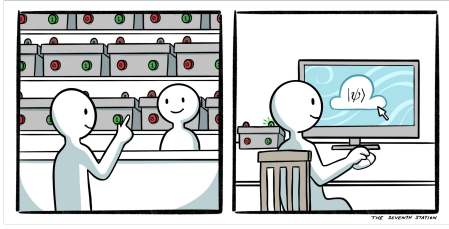
Quantum delegation with an off-the-shelf device

Arthur Mehta

University of Ottawa

Joint work with *Anne Broadbent* and *Yuming Zhao*, based on arXiv:2304.03448

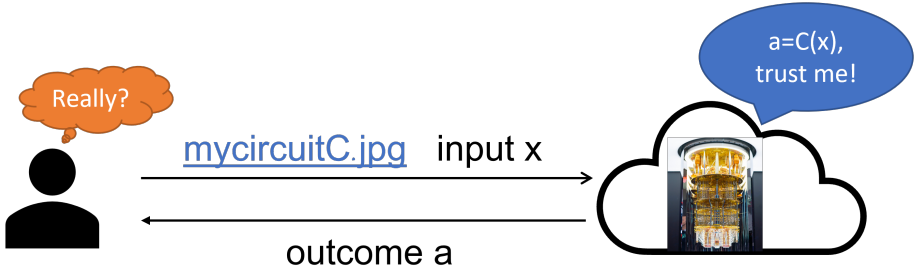


IQC Institute for Quantum Computing

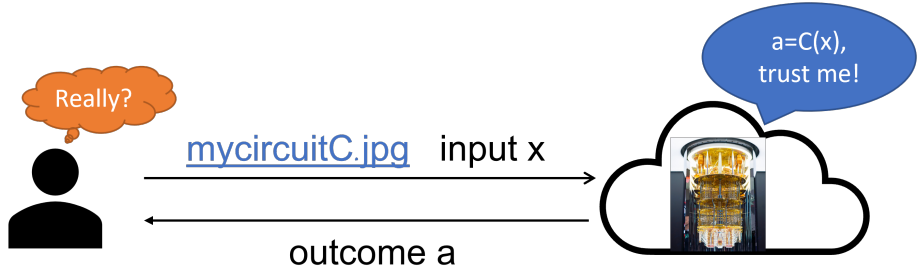
uOttawa

In 2077

Delegation of quantum computations



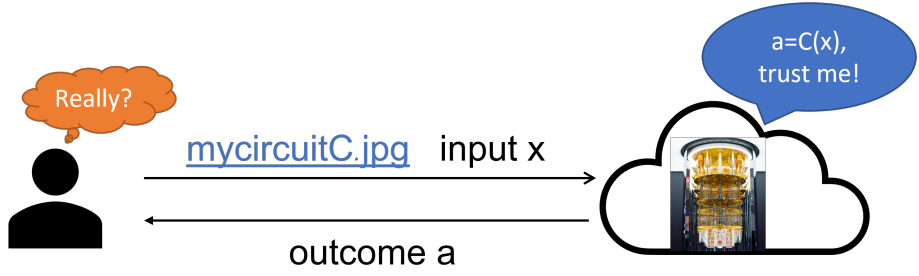
Delegation of quantum computations



Client: verifiable delegation

- I want to be convinced of the correctness,
- but I am not able to compare the results to the predictions

Delegation of quantum computations



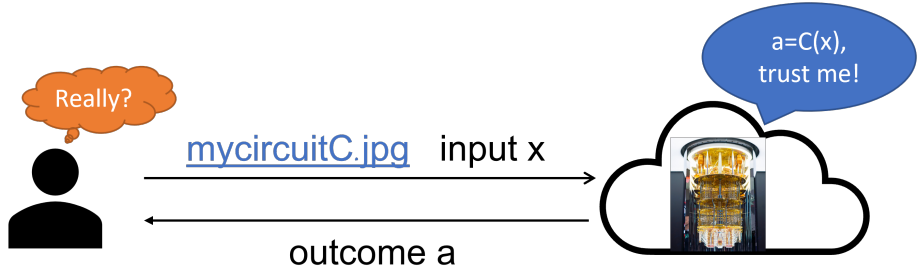
Client: verifiable delegation

- I want to be convinced of the correctness,
- but I am not able to compare the results to the predictions

Server: zero-knowledge proof

- We need to convince our clients that we are honest,
- but we don't want to reveal any inner-workings

Delegation of quantum computations



Client: verifiable delegation

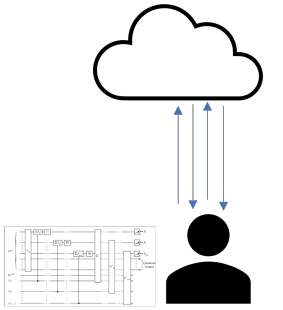
- I want to be convinced of the correctness,
- but I am not able to compare the results to the predictions

