様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １４ 日現在

機関番号：１３８０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００００１４

研究課題名（和文）量子ネットワーク上の長距離秘密鍵配送

研究課題名（英文）Secret key distribution over a long distance on a quantum network

研究代表者
尾張　正樹（Owari, Masaki）

静岡大学・情報学部・准教授

研究者番号：８０７２３４４４

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では、量子ネットワーク上における秘匿通信に関する研究を行った。特に、既存技術であるノード間の量子鍵配送を用いた秘密鍵共有を補完するために、量子ネットワークの安全性を向上させるために、ネットワーク符号を用いる手法の開発を試みた。結果として、single-shotのマルチプルユニキャスト通信において、量子ネットワーク符号が、量子ネットワーク上の与えられたエッジに対するEveの攻撃に対して秘匿性を持つための十分条件を明らかにした。また、ノード間の量子鍵配送を用いて鍵のリレーを行う場合に、ノードの乗っ取り攻撃に対する安全性を古典ネットワーク符号を用いて向上させる手法の開発を行った。

研究成果の学術的意義や社会的意義
従来技術である量子鍵配送プロトコル(QKD)は、非常に強い安全性を保障するが、送受信者間で何度の通信を行う必要があるなど、コストの非常に高いプロトコルである。一方で、本研究で開発した手法を用いるとは、QKDよりも低いコストで、QKDよりも弱い安全性を得ることができる。また、本研究で開発した手法は、非物理層に属するプロトコルであるため、物理層のプロトコルであるQKDと同時に用いることで共存可能であるという特徴も持つ。このように、本研究結果は、従来手法であるQKDを補完する手法として、将来の量子ネットワークの安全性に寄与すると考えられる。

研究成果の概要（英文）：Here, we studied a secret communication on a quantum network. We especially focused on using network coding for improving security on quantum networks in order to complement a quantum key distribution (QKD) among nodes. As a result, we derive a sufficient condition for a quantum multiple-unicast network code to have a secrecy for Eve’s attack on a set of edges. Further, we develop a method for improving a security for Byzantine attacks on a relay scheme of keys generated by QKD by using classical network coding.

研究分野：量子情報

キーワード：量子情報　量子ネットワーク　ネットワーク符号　量子鍵配送　量子通信　安全性評価

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

量子情報処理における最も重要な暗号プロトコルである量子鍵配送(QKD)は、実用化の段階を迎えており、その性能や限界が明らかになっている。QKD は究極の安全性を保障する代わりに、最終的な秘密鍵の生成までに、送受信者間で複数回の情報通信を行う必要があり、実行のためのコストが高いものになっている。一方で、デバイス開発技術の発達により、多数の量子コンピュータが量子通信路で接続された量子ネットワーク(量子インターネット)が近い将来に実現すると考えられている。従来、QKD は 2 者間通信を目的として研究が行われてきたため、QKD を用いるにせよ、用いないにせよ、多数の中間ノードを持つ量子ネットワークに特有の安全性の解析が必要とされている。

２．研究の目的

1 つの量子通信路を用いて送信者と受信者間で秘密鍵を共有する QKD は、高い安全性を持つが、高コストでもある。

(1) 量子通信路からなる多数のエッジと量子コンピュータからなる多数のノードから構成された量子ネットワーク上においては、個々のエッジの安全性は QKD を用いて保証することはできても、中間ノードを乗っ取られた場合には、完全性が担保できない。この問題を解決するため、ネットワーク上の少数のノードのみが乗っ取られた場合に、安全性を保障する手法の開発を目指す。

(2) 量子ネットワーク上の多数のエッジが同時に盗聴されることは現実的には可能性が低いと考えられる。そのため、特定のエッジへの攻撃にのみ安全を持つ、QKD よりも低コストなプロトコルの開発を 2 つ目の目標とした。

３．研究の方法

上記の課題(1)(2)は、共にネットワーク符号の技術を応用することで解決することができる。ここで、ネットワーク符号とは、ネットワーク上の中間ノードで非自明な演算を行うことで、ネットワーク全体のスループットや安全性の向上を目指す技術のことである。 課題(1)に関しては、各ノード間で QKD により得られた秘密鍵を使って、鍵のリレーを行う際にノードの乗っ取りに対して安全性を持つようなネットワーク符号を用いることで解決ができる。一方で、課題(2)に関しては、ネットワーク符号を用いた量子ネットワーク上のネットワーク通信プロトコル(量子ネットワーク符号)が、特定のエッジへの攻撃に対して秘匿性を持つための条件を解析することで問題の解決を行った。

