研 究 終 了 報 告 書

「セキュアクラウド量子計算における量子スプレマシー」

研究期間: 2017 年 10 月～2021 年 3 月
研 究 者: 森前 智行

1. 研究のねらい

量子計算が古典計算よりも本当に高速であるのかどうかまだ実は証明がなされていない。近年、量子計算機の出力確率分布を古典計算機では効率的にサンプルできない、という量子超越性、というものが注目を集めている。これは、多項式階層の無限性という計算量理論的仮定に基づき、量子計算機が高速にある種の確率分布をサンプルできるが、古典計算機では多項式時間では不可能であることを示すものであり、理論的結果だけでなく、多くの実験も行われている。量子超越性が実験的に注目を集める一つの理由は、完全な量子計算機を作らなくても、弱い計算能力を持つマシンであっても、量子の高速性をデモンストレートできるという点にある。例えば、深さが4しかない回路や、交換するゲートのみからなる量子回路、相互作用なしの光量子計算機といったようなものが知られている。

本研究では、従来は多項式時間でしか知られていなかった量子超越性を指数時間まで拡張することを目指す。これにより、100量子ビット程度の近い将来に実現できるマシンであっても量子超越性が示せることが期待できる。

量子超越性の実験的実現には、検証も重要である。つまり、実験室で作られる量子計算機が正しく動作しているのかを確認する手法が必要となる。これは、クラウド量子計算の安全性とも関係する。量子計算は高価で巨大なので、クラウド的に利用されると考えられる。実際、IBM がクラウドサービスを開始している。クラウド量子計算において、サーバーが正しい量子計算を行っているかどうかを検証する問題は量子計算の検証と呼ばれ、長い間の未解決問題である。本研究では、これに取り組むことにより、クラウド量子計算の安全性、量子超越性の検証を統一的視点から理論的に研究する。

2. 研究成果

(1)概要

本研究においては量子超越性と量子計算の検証に取り組んだ。まず、量子超越性については、Fine-grained 量子超越性を証明することに成功した。従来の量子超越性は、多項式階層が崩壊しない限り古典計算機では多項式時間では量子計算がシミレートできない、というものだったが、それでは、50量子ビット程度の現在実現されているマシンで本当に古典計算機でのシミレーションが不可能であるのか不明である。そこで本研究では指数時間での古典シミレート不可能性を示すことを目指した。

本研究のもう一つのテーマは量子計算の検証である。量子計算が正しく動作しているかを古典計算のみでチェックできるか、というのは長年の未解決問題である。1量子ビット測定が可能であればできる、ということを私がさきがけ以前の研究で証明している。また、LWE が量子計算機では解けないという耐量子暗号における標準的な仮定に基づき、計算量的健全性

のもとで、完全古典の検証者が量子計算の検証ができる、ということが2018年にバークレーの Mahadev によって示されている。本研究では、完全古典検証者かつ、情報理論的健全性のもとで量子計算の検証が可能であるか、という未解決問題に取り組んだ。

（2）詳細

まず、一つ目の指数時間古典シミレート不可能性につちえは、本研究では多項式階層ではなく、Fine-grained complexity theory における仮定に基づき、量子超越性を示すというアプローチをとった。Fine-grained complexity theory というのは古典の計算機科学において近年注目されている研究分野であり、従来の帰着は多項式を保存するか否かしか見ていないが、Fine-grained complexity theory においては多項式の次数まで詳細にみる帰着を考えることにより、古典アルゴリズムの下界についてより詳細な結果を得ることに成功している。その中でも特にメジャーな仮定として、Strong exponential time hypothesis (SETH)というものがある。これは、有名な P≠NP の仮定をより悲観的にしたものであり、ある種の問題は指数時間であっても解けないだろうという予想である。本研究では、この SETH に基づく仮定から出発して、IQP や Clifford+T 回路といった、量子計算におけるスタンダードな回路にたいして、その出力確率分布は指数時間であってもシミレートできないことを証明した。また、これを持ちいることにより、Stabilizer rank という、量子状態の「マジック度」を測る指標に対する予想「Stabilizer rank conjecture」が正しいことも証明した。本研究の完成後、似たような内容の研究を MIT の Aram Harrow のグループも行っていることが判明し、連絡をとって相互引用をすることとなった。

