QEnclave: A practical solution for secure quantum cloud computing

K. Zouridakis

June 2023

Outline

What is DQC?

Delegated Quantum Computing (DQC) is a method of performing quantum computations on a remote quantum computer.

How does DQC work?

DQC works through the use of 2 types of protocols:

- **Prepare-and-send** protocols:
  - The client prepares a certain number of quantum states and sends them to the server.
- **Receive-and-measument** protocols:
  - The client receives single-qubits from the server and measures them.

Before we cover the DQC technical details, we need some Quantum computing theory.

Qubit

A quantum bit (or qubit) is a quantum system that is analogue to a classical bit. It lives in a two-dimensional Hilbert space $\mathcal{H}$. We denote a qubit as:

$$|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum computing theory (cont.)

Arbitrary qubit

We denote an arbitrary qubit as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.
This means that qubit $|\psi\rangle$ is in a superposition of $|0\rangle$ and $|1\rangle$ before measurement (that is, if $\alpha, \beta \neq 0$).
After measurement, the qubit collapses to either $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2$ and $|\beta|^2$ respectively.

About quantum gates

Quantum gates

Quantum gates are unitary operators that act on qubits. They are represented as matrices. For example, the Hadamard gate, which is used in this paper, is represented as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

About quantum gates (cont.)

The Hadamard gate

The Hadamard gate is a single-qubit gate that is used to create superpositions. Particularly, it transforms:

$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

About quantum gates (cont.)

The QEnclave uses a $Z(\theta)$ gate, which performs a rotation of θ (θ is chosen uniformly at random as we will see later).

The $Z(\theta)$ gate

The $Z(\theta)$ gate maps:
$|\pm\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta}|1\rangle)$

Quantum gates like $Z(\theta)$ or H are generally called **Unitary maps**.

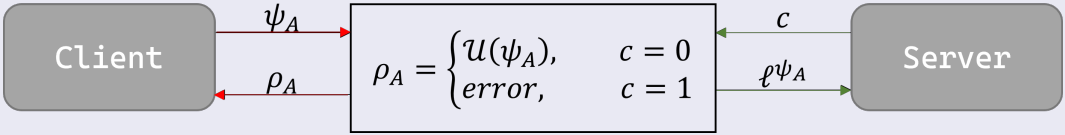
Density matrix

Representation of quantum states as density matrices

The density matrix is a way to represent a quantum state. It is defined as:
$\rho = |\psi\rangle \langle\psi|$
Density matrices are used to represent mixed states (states that are not pure, i.e. they are in a superposition). $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$, where p_i is the probability of the state $|\psi_i\rangle$.

The DQC protocol

How does it work?



The client prepares a number of qubits in a certain state ψ_A and sends them to the server. The server performs a quantum computation (by passing the qubit through a quantum gate $\mathcal{U}$) and sends the qubit back to the client. The client measures the qubit and gets the result of the computation.

The DQC protocol (cont.)

Parameter analysis

ψ_A is the quantum state that the client generates.
$\mathcal{U}$ is the quantum gate that the server applies to the qubit.
ℓ^{ψ_A} is the allowed leak of information about ψ_A to the server.
c is the verification variable. It is initialized to 0. If the verification fails, c is set to 1.
ρ_A is the output of the computation. If $c = 0$, then ρ_A is the output of the computation. If $c = 1$, then ρ_A returns with an error.

The DQC protocol (cont.)

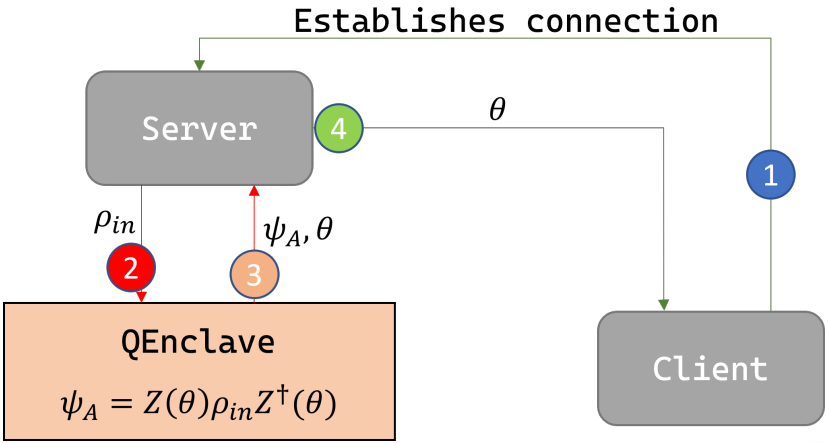
What is there to change? Behind the motive of the QEnclave

We notice that the DQC protocol requires the client to have some quantum computation capabilities. This is not ideal, as the client may not have the resources to perform quantum computations.
The client generates a **quantum state** ψ_A.
The client performs a **quantum measurement** on the the output ρ_A.
The DQC protocol uses a Remote State Preperation protocol to perform the quantum computation, as the client has to **prepare** a quantum state ψ_A. This is where the QEnclave comes in.

What it offers:

- A secure DQC (Delegated Quantum Computing) platform using only **classical controls**.
- Uses RSR (Remote State Rotation) to perform quantum operations instead of RSP (Remote State Preparation).
- Weakens the requirements for quantum hardware on the client side.
- While the RSR is "weaker" than RSP, security is still guaranteed.

How does it work?



How does it work? The RSR protocol

1. The client establishes a connection to the server.
2. The server generates a quantum state ρ_{in}.
3. The QEnclave performs a rotation of angle θ (chosen uniformly at random from set $\mathbb{Z}_{\frac{\pi}{4}}$) on ρ_{in}. The result is ψ_A.
4. The server returns the angle θ to the client. The client can now manipulate ψ_A by changing θ.

Why use the RSR protocol?

We notice that the client does not have to prepare a quantum state, or measure it. Instead, all the quantum computation is done between the server and the QEnclave. As a result, the client does not need to have quantum hardware nor does it need to establish a connection through a quantum channel. The quantum channels are colored in red in the diagram, and the classical channels are colored in green.

Why use the RSR protocol?

The client can perform quantum operations on the state by changing the angle θ. Quantum gates do nothing more than rotate the state by a certain angle. As a result, the client can emulate quantum gates by changing the angle θ.

Why use the RSR protocol?

Besides the fact that the client does not need to have quantum hardware, getting rid of the quantum channel is also important. Quantum channels are very fragile and expensive to maintain. Each client would require a single-photon source, a quantum channel, and a single-photon detector. Single-photon sources are expensive and lack operational accuracy. So, setting up a quantum environment for each client is not feasible.

Thank you!