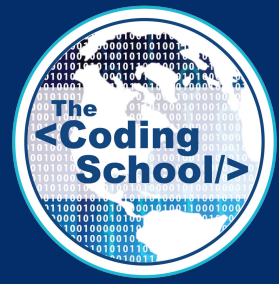


INTRO TO QUANTUM COMPUTING

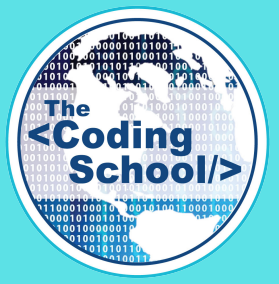
LECTURE #19

QUANTUM COMPUTATION PT. 4 :

QUANTUM KEY DISTRIBUTION (BB84)

FRANCISCA VASCONCELOS

3/14/2021



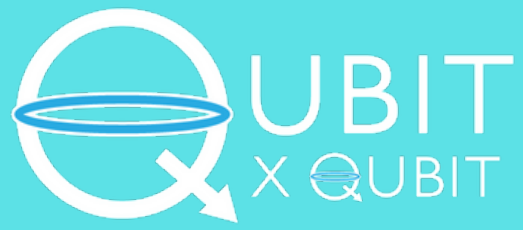
ANNOUNCEMENTS

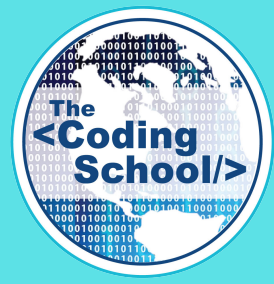
QUANTUM COMPUTATION LECTURE SERIES

Lecture 1 – The Quantum Circuit Model *How can we perform computation with quantum systems?*	CONCEPTS
Lecture 2 – Qiskit Tutorial *How can we program quantum circuits?*	PROGRAMMING
Lecture 3 – Quantum Circuit Mathematics *How can we represent quantum circuits mathematically?*	MATH
Lectures 4-6 – Introductory Quantum Protocols and Algorithms *How can we leverage quantum for cryptography, teleportation, and algorithms?*	APPLICATION

TODAY'S LECTURE

1. What are Quantum Protocols?
2. What is Quantum Cryptography?
3. Classical Key Distribution
4. BB84 Quantum Key Distribution Protocol
    a) BB84 Protocol - Theory
    b) BB84 Protocol - Demo





WHAT ARE QUANTUM PROTOCOLS?

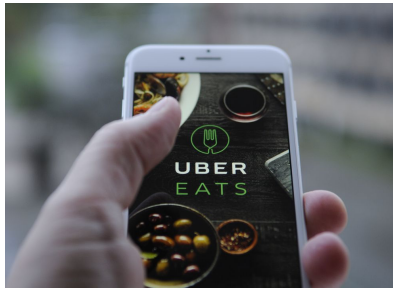
“PROTOCOL”

The word ***protocol*** can have different meanings depending on the context... In computer science, a protocol is *a set of rules or procedures for transmitting data* between 2 entities.

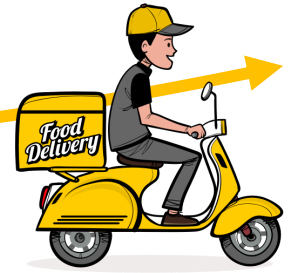
For example, the ***Internet Protocol Suite*** (frequently known as TCP/IP) is a set of communication protocols used in the Internet and similar computer networks. It specifies how data should be packetized, addressed, transmitted, routed, and received!

PROTOCOL EXAMPLES

01000110101...



$|01000110101\ \ldots\rangle$



QUANTUM PROTOCOLS

Quantum protocols are also *a set of rules or procedures for transmitting data* between 2 entities.

However, quantum protocols leverage quantum information! A good quantum protocol will achieve some sort of advantage to classical protocols.

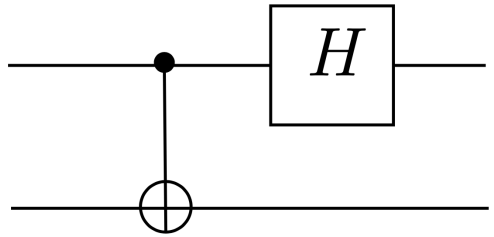
Usually, quantum protocols transmit data ***more efficiently*** or ***more securely*** than classical protocols!

We already saw two examples of ***efficient*** quantum protocols last class: ***Superdense Coding*** and ***Quantum Teleportation***!

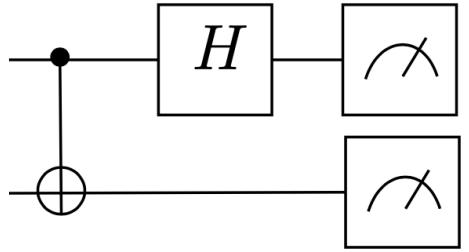
RECAP: SUPERDENSE CODING & QUANTUM TELEPORTATION

Both superdense coding and quantum teleportation leverage ***Bell states*** and ***Bell measurements***.

We can ***entangle*** our qubits with the circuit:



We can perform a ***Bell measurement*** using the circuit:



We can perform different operations on this entangled state, to generate the 4 different types of ***Bell states***:

message	transformation	***BELL STATES***
00	$\mathbb{I}_A \otimes \mathbb{I}_B$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\beta_{00}\rangle$
01	$X_A \otimes \mathbb{I}_B$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\beta_{01}\rangle$
10	$Z_A \otimes \mathbb{I}_B$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\beta_{10}\rangle$
11	$X_A, Z_A \otimes \mathbb{I}_B$	$\frac{\|10\rangle-\|01\rangle}{\sqrt{2}} = \|\beta_{11}\rangle$

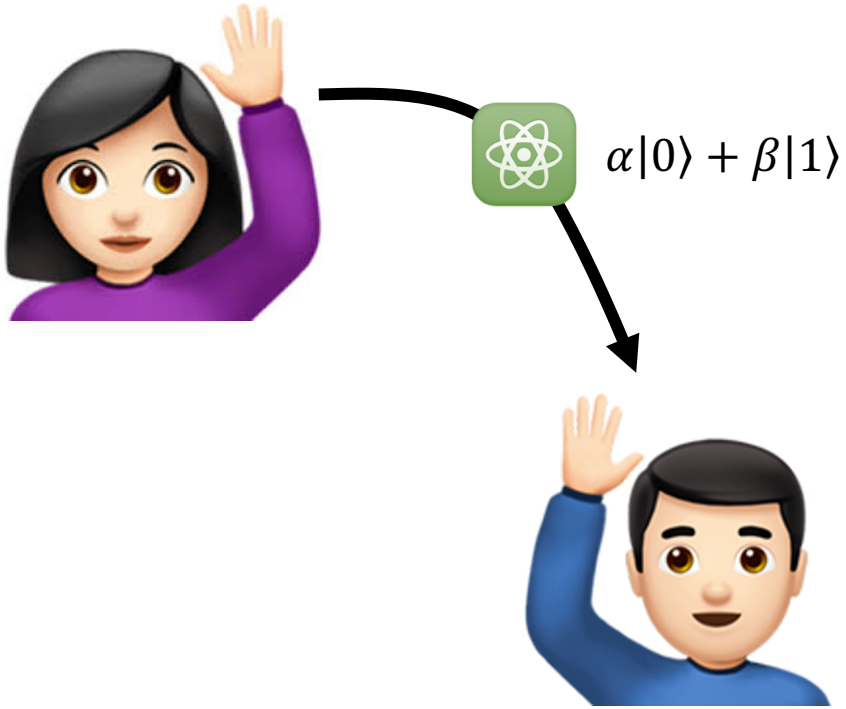
Performing ***Bell measurements*** on ***Bell states*** returns classical bit messages!

