# Quantum Communication and Cryptography

PHYS/CSCI 3090

Prof. Alexandra Kolla

Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith

Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html

# Come see us!

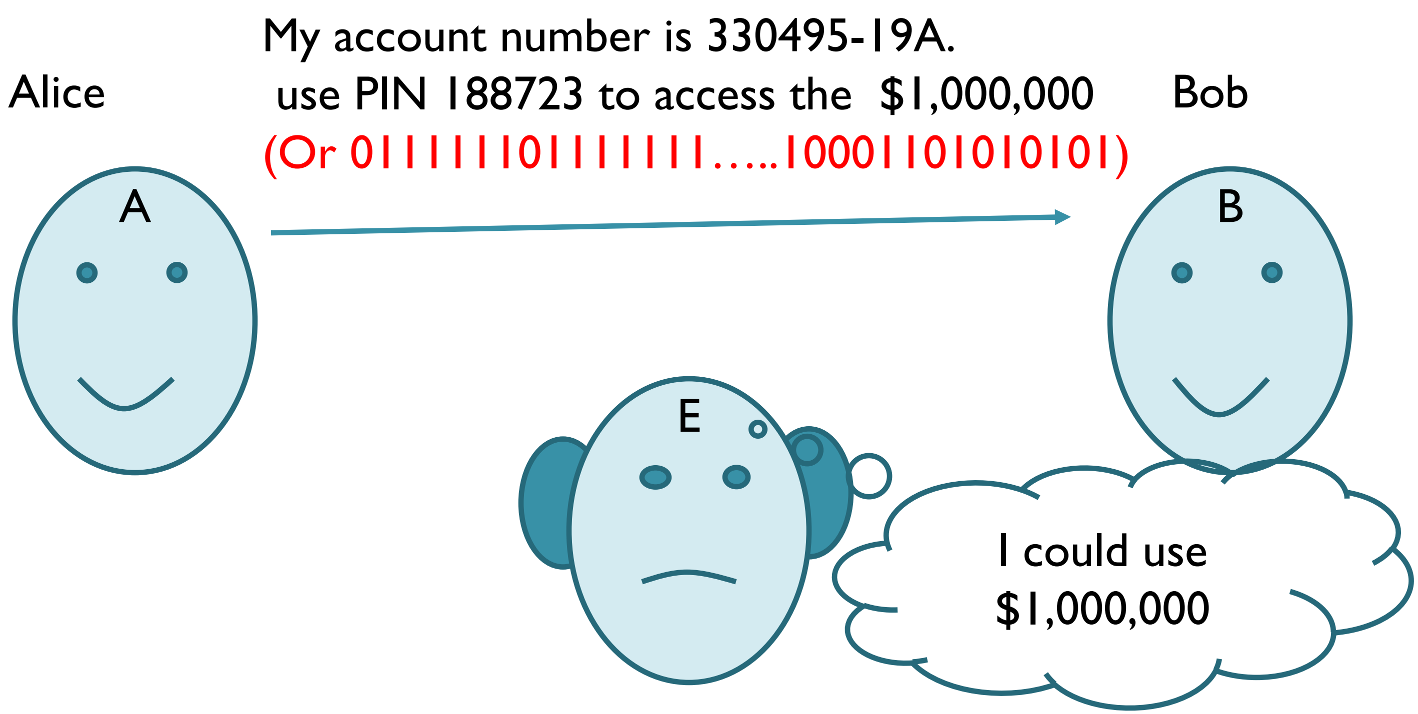
- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, JILA X317.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, DUANG2B90 (physics help room)
- Steven Kordonowy: Th 11am-12pm, ECAE 124.
- Matteo Wilczak: Wednesday, 1-2pm, DUANG2B90 (physics help room)

# New topic: few qubit protocols (Chapter 6)

- Looking at some simple protocols on just a few qubits.
- Not exactly computing, but more about communication (and also cryptography)

