Secure Quantum Information Transfer

Charles Averill

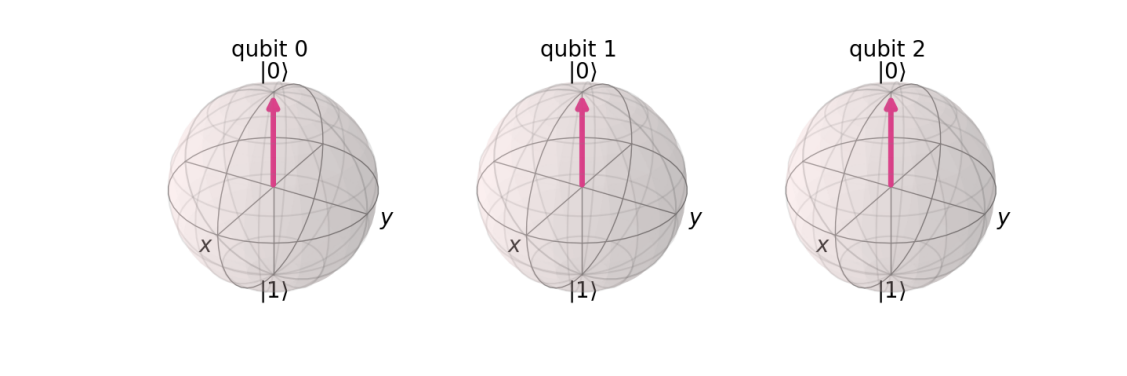
Computer Security Group
The University of Texas at Dallas

November 30, 2022

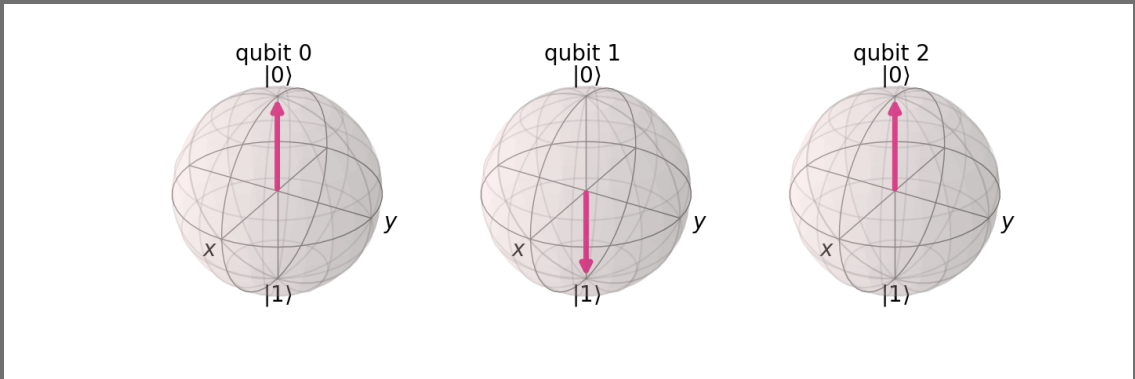
Introduction to Quantum Computers

- Classical computers implement data structures called "bits" that can be either "off" or "on" (0 or 1, low or high, etc.)
- Quantum computers implement data structures called "qubits" that can be either "off" or "on", OR in a **quantum superposition** of "off" and "on". This means that they are in both states, with a probability to be **measured** in either of the states
- Like classical computers, quantum computers utilize logic gates to manipulate qubit data. However, these are not standard gates. They depend on a bunch of factors like the phase of your qubits (that's a long story) and the measurement basis you choose (that's also a long story)