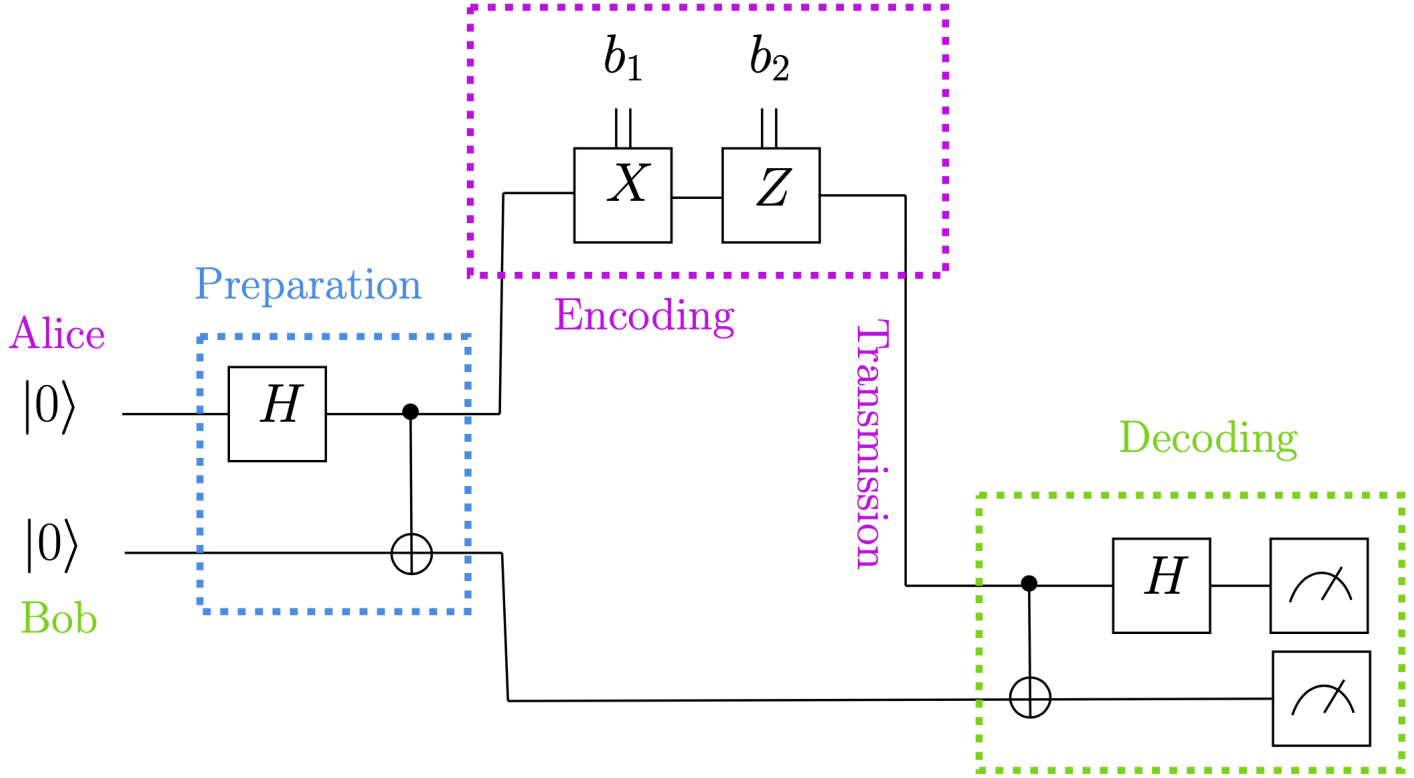
BELL STATES	***BELL MEASUREMENT***	message
$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\beta_{00}\rangle$	→	00
$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\beta_{01}\rangle$	→	01
$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\beta_{10}\rangle$	→	10
$\frac{\|10\rangle-\|01\rangle}{\sqrt{2}} = \|\beta_{11}\rangle$	→	11

RECAP: SUPERDENSE CODING

Superdense coding is a quantum communication protocol to "efficiently" transmit **2** classical bits of information with only **1** qubit! *

$00, 01, 10, 11$

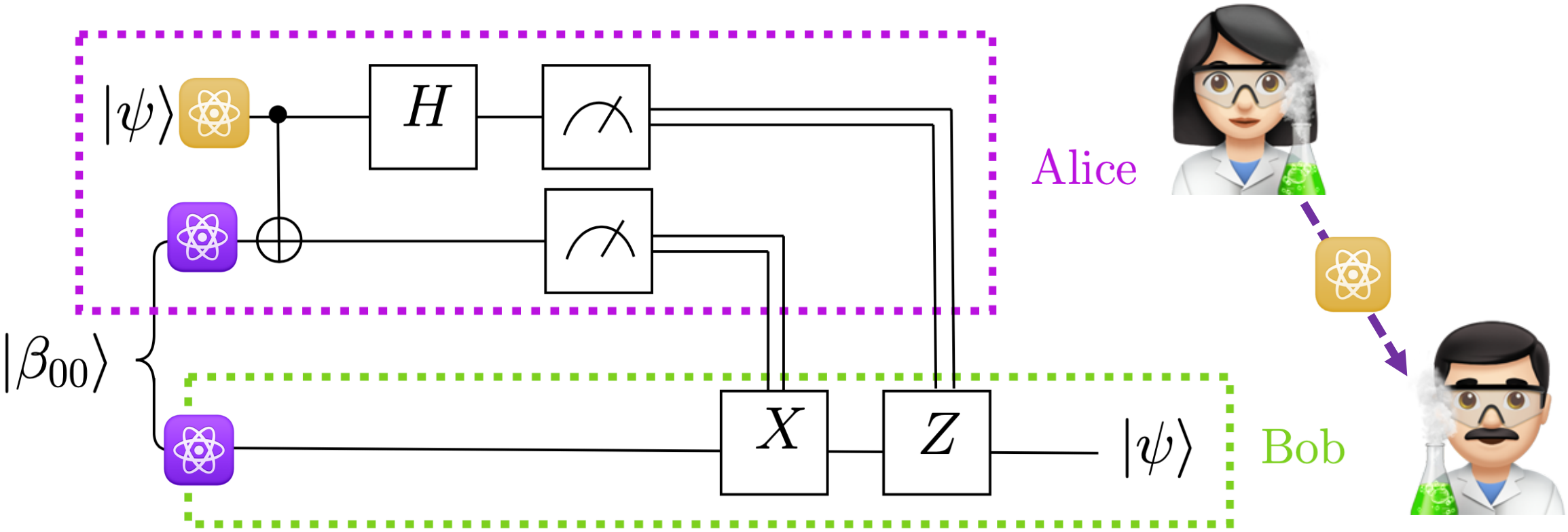




** This assumes that an entangled Bell pair has already been shared between the sender and receiver.*

RECAP: QUANTUM TELEPORTATION

Quantum teleportation is a quantum communication protocol to "efficiently" transmit a quantum state only using classically communication channels! *

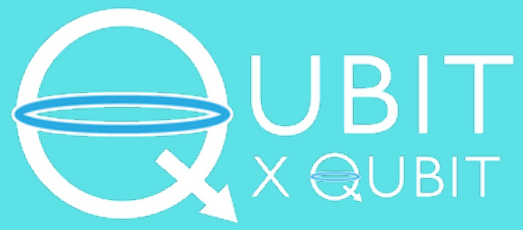


** This assumes that an entangled Bell pair has already been shared between the sender and receiver.*

QUANTUM OPERA

The Superdense Coding and Quantum Teleportation protocol assumption:

We are living in a world where bell states are easily shared or transmitted at no cost....

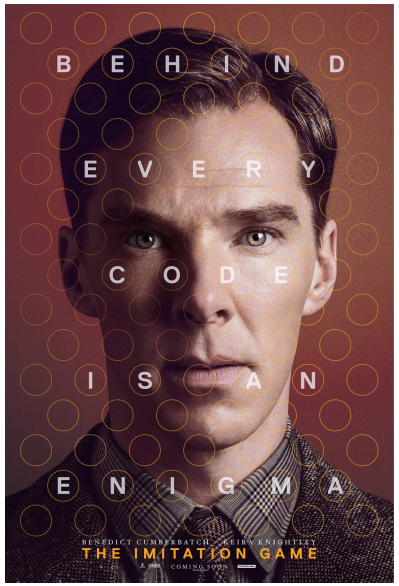


WHAT IS QUANTUM CRYPTOGRAPHY?

DEFINE CRYPTOGRAPHY

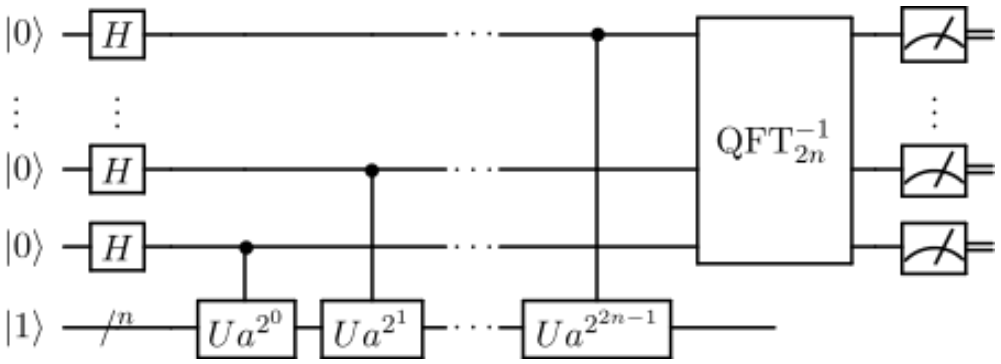
Cryptography is the practice/study of techniques for secure communication in the presence of third party adversaries.

