🖊️

Seminar 9

Created	@November 12, 2022 8:16 PM
Class	Quantum Computing Fundamentals
Type	Seminar
Reviewed	□
Date	@November 13, 2022
Materials	week8_concepts.pdf

Quantum Key Distribution

Week 8 | November 13th, 2022

- Measurement Bases, Cryptography, & The Basics of QKD
- The QKD protocol:
  - Alci and Bob
  - Alice, Bob, and Eve
- QKD in the real world

First Protocol: Quantum Key Distribution

- QKD is a protocol with applications in cybersecurity
- Uses the quantum properties of measurement to securely share a key that encodes a secret message
- Three basic concepts:
  - Measurement & Measurement Bases

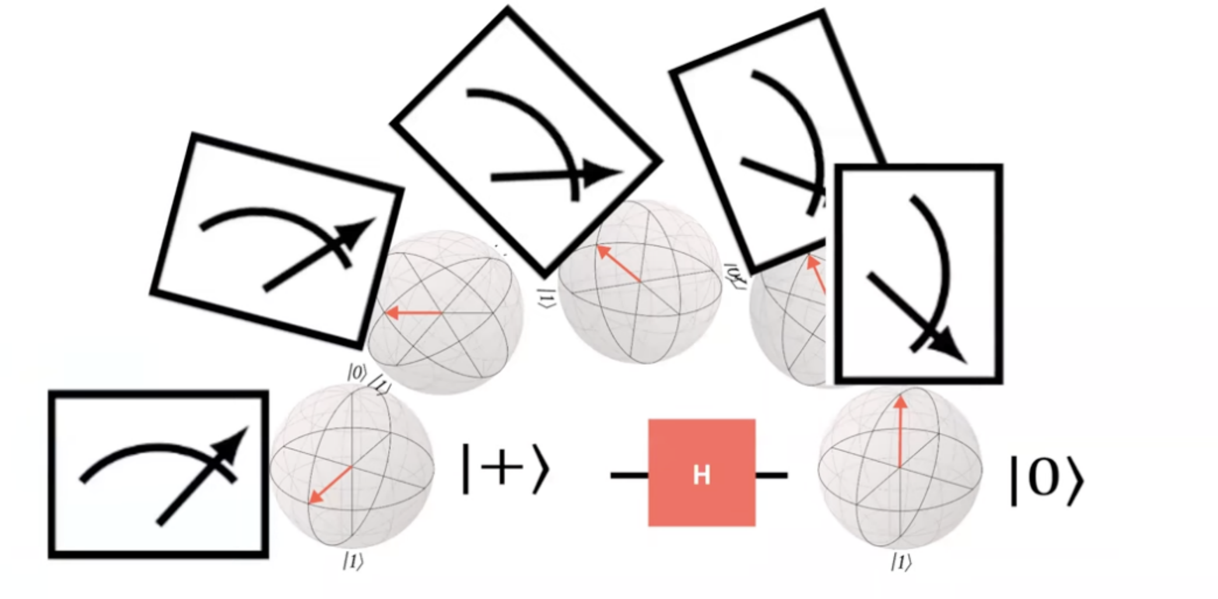
    - Basics of Cybersecurity & cryptography
    - Setup of protocol

Overview:

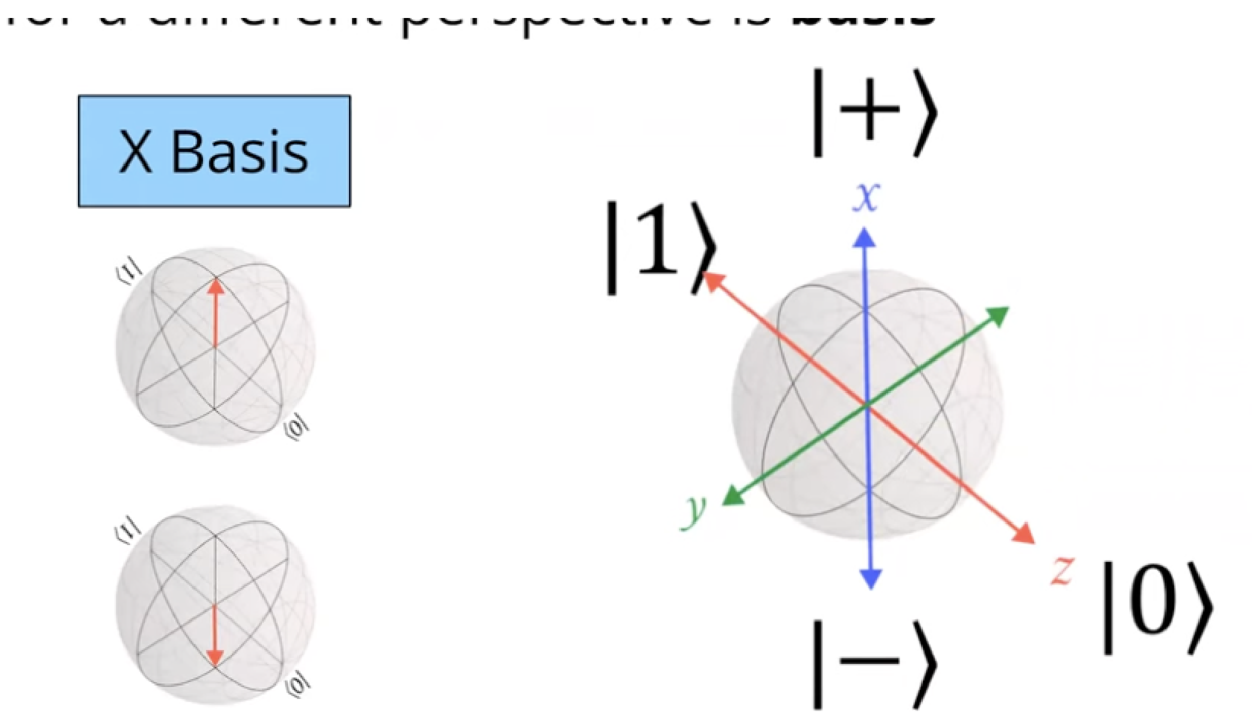
- Setting the Stage
- The QKD Protocol
- Introducing an Eavesdropper
- QKD in the Real World

***Key**: Just as we can apply a Hadamard gate to create superposition, we can also use it to reverse superposition

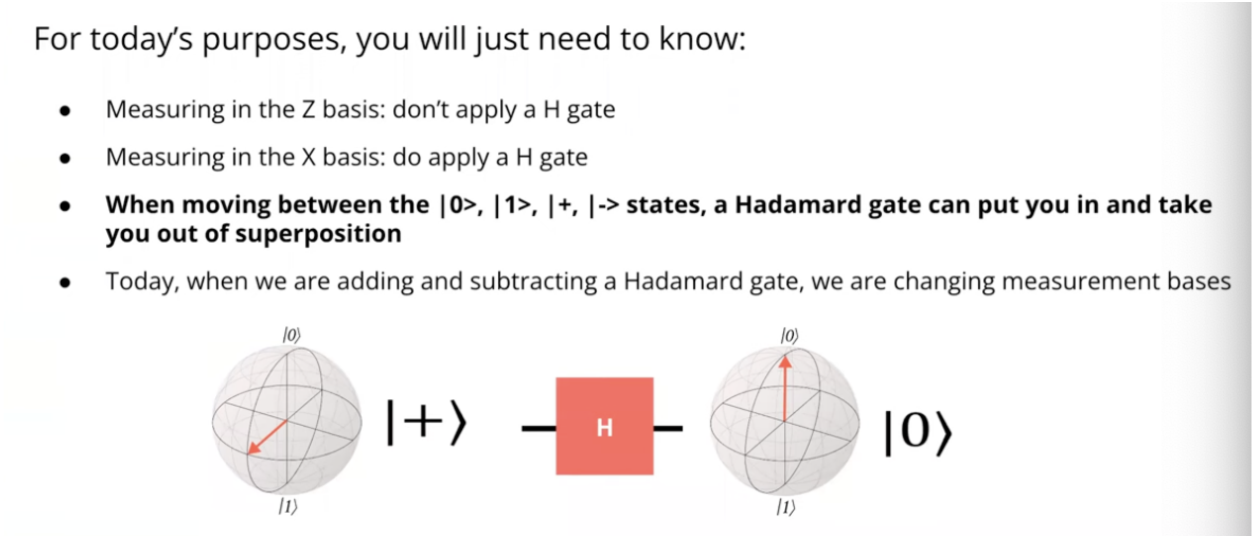
***Key**: Because gates are rotations of teh Bloch sphere, we can also imagine them as just rotating the angle we’re looking at or measuring the qubit from:



The word we use for a different perspective is *basis. The X-Basis is represented below:*



The Hadamard gate moves the us into the X-basis and performing the measurement in this basis. if we were in the X-basis, applying a H gate would take us into the Z-basis. Hadamard performs a change of basis with respect to our measurements.