Manipulating Qubits

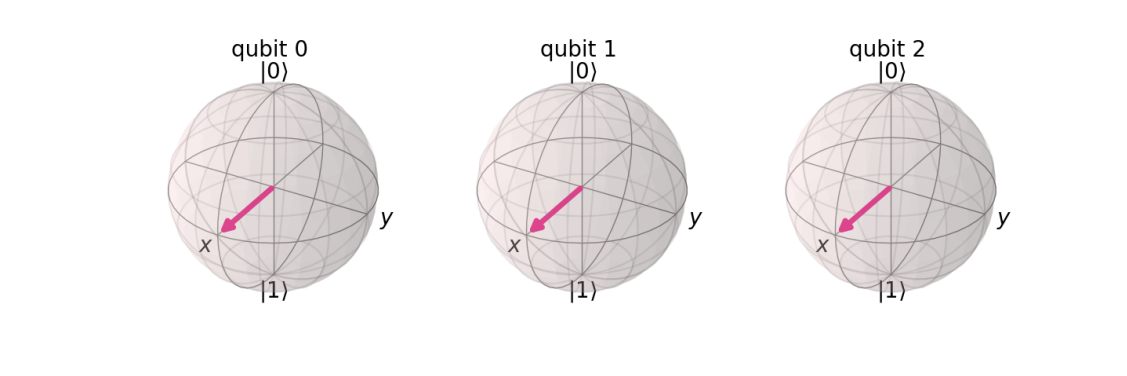


3-Qubit Circuit initialized to $|\psi\rangle = |000\rangle$

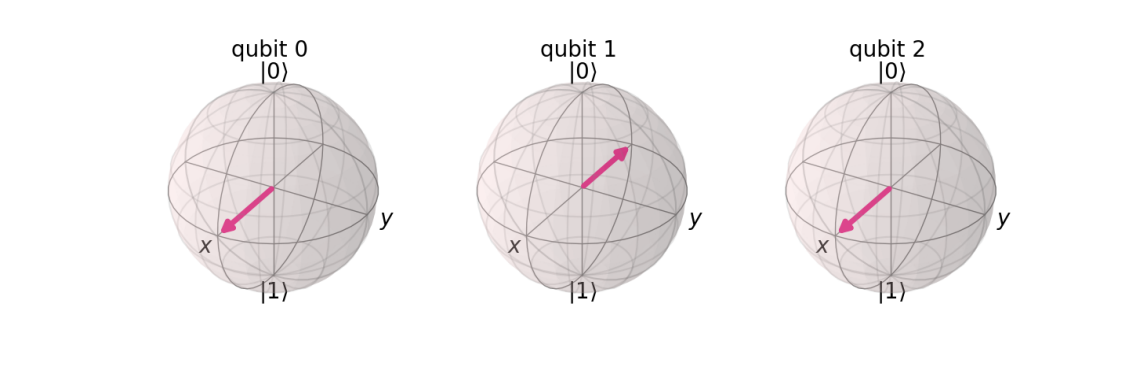


3-Qubit Circuit initialized to $|\psi\rangle = |010\rangle$

Manipulating Qubits



Initialized to $|\psi\rangle = \frac{\sqrt{2}}{4}(|000\rangle + |001\rangle + |010\rangle + \cdots + |111\rangle)$



Initialized to $|\psi\rangle = \frac{\sqrt{2}}{4}(|000\rangle + |001\rangle + |100\rangle + \cdots - |010\rangle - |011\rangle - \cdots)$

Manipulating Qubits

- Don't worry too much about the math. What's important to know is that it encodes the probability of measuring the qubits to be in one of those states (we do this by computing $\langle\psi|\psi\rangle$, don't worry about that)
- We can see how a qubit can be exactly in the $|0\rangle$ or $|1\rangle$ state, or in a superposition of states
- We can collapse these multi-states (superpositions) by measuring all qubits (or only collapse some multi-states while leaving others alone by only measuring some qubits). When we collapse the superposition, we get a definitive state like $|010\rangle$ or $|111\rangle$ instead of that mess we saw in the second set of figures
- Additionally, if the qubits are entangled (we'll show how to do this later), measurement results of one qubit will **alter** measurement probabilities of another

Who cares?