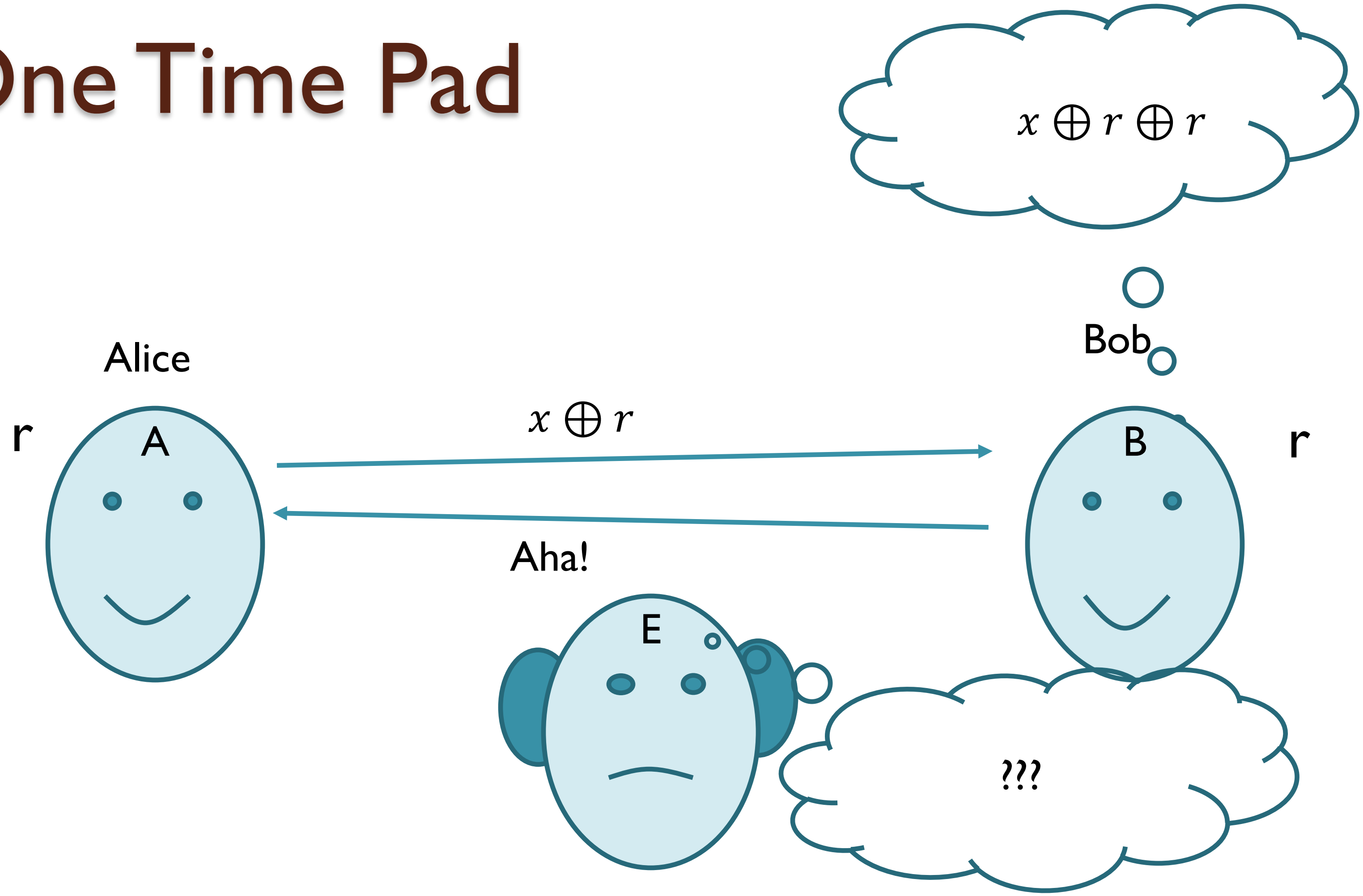
- Last class: started BB84 quantum key distribution protocol.

# Alice, Bob, and Eve




- Alice wants to send a secret message / binary string to Bob
- She cannot risk Eve learning it

# One Time Pad




- Alice wants to send a secret message / binary string
- She cannot risk Eve learning it
- If Alice XORS her message x with a random n-bit string,

then she sends a random message and eve cannot learn anything!

- If Bob knew r, he could decode x.
- How can they share a random string r, that Eve cannot find?

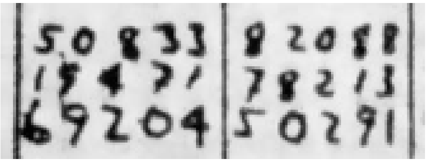
# One Time Pad: how to get one

- Make two copies of a bunch of random strings.
- Use a trusted courier to send the pad to the person you want to talk to
- Put it in a locked briefcase on the way.
- Use a trusted courier to send the key.
- But. What if the courier is a bad guy.