For today’s purposes, you will just need to know:

- Measuring in the Z basis: don’t apply a H gate
- Measuring in the X basis: do apply a H gate
- **When moving between the |0>, |1>, |+, |-> states, a Hadamard gate can put you in and take you out of superposition**
- Today, when we are adding and subtracting a Hadamard gate, we are changing measurement bases

Cybersecurity, Cryptography, and QKD

- Quantum key distribution is a quantum protocol with applications in cybersecurity.

QKD is a cryptographic quantum protocol. Cryptography is a subset of cybersecurity. It is the practice of techniques for secure communication in the presence of third party adversaries. the goal of cryptography is to construct protocols that prevent third parties from reading private messages

Two important concepts: Channels & Keys

- We send encrypted messages over a *channel*
  - Public channel could include phone, email, or social media direct messages
  - Private channels could include optic fiber
  - Channels can be classical or quantum
- We use a *key* to encrypt & decrypt a message:
  - The key is a critical piece if information
  - If eavesdroppers can intercept the key, they can gain access to our valuable digital assets

Alice & Bib will be senders and receivers while we learn today's cryptography protocol. Alice has a message at UC Santa Barbra Quantum Lab and wants to send this to Bob to University to Waterloo Quantum Lab

Basics of QKD

- Alice & Bob are trying to send each other a secret message
- In order to protect their messages, Alice and Bob share a private key encrypt/decrypt their messages
- The Problem: A third party person (Eve) is trying to listen in on this conversation. Alice and Bob are trying to protect their information form getting stolen form Eve

In cryptography we need some way to communicate so that even if Eve is listening she cannot understand what they are saying. They do this by agreeing upon a random set of bits that they can encode and decode messages but will make it look very random to Eve. This random set of bits is called a key!

Goal of QKD

The Goal of Key Distribution is to confirm that our communication channel is secure - that our **key** was only shared between the sender and intended recipient.

The goal of QKD is to perform KD using quantum properties. Different QKD protocols use quantum properties differently.

Today we will look at the BB84 Quantum protocol:

- Superposition to “hide” choices made by Alice and Bob
- Quantum measurement to detect the presence of Eve in a way that classical protocols cannot

The QKD Protocol

In order to create a decide upon a key, Alice and Bob will begin by encoding 0’s and 1’s into qubits. but we can’t send qubits over a phone line…we need a “quantum phone line”. the technical term is a quantum channel.

Now, Alice has sent her qubits to Bob through their quantum channel. Bob then measures in the Z-basis to get the key. He will measure the states with full probability (100%) since there is no superposition.

However…

If Eve is listening and manages to tap into the quantum channel. Eve can now measure in the Z-basis and so it would change the state of the system and now Eve can send this to Bob. Eve now has access to this key and can decode all the messages. Eve did not disturb the q-state and Alice/Bib would not know that Eve had gotten into the quantum-channel.

- This whole process so far has no quantum properties leverages and only classical means were used besides the mention of the quantum channel mechanism

Reminder:

- Using qubits alone doesn’t keep our channel secure
- We will need to introduce quantum resources to help us detect Eve’s presence. Today will look at the first approach ever proposed called BB84 that uses superposition

New Approach:

- Alice creates a bit string, then decodes to randomly prepare some of her bits in a superposition. By applying a Hadamard gate to random qubits, some qubits will be pout into superposition