- Quantum Computing Researchers do!
  - Grover's algorithm lets you search through unsorted data in $O(\sqrt{N})$ time, way faster than with a classical computer!
- Security engineers with foresight do!
  - Shor's algorithm could break encryption as we know it. RSA encryption (used in a boatload of internet communication protocols) would be broken by Shor's algorithm, but some algorithms like SHA256 are still quantum-safe (for now)
- These algorithms took about 4 weeks each to explain in my Quantum Algorithms course (PHYS 4V11 with Prof. Zhang, anyone interested in this should take it). We should talk about something simpler that you can grasp, so I'll be introducing the concept of secure quantum communication

Quantum Entanglement

- Quantum communication relies on the concept of entangled qubits, whose states affect each other
- Let's introduce two quantum logic gates: Hadamard and CNOT
- The Hadamard gate puts a qubit into the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, so the qubit has a 50% chance to be measured as either a 0 or a 1 (this gate is in-place)
- The CNOT gate takes two qubits as input, a control qubit and a target qubit. If the control qubit is in the state $|1\rangle$, it will flip the state of the target qubit (even if it's in a superposition of states!)

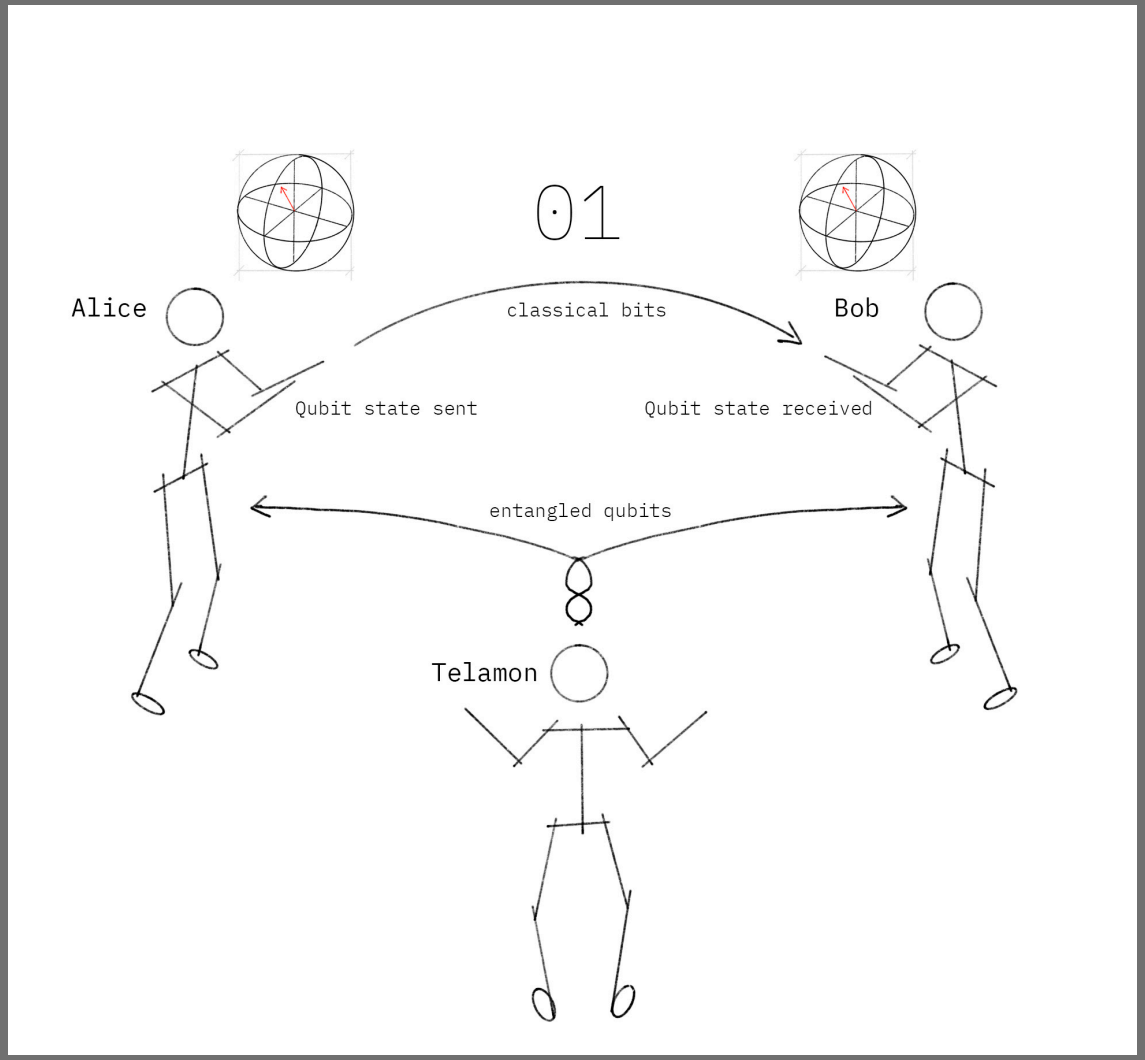
Quantum Entanglement

- Assume a 2-qubit computer. If we use the Hadamard gate on qubit 0, it will be in the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
- Then, if we use a CNOT gate with qubit 0 as control and qubit 1 as target, qubits 0 and 1 will be entangled
- Measuring q0 as the state $|0\rangle$ will force q1 into state $|0\rangle$
- Measuring q0 as the state $|1\rangle$ will force q1 into state $|1\rangle$
- This is because q0 had a 50% chance to be either a 0 or a 1, so q1 doesn't know what state it's in until q0 is measured! That's so cool!
- When q0 is measured, q1 will **immediately** update its state, no matter where in the universe it is. Einstein called this "spooky action at a distance"
- We will abuse this to communicate!

Quantum Transportation

- Alice wants to send Bob some data (1 bit of information)
- Alice and Bob will each first receive one of two entangled qubits from their friend Telemon. Let's say Alice receives q1 and Bob receives q2
- Alice will encode the information she wants to send to Bob into q0
- Alice will perform some operations (not important) on her entangled qubit and the qubit she wants to send. Then, she measures the two (getting a classical state for each bit) and sends those bits to Bob classically (over the internet)
