＜　量子情報処理の発展に向けたマルチユーザー量子暗号の安全性の検討　＞

研究年度　平成３１年度
研究期間　平成３１年度～平成３１年度
研究代表者名　吉田雅一
共同研究者名

● 概要

量子暗号は，量子コンピュータや量子通信などを用いた量子情報処理を支える次世代の暗号技術である．本研究では，マルチユーザー量子暗号の安全性について検討する．従来提案されている量子暗号は，送信者と受信者間で用いるものが多い．一方で，本研究では，送信者と複数の受信者間で用いるマルチユーザー量子暗号を研究対象とする．また，量子暗号の安全性に関しては，符号理論の知見をもとに盗聴者への情報漏洩の可能性を検討することが多い．一方で，本研究では，盗聴者と送信者の間に成り立つ物理原理を導くことで検討を行う．その結果，情報漏洩が起こりえないことへ，物理現象としての直感的な理解を与える．

● 内容および成果

Shor の素因数分解アルゴリズムを実行可能な量子コンピュータが開発されると，現在広く使用されている暗号方式が危殆化する．そのため，量子コンピュータであっても解読することができない暗号方式が必要である．その候補の一つが量子暗号である．

量子暗号とは One time pad と量子鍵配送を組み合わせて構成される暗号方式である．ここで，One time pad とは送受信者間で共有する乱数列からなる共通鍵を用いて，暗号化・復号する暗号方式である．また，量子鍵配送とは，one time pad で使用する共通鍵を共有する技術である．代表的な量子鍵配送として BB84 [1] がある．BB84 は，盗聴者の存在を検知する機能を有し，無条件安全 [2]を満たす．ここで，無条件安全とは，盗聴者が物理法則に従ういかなる操作を実行可能だとしても，盗聴を検知されずに鍵の情報を得ることができないことである．

量子鍵配送の一つに Mean King 問題 [3] を応用した量子鍵配送 [4] がある．Mean King 問題とは，物理学者 Alice と王様 King が登場する物語 [5] としてよく語られる，King の出題に Alice が正しく答えられるかという問題である．また，Alice が King の出題に正しく答えることができるのであれば，その答えを互いの共通鍵にするというのが，Mean King 問題を応用した量子鍵配送の概要である．

本研究において検討する量子鍵配送は，一人の送信者と複数の受信者がいて，送信者が各受信者それぞれと共通鍵を共有するものである．この量子鍵配送は Mean King

問題を拡張し，利用することで実現する [6]．同鍵配送では，Alice と複数の King がいて，Alice は各 King と共通鍵を共有することができる．文献 [6]では，拡張した Mean King 問題の解を構成するための十分条件が示されている．文献 [7]では，同問題の解が一組示されており，その解を用いて具体的に量子鍵配送を構成している．文献 [8]では，文献 [7]において示されている拡張した Mean King 問題の解とは異なる解を一組示し，その解とすでに示されている解を用いて量子鍵配送を構成している．また，構成した量子鍵配送に対して盗聴者がインターセプト・リセンド攻撃を行った場合, 構成した量子鍵配送が盗聴者の存在を検知できるかを検討している. その結果, Alice が 2 人の King（King1,King2）と量子鍵配送を行う設定において，盗聴者が King2 に対してインターセプト・リセンド攻撃を行なった場合，Alice と各 King とが共有する篩鍵に誤りが発生することを示し，構成した量子鍵配送がインターセプト・リセンド攻撃に対してロバストネスを満たすことを示している．

本研究では，文献 [8]において構成された拡張した Mean King 問題を応用した量子鍵配送の安全性を検討した．具体的には，Alice が 2 人の King（King1,King2）と量子鍵配送を行う設定において，盗聴者がインターネット・リセンド攻撃よりも一般的な攻撃を行う場合を検討した．その結果，盗聴者が情報を搾取すればするほど，Alice と各 King が共有する篩鍵に誤り率が高まることを示した．また，この結果より，篩鍵の誤り率が 0 であるならば，盗聴者に鍵の情報が渡っていないとも言える．

- 参考文献

[1] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution And Coin Tossing," Proc. of IEEE International Conference on Computers Systems and Signal Processing, pp. 175-179 (1984).

[2] D. Mayers, “Unconditional Security in Quantum Cryptography," Journal of the ACM, Vol. 48, Iss. 3, pp. 351-406 (2001).

[3] L. Vaidman, Y. Aharonov, and D. Z. Albert, “How to ascertain the values of σx, σy, and σz of a spin-1/2 particle," Phys. Rev. Lett. 58, pp. 1385-1387 (1987).

[4] J. Bub, “Secure key distribution via pre- and postselected quantum states," Phys. Rev. A 63, 032309 (2001).

[5] Y. Aharonov and B.-G. Englert, “The Mean King's Problem: Spin 1," Z. Naturforsch., A:Phys. Sci. 56a, 16 (2001).

[6] 吉田雅一, 森岡将貴, 程俊, “高次元量子誤り訂正符号を用いた Mean King 問題の解法とその応用," 第 39 回情報理論とその応用シンポジウム予稿集, pp. 366-371 (2016).

[7] 中山歩, 吉田雅一, 程俊, “拡張した Mean King 問題を応用した量子鍵配送の

検討," 第 37 回量子情報技術研究会資料, pp. 68-71 (2017).

[8] Ayumu Nakayama, Masakazu Yoshida, and Jun Cheng, "Quantum Key Distribution using Extended Mean King's Problem," The International Symposium on Information Theory and Its Applications 2018, pp. 339-343, Oct. 28-31, Singapore, (2018).