# One Time Pads

Actual Pad

Leo Marks,
Special Operations Executive



Message
Key
cryptogram

One time pad worksheet
Used by Che Guevara

One approach: everyone carries around a bunch of random bits.
One "key" for each person you need to talk to.

Not great:
1) you need lots of different pads.
2) someone can peek at your pad, then learn your messages. Have to guard the pad constantly!

# One Time Pad: how to get one

- Make two copies of a bunch of random strings.
- Use a trusted courier to send the pad to the person you want to talk to
- Put it in a locked briefcase on the way.
- Use a trusted courier to send the key.
- But. What if the courier is a bad guy.
- With BB84, you don’t have to trust anybody. Trust quantum mechanics instead!

# BB84 (Bennett-Brassard-1984)

- Alice sends Bob a long sequence of qubits randomly chosen to be in one of the four states:
- $|0\rangle, |1\rangle$ (type 1)
- $\mathrm{H}|0\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle), \mathrm{H}|1\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$

(type H)

- When Alice wants to send the bit 0, she randomly sends either

$|0\rangle$ or $\mathrm{H}|0\rangle$.

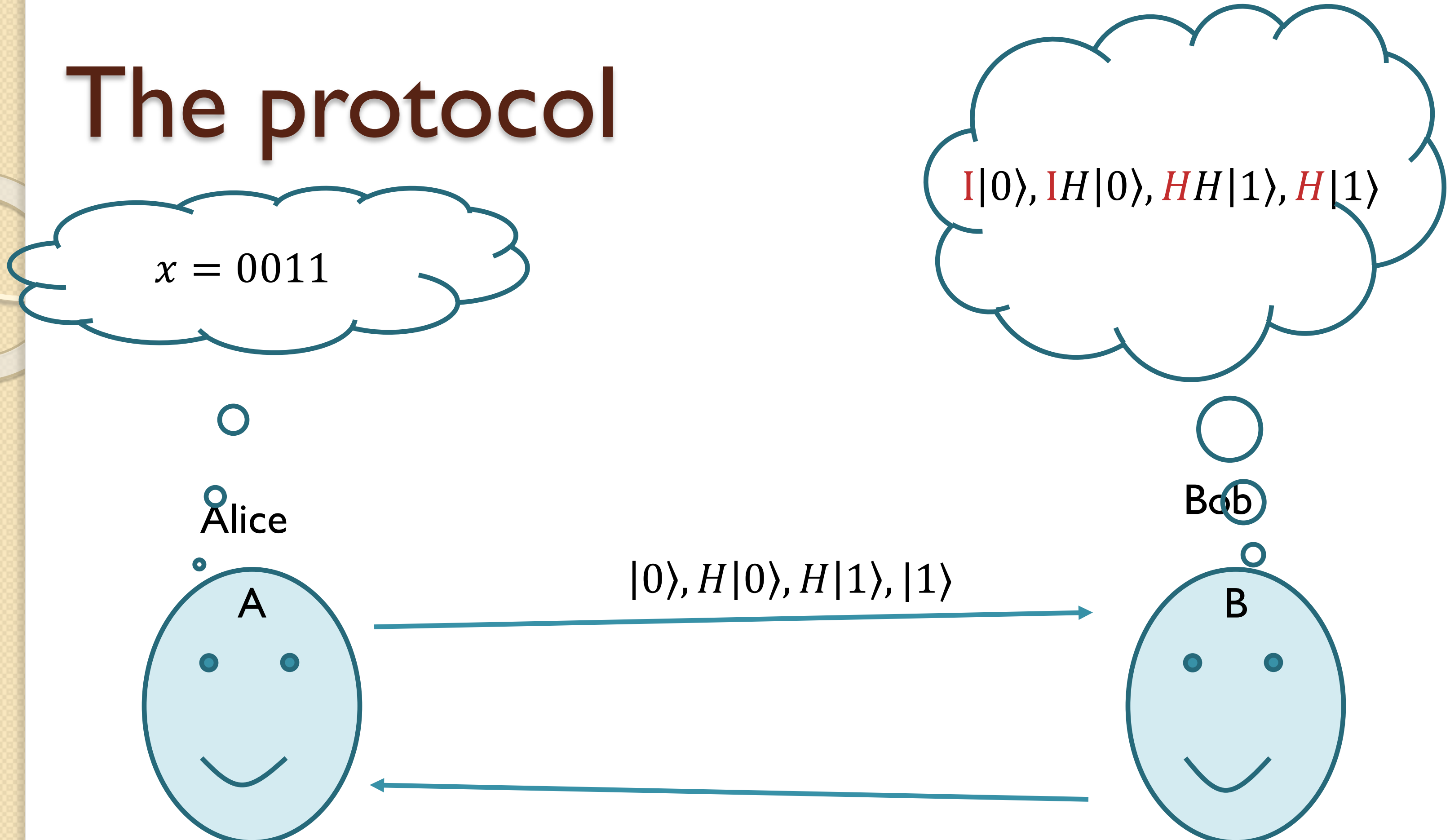
- When she wants to send the bit 1, she randomly sends

