科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ６ 日現在

機関番号：１２６０８
研究種目：若手研究(B)
研究期間：2010～2013
課題番号：２２７６０２６７

研究課題名（和文）従来捨てていた測定結果を用いた量子暗号の鍵レートの向上

研究課題名（英文）Improving the Key Rate of Quantum Key Distribution Protocols by Using Unused Measurement Outcomes

研究代表者
松本　隆太郎（Matsumoto, Ryutaroh）

東京工業大学・理工学研究科・准教授

研究者番号：１０３３４５１７

交付決定額（研究期間全体）：（直接経費）　　3,000,000円、（間接経費）　　900,000円

研究成果の概要（和文）：従来の量子鍵配送プロトコルでは、プロトコル中で得られる測定結果の一部のみを利用することが多い。本研究では、すべての測定結果を用いることで量子通信路の推定をより正確に行い、鍵レートを向上させることを目指した。キュービットが有限個の単一光子BB84プロトコルと、キュービットが十分多い場合の単一光子B92プロトコルについて前述のアプローチで通信路推定方法を見直し安全性解析をやりなおし、鍵レートが向上することを確認し、それぞれ学術雑誌と国際会議で発表した。

研究成果の概要（英文）：In the conventional quantum key distribution protocols, only part of measurement outcomes are usually used for channel estimation. In this research, we propose to use all the measurement outcomes and to improve their key rates. We considered the single-photon BB84 protocol with the finite number of qubits and the single-photon B92 protocol with the infinite number of qubits. We modified their channel estimation procedures according to the above approach, and redo their security analysis. We verified that their key rates are increased and reported those findings in an academic journal and an international conference.

研究分野：工学

科研費の分科・細目：電気電子工学・通信・ネットワーク工学

キーワード：量子暗号　B92　BB84　通信路推定

１．研究開始当初の背景

従来の情報セキュリティ技術では、素因数分解の困難さなど特定の問題の計算困難性にその安全性が基づいている。一方、情報理論的に安全なセキュリティ技術は計算量的な仮定無しにその安全性を保証し、量子鍵配送プロトコル（QKD プロトコル）はその中で代表的な手法であり、実用化に最も近いと見なされている。QKD プロトコルの中で良く知られたものに、BB84 プロトコル、B92 プロトコルなどがある。

QKD プロトコルは（１）量子媒体の伝送、（２）量子通信路の推定、（３）誤り訂正、（４）秘匿性増幅、の４つのステップからなる。この中で２番目の量子通信路の推定について、従来法はプロトコル中で得られる測定結果の一部しか用いていなかった。

一方、QKD プロトコルの研究においては、まず量子通信路推定に用いる測定結果が十分多数の量子媒体の伝送・測定の結果として得られると仮定し、漸近的な解析を行うことが多い。その後に、伝送される量子媒体の数を有限個とし、そのときに使用できる量子通信路推定法と安全性の解析を行うことが多い。

２．研究の目的

上記のことを踏まえ、従来用いられていなかった測定結果を量子通信路推定に用い、通信路をより正確に推定し、様々な QKD プロトコルにおいて通信路推定以外のステップを変更せずに、安全に得られる秘密鍵の長さを増加させることを目指した。

３．研究の方法

2005 年に Renato Renner はその博士論文において、かなり多くの QKD プロトコルの安全性ならびに安全に取り出せる秘密鍵の長さを与える理論を提案した。その概要は以下の通りである。X を送信者のビット、E を量子通信路の環境系を表す量子状態、S(X|E)を条件付き量子エントロピーとする。
このときに、１量子媒体から得られる秘密鍵は S(X|E)から誤り訂正のために公開通信路で交換されたビット数を引いたものになる。

ここで、多くの QKD プロトコルでは、量子通信路を測定結果から１つに絞り込むことが出来ず、ありうる量子通信路の集合を決定し、その集合の中で最も小さい条件付き量子エントロピーを与える量子通信路を求める必要がある。

研究代表者は、条件付き量子エントロピーが量子通信路の凸関数であり、かつ通信路の集合が凸集合になることに注目し、凸最適化を用いてさまざまな QKD プロトコルにおける秘密鍵の長さを統一的に解明する方法を提案した。