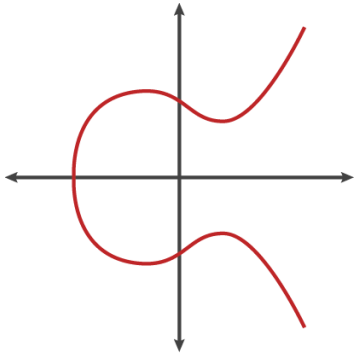
It is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.



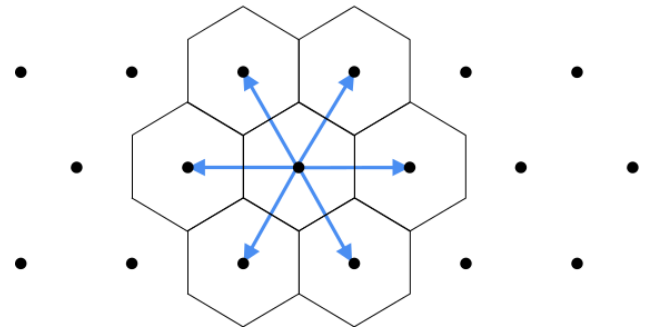
POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography is the field devoted to studying algorithms robust to attack by a quantum computer.





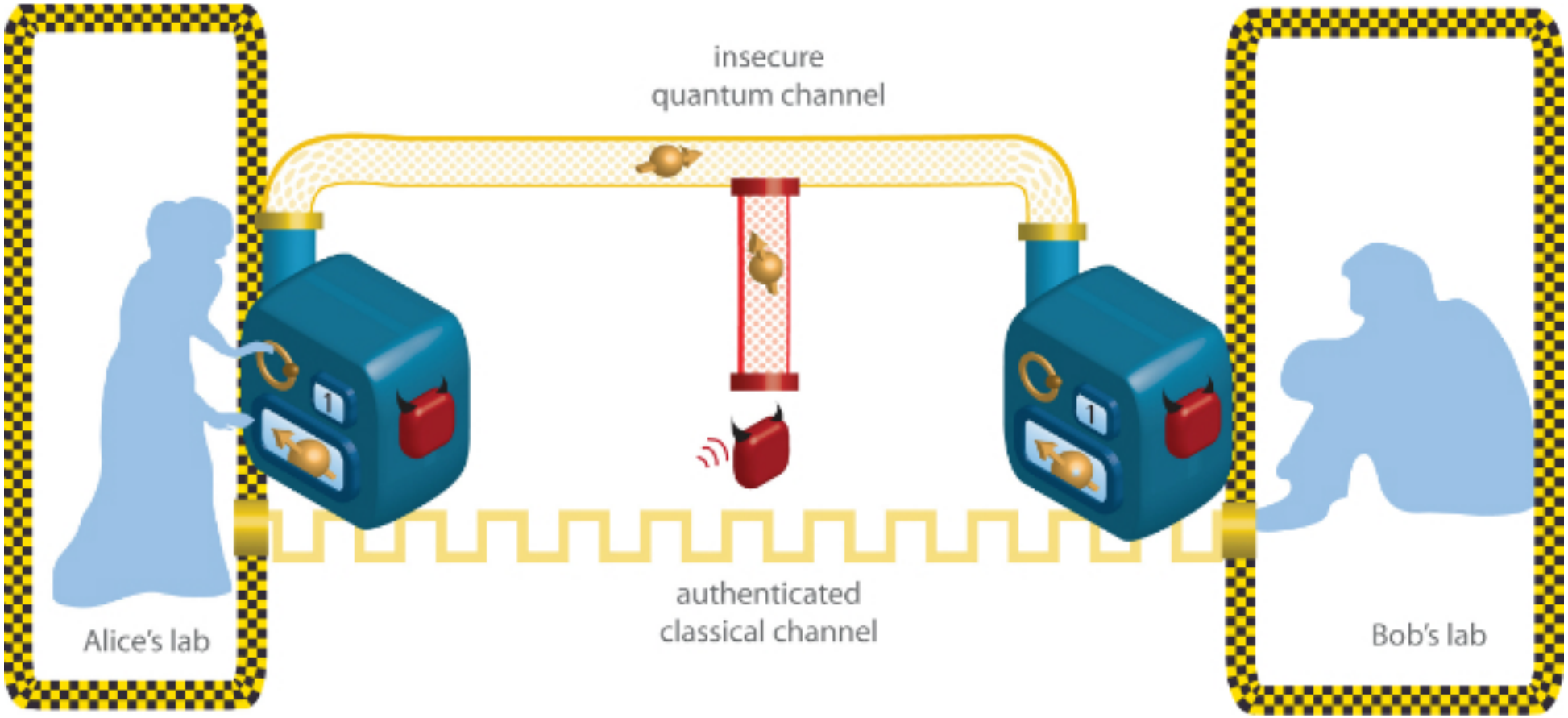
Elliptic-Curve Cryptography

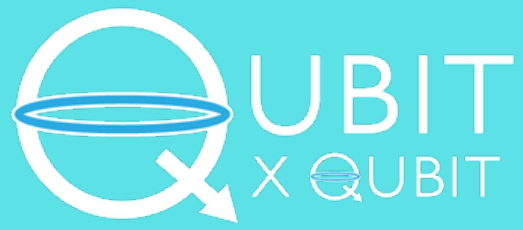


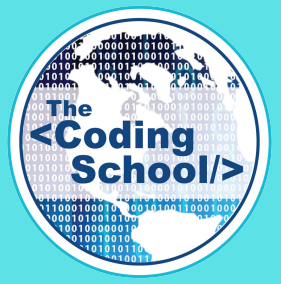
Lattice-Based Cryptography

QUANTUM CRYPTOGRAPHY

Quantum cryptography is the field of study dedicated to exploiting quantum mechanics to perform cryptographic tasks.







CLASSICAL KEY DISTRIBUTION

ENCRYPTION AND DECRYPTION

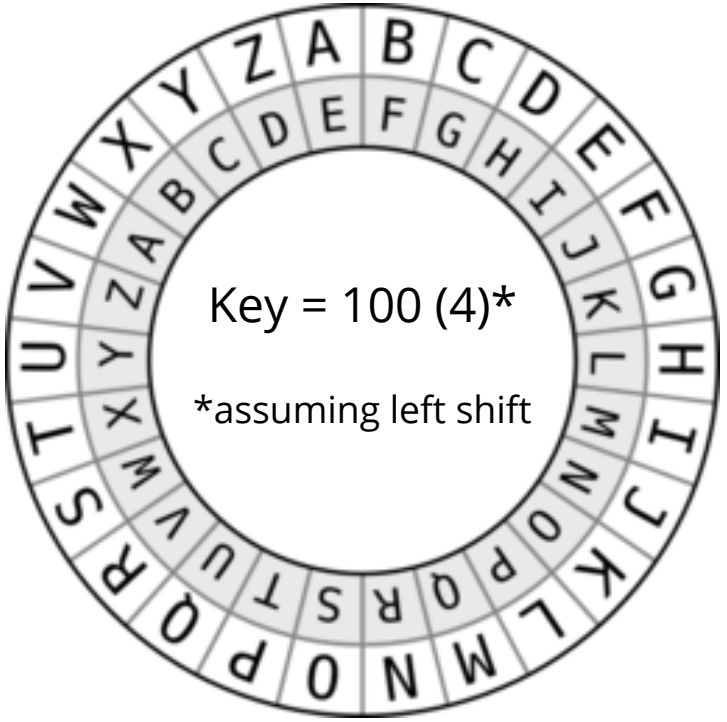
Encryption is the process of encoding/scrambling a message so that it can only be read by desired parties.

Decryption is the process of converting the encrypted message back into a readable form.

