量子の状態制御と機能化
2017 年度採択研究者

2019 年度
実績報告書

森前　智行

京都大学基礎物理学研究所
講師

セキュアクラウド量子計算における量子スプレマシー

§1. 研究成果の概要

本研究では、セキュアクラウド量子計算における量子スプレマシーについて研究を行った。特に、量子スプレマシーについては、従来の量子スプレマシーよりも強力な Fine-grained quantum supremacy についての成果を挙げた。従来の量子スプレマシーは量子計算は古典計算機では多項式時間でシミレートできない、というものであったが、古典計算機科学の分野で研究されている Fine-grained complexity theorey における SETH（Strong exponential time hypothesis）等の仮定を用いることにより、量子計算は古典計算機では指数時間でもシミレートできないことを証明した。

クラウド量子計算のセキュリティについては、Trusted center model による量子計算の検証プロトコルを提案した。私が以前提案した Post-hoc プロトコルの場合、検証者は多少の量子的能力が必要となる。この Post-hoc プロトコルと耐量子暗号を組み合わせることにより、古典検証者でも量子計算が可能であるという結果を Mahadev が示したが、このプロトコルの場合、安全性が計算量的なものになる。(Learning with error が量子計算でも解けないという仮定）今回、Trusted center がランダムな BB84 状態を証明者に、その古典的記述を検証者におくるような設定を導入し、完全古典検証者が情報理論的安全性で量子計算の検証ができることを示した。さらに、最近 Broadbent と Grilo により提案された QMA のゼロ知識証明プロトコルを応用し、Trusted center model でもゼロ知識も達成できることを示した。