Economic rationality makes cloud quantum computing reliable

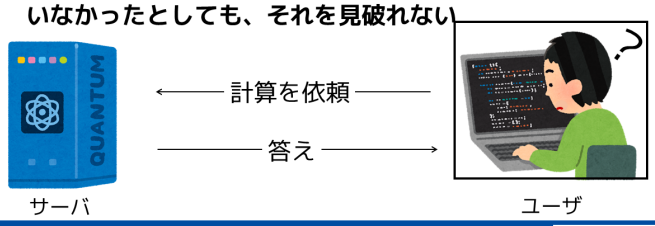
09 経済合理性に従うクラウド量子計算サーバは信頼できる

欲張りが提供する量子クラウドはちゃんと動く

どんな研究	量子コンピュータをクラウド方式で運用する際、ユーザがサーバから受け取る計算結果の正しさを保証する手法についての研究です。量子コンピュータにはノイズの影響を受けやすいという性質があるため、実用的なクラウド量子計算の実現には、そのような保証機能の実現が不可欠です。
どこが凄い	保証機能を既存の通信技術で実現する場合、従来手法では、量子コンピュータの動作を短時間に制限する必要があります。今回、我々は、経済合理性の概念を導入し、短時間制限を取り除くことに成功しました。本成果は従来よりも幅広い量子コンピュータアーキテクチャに適用可能です。
めざす未来	我々の手法を発展させることで、既存の（古典）ネットワークに大規模量子コンピュータを組み込むことをめざします。これにより、大規模量子コンピュータが実現した際、世界中誰でもどこからでも量子コンピュータの恩恵を受けられるようなネットワークの構築が可能になります。

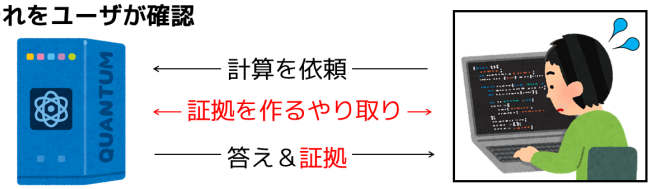
クラウド量子計算の実現に向けた課題

- 量子コンピュータは高い計算能力を持つが、ノイズの影響を受けやすく、**メンテナンスに専門知識が必要**なため、これをクラウドサービスとして提供する**クラウド量子計算**が現実的
- 量子コンピュータは現在のコンピュータでは解けない問題に利用するため、得られた結果の正しさ確認することはユーザには困難であり、**サーバが実は量子コンピュータを使っていなかったとしても、それを見破れない**



既存のアプローチの限界

依頼通りに量子コンピュータで計算した**証拠をサーバに作らせて、それをユーザが確認**



量子コンピュータをもってしても**証拠の偽造ができないようにするため、強い仮定や余分なやり取りが必要**
既存手法①：量子コンピュータでも破れない複雑な暗号を仮定
既存手法②：ユーザに特殊な量子通信デバイスが必要

⇒ユーザへの負担が大きく、この方法での実現は課題が多い

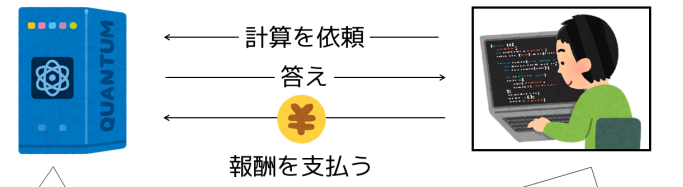
証拠の生成が不要なクラウド量子計算

我々の結果：経済合理性を用いて、量子コンピュータの動作を保証する手法の提案と数理証明

ポイント
- 証拠を生成・確認する代わりに、サーバからの答えに応じて**報酬を支払う仕組みを導入**
- サーバが依頼通りに量子コンピュータを使っている場合のみ、サーバが得られる報酬額が最大になるような**報酬額の計算アルゴリズムを考案**
- 従来手法よりも幅広い量子コンピュータアーキテクチャに適用可能

正しい答えを送った時だけサーバの報酬が最大化されるため、合理的なサーバは必ず正しい答えを送ってくれる！！

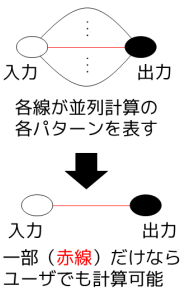
（※報酬の最大値は問題サイズに依存せず、状況に応じて調整可能）



貰う報酬を最大にしたい＝経済合理性

報酬を払うだけで良いから簡単だ～
- 正しい答えが得られる
- 証拠を作るための余分なやり取りが不要

数理証明の概要
①量子コンピュータの並列計算を、容易に計算できる複数の（ただし膨大な数の）計算に分解
②ユーザは分解した計算のごく一部をランダムに実行し、サーバからの答えと照合して正しさの度合いに応じて報酬額を決める
③ランダムに実行し報酬額を決めるため、不適切な報酬額になる場合もあるが、その平均値は正しい答えを送った時にしか最大化されないことを証明



関連文献

[1] Y. Takeuchi, T. Morimae, S. Tani, “Sumcheck-Based Delegation of Quantum Computing to Rational Server,” in *Proc. the 16th International Conference on Theory and Applications of Models of Computation (TAMC)*, 2020.

連絡先

竹内 勇貴 （Yuki Takeuchi） メディア情報研究部 情報基礎理論研究グループ
Email: cs-openhouse-ml@hco.ntt.co.jp