SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

拡張したMean King問題を応用した量子鍵配送の安全性の検討Ⅱ：識別可能性と情報攪乱

Study on Security of Quantum Key Distribution using Extended Mean King's Problem: Distinguishability and Information Disturbance

米田 昌矢 *　　吉田 雅一 *
Masaya Komeda　　Masakazu Yoshida

キーワード 量子暗号，量子鍵配送，mean multi-kings 問題，情報搾取と情報攪乱

あらまし

量子コンピュータの進展に伴い，RSA 暗号などの安全性は危殆化する．一方で，one time pad と量子鍵配送の組み合わせである量子暗号は，量子コンピュータの進展に関わらず無条件安全性を保証することが期待される．

量子鍵配送の一つに，mean multi-kings 問題（mean king 問題の拡張の一つ）を用いた量子鍵配送がある．この量子鍵配送の正規ユーザは，Alice と King たち（King_1, King_2,..., King_n と呼ぶことにする）であり，Alice は各 King_j と共通鍵を共有することができる．同量子鍵配送の概要は次の通りである．まず，Alice は各 King_j へ量子ビットを送る．各 King_j はあらかじめ決められた測定の候補から一つを選び，その測定で量子ビットを測定し測定値を得る．この測定値が，各 King_j の共通鍵となる．各 King_j は，測定後の量子ビットを Alice へ送る．Alice は，受け取った量子ビットを測定し測定値を得る．その後，各 King_j は自身が選んだ測定の種類を Alice へ伝える．Alice は，自身の測定値と各 King_j から伝えられた測定の種類を用いて各 King_j の測定値を推定する．このとき，推定結果が Alice の共通鍵となる．

文献 [1, 2] では，同量子鍵配送を提案するとともに，盗聴行為への耐性を検討した．具体的には，$n = 2$ としたとき，intercept-resend 攻撃への耐性を検討し，Alice と King たちが共有するビットの誤り率を示した．その結果として，intercept-resend 攻撃が実行されたときビットの誤り率は 0 とはならないことが明らかになり，盗聴を検知可能だとわかった．

本発表では，文献 [1, 2] の発展的成果として学術論文誌にて発表した結果 [3] およびその追加研究の結果を紹介する．具体的には，盗聴者による情報搾取と正規ユーザが得る情報の攪乱の関係性を考察する．BB84 プロトコルにおいて，この様な関係性はいわゆる情報攪乱定理として知られている．ここでは，$n = 2$ の場合に着目する．Eve は自身で用意した量子系と King たちが Alice へ渡す量子ビットを相互作用させた後，Eve は自身にとって有利となるタイミングで自身の量子系に任意の測定を行い，King の測定値を推定する．この設定において，Eve の鍵の識別可能性と正規ユーザが共有する鍵の誤り確率との間に成り立つトレードオフ不等式を示す．トレードオフ不等式は，Eve が鍵を識別できればできるほど必然的に正規ユーザが共有する鍵の誤り率を高めることを示している．逆に，Eve は鍵の誤り率を 0 に保つ行為では有意に鍵を識別することはできないと言える．

参考文献

[1] 中山歩，吉田雅一，程俊，2018 年暗号と情報セキュリティシンポジウム，2A4-4　(2018).

[2] A. Nakayama, M. Yoshida, and J. Cheng, The 2018 International Symposium on Information Theory and Its Applications, pp. 339-343 (2018).

[3] M. Yoshida, A. Nakayama, and J. Cheng, Entropy, Vol. 22, Issue 11, 1275 (2020).

* 大阪産業大学デザイン工学部 〒 574–8530 大阪府大東市中垣内 3 丁目 1–1. Faculty of Design Engineering, Osaka Sangyo University, 3–1–1 Nakagaito, Daito, Osaka, 574-8530, Japan. s18h043@ge.osaka-sandai.ac.jp