either $|1\rangle$ or $\mathrm{H}|1\rangle$.

- Bob, once he receives each qubit, he randomly decides

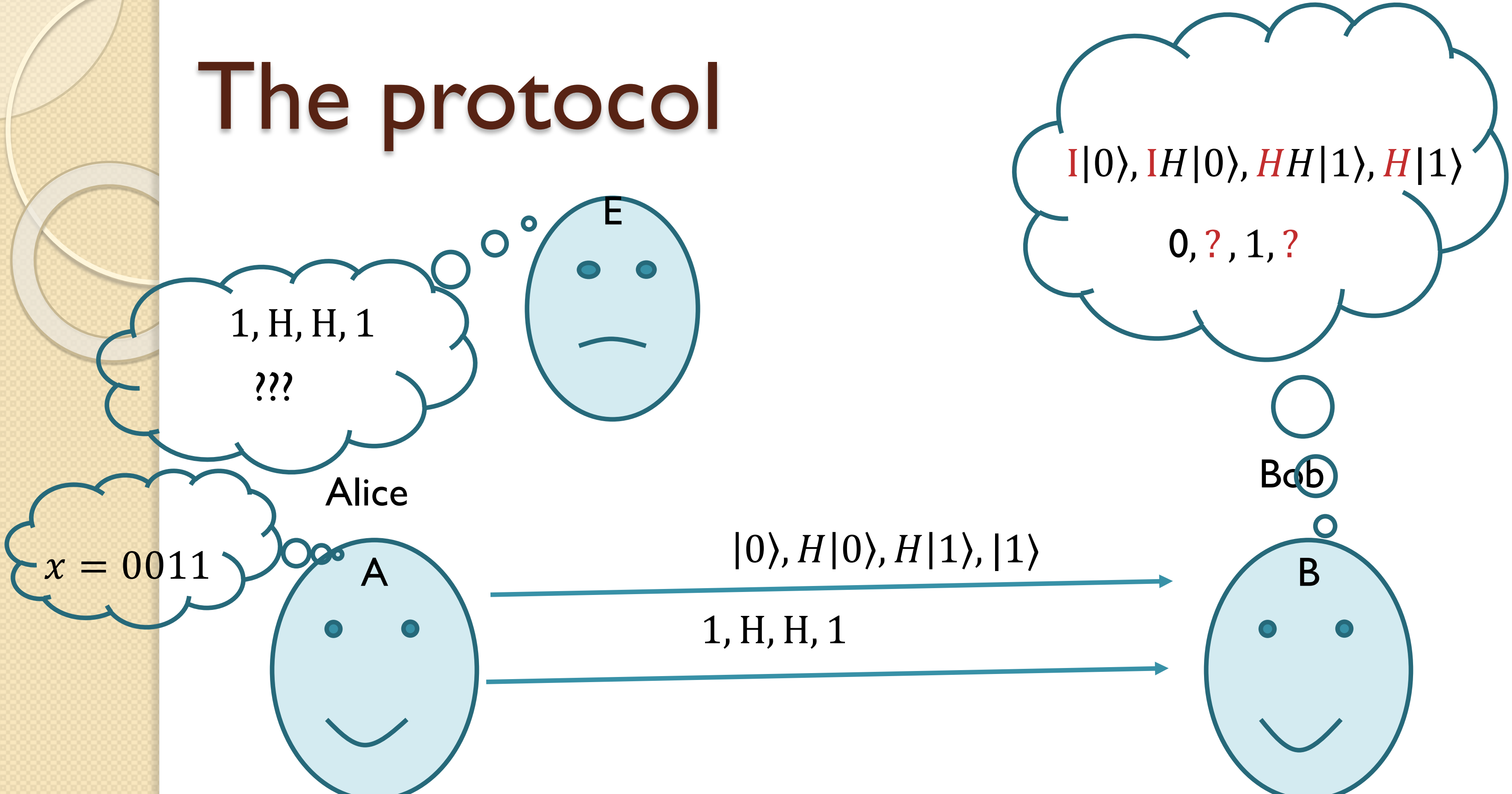
to apply either $I$ (type I measurement) or $\mathrm{H}$ (type H measurement) to the qubit and then measure in the standard basis.