Caesar Cipher: Left Shift of 4

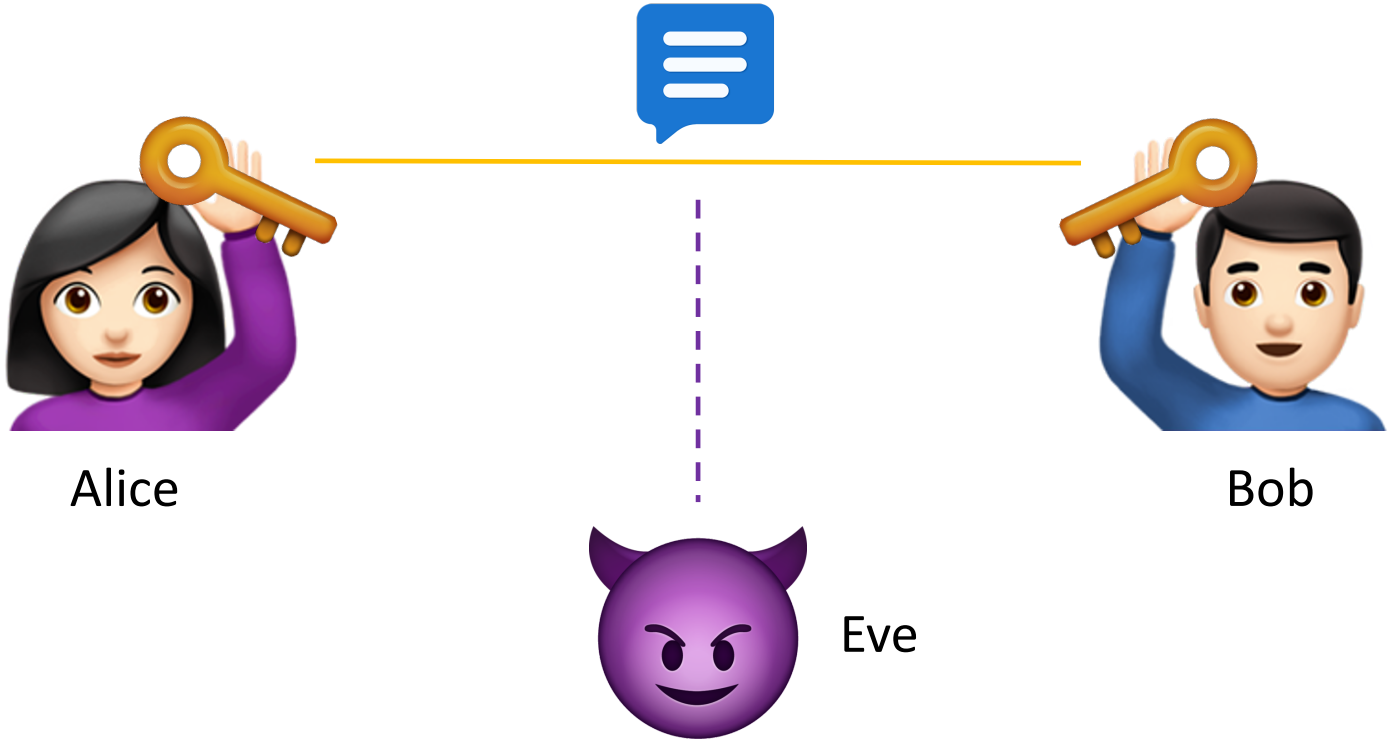
CRYPTOGRAPHIC KEY

A ***key*** is simply a long string of 0s and 1s, which can be used to ***encrypt*** and ***decrypt*** a message.



SYMMETRIC KEY CRYPTOGRAPHY

There are two parties (Alice and Bob) who are trying to exchange private messages.

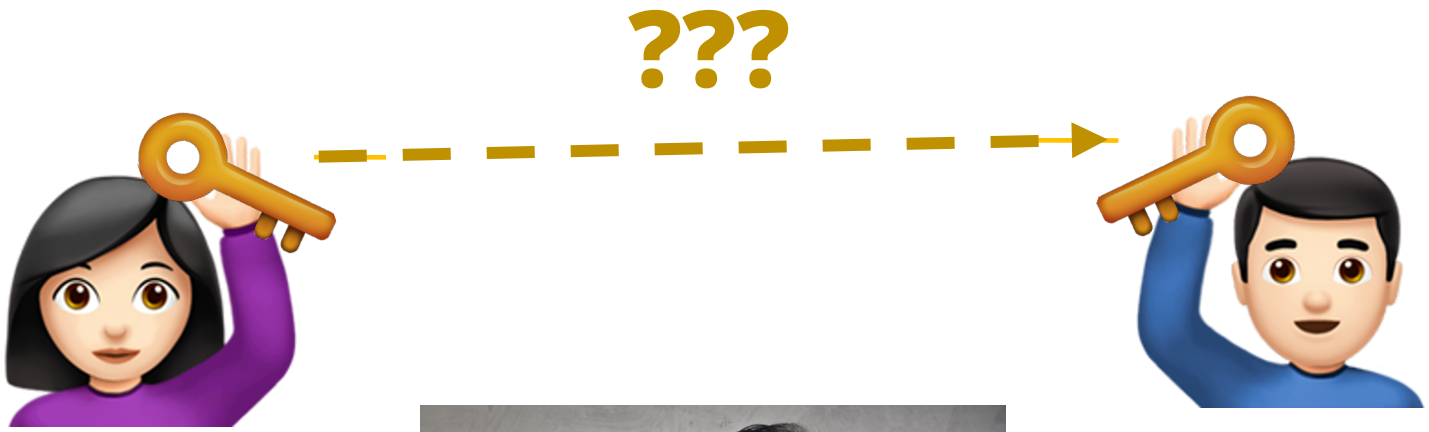


However, they are aware that an eavesdropper (Eve) is trying to listen on their conversation for malicious purposes.

In order to protect their message, Alice and Bob share a private key to encrypt/decrypt their messages.

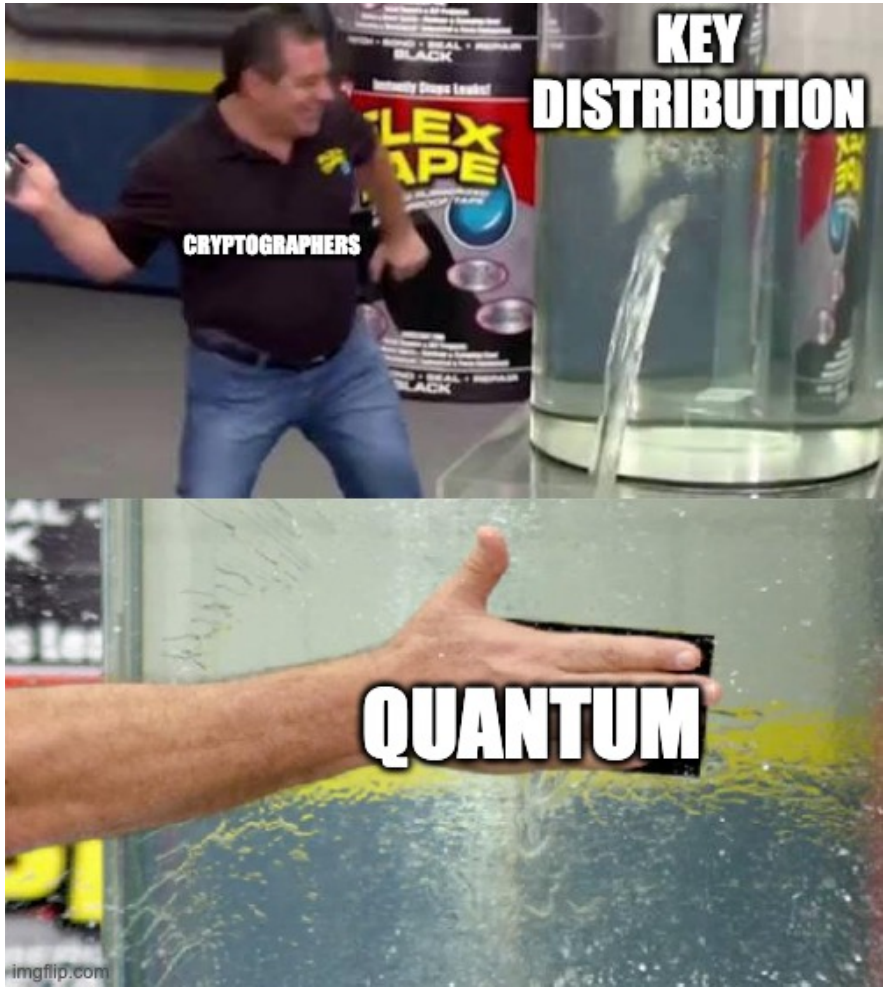
CLASSICAL SYMMETRIC KEY CHALLENGE

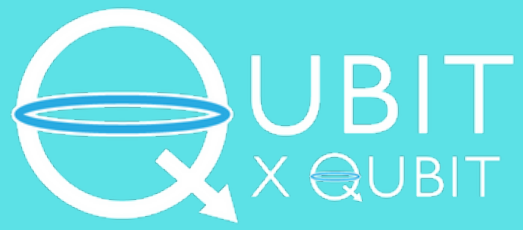
In classical symmetric key cryptography, the main challenge is securely sharing the private key between Alice and Bob...

