Week 8 Summary of Key Concepts

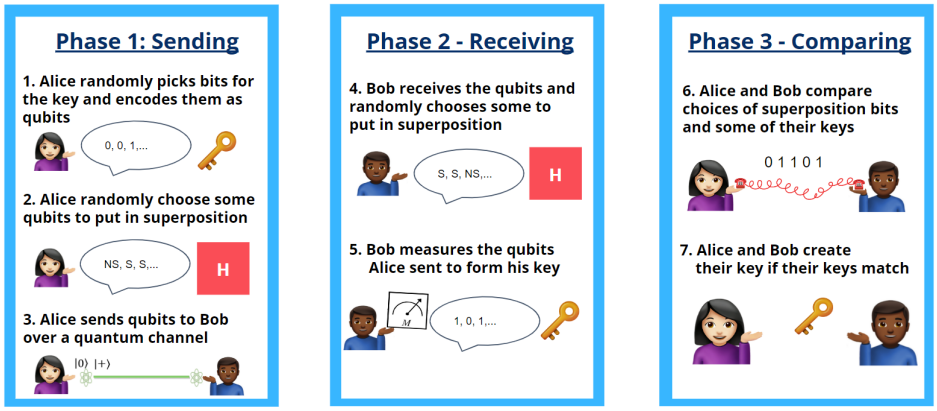
Lecture

In lecture this week, we discussed measurement bases, cryptography and the basics of QKD. We explored the QKD protocol and discovered how QKD is applied in the real world.

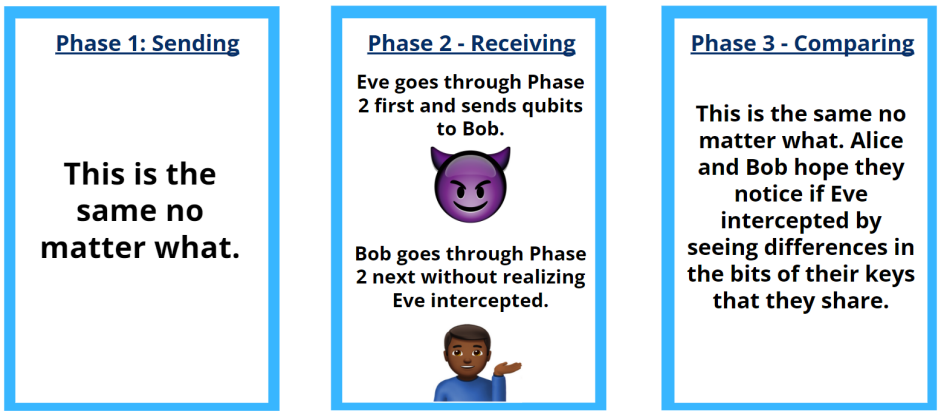
1. **Quantum Key Distribution (QKD)** is the first quantum protocol you will learn.
    a. It has applications in **cybersecurity** and uses the quantum properties of measurement to securely share a key that encodes a secret message.
    b. **Cryptography** is a subset of cybersecurity used for secure communication in the presence of third party adversaries.
    c. We send encrypted messages over a **channel**. We use a **key** to encrypt and decrypt a message. Example: Alice and Bob, and Eve

2. The **goal** of QKD is to confirm that our communication channel is secure.
    a. The QKD protocol **BB84** uses **superposition** to hide choices made by Alice and Bob and **quantum measurement** to detect the presence of Eve.
    b. How it works:
        i. Alice and Bob need a qubit for each bit of their intended key and a **quantum channel** to communicate over.
        ii. Alice and Bob both apply an **H gate** to (create/destroy superposition for) random qubits, hoping most of them match up.
        iii. Alice and Bob can communicate publicly (meaning Eve can listen in) about their random **superposition** choices afterwards since it's unlikely that Eve would have happened to make all the same choices as both Alice and Bob.
        iv. By measuring the qubits before they get to Bob, Eve fundamentally changes the **superposition** qubits' states. This change is detectable by Alice and Bob once they publicly share some of their bits.

c. QKD **without Eve**:



d. QKD **with Eve intercepting**:



3. Many quantum algorithms and protocols are not usable yet, but QKD is being implemented right now.
    a. Low cost, in-air, short distance QKD is used for Internet of Things or contactless payment.
    b. Fiber-cable, medium distance QKD is used for inter-database communication like in a regional company.
4. QKD is a protocol within **quantum communication**.
    a. **Quantum communication** is the field of study related to the transmission of quantum states between two or more parties.

Lab

In the lab this week, we implemented the BB84 protocol using Qiskit. This lab is almost entirely in the notebook instead of the slides to allow you to do something in Qiskit and gain a deeper understanding of how BB84 works.