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 28 年度

研究開発課題名：

量子セキュアネットワークの安全性評価に関する理論研究

研究開発機関名：

日本電信電話株式会社

研究開発責任者

玉木　潔

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

課題1、物理暗号と量子セキュアネットワーク全体の安全性向上

量子セキュアネットワーク全体の実装安全性を強化するために、まずは物理層のサイドチャネルや不完全性の洗い出しを行い、それらの対策提案を行う。特に今年度は、有限の精度をもつ装置を用いた量子鍵配送装置の有限パルス数における秘密鍵生成率を計算する方法を与える。また、現実的な装置を用いたRRDPSプロトコルの鍵生成率を計算する方法の導出を試みる。後者の研究に対しては、とりあえずは無限パルス数を仮定する。最後に連続量量子鍵配送については、信用できない参照光を考慮したホモダイン測定やヘテロダイン測定を表現する理論の構築を目指す。

課題2、量子セキュアネットワーク全体の安全性基準書の作成

安全性評価基準書を改定する。

課題3、量子鍵配送の通信距離延長及び通信速度向上検討

今年度は、量子インターネットに対する一般的な制約を導き、それに基づき、既存の量子中継方式に対する理論限界を導出する。また、この限界から、量子中継方式に必要となるデバイスの最低限の要請を明らかにすることを目指す。同時に、他者間量子インターネットプロトコルに適用可能な理論限界の導出も試みる。

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

課題１について：まず、有限の精度をもつ装置を用いた量子鍵配送装置の有限パルス数における秘密鍵生成率を計算する方法についてであるが、装置の不完全性をどこまで取り入れるかに応じて、問題の難易度が大幅に変わる、という当初は予想できなかった状況に陥ったため、現在、どのような方向性で問題設定を行うのがよいかについて、実際の装置の性質と照らし合わせて検討している段階である。その一方で、デコイBB84方式で使われる送信機に対するサイドチャネル攻撃対策方法をスペインのヴィーゴ大のカーティー教授と東芝ヨーロッパのルカマリーニ博士と共同で考案し、論文化した。

次にRRDPSについてであるが、従来のRRDPSでは受信器が選択するべき光路差のセッティングが非常に多かったが、我々はこれを少数にすると何が起きるかについて調べた。この新たなプロトコルはオリジナルのDPSより鍵生成率が高いが、RRDPSよりは低い、ということを結論付けた。この我々の新たなプロトコルにより、実験装置の性能や要求する鍵生成率に応じて適切なDPS型プロトコルを選択できるようになり、実験における選択肢を増やした。この結果は学術誌Phys. Rev. Aにて発表をした。

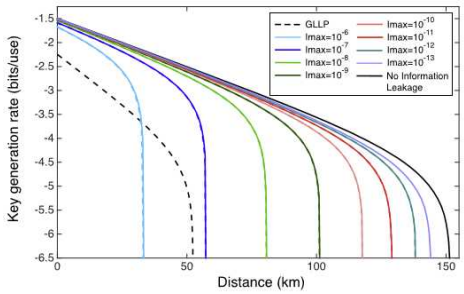
信用できない参照光を考慮したホモダイン測定やヘテロダイン測定を表現する理論の構築については、現在も研究中であり、基本となる考え方の拡張を試みている段階である。

課題２について： 安全性評価基準書の執筆を NICT,北海道大学、NEC などとの共同の下で行った。

課題３について： 今年度は、任意の量子ネットワーク上で行う任意の 2 者間量子通信プロトコルに対し、ネットワーク上の通信路の特性だけで決まる一般的な理論限界を与えた。この理論限界は、単一通信路の秘匿通信容量や量子通信容量の上界である Takeoka-Guha-Wilde（TGW）限界を一般化することで得られた。従って、本理論限界は TGW 限界の「任意の通信路に対して評価可能」という特性を引き継ぎ、量子ネットワークがどのような通信路で構成されていようとも評価できる。この成果は論文としてまとめられ、今年度 Nature Communications から出版された。

2-2 成果

ここでは、今年度の主な成果である課題１のサイドチャネル攻撃対策についての説明を行う。サイドチャネル攻撃がある元でのデコイ BB84 量子鍵配送は、送信者が送信する光パルスとサイドチャネル光の２モードの量子鍵配送と見なせる、という基本的な考え方から出発した。まず、強度変調器に対するサイドチャネル攻撃、つまりデコイ法においては、送信者がパルスを放出した下で受信機が検出事象を得る確率を、サイドチャネル光を利用することにより操作することが盗聴者の目的の一つである。しかし、この操作はサイドチャネル光から導出されるトレース距離によって律速されていることに気づき、この考え方を発展させることに成功した。位相変調器については既存の理論を発展させた。これらにより、我々はどのようなサイドチャネル攻撃のモデルが与えられても、そこから得られる鍵生成率を計算する処方箋を与え、この結果を学術誌 K. Tamaki, M. Curty, and M. Lucamarini, NewJ.Phys.18(2016)065008 にて発表した。以下に、該当論文から抜粋した鍵生成率の一例を示す。このグラフでは左から右へグラフが移り変わるにつれて、サイドチャネル光の強度が弱くなっている状況を考えている。



2-3 新たな課題など

サイドチャネル対策については、位相変調器については鍵生成率を向上させるために理論をより発展させる必要がある。また、有限の精度をもつ装置を用いた量子鍵配送については、問題が非常に複雑であるため、問題解決のために新たなアイディアが必要であるので、チーム内でさらに議論を進める予定である。

３．アウトリーチ活動報告

特になし。