Server: zero-knowledge proof

- We need to convince our clients that we are honest,
- but we don't want to reveal any inner-workings

Goal: **zero-knowledge verifiable** delegation of quantum computations

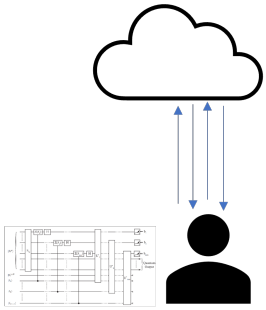
Previous proposed protocols

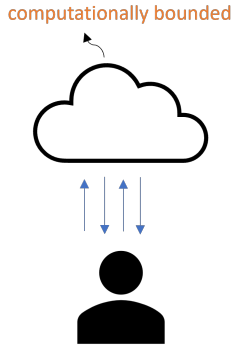


limited, trusted quantum devices

- Not fully device independent.

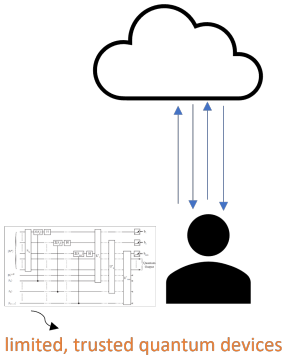
Previous proposed protocols



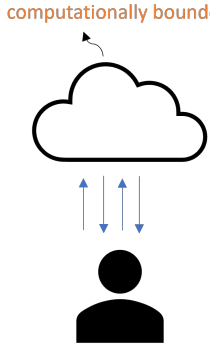


- Not fully device independent.
- Computational and hardness assumptions.

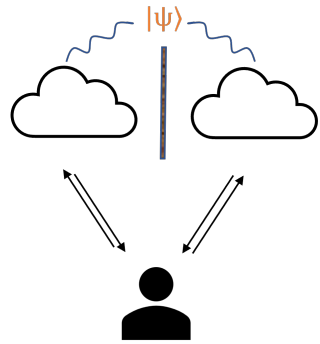
Previous proposed protocols



- Not fully device independent.

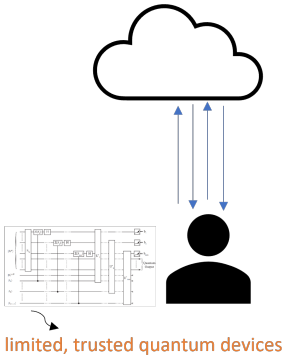


- Computational and hardness assumptions.

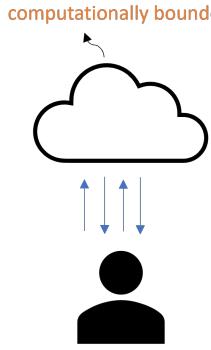


- Difficult to enforce isolation.
- Requires 6 or more servers for zero-knowledge.

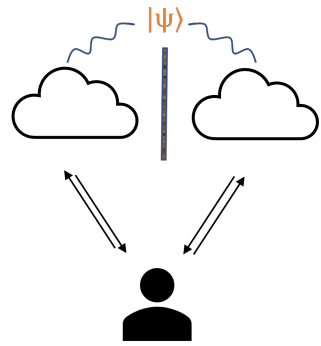
Previous proposed protocols



- Not fully device independent.



- Computational and hardness assumptions.

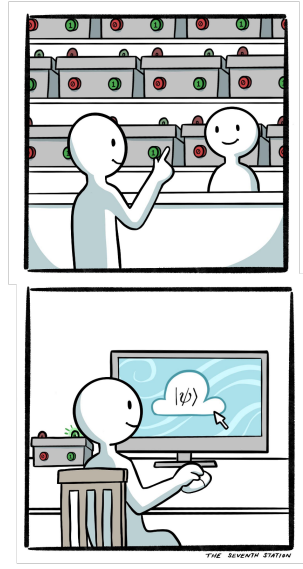


- Difficult to enforce isolation.
- Requires 6 or more servers for zero-knowledge.

Our model: a **single** quantum server + an **untrusted** device, all in a **single** round

The OTS model

A client wants to delegate a quantum computation $\mathcal{C}(x)$

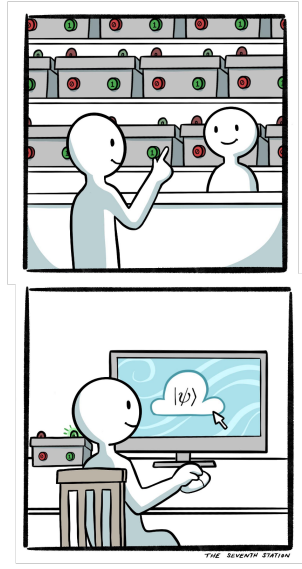


The OTS model

A client wants to delegate a quantum computation $\mathcal{C}(x)$

Set-up: Purchase an off-the-shelf based on $|x|$.