二つ目の量子計算の検証については、完全古典かつ情報理論的健全性のもとでの量子計算の検証の可能性を研究した。まず、BB84 状態をランダムに証明者に送り、その古典的記述を検証者に送るような Trusted center を導入することにより、完全古典かつ情報理論的健全な検証が可能であることを証明した。Trusted center が取り除ければ、未解決問題の解決になるが、それは BQP が MA に入るという、信じられていないことが起こらない限り不可能である、ということも証明した。また、そのプロトコルが QMA のゼロ知識証明になっていることも示した。最近、Brakerski と Yuen が、Quantum randomized encoding という概念を提案し、その具体例を構築した。本研究では、それと量子計算の検証との関連についても調べ、よい Quantum randomized encoding ができたら、よい量子計算の検証プロトコルも作れるが、古典エンコーディングの Quantum randomized encoding は No-cloning が破れない限り不可能であることも示した。また、ブラインド量子計算と Quantum randomized encoding は非常に似ているが、その大きな違いは、最後の状態が Quantum one-time pad で暗号化されていることである。そのカギを送れば Quantum randomized encoding と同じ状況が実現できるが、それは安全性が破れてしまうことを証明した。

これら二つのテーマについて計画以上の成果が得られた。

3. 今後の展開

Mahadev の結果の大きなメッセージは、耐量子暗号を組み合わせることにより、これまでにない新しい機能をもつ量子暗号プロトコルが実現できる、ということである。本研究は主に量子の性質を使うことにより、情報理論的安全なプロトコルを考えていたが、Mahadev で用いられていたようなLWEにもとづく耐量子暗号的関数を利用することにより、さらにいろいろな機能が可能になると期待できる。例えば、本研究で構築したプロトコルの、公開鍵量子マネーへの応用などが期待される。

4. 自己評価

本研究は計画以上の達成状況であった。研究実施体制についても特に問題なく進めた。波及効果については、今後より実用的な量子計算機が実現していくなかで、その高速性の理論的サポート、あるいは正しく動作しているかの検証、といった面で重要な貢献をしていくと考えられる。また、10年あるいは20年かけて大規模な量子計算機をつくることが世界中で目指されているが、あまり指摘されない点として、実はそれよりも前に、いろいろな量子暗号プロトコルの実現のほうがやりやすい、ということがある。本研究の成果や、本研究に関連する様々な量子暗号プロトコルというのは、そのような量子計算機の実現という長期的な研究に対し、途中での重要なマイルストーンとなる。

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数:9件

1. Morimae and Tamaki, Additive-error fine-grained quantum supremacy, Quantum 2020 4, 329
Fine-grained complexity theory における SETH like な仮定に基づいて、IQP や Clifford+T 回路の出力確率分布を古典計算機で指数時間でサンプルするのが不可能であることを証明した。
2. Morimae, Trusted center verification model and classical channel remote state preparation, arXiv:2008.05033
ランダムな BB84 状態を証明者に送り、その古典的記述を検証者に送るような Trusted center を導入することにより、完全古典検証者による、情報理論的健全な量子計算の検証プロトコルを構築することに成功した。
3. Morimae, Quantum randomized encoding, verification of quantum computing, no-cloning, and blind quantum computing, arXiv:2011.03141
よい Quantum randomized encoding ができれば、よい量子計算の検証プロトコルが作れることを示した。また、古典エンコーディングによる Quantum randomized encoding は No-cloning が破れない限り不可能であることを示した。

（2）特許出願

研究期間累積件数：0件（特許公開前のものも含む）

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）