４．研究成果

(1)　従来の古典ネットワーク符号の研究は、ネットワークへの盗聴に対する秘匿性の研究と、ネットワーク上へのノイズの混入に対する回復可能性の研究が独立に行われてきた。しかし、盗聴者が積極的にノイズをネットワークに混入することにより、ネットワークから盗聴できる情報量を増やせるかどうかという問題は未解決であった。まず、本研究においては、まずこの問題の解決を目指した。結果として、線形ネットワーク符号に対しては、盗聴者はノイズを混入することにより、獲得する情報量を増やすことはできないことを証明した。さらに、ネットワーク上の送信者から受信者への送信レートが m_0 であり、盗聴者が混入するノイズのレートが m_1、盗聴者が得る情報のレートが m_2 である場合に、レート m_0-m_1-m_2 で安全に情報を通信できるネットワーク符号が漸近的に存在することを証明した。一方で、もし盗聴者が攻撃を行った場合の回復可能性は課さずに、盗聴者の攻撃に対する秘匿性のみを課す場合には、レート m_0-m_2 で盗聴者に情報を与えずに情報を通信できるネットワーク符号が漸近的に存在することを証明した。

　次に、ネットワーク上の隣接ノード間で QKD を用いて共有をした秘密鍵を用いて、送受信ノード間で秘密鍵を共有するために、遠距離のノード間で次に上記で行った解析を応用した。特に、回復性を課さない場合に秘匿性を保つネットワーク符号を用いて、様々なネットワーク上で、秘密鍵を共有可能なレートを求めた。

　最後に、非線形なネットワーク符号に対しては、盗聴者はノイズの混入により獲得できる情報量を向上させることができることを示した。特に、Figure 1 で表される One-hop リレーネッ

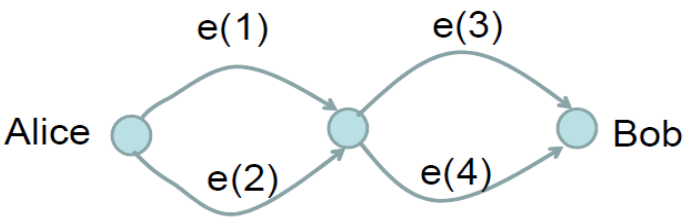

Figure 1：One-hop リレーネットワーク

トワーク上で定義される非線形ネットワーク符号おいて、盗聴者は中間ノードの前後で 1 本ずつのエッジを盗聴するだけでは入力情報を完全に得ることはできないが、中間ノードの前でノイズを混入することにより、入力情報を完全に入手できることを示した。さらには、One-hop リレーネットワークにおいて、複数の自然な仮定をネットワーク符号に関して課すことで、ノイズを混入することで盗聴可能な情報量が増える標数 2 の有限体上のネットワーク符号は、上記の例に限られることを証明した。また、任意の標数 2 の有限体上のネットワーク符号は、上記の攻撃に対して安全ではないが、標数 3 の有限体上においては安全なネットワーク符号が存在することを証明した。

(2) 古典ネットワークにおけるネットワーク符号と同様に、量子ネットワークにおいても中間ノードにおける非自明な演算を利用する量子ネットワーク符号の研究が行われてきた。しかし、従来の量子ネットワーク符号の研究は、スループットを増加させることにのみ目的を絞っており、安全性への寄与に関する研究がなされていなかった。一方で、上記(1)において説明したように古典ネットワークの研究においては、ネットワーク符号は安全性の向上にも寄与することが知られている。そのため、量子ネットワーク符号も量子通信の安全性に寄与することが期待される。

我々は、まず、Figure2 で表されるバタフライネットワークを考えた。バタフライネットワーク上の量子ネットワーク符号は既知であったが、従来のプロトコルでは安全性が保障されなかった。古典ネットワーク符号においては、Figure2 で表されるように送信ノード間で古典秘密情報を共有することで、任意の一つのエッジを盗聴されても安全な古典通信が可能である。一方で、この古典ネットワーク符号を用いて標準的な手法で構築した、同じ形状の量子ネットワーク上の量子ネットワーク符号は、1 つのエッジ(量子通信路)に対する攻撃とネットワーク間の古典通信の盗聴により、情報が盗聴されることを示した。さらには、受信ノード間においても古典秘密情報を共有することができれば、任意の一つの量子通信路を盗聴者に攻撃され、更にネットワークでの古典情報通信をすべて盗聴されたとしても安全性が保障されることを証明した。

