数理・情報のフロンティア　　2022 年度
2021 年度採択研究代表者　　年次報告書

水谷 明博

三菱電機(株) 情報技術総合研究所
研究員

現実的な装置を用いた情報理論的安全な量子情報処理の実現

研究成果の概要

量子暗号は、秘密鍵と呼ばれる情報漏洩が無い乱数列をユーザに配布することで、絶対安全な通信を可能にする。量子暗号の安全性証明はユーザの装置に数学的なモデルを仮定する必要があるが、実際の物理特性を反映した仮定でなければ実システムの安全性保障はできない。そこで、最も代表的な量子暗号方式である BB84 方式に対して、複数の現実的な不完全性を取り入れた装置モデルに基づく安全性証明を与えた。本結果を論文にまとめプレプリントサーバで公開した[1]。

他の代表的な量子暗号方式に、簡易な実験系で実装可能という利点を持つ差動位相シフト(DPS)方式がある。これまでの DPS 方式の安全性証明は、秘密鍵長が無限の極限という非現実的な状況でしか与えられていなかった。今回、DPS 方式の実現に向けて、鍵長が有限という実際の状況での安全性証明を与え、現実的な通信時間でも鍵生成速度は漸近極限の速度から大きく低下しないことを明らかにした。本結果を論文にまとめプレプリントサーバで公開した[2]。

量子計算は現代の計算機よりも複雑な問題を効率的に計算できる。将来大規模な量子計算機が実現してもクラウドでの利用が想定され、ユーザの立場に立つと安心してクラウド利用できることが望まれる。今回、マジック状態と呼ばれる万能量子計算の実現に不可欠なリソース状態の生成と測定をどれだけの精度で実現できているかを古典計算機しか持たないユーザが検証するプロトコルを考案した。本結果を論文にまとめ米国物理学会が発行する国際雑誌 Physical Review A から出版された[3]。

また、量子計算の計算量について研究を行った。量子計算機は可逆な計算機と言われるが、可逆なのはユニタリ変換だけであり、測定は非可逆である。そこで、測定も可逆にすることでどれだけ計算能力が上がるかを代表的な計算量クラスとの包含関係を示すことで明らかにした。本結果を論文にまとめプレプリントサーバで公開した[4]。

【代表的な原著論文情報】

[1] M. Pereira, G. Currás-Lorenzo, Á. Navarrete, A. Mizutani, G. Kato, M. Curty, K. Tamaki, “Modified BB84 quantum key distribution protocol robust to source imperfections”, arXiv:2210.11754 (2022).

[2] A. Mizutani, Y. Takeuchi, K. Tamaki, “Finite-key security analysis of differential-phase-shift quantum key distribution ” arXiv:2301.09844 (2023).

[3] A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, S. Tani, “Computational self-testing for entangled magic states”, Physical Review A **106**, L010601 (2022).

[4] R. Hiromasa, A. Mizutani, Y. Takeuchi, S. Tani, “Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection ”, arXiv:2206.05434 (2022).