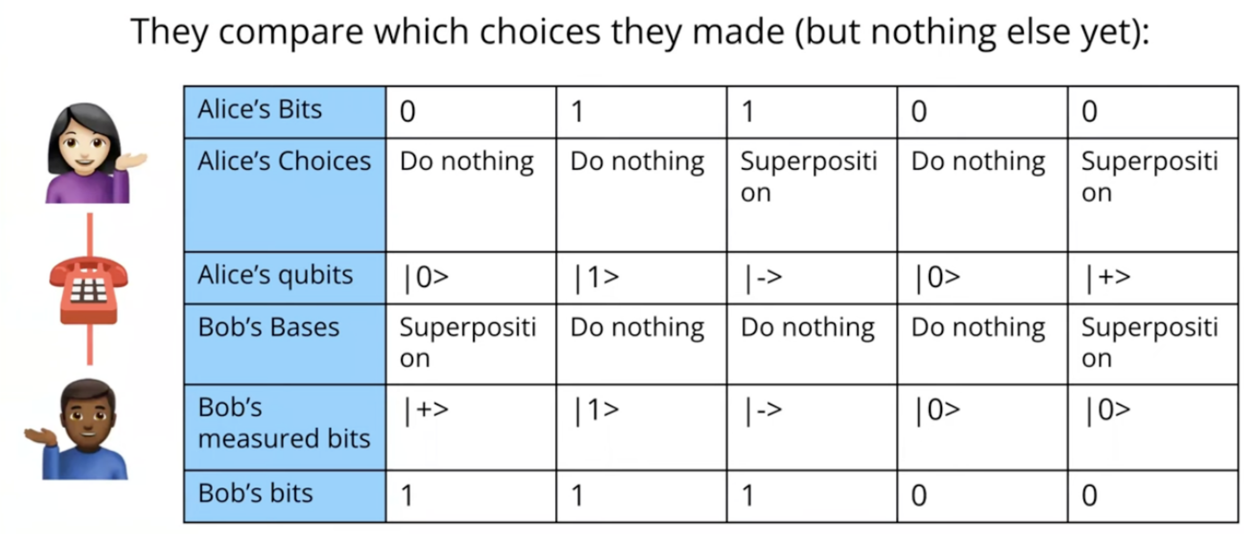
- Now, the quantum channel is used to send this to Bob. However, there are two qubits in superposition. Bob has a 50% chance of measuring the wrong result for each superposition bit. Since Bob doesn't know which qubits exactly are in superposition.

Reminder:

- Alice and Bob are doing this because they have no way to tell each other information without Eve hearing. Ao Alice cannot just tell Bob which qubits she put into superposition.
- So Bob is going to guess which qubits Alice put in superposition and undoes this by applying an H gate to them
- Bob hopes he guessed the right bits, he measures to get a key
    - However, the key he measures in some scenario will not match the key Alice had initially prepared.
    - This is OK! Bob and Alice can still make the protocol work
- Alice calls Bob through a classical channel and check which ones they happened to agree upon.

Key: It's ok for Alice and Bob to share which bases they used over a public channel, since it doesn't mean anything to those who don't have the qubits.

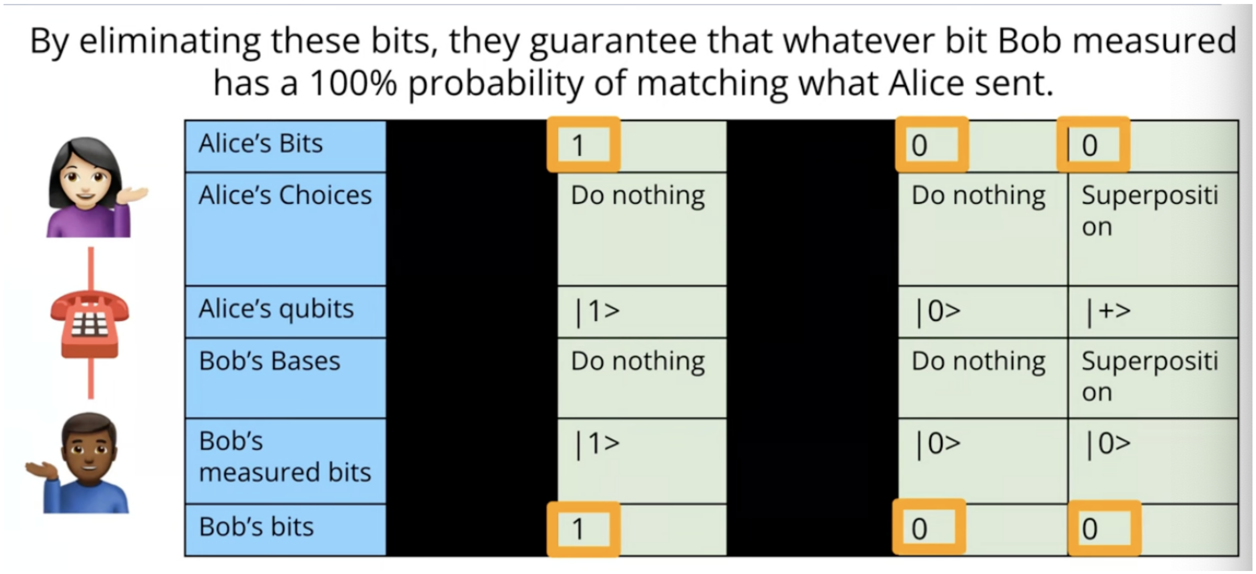
- Alice and Bob compare bases and eliminate qubits where they did not match up
- The trick is to send a large number of qubits so that if some qubits are taken off, it still is a sufficient amount of qubits for encryption