# The protocol




- If both Alice and Bob chose type I or they both chose type H, then their respective bits agree after Bob measures.
- How do they know which bits agree?

# The protocol




- If both Alice and Bob chose type I or they both chose type H, then their respective bits agree after Bob measures.
- How do they know which bits agree?
- Alice sends Bob over an insecure channel, which qubits were type I and type H.
- She does not reveal if the bit was 0 or 1 to begin with.
- For those qubits that Alice's choice agrees with Bob's measurement, Bob learns the actual value of the original bit Alice wanted to send.
- They throw out the rest.

# A possible attack by Eve

- During transmission, Alice sends one of four states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$
- Eve wants to know which one is sent
- A natural attack is for Eve to pick a random basis and measure in that.
- Let's say Alice transmits in $\{|0\rangle, |1\rangle\}$, Eve Measures $\{|0\rangle, |1\rangle\}$, and Bob measures $\{|0\rangle, |1\rangle\}$.
- Eve and Bob both learn the bit. Not good!

# A possible attack by Eve

- During transmission, Alice sends one of four states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$
- Eve wants to know which one is sent
- A natural attack is for Eve to pick a random basis and measure in that.
- Let's say Alice transmits in $\{|0\rangle, |1\rangle\}$, Eve Measures $\{|+\rangle, |-\rangle\}$, and Bob measures $\{|0\rangle, |1\rangle\}$.
- What then?

# Concept Test

Alice transmits $|1\rangle$,
Eve Measures $\{|+\rangle, |-\rangle\}$
Bob measures $\{|0\rangle, |1\rangle\}$.

What is the probability Bob measures $|1\rangle$?

A) 0
B) 1
C) 0.5
D) 0.75

# Concept Test

Alice transmits $|1\rangle$,
Eve Measures $\{|+\rangle, |-\rangle\}$
Bob measures $\{|0\rangle, |1\rangle\}$.

What is the probability Bob measures $|1\rangle$?

A) 0
B) 1
C) 0.5
D) 0.75

Alice transmits $|1\rangle$,
Eve Measures $\{|+\rangle, |-\rangle\}$
Bob measures $\{|0\rangle, |1\rangle\}$.
What is the probability Bob measures $|1\rangle$?

# A possible attack by Eve

- During transmission, Alice sends one of four states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$
- Eve wants to know which one is sent
- A natural attack is for Eve to pick a random basis and measure in that.
- If she does this, it will introduce some disagreements in Alice's and Bob's bit strings.
- By sacrificing a small fraction of their key (publicly announcing the values and comparing) they can detect such meddling.
- If their keys are always in agreement, then they can have high confidence no eavesdropping has occurred.

# A perfect attack!

- What eve really wants is an operation that does this:
- $|0\rangle \rightarrow |0\rangle|0\rangle$
- $|1\rangle \rightarrow |1\rangle|1\rangle$
- $|+\rangle \rightarrow |+\rangle|+\rangle$
- $|-\rangle \rightarrow |-\rangle|-\rangle$

- If she had such a machine, she could learn everything about Alice's and Bob's key.

# A perfect attack!

- What eve really wants is unitary that does this:
- $|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$
- $|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$
- $|+\rangle|0\rangle \rightarrow |+\rangle|+\rangle$
- $|-\rangle|0\rangle \rightarrow |-\rangle|-\rangle$

- If she had such a machine, she could learn everything about Alice's and Bob's key. Just wait until Alice announces the basis she used, and then measure in that basis!