- Depending on which bits Alice measured and sent, Bob will conditionally transform the state of his entangled qubit. After these transformations, Bob's q2 will have an identical state as Alice's q0!

Quantum Transportation



Quantum Transportation

- That's all fine and dandy, but so what? Why didn't Alice and Bob just communicate their 1 bit over the internet? It's faster, and it doesn't require complicated quantum hardware!
- Sure, but it's not that we can send messages with this protocol that's cool. We can use this to distribute one-time pad cryptographic keys that allow us to determine if someone is spying on our communications with an intercept-resend attack!
- We can also do other stuff but this one is pretty easy to understand

BB84 Protocol

- BB84 is the first quantum key distribution algorithm, allowing one party to send a private key to another party over a provably secure private channel
- It uses the quantum teleportation protocol that we just outlined, but with an extra bit: measurement angles
- You can perform quantum measurements on photons with rectilinear or diagonal filters, these alter the phase of the photon. It's more complicated but don't worry about it
- Alice will send a string of qubits encoding private key data to Bob, and will randomly pass each of the qubits through one of the two filters. Bob will receive the qubits and pass them randomly through filters again, recording what he measures.

BB84 Protocol

- Bob tells Alice that he has received her message. They will then compare the random filters they each used to send and receive their data. They will discard measured bits where the filters didn't match
- Now, Alice and Bob will publicly decide which bit positions of the remaining bits will comprise of the private key. Tada!
- They can even determine whether or not a third party, Eve, has been spying on their qubit transmissions. The no-cloning theorem states that it is impossible to create a perfect copy of an unknown quantum state, so if Eve tries to intercept and resend a message, there is a 50% chance that the resent message will include errors
- Alice and Bob will see that the set of qubits in which they used the same filter is too small (because Eve's measurements changed the "matching" filter on Alice's side with a probability of 50%) and will know that Eve has been **eve**sdropping

Sources

- Quantum Teleportation in Qiskit
- Detection of Eavesdropping in Quantum Key Distribution using Bell's Theorem and Error Rate Calculations

Further Reading

- Quantum zero-knowledge proofs
- Quantum coin flipping