４．研究成果

まず、BB84 プロトコルにおいて、伝送する量子媒体が有限である場合を検討した。このとき、推定に用いることができる標本の大きさが有限であるため、点推定を用いると推定誤差の評価が困難になる。そこで推定失敗確率を明示的に与える区間推定を量子通信路に用いることにした。

Scarani と Renner による従来法では区間推定を行うために、二項分布の裾確率の上界として変動距離を用いた上界式を採用していた。しかし、用いる上界式が緩ければ安全性を保証できる秘密鍵の長さも小さくなる。そこで、裾確率の上界式として色々な上界式を用いて区間推定を行った。その結果、Klar による上界式を用いると大幅に秘密鍵の長さを向上できることがわかった。

また上記の方法では通信路推定に用いる測定結果の種類は従来法と変わらなかったが、利用可能なすべての測定結果を用いる通信路推定手続きも提案した。それを従来法と比較し、depolarizing 通信路では従来法よりも得られる秘密鍵の長さが少なく、amplitude damping 通信路では多くなることを明らかにした。

次に従来あまり研究されていなかった B92 プロトコルに対して凸最適化の手法を適用することを考えた。B92 プロトコルでは、誤り訂正のための公開通信路に

送測通こロ密法損路合研こ密しにがるに者き者る。ント秘手て信場来、秘に年お信定知のピ鍵を案のに究れ鍵た。Journal of Physics A: Theoretical and Mathematical に雑誌論文として掲載した。

従来の B92 の解析では、depolarizing 通信路において、depolarizing 率が 4.2 まが出しかな方秘密鍵を生成すること提案が出しが来た。今回我々が提案した方法では、depolarizing 率が 6.3 まで秘密鍵を生成することが可能であることがわかった。この結果を 2013 IEEE International Symposium on Information Theory にて、査読付国際会議論文として発表した。

5．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

(1) K. Sakakibara and R. Matsumoto, “Exact computation of tail probability of hypergeometric distribution and its application to quantum key distribution,” IEICE Communications Express, vol.3, no.2, pp.68-73, February 2014.（査読あり）

(2) Y. Sano, R. Matsumoto, and T. Uyematsu, “Secure Key Rate of the BB84 Protocol Using Finite Sample Bits,” Journal of Physics A: Mathematical and Theoretical, vol.43, no.49, p.495302, December 2010.（査読あり）

〔学会発表〕（計 6 件）

(1) K. Sakakibara, R. Matsumoto, and T. Uyematsu, ``Exact Computation of Tail Probability of Hypergeometric Distribution and its Application to Quantum Key Distribution,'' Poster Presentation at the 3rd Annual Conference on Quantum Cryptography, Waterloo, Canada, Aug. 5--9, 2013.

(2) R. Matsumoto, ``Improved Asymptotic Key Rate of the B92 Protocol,'' Proc. 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7--12, 2013.

(3) R. Matsumoto, “Fast exact computation of the tail probability of a hypergeometric distribution and its application to quantum cryptography,” Japan-Singapore Workshop on multi-user quantum networks, National University of Singapore, September 17-20, 2012.

(4) K. Sakakibara, R. Matsumoto, and T. Uyematsu, “Esitimation of Phase Errors without the Gaussian Approximation and Improvement of the Secure Key Rate of BB84 Protocol,'' Poster Presentation at the 2nd Annual Conference on Quantum Cryptography, Singapore, Sept. 10--14, 2012.

(5) R. Matsumoto, “Information Theoretic Security and Quantum

Cryptography, International Conference on Information and Communication Technology for Embedded Systems (IC-ICTES 2011), Pataya, Thailand, January 27-29, 2011.

(6) Y. Sano, R. Matsumoto, and T. Uyematsu, “Secure Key Rate of the BB84 Protocol Using Finite Sample Bits,” Proc. 2010 IEEE International Symposium on Information Theory, pp. 2677-2681, Austin, Texas, USA, June 13, 2010.

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等
http://www.rmatsumoto.org/research.html

６．研究組織
(1)研究代表者
松本　隆太郎（MATSUMOTO, Ryutaroh）
研究者番号：10334517
東京工業大学・理工学研究科・准教授

(2)研究分担者

(3)連携研究者