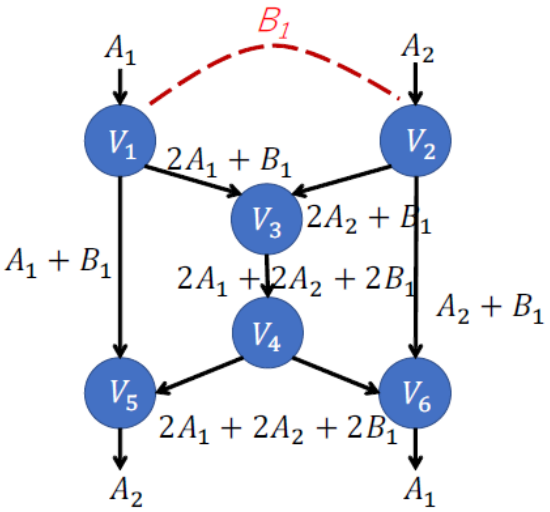

Figure 2：バタフライネットワーク上の古典ネットワーク符号による情報の流れ

この古典ネットワーク符号を用いて標準的な手法により構築したものが本研究において安全性が証明された量子ネットワーク符号である。

V_1, V_2：送信ノード，　V_5, V_6：受信ノード，

A_1, A_2：送信情報，　　B_1：古典秘密情報

次に、この結果を任意の量子ネットワーク上の mutiple-unicast 通信に拡張することを目指した。上記の結果から、対応する古典ネットワークにおいて符号が安全であったとしても、その量子ネットワークへの拡張は必ずしも安全にはならないことを見出していた。この点に注意をしながら一般の量子ネットワーク符号に関する安全性の解析を行うことで、量子ネットワーク符号の安全性を担保するためには、対応する古典ネットワーク符号が安全するのみでは不十分であり、さらに対応する古典ネットワークが盗聴者の攻撃に対して頑強である必要があるということを証明した。さらに、盗聴者の攻撃に対して安全かつ頑強な任意の古典ネットワーク符号をもとにして、盗聴されても秘匿性の保たれる量子ネットワーク符号を作成する方法を与えた。この一般的な手法を用いることで、任意の 1 量子通信路が盗聴されても安全な非自明な n 人の送信者がそんざいする量子ネットワーク符号や、任意の 2 つの量子通信路が盗聴されて

も安全な量子ネットワーク符号を構築した。また、安全な量子ネットワーク符号と量子秘密分散との関係性を明らかにした。

最後に、上記の安全な量子ネットワーク符号プロトコルでカバーしきれなかった点を補う新たなプロトコルの開発に取り組んだ。上記で、得られた安全な量子ネットワーク符号プロトコルには大きく分けて 2 つの点で、改善の余地があった。前年度の手法の 1 つ目の問題点は、プロトコルが保証するのは秘匿性のみであり、盗聴者が攻撃を行った場合には、通常量子状態は破壊されてしまい、受信ノードは正常な受信ができないという点である。この点を改善することを目指して、今年度は、攻撃を受けても入力量子状態の復元が受信ノードで可能であるようなプロトコルの構築を目指した。結果として、N 個の出力ノードと 1 つの受信ノードをもち、さらにネットワークの形状に一定の制限を置いた場合には、攻撃を受けた場合にも受信ノードにおいて入力量子状態の復元ができることを示した。上記の手法の 2 つ目の問題点は、プロトコルが通信路への攻撃しか想定をしていない点である。実際の量子ネットワークにおいては、量子通信路を盗聴されることより、むしろノードを乗っ取られる方が、より起きやすい攻撃だと考えられる。そこで、本年度は、前年度のプロトコルに対する、ノードを乗っ取られた場合の安全性についての解析を行った。結果として、2 個の送信ノード、1 個の受信ノード、2 個の中間ノードからなる非常に簡単なネットワークの場合には、中間ノードを乗っ取られたとしても安全性が保障されることを証明した。

５．主な発表論文等

〔雑誌論文〕（計 3 件）

(1) Go Kato, Masaki Owari, Masahito Hayashi, "Single-Shot Secure Quantum Network Coding for General Multiple Unicast Network with Free Public Communication", Lecture Note in Computer Science, Vol.10681, pp 166-187, (2018) 査読あり
(2) Owari Masaki、Kato Go、Hayashi Masahito , "Single-shot secure quantum network coding on butterfly network with free public communication" , Quantum Science and Technology, Vol.3, Number 1, 014001, (2018) 査読あり
(3) Masahito Hayashi, Masaki Owari, Go Kato, Ning Cai,"Secrecy and robustness for active attack in secure network coding", Proceedings of 2017 IEEE International Symposium on Information Theory (ISIT), pp.1172 - 1176 (2017) 査読あり

〔学会発表〕（計４件）

(1) 武田玲志，尾張正樹，“中断可能な完全サンプリングのための量子アルゴリズム”，情報学シンポジウム 2018，2018 年 12 月 22 日,静岡大学
(2) （招待講演）Go Kato, Masaki Owari, Koji Maruyama, “Hilbert space structure induced by quantum probes”, International Workshop on Quantum Information, Quantum Computing and Quantum Control,（国際学会）,2018 年 11 月 6-8 日，中国・上海
(3) Masahito Hayashi, Masaki Owari, Go Kato, and Ning Cai, “Secrecy and Robustness for Active Attack in Secure Network Coding and its Application to Network Quantum Key Distribution”, 10th International Conference on Information Theoretic Security（国際学会）, 2017 年 11 月 29 日-12 月 2 日，中国・香港
(4) （招待講演）尾張正樹、林正人，“セキュア量子ネットワーク符号”，量子情報と有限長理論の新展開，2017 年 8 月 3-5 日，名古屋大学

６．研究組織

(1)研究分担者

研究分担者氏名：林 正人

ローマ字氏名：Hayashi Masahito

所属研究機関名：名古屋大学

部局名：多元数理科学研究科

職名：教授

研究者番号（8 桁）：40342836