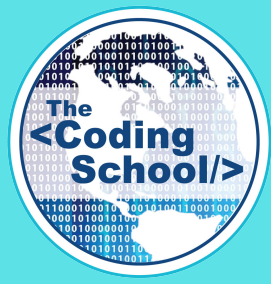


Alice

Bob







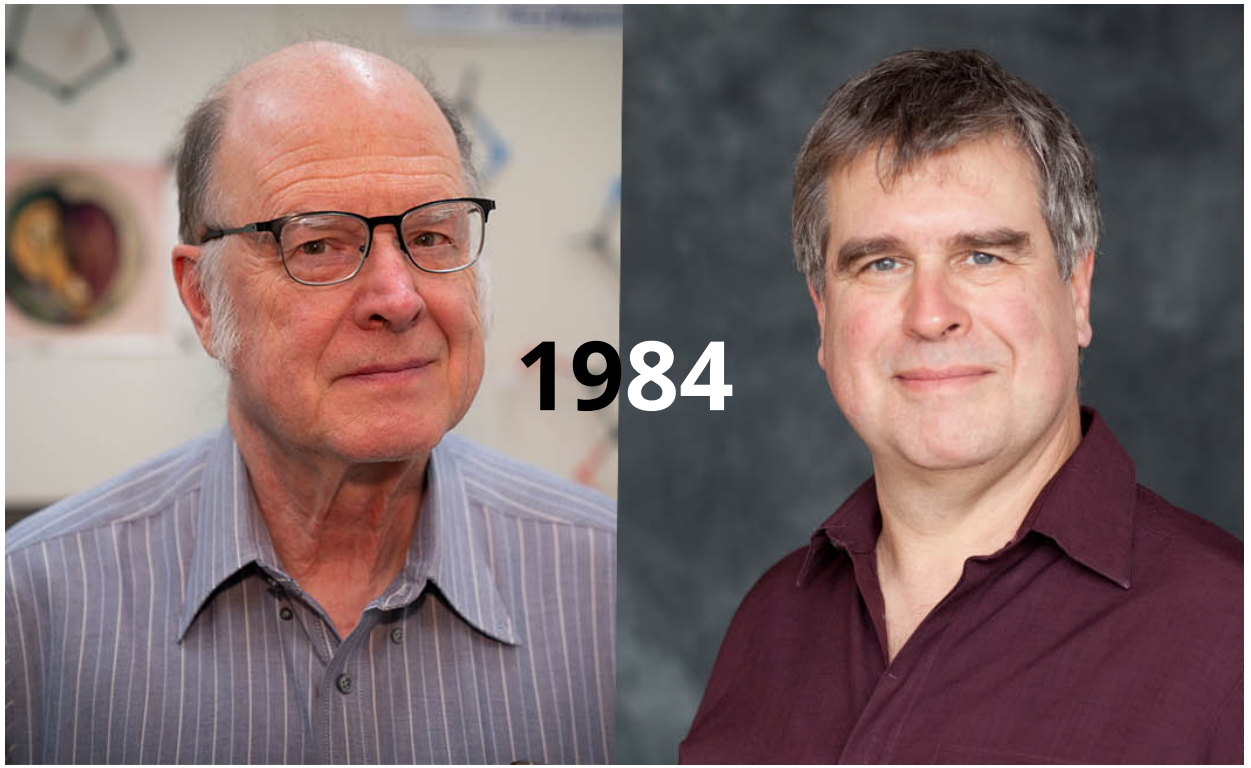
QUANTUM KEY DISTRIBUTION

THE BB84 QKD PROTOCOL

BB84 is a ***quantum key distribution protocol*** that was invented by Charles Bennett and Gilles Brassard in 1984.

It uses quantum mechanics in order to distribute a symmetric key!

Not BB-8 !



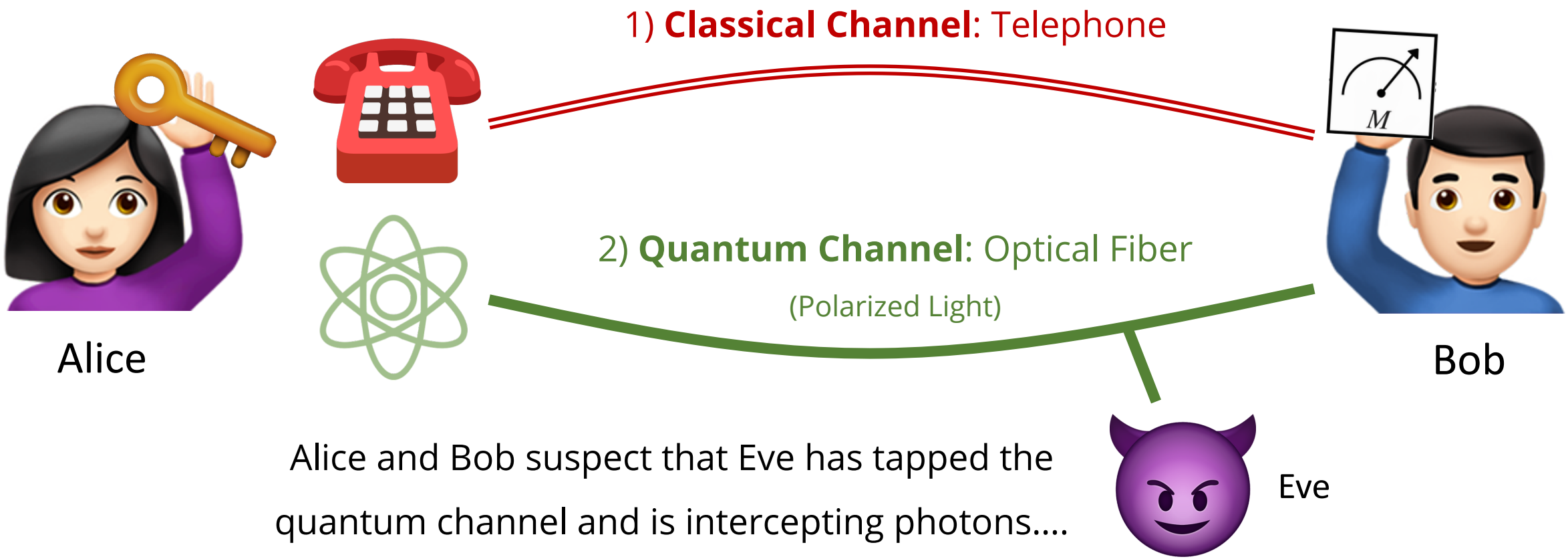
Charles Bennett

Gilles Brassard

BB84 - OVERVIEW

Alice has generated a key, which she wants to share with Bob.

She has two communication channels:



Alice and Bob suspect that Eve has tapped the quantum channel and is intercepting photons....

BB84 – MAIN IDEAS

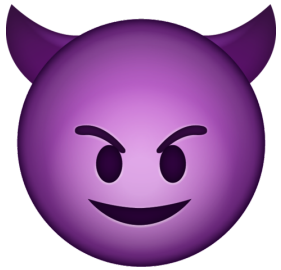
iDEaL wOrLd: already have secure channel, send key, use key

Next best thing: send key, know if someone intercepted the key, if so throw away and try again, otherwise use key

BB84 – MAIN IDEAS

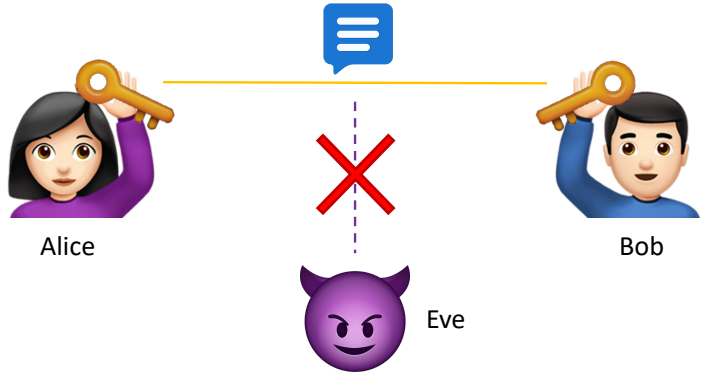
The BB84 protocol does ***not*** prevent Eve from intercepting the key!

Instead, the BB84 protocol allows Alice and Bob to ***statistically deduce*** if Eve has tapped the communication channel and is intercepting their key.



If their quantum communication channel is not secure, Bob should disregard the transmitted key. Alice and Bob will need to find another quantum channel and try again.

Once Alice and Bob are confident that they have ***securely*** transmitted their key, they can use a typical encryption scheme with the the key to transmit their secret message!



