2019年 11月 28日

東京大学光イノベーション基金奨学金

研究経過報告書

奨学厚生担当理事　殿

所属研究家・専攻	工学系研究科　物理工学専攻
学生証番号	37-186564
申請者氏名	(ふりがな) まえだ けんと 前田　健人

研究テーマ	高い有限長性能をもつ量子暗号プロトコルの探求
研究経過報告	1. 研究の学術的背景 秘匿通信に利用する鍵を共有するにあたり、光の量子力学的な性質（不確定性関係など）を利用した「量子鍵配送（QKD)」では、盗聴者の計算能力に仮定を置くことなく鍵の安全性を担保できる。レーザーや光子検出器など汎用的に用いられる光学技術の範囲で実装可能であり、計算機性能の向上で脆弱化が懸念される既存暗号方式の代替策として期待される。 実装上有意義な研究の一つに、QKDの波長分離性の向上の試みが挙げられる。波長分離と親和性の高い測定手段（ヘテロダイン測定など）を用いたプロトコルができれば、多重化により時間当たりの鍵効率を高めたり、敷設済みの通信路上で通常の通信と別帯域のQKD通信を共存させて利用したりできる。一方、分離性の高い測定手段を定式化する上では連続量（無限次元）量子系としての光の性質が現れるため、既存のQKDの安全性証明手法を適用しづらいという困難もある。 2. 研究経過 ヘテロダイン測定・ホモダイン測定を用いたQKDプロトコルで、送信者（アリス）のbit値の情報をレーザー光の位相の情報に載せて送るものを考察の対象とする。 研究初期には申請者が前回の研究で利用した「演算子優越法」による評価を試みたが、満足のいく鍵生成レートが得られなかった。これらの測定がもともと大きな誤差幅を持つため、盗聴者への情報漏えい量をかなり厳しい不等式で評価しなければ鍵を取れないことに起因していると考えられる。 続いてより厳しい評価を行うため、(1)受信者（ボブ）のもとに届く状態がどの程度理想に近いか（理想状態との「忠実度」という指標）を測定結果のみから推定する数学的方法の開発と、(2)実際に忠実度が高い（bit値のエラーが1パーセント発生する程度の）状態がボブに届いているときの鍵生成レートの計算を行った。(1)では、1回ごとのヘテロダイン測定結果を特殊な関数で後処理し平均をとることで、忠実度の下限値を推定できることがわかった。(2)についても、通信時間が十分に長いと仮定できる場合には”Reverse reconciliation”などの後処理のテクニックを用いることで、通信路の透過率が0.7（光ファイバーで7km程度）の時に鍵を取り出せることがわかった。 3. 今後の研究計画 上記の部品(1)(2)が揃ったため、通信時間が十分に長いという仮定を取り外し、安全性証明を完成させることを目標とする。まず、統計ゆらぎを評価する「Azumaの不等式」の方法を用い、(1)で監視した量から、(2)の忠実度などのパラメータを絞り込む条件式を立てる。その後、凸最適化の手法を用い、絞り込んだパラメータ範囲で鍵生成レートが最小化する点（盗聴者が狙う攻撃方法）を見つける。この点での鍵生成レートの値を真の鍵生成レートとし、透過率ごとの鍵生成レートを出力させる。以上の結果を論文にまとめる。

上記の通り相違ありません。

指導教員：小芦雅斗　印

所属部局：工学系研究科