研究課題別事後評価結果

１．研究課題名：　セキュアクラウド量子計算における量子スプレマシー

２．個人研究者名

森前　智行（京都大学基礎物理学研究所　准教授）

３．事後評価結果

本研究では、量子計算は古典計算より速いのかという根本的な問いに対する理論的な条件を示すこと（量子スプレマシー）とクラウド量子計算において実際にサーバーで正しく安全に量子計算が行われているかをチェックする手法を理論的に導くことに取り組んだ。

量子計算は古典計算より速いのか？という根本的な問いに対する解を理論的に導くことを目指すためには指標としてクエリ数（サブルーチンの呼び出し回数）と実際の計算時間を使う二つの場合に分かれる。サブルーチンを呼び出す回数を指標とするグローバータイプの問題では、古典ではその回数の下界をしばしば見積もることができ、その場合、量子でそれより少ないときに量子が速いと言える。一方、直接的に計算時間を指標する場合では、古典計算による計算時間の下界を見積もる手法が確立されていないため、厳密な量子優位性を主張することは難しい。しかし、計算時間を指標とする場合でも、サンプリング問題に特化すると、ある仮定のもとで、量子優位性を主張できる場合がある（量子スプレマシー)。従来の量子スプレマシーでは、古典計算では多項式時間で解けないという結論であったが、本研究は、古典計算では「ある係数を有する指数時間」をかけても解けないだろうという、より強い結論を導くことに成功した。これにより、量子スプレマシーに関する知見を大きく発展させ、実験における、より強い意味でのスプレマシーに貢献することが期待される。

また、安全・着実なクラウド量子計算の検証では、利用者がクラウドを介して安全に通信を行い、さらには正しい量子計算結果を得ることを目指す。検証という概念は計算機科学におけるもっとも中心的かつ重要なテーマである。そこで本研究では情報理論的な安全性と、古典計算と古典通信のみをもちいたクラウド量子計算結果の検証ができるかを検討した。前提は検証者が古典計算機と古典通信しか持たないということである。その結果、現時点においては信頼できるアシスタント(trusted center: tc)を置き、tc が検証者に古典情報、量子サーバーに量子通信路を介して量子情報を配るというプロトコルを見出し、この方法を使えば安全かつ検証可能なクラウド量子計算が実行できることを示した。今後は tc の役割を古典に寄せることや、最終的には tc を省くことができるかが目標となる。

森前氏は古典計算と量子計算の性能を科学的かつ厳密に比較し、秘匿性も含めた実装における問題に取り組む希有な研究者で、今後も実験家や開発者に指針を与え続けることが大いに期待される。