# Clicker Question

- Suppose there was a unitary that did this:
- $|0\rangle|0\rangle \to |0\rangle|0\rangle$
- $|1\rangle|0\rangle \to |1\rangle|1\rangle$
- $|+\rangle|0\rangle \to |+\rangle|+\rangle$
- $|-\rangle|0\rangle \to |-\rangle|-\rangle$

It would

A) Preserve inner products
B) Violate state normalization
C) Not be a unitary
D) Violate causality

# Clicker Question

- Suppose there was a unitary that did this:
- $|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$
- $|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$
- $|+\rangle|0\rangle \rightarrow |+\rangle|+\rangle$
- $|-\rangle|0\rangle \rightarrow |-\rangle|-\rangle$

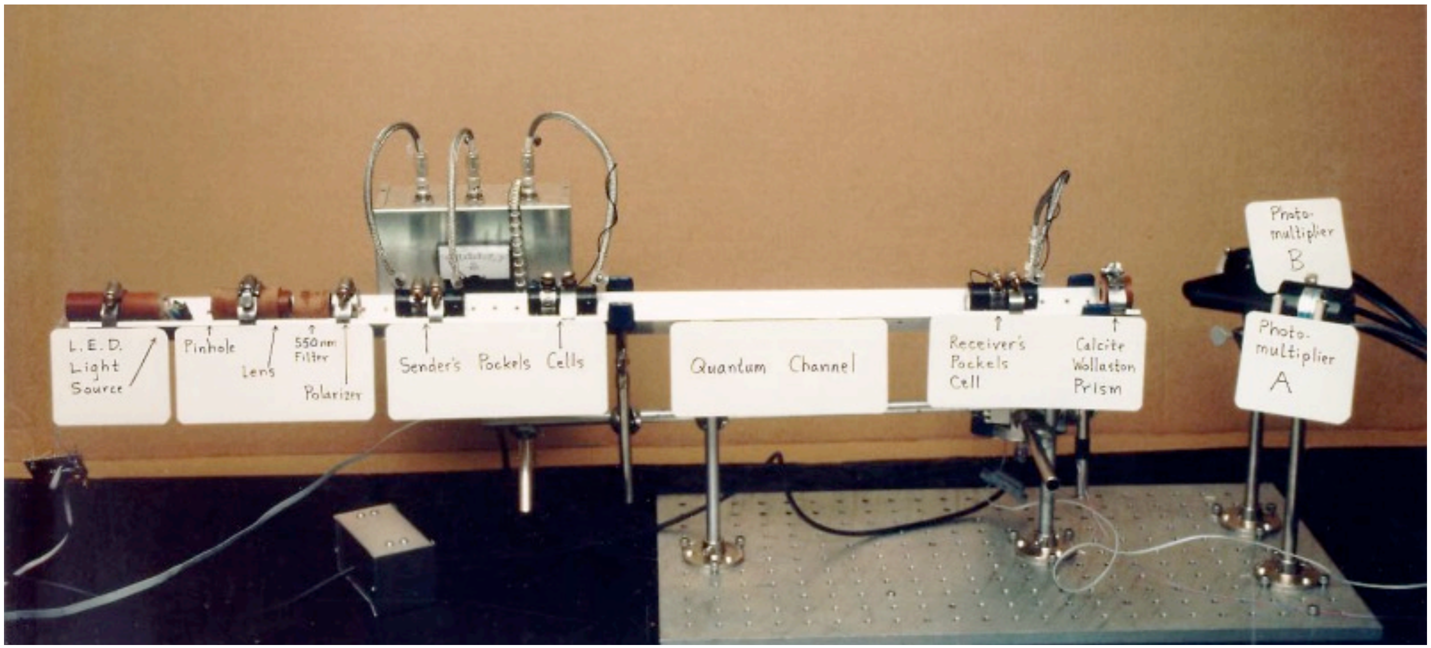
It would

A) Preserve inner products
B) Violate state normalization
C) Not be a unitary
D) Violate causality