THE BB84 PROTOCOL - PRE-KNOWLEDGE

Before running the protocol, Alice and Bob need to establish a common ground.

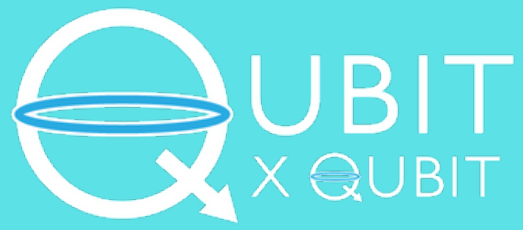
Alice Bob

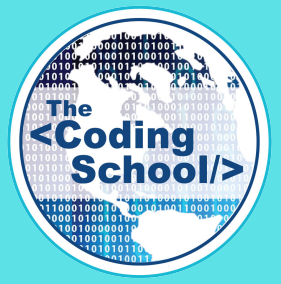
As part of the ***protocol***, they decide that any quantum bits Alice sends through the quantum communication channel must be encoded in one of the following 2 bases:

(1) Horizontal-Vertical Polarization: Basis States:

(2) Diagonal Polarization: Basis States:

Bob also knows any quantum bits he receives will be encoded in one of those 2 bases, but not necessarily which basis.





BREAK TIME!

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

   -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

   -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

   -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

   -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(1) SELECT ENCODING

For each of the 10 bits, Alice randomly selects a basis (× or +) to ***encode*** each bit.

Alice

10-Bit Key: 0 1 0 1 0 0 0 0 1 0

Randomly Selected Encoding Bases: × + + × × + × × + +

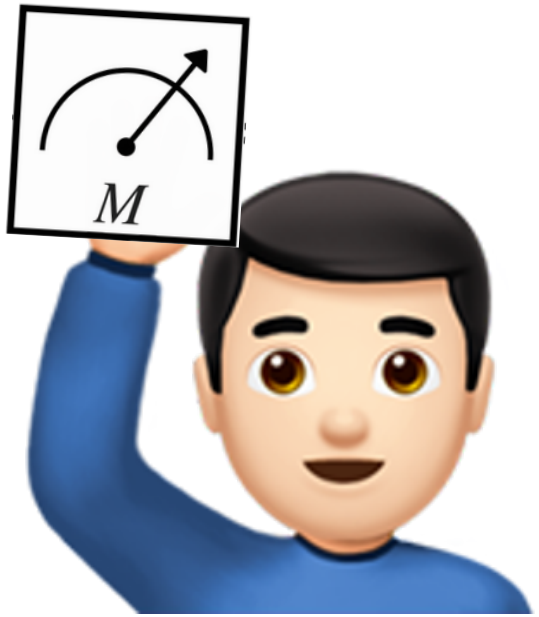
THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.
   -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)
   -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(2) SELECT MEASUREMENT

For each of the 10 bits, Bob randomly selects a basis (× or +) to ***measure*** each bit.



Bob

Randomly Selected Decoding Bases: + + + × × × × + + +

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(3) ENCODE QUANTUM STATES

Alice creates the n polarized bit states and sends them to Bob, who measures them (in the pre-determined bases).

Alice's 10-Bit Key:	0 1 0 1 0 0 0 0 1 0
Randomly Selected Encoding Bases:	× + + × × + × × + +
Encoded Key:	

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

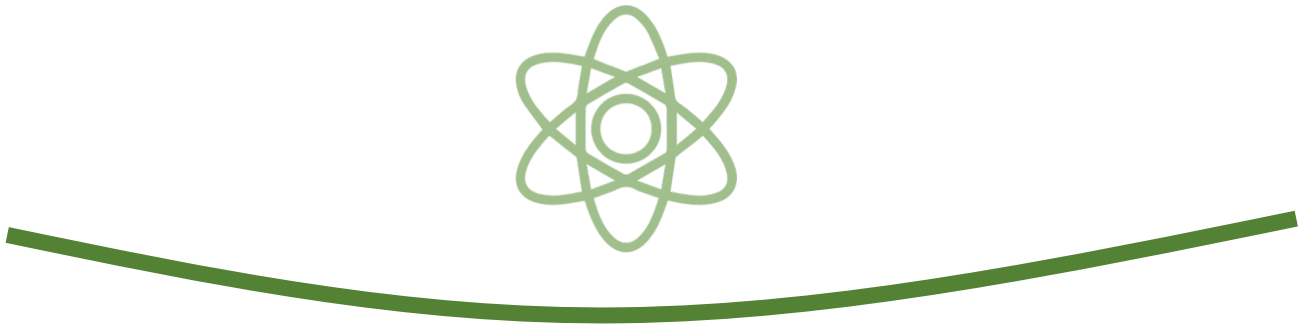
    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

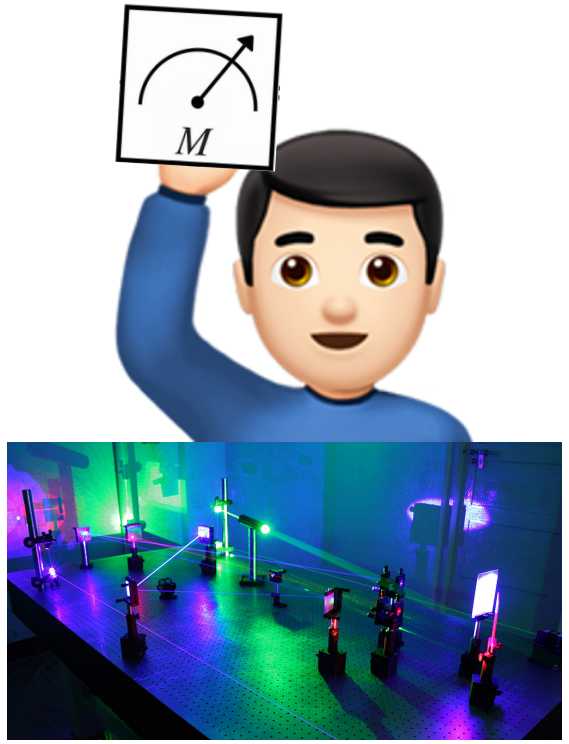
    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(4) SEND QUANTUM STATES

Alice sends the encoded quantum states to Bob, via the quantum channel.





$|\nwarrow\rangle$ $|\uparrow\rangle$ $|\downarrow\rangle$ $|\nearrow\rangle$ $|\nwarrow\rangle$ $|\downarrow\rangle$ $|\nwarrow\rangle$ $|\nwarrow\rangle$ $|\uparrow\rangle$ $|\downarrow\rangle$

(Alice's Encoded Key)

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

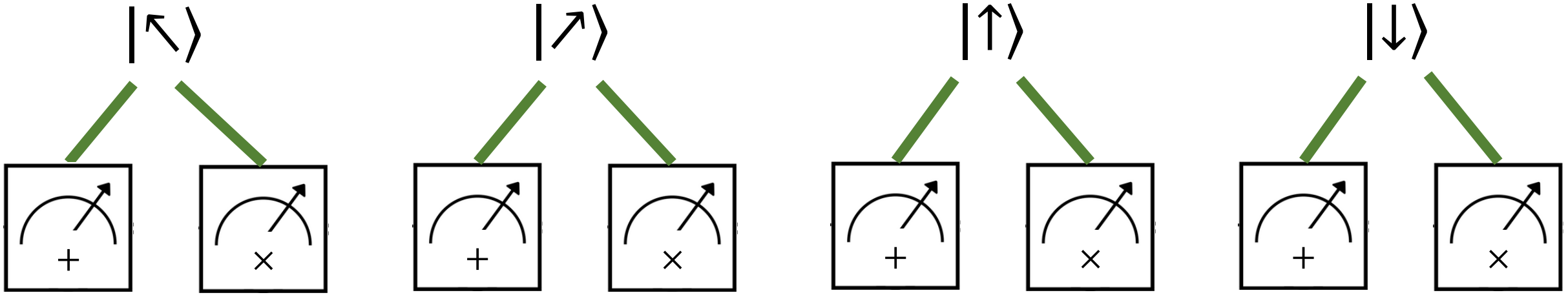
    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(5) MEASURE QUANTUM STATES

Bob measures all the quantum states he receives from Alice (using his randomly selected bases).

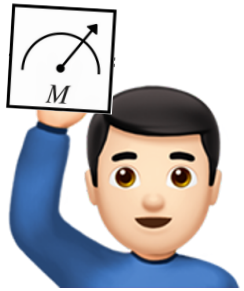
Let's recall how measurement works with different bases...