- Shares an entangled state with the server.
- Can make measurements on few qubits.



The OTS model

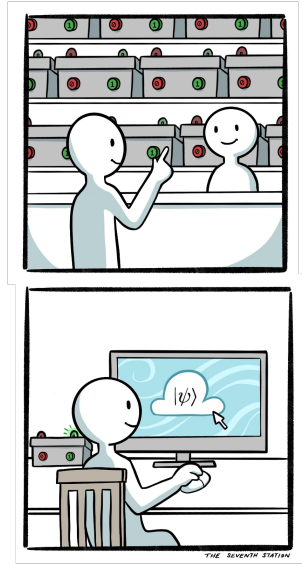
A client wants to delegate a quantum computation $\mathcal{C}(x)$

Set-up: Purchase an off-the-shelf based on $|x|$.

- Shares an entangled state with the server.
- Can make measurements on few qubits.

Verify: Play a game G_x:

- Send question q to server and press some buttons on OTS device.
- Compare server response with measurement results from device.



The OTS model

A client wants to delegate a quantum computation $\mathcal{C}(x)$

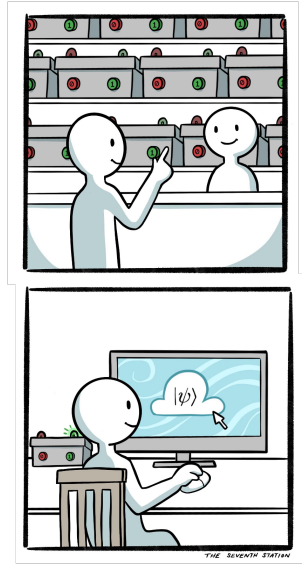
Set-up: Purchase an off-the-shelf based on $|x|$.

- Shares an entangled state with the server.
- Can make measurements on few qubits.

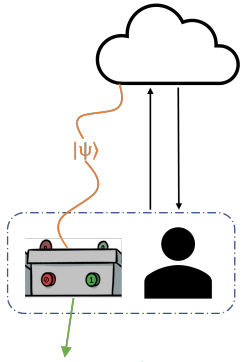
Verify: Play a game G_x:

- Send question q to server and press some buttons on OTS device.
- Compare server response with measurement results from device.

Note The shared state only depends on $|x|$



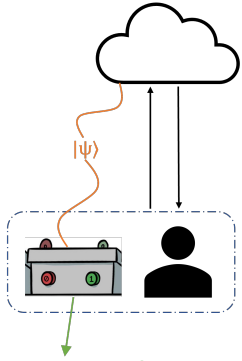
The OTS model in action



A measurement device

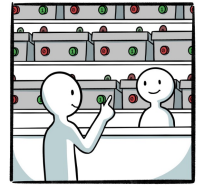
- Small: measures 6 qubits
- Untrusted: DI techniques
- Off-the-shelf: entangled state, only depends on the size of the problem

The OTS model in action

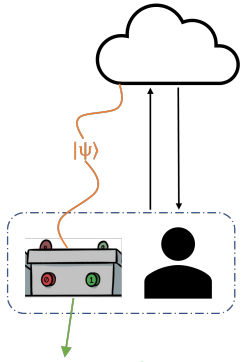


A measurement device

- Small: measures 6 qubits
- Untrusted: DI techniques
- Off-the-shelf: entangled state, only depends on the size of the problem

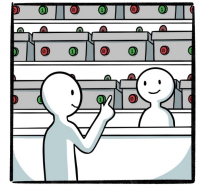


The OTS model in action



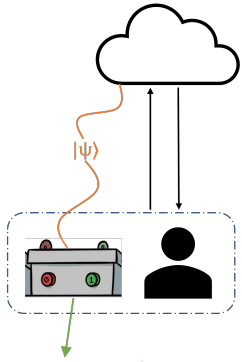
A measurement device

- Small: measures 6 qubits
- Untrusted: DI techniques
- Off-the-shelf: entangled state, only depends on the size of the problem



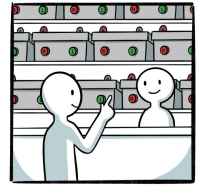
1. Circuit-to-Hamiltoniam construction
   $\mathcal{C} \to H$: $\mathcal{C}$ accepts $\Leftrightarrow$ $\lambda_0(H)$ is small

The OTS model in action



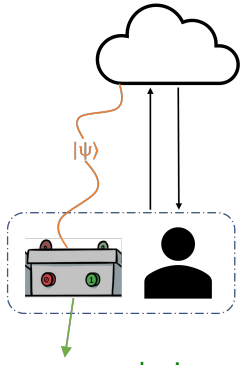
A measurement device

- Small: measures 6 qubits
- Untrusted: DI techniques
- Off-the-shelf: entangled state, only depends on the size of the problem