They compare which choices they made (but nothing else yet):

Alice's Bits	0	1	1	0	0
Alice's Choices	Do nothing	Do nothing	Superposition	Do nothing	Superposition
Alice's qubits	|0>	|1>	|->	|0>	|+>
Bob's Bases	Superposition	Do nothing	Do nothing	Do nothing	Superposition
Bob's measured bits	|+>	|1>	|->	|0>	|0>
Bob's bits	1	1	1	0	0

which becomes…



By eliminating these bits, they guarantee that whatever bit Bob measured has a 100% probability of matching what Alice sent.

Alice's Bits	[redacted]	1	[redacted]	0	0
Alice's Choices	[redacted]	Do nothing	[redacted]	Do nothing	Superposition
Alice's qubits	[redacted]	|1>	[redacted]	|0>	|+>
Bob's Bases	[redacted]	Do nothing	[redacted]	Do nothing	Superposition
Bob's measured bits	[redacted]	|1>	[redacted]	|0>	|0>
Bob's bits	[redacted]	1	[redacted]	0	0

At the end of the day, they lost some bits, but both of their keys match and they never revealed what the bits were in this exchange, so this public exchange doesn't reveal anything useful. **They only communicate whether a qubit is in superposition or no in their public channel exchange!**

Introducing Eve:

Let's repeat the protocol, but see what happens when an eavesdropper is present. Now since Eve is listening, Eve will intercept those qubits and performa measurement. While performing this measurement, she also has a 50% chance of getting each superposition bit wrong and the measurement changes states, so the qubits she sends on to Bob have now been changed! When these modified qubits are sent to Bob, those Qubits will not be in superposition and now has changed the key in and of itself.

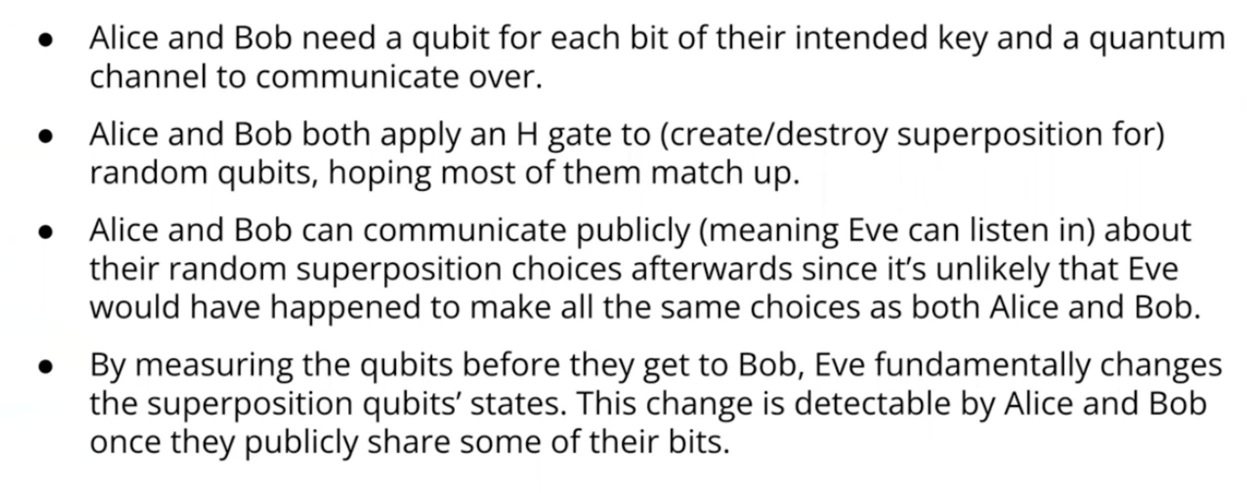
Bob will subsequently receive an altered form of the key. Bob does not know of this change yet. He continues with his guesswork as usual.

