09

Economic rationality makes cloud quantum computing reliable

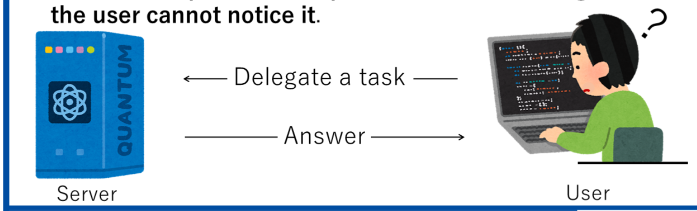
Being greedy makes quantum computers work well

Abstract

We consider cloud quantum computing and have proposed a method guaranteeing the correctness of the answer received from a cloud-quantum-computing server. Since quantum computers are strongly affected by noises, it is indispensable to realize such a method for practical cloud quantum computing. Previous methods work only under the assumption that a verified quantum computer runs in a sufficiently short time or a user can perform quantum communication with the server. By introducing the economic rationality, we have succeeded to remove these assumptions. Furthermore, our method can be applied to a broader class of quantum-computing architectures than that of previous methods. We aim to incorporate large-scale quantum computers into the existing worldwide network by developing our method, which makes it possible to deliver the high computational capability of quantum computers to everyone all over the world.

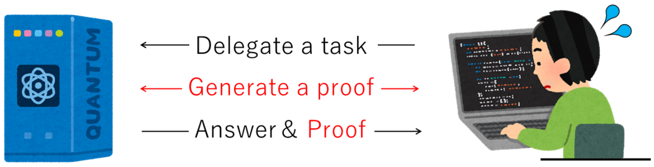
Challenges to realize cloud quantum computing

- Although quantum computers have high computational capability, they are strongly affected by noises. Since **their maintenances require the specialized knowledge**, it is pragmatic to use them **in the cloud service**.
- It is difficult for a user to verify whether the answer given by a server is correct. For example, **even if the server does not use his/her quantum computer to solve the delegated task, the user cannot notice it**.



Limits of existing methods

The server generates a proof guaranteeing that the server runs his/her quantum computer as requested, and **the user checks it**.



In order to make it impossible to forge a proof even with a quantum computer, **a strong assumption or an additional communication is required**.
Existing method 1: it is based on a post-quantum cryptography.
Existing method 2: quantum communication is necessary.
⇒ There are many challenges to be solved for the realization☹

Cloud quantum computing without proofs

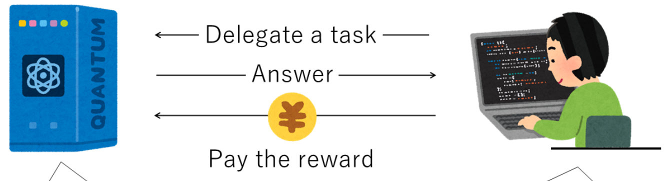
Our result: By using economic rationality, we have proposed a guaranteeing method for cloud quantum computing.

Points

- Instead of generating and checking proofs, **the user pays the reward to the server** depending on the received answer.
- **We have constructed a calculation algorithm for the reward** such that the reward is maximized only when the server honestly behaves as instructed by the user.
- Our method can be applied to a broader class of quantum-computing architectures than that of previous ones.

Since the reward is maximized only when the server sends the correct answer, the rational server certainly sends the correct answer!

(※ The maximum of the reward can be adjusted depending on the situation.)

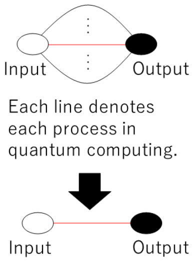


I would like to maximize the received reward.
= Economic rationality

- I can receive the correct answer.
- No additional communication is required.

Overview of our mathematical proof

① We decompose the quantum computation into a huge number of easy calculations.
② The user selects and performs a single calculation uniformly at random. Then he/she uses the result to derive the value of the reward for the server's answer.
③ Since the randomness is included in step 2, there is a possibility that the value of the reward is inappropriate. However, we have shown that the expected value of the reward is maximized only when the server sends the correct answer.



Each line denotes each process in quantum computing.

Although the user cannot efficiently simulate all processes simultaneously, it is possible for a single process (red line).

References

[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.

Contact

Yuki Takeuchi / Computing Theory Research Group, Media Information Laboratory
Email: cs-openhouse-ml@hco.ntt.co.jp