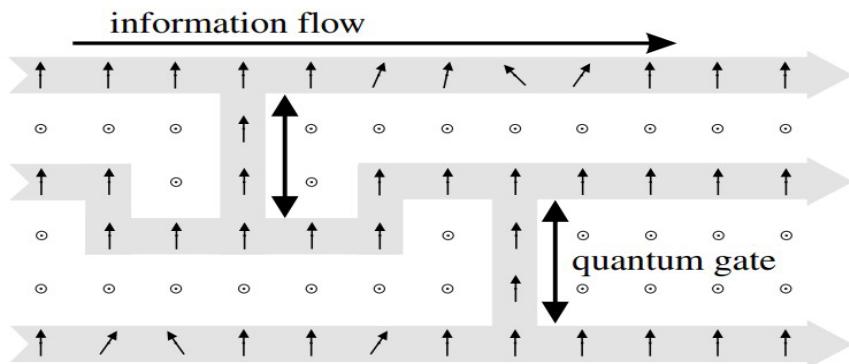


## Grover search using Blind Quantum Computation

In this challenge, the team should simulate the execution of Grover's algorithm in a secure, delegated way, using Blind Quantum Computation (BQC). BQC is a protocol for carrying out a computation on a remote quantum server, in such a way that the inputs to the computation remain hidden from the server.

In this challenge you are invited to implement Barz et al's protocol for BQC [1]. In their protocol, the only requirement on the client is the ability to transmit single-qubit states to the server, which in SquidASM can be done by performing quantum teleportation of single qubits. In contrast, the server is able to perform multi-qubit operations.

We will consider *one-way quantum computing*, or equivalently *measurement-based quantum computing*. In this model, one initially creates a large, entangled state (called *cluster state*), and performs single qubit measurements on part of the state in sequence. Because of the entanglement in the state, the choice of single-qubit measurement angles influences the nearby qubits. This therefore propagates information through the state, thereby doing a computation.



**Figure 1.** In the image, the circles represent qubits that are measured in the Z basis, which has the effect of removing them from the entangled state. The arrows represent the measurement angle of qubits in the X-Y plane, and this propagates information through the entangled cluster state. Image from [2]

In the BQC protocol of Barz et al, the angles of the four single-qubit states sent by the client to the server determine the exact cluster state, which in turn determined the measurement angles of the computation, ensuring that the computation remains hidden to the server.

In particular, we will use BQC to run Grover's algorithm: a quantum search algorithm that can find an element in an unstructured list of  $N$  elements in  $O(\sqrt{N})$  steps instead of the  $O(N)$  steps of a classical algorithm that just iterates through the list. An introduction to this algorithm can be found at [3]. The four-qubit triangle cluster from [1] allows for the blind implementation of Grover's algorithm for  $N=2$ .

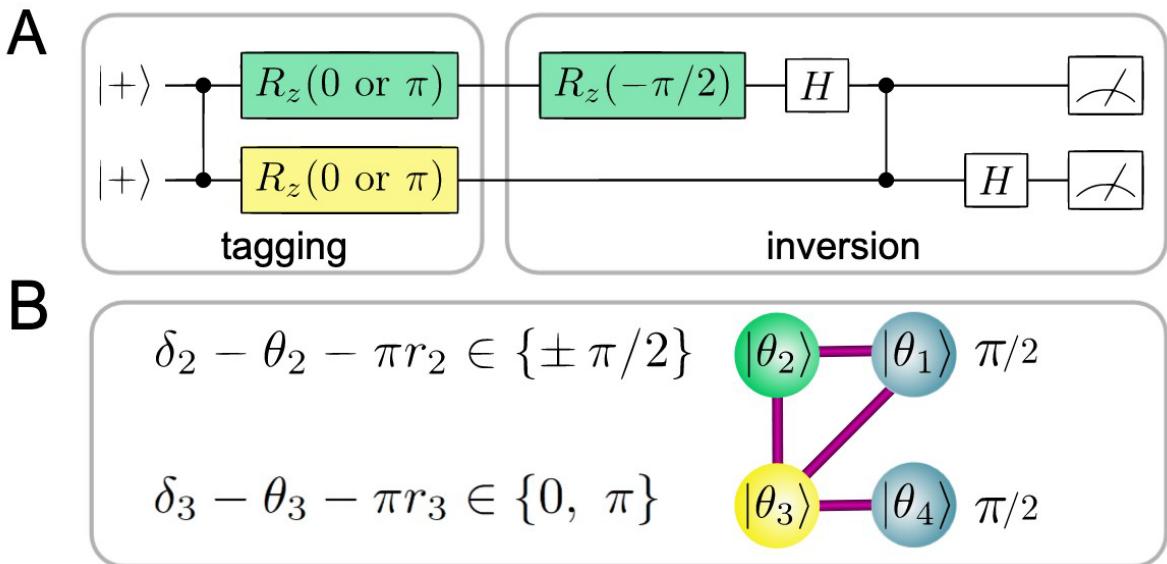
**Goal:** given a function  $f: \{0,1\}^2 \rightarrow \{0,1\}$ , delegate the finding of an  $x \in \{0,1\}^2$  such that  $f(x) = 1$  (using Grover's search) blindly to a quantum computer. We will assume that there exists only one such value  $x = 01$ , and ask you to reproduce Barz et al's results from [1, figure 4].

Let us recall the steps explicitly for the challenge:

1. The client generates 4 single-qubit states  $|\theta_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle)$  for  $\theta_1 = \theta_2 = 0$  and arbitrary  $\theta_2, \theta_3 \in \{0, \frac{\pi}{4}, \dots, \frac{7\pi}{4}\}$ , and sends them to the server.
2. The server generates a cluster state by performing controlled phase gates (CZ) on each qubit with its nearest neighbour.
3. Given that we want to tag  $x = 01$ , the client sends measurement angles  $\delta_2, \delta_3$  to the server (note that the client first needs to sample 2 random bits to hide the computation  $r_2, r_3 \in \{0, 1\}$ , and the measurement angles depend on the tagged item, see Figure 2).

To convince yourself that the BQC outcome coincides with Grover's search circuit, compare it with the non-blind computation by the client sending two  $|+\rangle$  states to the server and performing the circuit for the same tagged value.

If you are confident of having understood the algorithm, we invite you to generalize it for different tagged items and a non-optimized version of the algorithm where the client sends 4 randomized single-qubit states to the server (i.e. do not assume that  $\theta_1 = \theta_2 = 0$ ).



**Figure 2.** In A an example of a two-qubit Grover's search circuit. The first two gates act as an oracle, applying a phase shift to one of the four computational basis states that should be tagged (that is,  $x$  such that  $f(x)=1$ ). The second part of the circuit performs the amplitude amplification step to boost the probability amplitude of the correct term in the superposition state. B shows an implementation of this circuit using BQC, with a four-qubit cluster state. Here, the measurement of qubits 2 and 3 corresponds to the tagging of one of the elements, for example, a measurement with angles  $-\pi/2$  and  $\pi$  tags the state  $|01\rangle$ . Measuring the output qubits 1 and 4 with measurement angles of  $\pi/2$  identifies then which input was tagged. Image from [1].

[1] [h-ps://arxiv.org/pdf/1110.1381.pdf](https://arxiv.org/pdf/1110.1381.pdf)

[2] [h-ps://pennylane.ai/qml/demos/tutorial\\_mbqc/](https://pennylane.ai/qml/demos/tutorial_mbqc/)

[3] [h-ps://pennylane.ai/qml/demos/tutorial\\_grovers\\_algorithm/](https://pennylane.ai/qml/demos/tutorial_grovers_algorithm/)