切り替え速度を大幅に遅くできる可能性が浮上し、今年度にその検討を行っている。RR-DPS 方式に限らず、より多くの方式に適用できる理論として発展中であり、その整理を進めている。

2-2 成果

上記の装置において、実験で得られるシフト鍵の長さが有限であることも考慮に入れたうえで、必要な秘匿性増幅の大きさを求め、３０ｋｍ伝送に相当する通信路損失において、信号への擾乱を監視することなく秘密鍵が生成できることを実証した。さらに、光源の性質に関しての仮定が少なくて済むという RR-DPS プロトコルの特長の実証として、使用した光源についてオフラインの光子相関測定を行い、本実験のシフト鍵無限長極限の結果については、光源の性質を仮定するのではなく実験的な較正結果から保証できることも示した。

2-3 新たな課題など

今回の光源の較正実験では、シフト鍵が有限の場合のセキュリティ理論と組み合わせることができていない。光源の長期的なゆらぎや変化についてそもそも何を仮定すべきか、という根本的な問題も含むため、更なる見当が必要である。また、比較対象であるデコイ BB84 方式の光源較正の理論もまだ不十分であり、プロジェクトの他機関とも協力して検討する必要があると考える。

３．アウトリーチ活動報告

平成２７年１１月１８日に、青森県立三本木高等学校附属中学校にて、「光の正体と究極の暗号」と題した出張講義を行った。小芦雅斗、佐々木寿彦、鈴木泰成の 3 名で担当し、対象者は、同校中学三年生 80 名。講義内容は２部構成で、第１部（５０分）では偏光板とレーザーポインタを用いた実習教材による体験形式で、波としての光の性質、特に偏光について理解を深められるようにした。続いて、講義形式の第２部（５０分）で、粒子としての光の性質、量子力学の簡単な導入、微弱な光を利用した解読不可能な暗号である量子暗号について解説し、ImPACT の活動について紹介した。