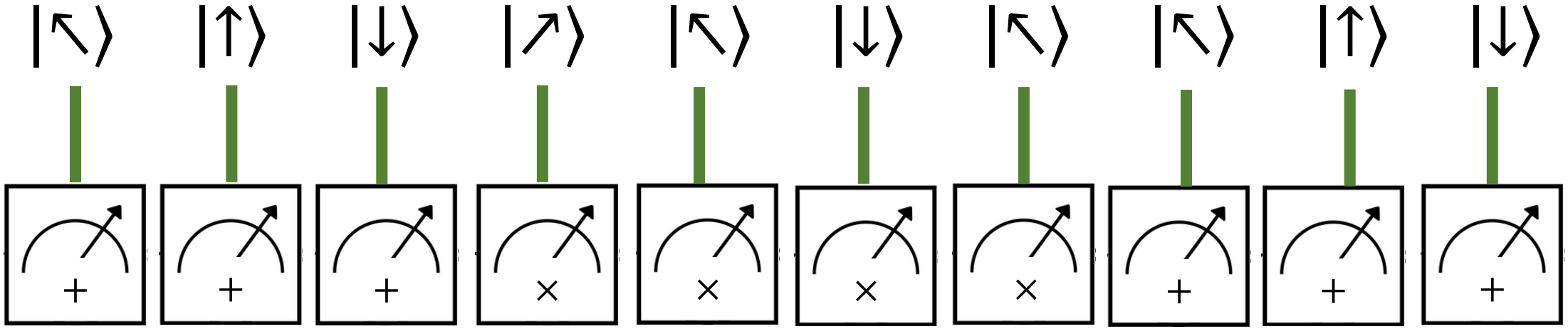
(5) MEASURE QUANTUM STATES

Bob measures all the quantum states he receives from Alice (using his randomly selected bases).

Alice



Bob



THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

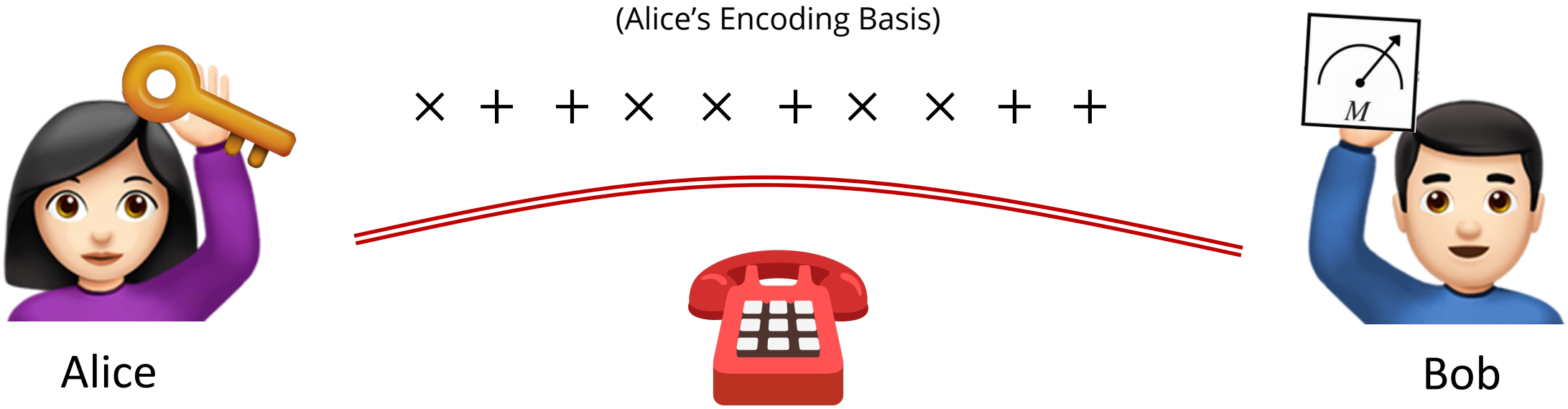
    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(6) CLASSICAL ANNOUNCE BASES

Alice announces which basis she used to encode each bit, via the classical channel.



THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(7) CLASSICAL ANNOUNCE BASES

Alice also announces a few of the classical bits of the key.

THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

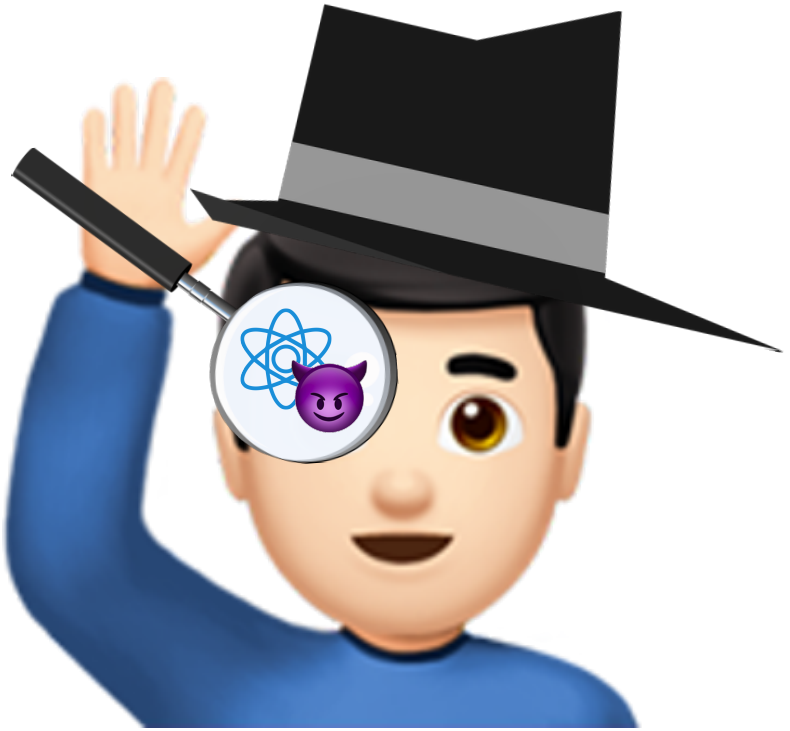
   -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

   -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

(8) ANALYSIS

Time for Bob to put on his detective hat! Using the following information, how can he detect whether on not Eve intercepted their key transmission?



Bob's Clues:

- His 10 measurement bases.
- Alice's 10 encoding bases.
- His 10 measured bit states.
- 4 of Alice's key bit states.

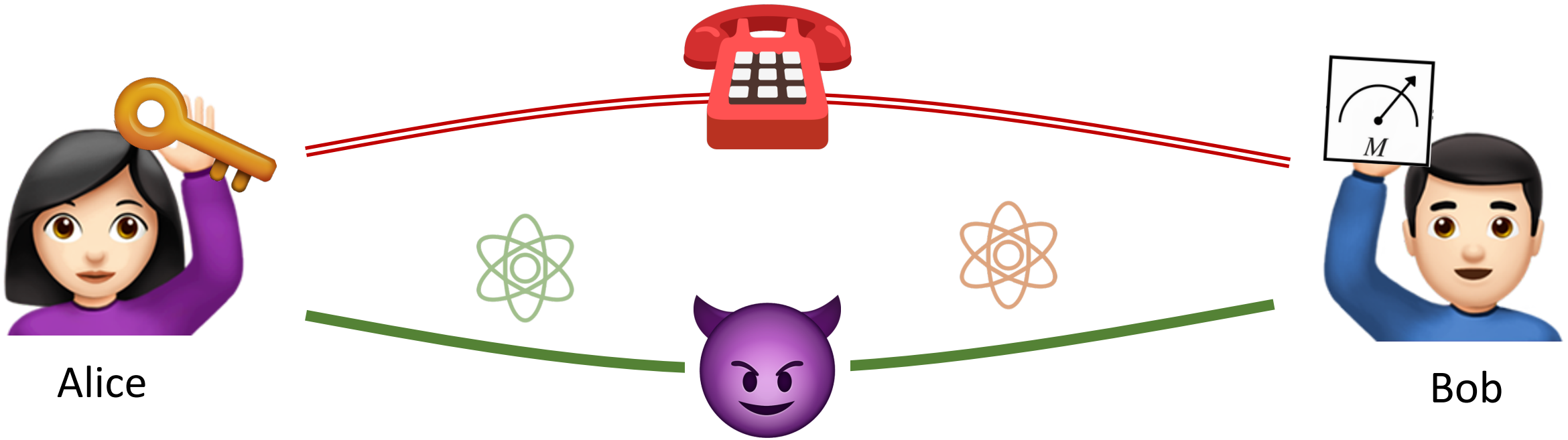
(8) ANALYSIS

What would Bob expect the first four bits to be if there was ***no eavesdropper***?