However, when they compare using a public channel (they still do not know of Eve's involvement), what ends up happening is that the states of the remaining qubits after elimination (by comparing bases (superposition or no) may still differ and the only way this happens is due to a Eavesdropper present. They find this out when they realize that even after the elimination, the bits of Bob do not match the bits of Alice

In order to detect this, they are forced to publicly share some (not all) of their measurement results. but if they send enough bits, they can afford to sacrifice a few for this privacy check.

Now Alice and Bob will have to try again, ideally using different quantum channel (which is not cheap).

Key Takeaways for BB84:



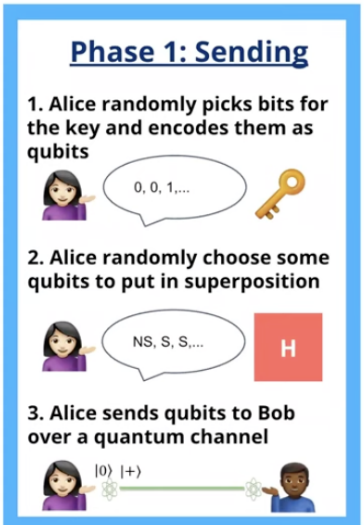
- Alice and Bob need a qubit for each bit of their intended key and a quantum channel to communicate over.
- Alice and Bob both apply an H gate to (create/destroy superposition for) random qubits, hoping most of them match up.
- Alice and Bob can communicate publicly (meaning Eve can listen in) about 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.
- 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.

There is a very small probability that Eve could go undetected since all of this is probabilistic decisions. It is very unlikely that Eve had made same choice as Alice and Bob and decreases as the number of qubits used increases.

No Cloning Theorem (Theory behind QKD BB84):

It turns out that it is proven that **Quantum States cannot be copied.**

If this was not true, then Eve could make a copy of Alice’s qubits on their way to Bob and then wait until Alice and Bob publicly communicate which ones are in superposition. Then she could measure the qubits no problem and secretly learn the key.

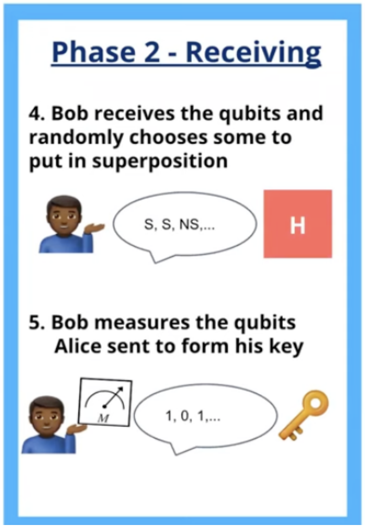


Phase 1: Sending

1. Alice randomly picks bits for the key and encodes them as qubits

2. Alice randomly choose some qubits to put in superposition

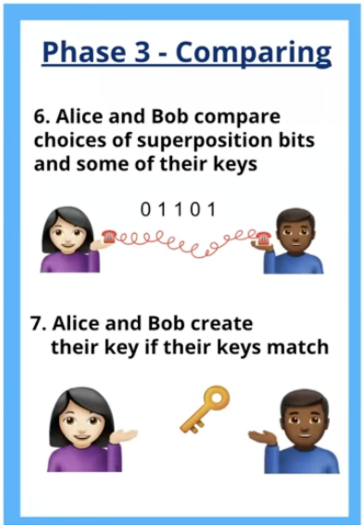
3. Alice sends qubits to Bob over a quantum channel