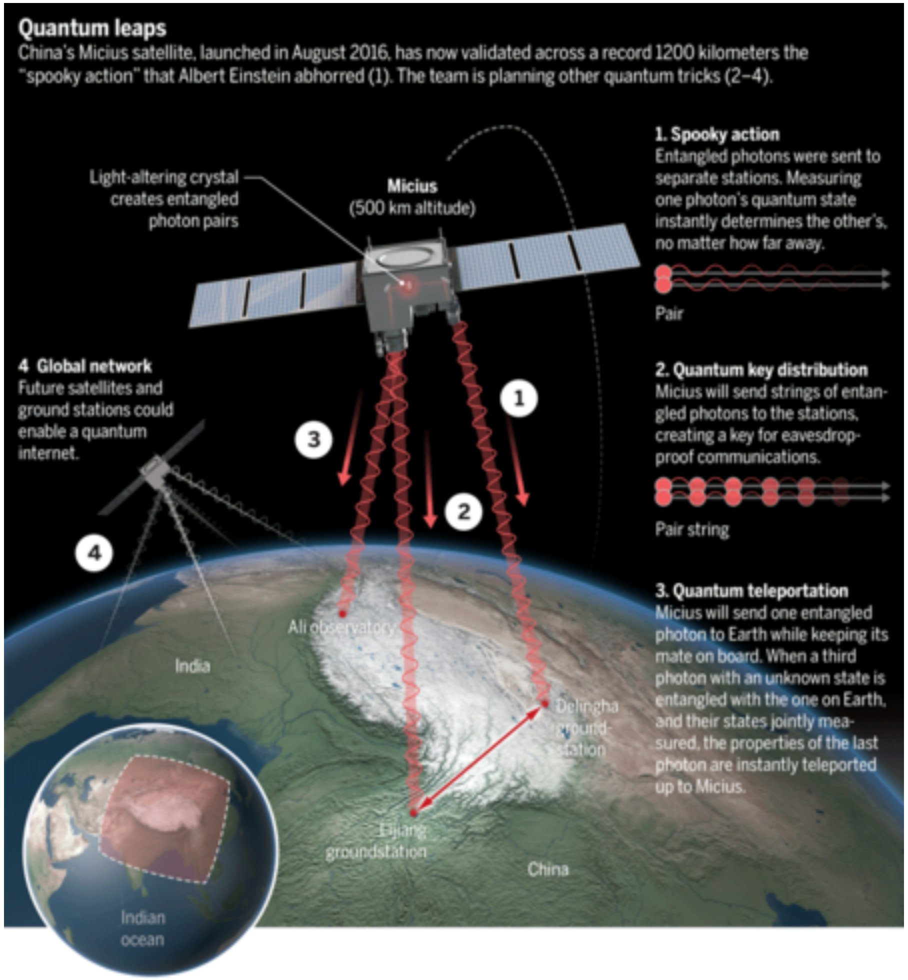
# Information gain/disturbance tradeoff

- This "perfect attack" is unphysical---it can't be implemented by unitary + measurements
- This is basically a consequence of the no-cloning theorem---you can't make copies of an unknown quantum state
- There's a more general phenomenon: if you do an operation that extracts even a little information about the state, it **must** disturb the state.
- In BB84, any such disturbance can be detected by Alice and Bob.
- Fancier analysis lets Alice and Bob figure out how much information about the key is leaked based on how much noise they observe.
- If it's not too much leaked, they can fix it up to be totally secure (hashing/privacy amplification)
- This fixing up is important because real systems will have noise, and would still like to be able to generate key.
- For us for now, just know that alice and bob can detect any attempt at eavesdropping, and can't be fooled into thinking they have secure key when they don't.

# BB84 aparatus



# QKD in space


Quantum leaps
China's Micius satellite, launched in August 2016, has now validated across a record 1200 kilometers the "spooky action" that Albert Einstein abhorred (1). The team is planning other quantum tricks (2–4).
Light-altering crystal creates entangled photon pairs
Micius (500 km altitude)
1. Spooky action
Entangled photons were sent to separate stations. Measuring one photon's quantum state instantly determines the other's, no matter how far away.
Pair
2. Quantum key distribution
Micius will send strings of entangled photons to the stations, creating a key for eavesdrop-proof communications.
Pair string
3. Quantum teleportation
Micius will send one entangled photon to Earth while keeping its mate on board. When a third photon with an unknown state is entangled with the one on Earth, and their states jointly measured, the properties of the last photon are instantly teleported up to Micius.
4 Global network
Future satellites and ground stations could enable a quantum internet.
1
2
3
4
Ali observatory
India
Delingha ground-station
Lijiang groundstation
China
Indian ocean

# What we’ve learned

- A one-time pad lets Alice and Bob communicate securely even if Eve listens in.
- They cannot do this remotely with classical signals
- They CAN do this remotely with quantum signals.

# Next Class

- More Alice and Bob
- Dense Coding
- Please read 6.4
- Note: we are skipping 6.3 for now.

# Problem Set

- New problem set will be on canvas this afternoon.
- It may not be on the course website till tomorrow.

# Dense Coding