Alice's Encoding Bases:	×	+	+	×	×	+	×	×	+	+
Bob's Measurement Bases:	+	+	+	×	×	×	×	+	+	+
First 4 Key Bits:	0	1	0	1						
Bob's Expectation (No Eavesdropper):										

(8) ANALYSIS

Now, what would Eve do if she was eavesdropping, but didn't want to be discovered?



BB84 was designed to make this hard for Eve and detectable by Bob!!!

Eve will intercept the quantum state, measure it like Bob would, and ***try to recreate*** the state again to send to Bob.

(8) ANALYSIS

Now let's see what happens when Eve is eavesdropping...

First 4 Key Bits:	0	1	0	1
Alice's Encoding Bases:	×	+	+	×
Eve's Measurement Bases:	+	+	×	+
Eve's Measurement Outcomes:	0	1	1	0
Eve's Encoding Bases:	+	+	×	+
Bob's Measurement Bases:	+	+	+	×

Bob's Expectation (No Eve):

\- 1 0 1

What does Bob measure with Eve?

HELP BOB!

What are the different possible measurement outcomes when Eve has intercepted the message?

Eve's Measurement Outcomes:	0	1	1	0
Eve's Encoding Bases:	+	+	×	+
Bob's Measurement Bases:	+	+	+	×

(8) ANALYSIS

When Eve ***is not*** spying, Bob will measure the first 4 bits:

	-	1	0	1

When Eve ***is*** spying, Bob will measure the first 4 bits:

25%	0	1	0	1
25%	0	1	0	0
25%	0	1	1	0
25%	0	1	1	1

Meaning that 75% of the time Eve is eavesdropping, using the measurement and encoding bases + + × +,

Bob will measure a different bitstring than what he expects!

(8) ANALYSIS

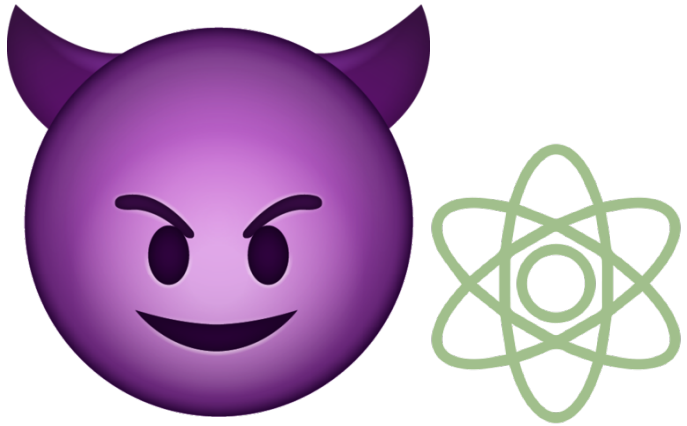
If Bob measured the expected bitstring, -101, either there was no eavesdropper or Eve got lucky!

What can Alice and Bob do to try and make sure Eve doesn't get lucky?

(8) ANALYSIS

If Bob thinks that ***Eve intercepted their message***, Alice and Bob need to:

throw everything away, find a new (more secure) quantum communication channel, and try again until Eve does not intercept their key



(8) ANALYSIS

If Bob thinks ***Eve did not intercept their message***, Alice and Bob can:

use all bits among the remaining 6, in which Alice and Bob chose the same measurement basis, as their key

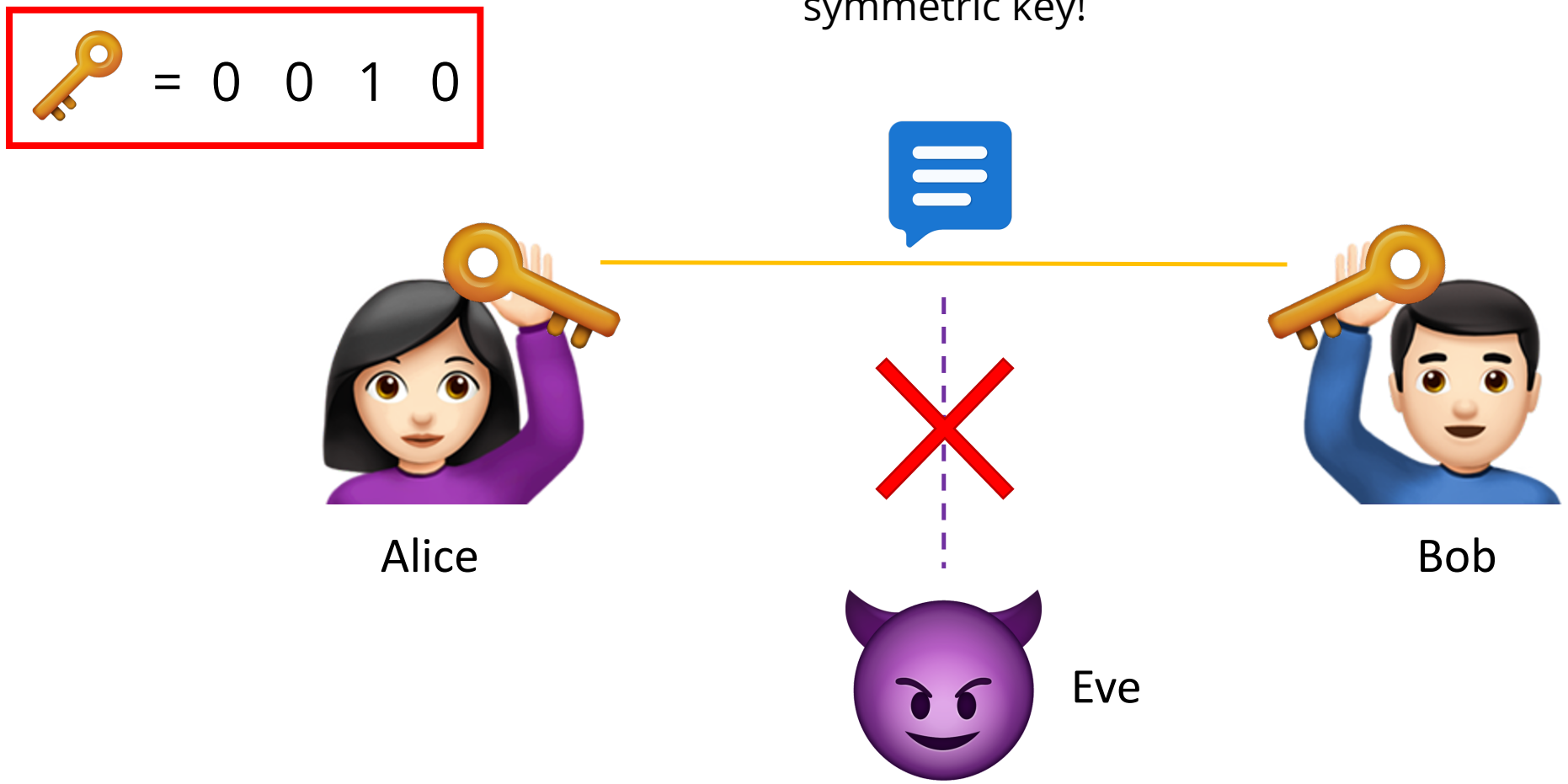
Alice's Key:	0	1	0	1	0	0	0	0	1	0
Alice's Encoding Bases:	×	+	+	×	×	+	×	×	+	+
Bob's Measurement Bases:	+	+	+	×	×	×	×	+	+	+

Final Symmetric Key:

Alice and Bob can now communicate securely in a classical communication channel encrypted with their symmetric key!

(8) ANALYSIS

Alice and Bob can now communicate securely in a classical communication channel encrypted with their symmetric key!



THE BB84 PROTOCOL

1. **SELECT ENCODING:** Alice randomly selects a basis (× or +) to encode each bit.
2. **SELECT MEASUREMENT:** Bob randomly selects a basis (× or +) to measure each bit.
3. **Q. ENCODE:** Alice creates the quantum states, encoded in the selected bases.
4. **Q. SEND:** Alice sends Bob the encoded states, via the quantum channel.
5. **Q. MEASURE:** Bob measures all the quantum states in his pre-selected measurement bases.
6. **C. ANNOUNCE BASIS:** Alice announces which basis she used to encode each bit, via the classical channel.
7. **C. REVEAL SOME BITS:** Alice reveals some of the bits she sent.
8. **ANALYSIS:** Bob performs analysis to determine if the message was intercepted by Eve.

    -> If so, Alice and Bob should move to a new quantum communication channel and try again; back to (1)

    -> If not, the key was securely transmitted!

Alice and Bob can now communicate via a channel encrypted using their quantum-distributed key!

BRACE YOURSELF...