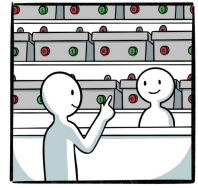
1. Circuit-to-Hamiltoniam construction
   $\mathcal{C} \to H$: $\mathcal{C}$ accepts $\Leftrightarrow$ $\lambda_0(H)$ is small
2. Teleport the ground state ρ of H

The OTS model in action



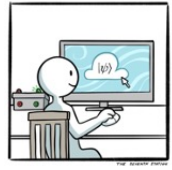
A measurement device

- Small: measures 6 qubits
- Untrusted: DI techniques
- Off-the-shelf: entangled state, only depends on the size of the problem



1. Circuit-to-Hamiltoniam construction
   $\mathcal{C} \to H$: $\mathcal{C}$ accepts $\Leftrightarrow$ $\lambda_0(H)$ is small
2. Teleport the ground state ρ of H

3. Estimates the ground energy of H



- Accepts if $\lambda_0(H)$ is low
- Rejects if $\lambda_0(H)$ is high

Main Results

Theorem (Broadbent, M, Zhao 2023)

All efficient quantum computations have verifiable delegation protocols in OTS.

Main Results

Theorem (Broadbent, M, Zhao 2023)

All efficient quantum computations have verifiable delegation protocols in OTS.

Corollary

Every language in QMA *has a* **two-prover** *one-round zero-knowledge proof.*

Main Results

Theorem (Broadbent, M, Zhao 2023)

All efficient quantum computations have verifiable delegation protocols in OTS.

Corollary

Every language in QMA *has a* **two-prover** *one-round zero-knowledge proof.*

Can amplified to constant completeness-soundness gap while preserving ZK.

Obstructions to device independence

Obstructions to device independence

Problem

Verifier's Task: Certify many EPR pairs.

Obstructions to device independence

Problem

Verifier's Task: Certify many EPR pairs.
Obstruction: The OTS device can only measure up to 6 qubits.

Obstructions to device independence

Problem

Verifier's Task: Certify many EPR pairs.
Obstruction: The OTS device can only measure up to 6 qubits.

Problem

Server's Task: Provide a zero-knowledge proof of honest behaviour.

Obstructions to device independence

Problem

Verifier's Task: Certify many EPR pairs.
Obstruction: The OTS device can only measure up to 6 qubits.

Problem

Server's Task: Provide a zero-knowledge proof of honest behaviour.
Obstruction:The honest server teleports the entire ground state ρ.

Technical Contributions (Informal)

Theorem

The low-weight Pauli braiding "self-test" n-EPR pairs using 6-qubit measurements.

Technical Contributions (Informal)

Theorem

The low-weight Pauli braiding "self-test" n-EPR pairs using 6-qubit measurements.

Theorem

For every $L \in \mathrm{QMA}$ there exists a family of verification circuits V_x s.t

- $V_x \mapsto H_x$ *an XZ-Hamiltonian,*
- *if $x \in L_{yes}$ and $|S| \leq 6$ then the reduced density $tr_{\overline{S}}(\rho)$ can be obtained in poly-time.*

Technical Contributions (Informal)

Theorem

The low-weight Pauli braiding "self-test" n-EPR pairs using 6-qubit measurements.

Theorem

For every $L \in \mathrm{QMA}$ there exists a family of verification circuits V_x s.t

- $V_x \mapsto H_x$ *an XZ-Hamiltonian,*
- *if $x \in L_{yes}$ and $|S| \leq 6$ then the reduced density $tr_{\overline{S}}(\rho)$ can be obtained in poly-time.*

Theorem

Very Informal: Prove an enhanced version of Gowers Hatami theorem from approximate representation theory.

Remarks and Open Problems

1. Noise tolerant device independent techniques.
   - LWPBT can be won well even with constant noise on EPR pairs.
   - The LWPBT has alot of entanglement left over after the test.

Remarks and Open Problems

1. Noise tolerant device independent techniques.
   - LWPBT can be won well even with constant noise on EPR pairs.
   - The LWPBT has alot of entanglement left over after the test.
2. We know $\mathrm{QMA} \subseteq \mathrm{OTS}$. Is it possible $\mathrm{OTS} = \mathrm{MIP}^*$?

Remarks and Open Problems

1. Noise tolerant device independent techniques.
   - LWPBT can be won well even with constant noise on EPR pairs.
   - The LWPBT has alot of entanglement left over after the test.
2. We know $\mathrm{QMA} \subseteq \mathrm{OTS}$. Is it possible $\mathrm{OTS} = \mathrm{MIP}^*$?
   - What if we lift the constant measurement requirement?
3. Applications to PoQK via self-testing.
   - Can we show our overall protocol self-tests for ground states?