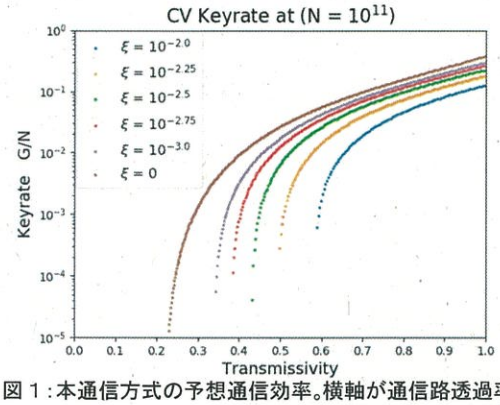
2020 年　3 月　25 日

東京大学光イノベーション基金奨学金

終了報告書

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
終了報告	1. 研究の学術的背景 「量子鍵配送（QKD）」は、量子力学の性質（不確定性関係など）を利用し、盗聴者の計算能力に仮定を置くことなく安全性を担保できる暗号通信方式である。レーザーや光子検出器などの汎用光学技術の範囲で実装でき、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。 異なる帯域で暗号通信を多重化したり、敷設済みの通信路上で他の通信と QKD を共存させたりする運用を可能にするため、QKD の波長分離性の向上が注目されている。しかし、それに適する測定手段（ヘテロダイン測定など）を用いた場合、無限次元量子系としての光の性質を扱い、有限の通信時間だけで情報漏えいの量を評価する必要がある点が困難であった。 2. 研究成果 上述の測定手段を用いた通信方式のデザインと、通信効率の計算を行うことに成功した。成果を論文として投稿予定である。 前回の報告までに、通信時間無限の極限で(1)受信者のもとに届く状態の忠実度（どの程度理想に近いか）を推定する方法の開発と、(2)実際に忠実度が高い場合の通信効率の計算を行った。以降の研究で、これを通信時間有限（有限長）の場合に拡張した。具体的には、統計ゆらぎを評価する「Azuma の不等式」と凸最適化の手法を利用し、有限長の場合にも(1)で監視した量を使って情報漏えい量を見積もり、(2)の目的を果たせることを確認した。その結果、通信路の透過率が 0.3 から 0.4 程度あれば、有限長でも波長多重化と秘匿性を両立して通信できることが明らかになった。  図 1：本通信方式の予想通信効率。横軸が通信路透過率、縦軸が総通信回数に対する秘匿通信 bit 数の割合であり、ξは通信路のノイズ量を表すパラメータである。
指導教員のコメント	量子レベルの微弱光信号の測定技術として、光子検出とホモダイン／ヘテロダイン検出があり、それぞれに長所を持ちますが、量子鍵配送に関しては、後者のセキュリティ理論は複雑で、未解決の問題が多く残っています。前田氏は、OASIS の研究奨励金をいただけることになってから、腰を落ち着けてこの難題に取り組むことができました。その結果、有限の通信時間を考慮してセキュリティを確立するための大きなハードルをクリアできたと考えています。また、前田氏は、この 3 月に東京大学総長賞を受賞しています。OASIS 奨学生のこれまでの卒業生は、総じて非常にレベルが高いという印象でしたが、前田氏も、その期待に十二分に答えてくれたと思います。

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