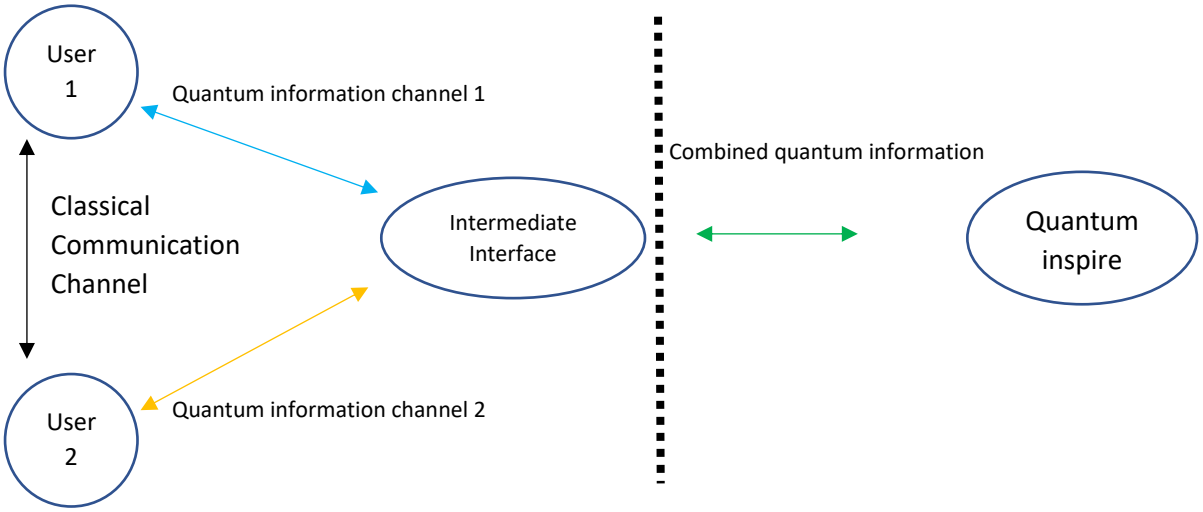
IQuHackathon Quantum Encryption challenge:

Description:
For this challenge you will be tasked with creating an interface and method to use quantum key distribution to send an encrypted message between the members of your team.

Background:

As you might know, one of the major potential threats of a quantum computer is the ability to run an algorithm called Shor's algorithm, which can efficiently do prime factorization. Because almost all contemporary encryption schemes rely on prime factorization, this could lead to large data security issues. Beyond just breaking current encryption, quantum computers also enable new methods of encryption that do not rely on prime factorization. One of these methods, Quantum Key distribution lies at the heart of this challenge.

Challenge goal:
The goal is to create an interface and method that allows two users to create a shared key through the use of a quantum computer. These quantum computer are accessible online through the quantum inspire framework, which can be programmed through using the languages cQASM or OpenQASM (e.g. with Qiskit).
Due to this year's event being online it will be necessary for the interface to be able to do this through the internet.
Another thing that needs to be kept in mind is that the current quantum computer interface only has 1 channel for input and 1 for output, meaning that it is currently not possible for each party to do their measurements fully independently. To make up for this, it will be necessary to make some kind of an intermediate interface to ensure that both parties do not see each other's measurement results. This means that your network structure would likely need to look something like this:

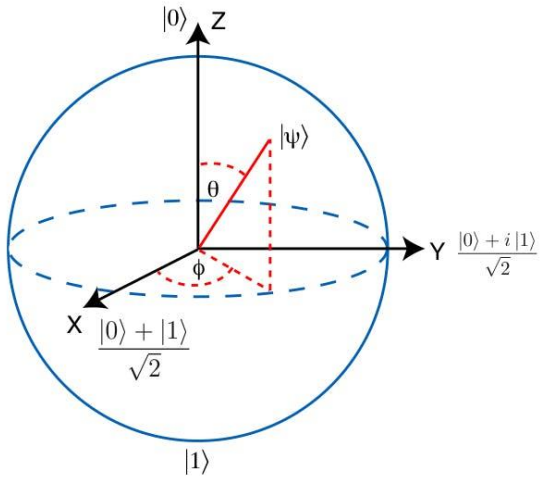


Here, both users send/receive their own half of the measurement information to an intermediate third party, which then should send/receive the combined quantum operation to/from the quantum computer.

Extra things to aim for:

Along with getting the system working there are some additional things your team could aim for to get an edge over the competition. These include for example:
Expanding the system to work with more than 2 people at once.
Using a different key distribution algorithm than in the examples.
Making a fancy very nice to use user interface.
Etc Etc.

Quantum key distribution:
To properly be able to construct this system, some background on quantum mechanics will also be necessary.
Quantum key distribution relies on the property quantum bits have to be in superposition. Unlike classical bits which can only either be in a 0 or 1 state, qubits are able to be in a linear combination of the two. An easy visualization of superposition is by using an vector pointing at a the surface of a sphere, called the bloch sphere.



Thinking of superposition like this lets us describe a superposition state as a combination of two rotation angles around the Z and X axis:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

An important property of superposition is that when the qubit's state is measured the outcome will always either be a 0 or 1. The degree of superposition effects the probability of the outcome. For example, if the state is fully pointing up to the 0 state, there will be a 100% chance of the outcome being 0, likewise if the state is at the hallway point pointing towards the X or Y axis, there will be a 50/50 chance to get either outcome.

To further complicate things, the above example only applies when the measurement is done along the Z direction, nothing stops one from doing their measurement in the X or Y direction instead. In case of a X axis measurement, now the state fully pointing up towards 0 will be 50/50 and the state pointing towards the positive X axis (often referred to as the + state, with the negative x-axis being the – state) will have a 100% chance of having the outcome 0.

Key distribution makes use of this property by preparing a number of random states and having both parties measuring them in random directions. If both parties measure in the same direction they will

know they have gotten the same outcome, but in the case of different directions there is a 50% chance their outcomes will differ.

By repeating this process enough times to suppress the possibility of a third party being able to beat the repeated 50% odds by sheer chance, it is possible to do a form of encryption that can only be broken if somebody manages to intercept both the channel used to communicate what directions where measured in, and also manages to get direct access to one party's qubits.

For more in depth explanations of the above here are nice sources:

Basics on qubits and superposition: What is a qubit? (quantum-inspire.com)

More in depth explanation of the bloch sphere visualization: bloch-sphere-rotations.pdf (univie.ac.at)

In depth explanation of the different techniques to do quantum key distribution **(strongly recommend reading this one)**: Quantum Key Distribution - QKD (wustl.edu)