Phase 2 - Receiving

4. Bob receives the qubits and randomly chooses some to put in superposition

5. Bob measures the qubits Alice sent to form his key

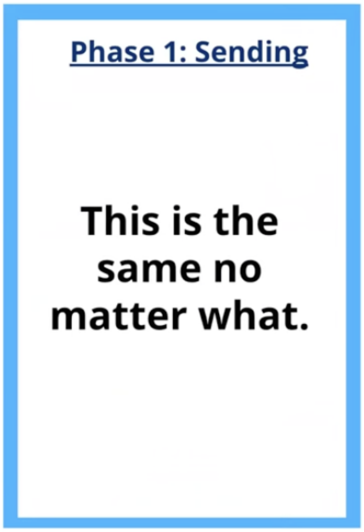


Phase 3 - Comparing

6. Alice and Bob compare choices of superposition bits and some of their keys

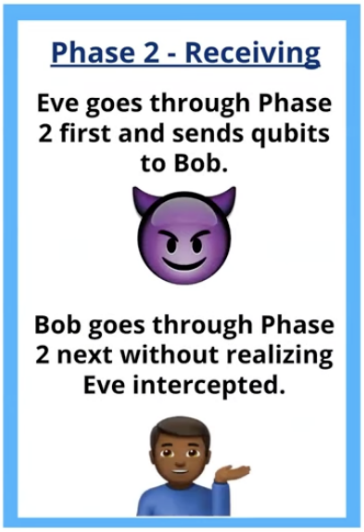
7. Alice and Bob create their key if their keys match

If Eve intercepts…



Phase 1: Sending

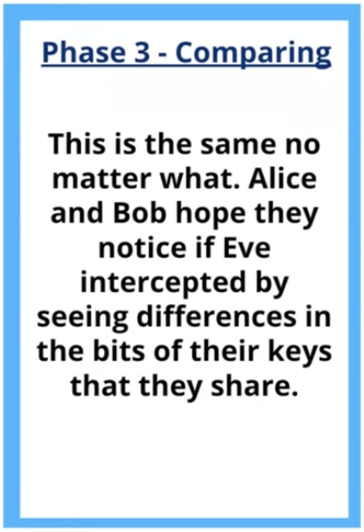
This is the same no matter what.



Phase 2 - Receiving

Eve goes through Phase 2 first and sends qubits to Bob.

Bob goes through Phase 2 next without realizing Eve intercepted.



Phase 3 - Comparing

This is the same no matter what. Alice and Bob hope they notice if Eve intercepted by seeing differences in the bits of their keys that they share.

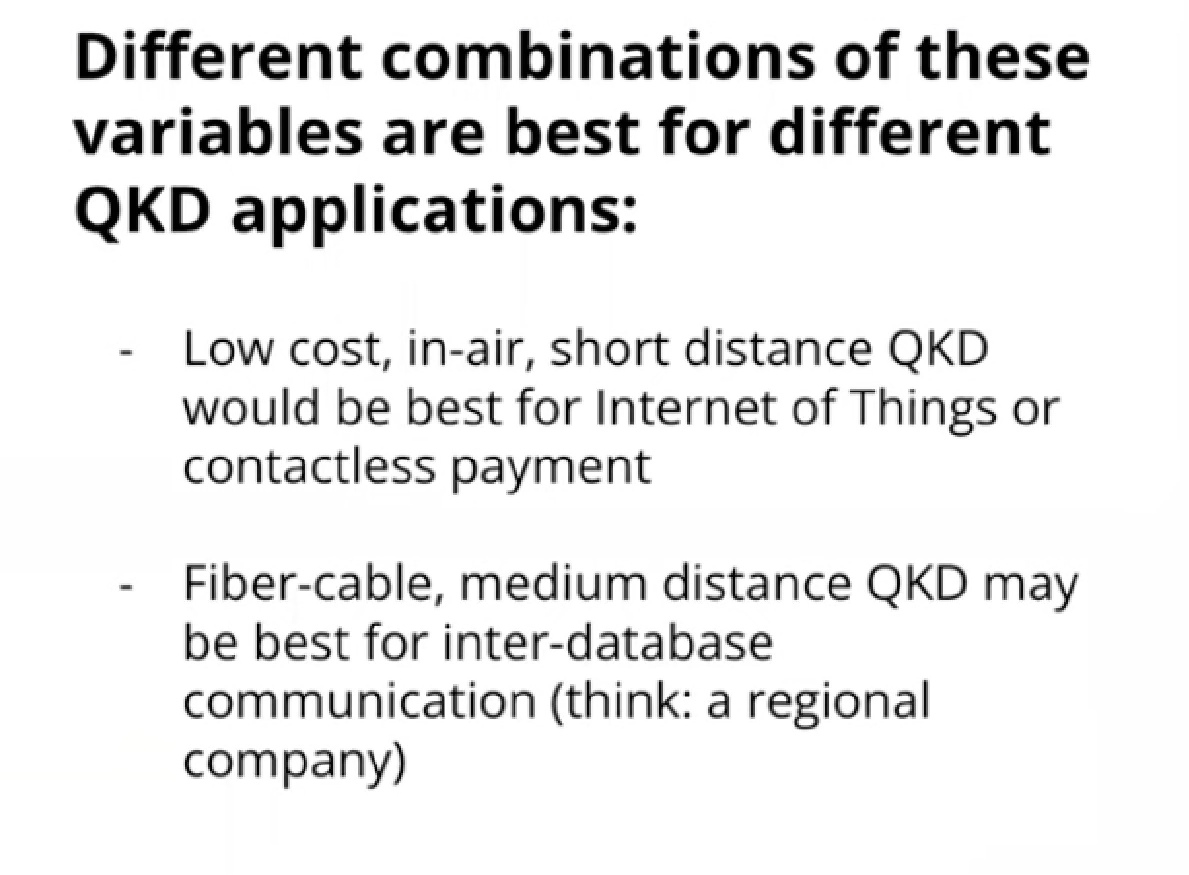
QKD in the Real World:

- Many quantum algorithms and protocols are not yet usable. Powerful algorithms that assume perfect, fault-tolerant hardware, which is likely decades away. However

QKD is something we can implement now.

  - QKD works with classical systems to secure a communication channel.
  - We have what we need to start developing these systems.
  - Companies are working on implementing BB84 in real life

- QKD has made it to space!
  - The team simultaneously transmitted a pair of secret keys to allow two ground stations in China, located more than 1, 1120 km apart, to establish a direct link.
- Not all QKD protocols are the same (multiple components):
  - Device used
  - Meidum (in air, via cable)
  - Distance between senders
  - Cost of implementation

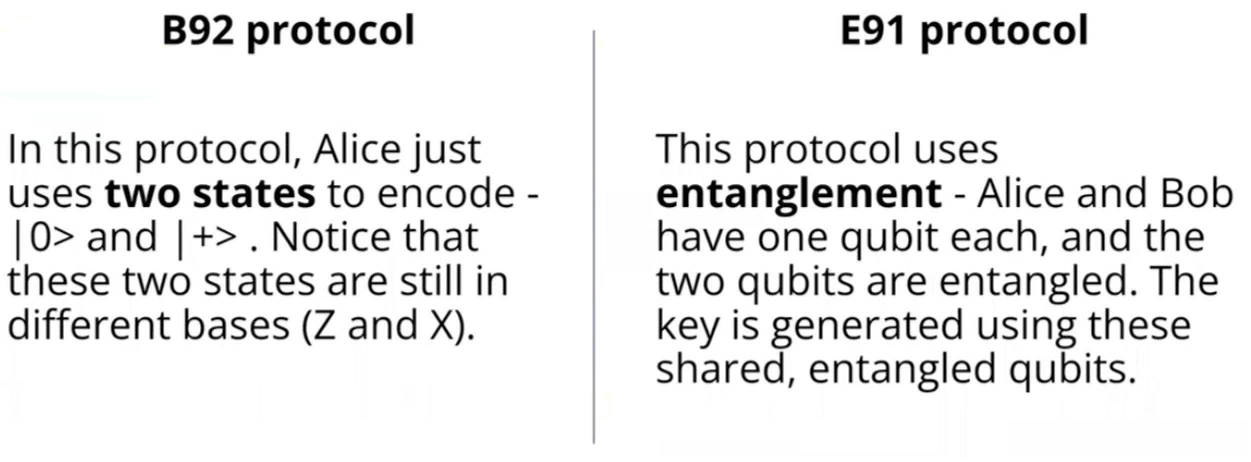


Different combinations of these variables are best for different QKD applications:

- Low cost, in-air, short distance QKD would be best for Internet of Things or contactless payment

- Fiber-cable, medium distance QKD may be best for inter-database communication (think: a regional company)

Two Alternative QKD Protocols:



B92 protocol

In this protocol, Alice just uses **two states** to encode - |0> and |+> . Notice that these two states are still in different bases (Z and X).

E91 protocol

This protocol uses **entanglement** - Alice and Bob have one qubit each, and the two qubits are entangled. The key is generated using these shared, entangled qubits.

As the protocols increased in complexity, the security of these communication is increased with fewer qubits used.

QKD is a protocol within quantum communication which is the field of study related to the transmission of quantum states between two or more parties.

Other applications of Quantum Communication beyond QKD:

- Quantum Teleportation of Information (quantum Internet)
- Quantum Coin Flipping