Quantum Communication and Cryprography

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)

The class so Far

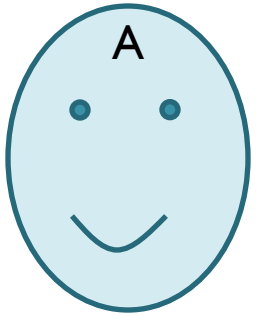
- We studied the basic elements of quantum computing: qubits, quantum states, measurements
- We used these to see some cool algorithms: Deutsch, Bernstein Vazirani, Simon's algorithm.
- These show that there are things that quantum computers can do easily that classical computers find hard.

Today

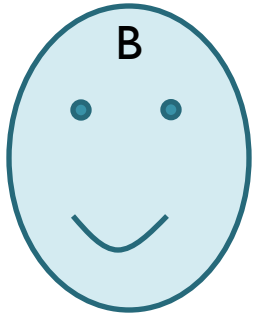
- We will start looking at some simple protocols one just a few qubits.
- These are not exactly computing, but more about communication (and also cryptography)

Introducing Alice and Bob

Alice

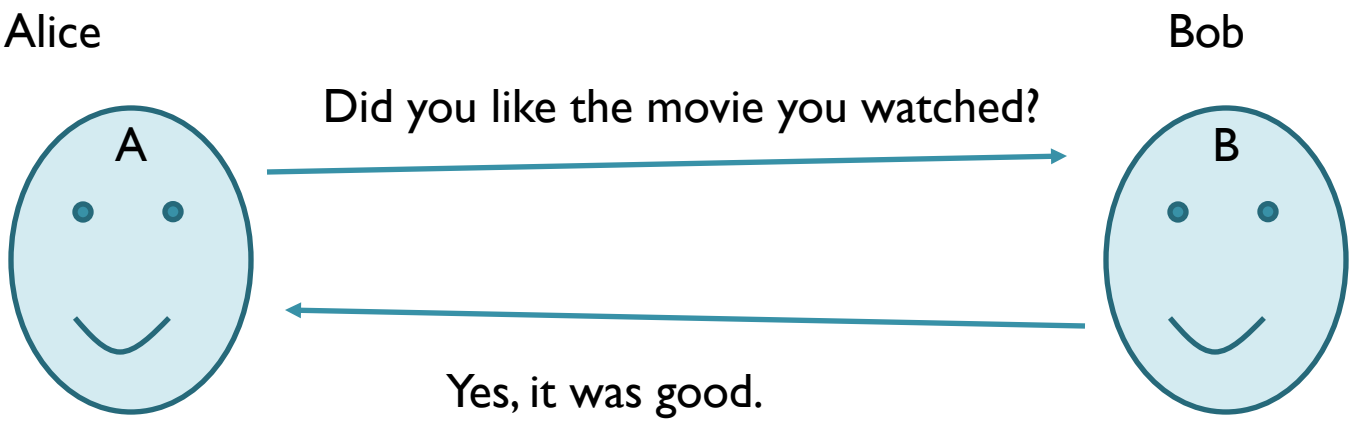


Bob



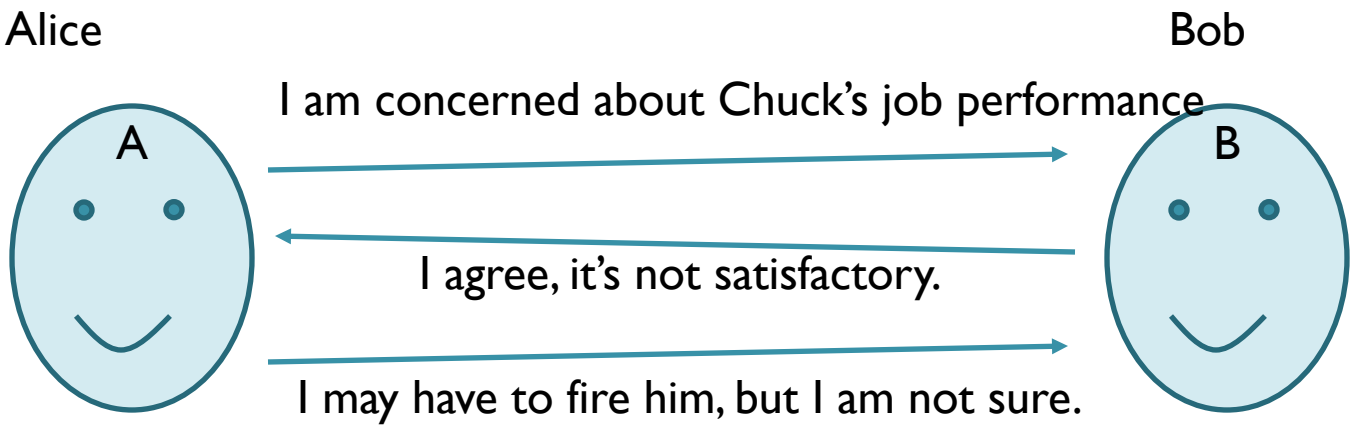
Alice and Bob live in different places.
But they can talk to each other over the phone.
They can also send a few qubits back and forth to each other over the quantum phone.
This chapter is about how sending qubits can be useful.

Introducing Alice and Bob



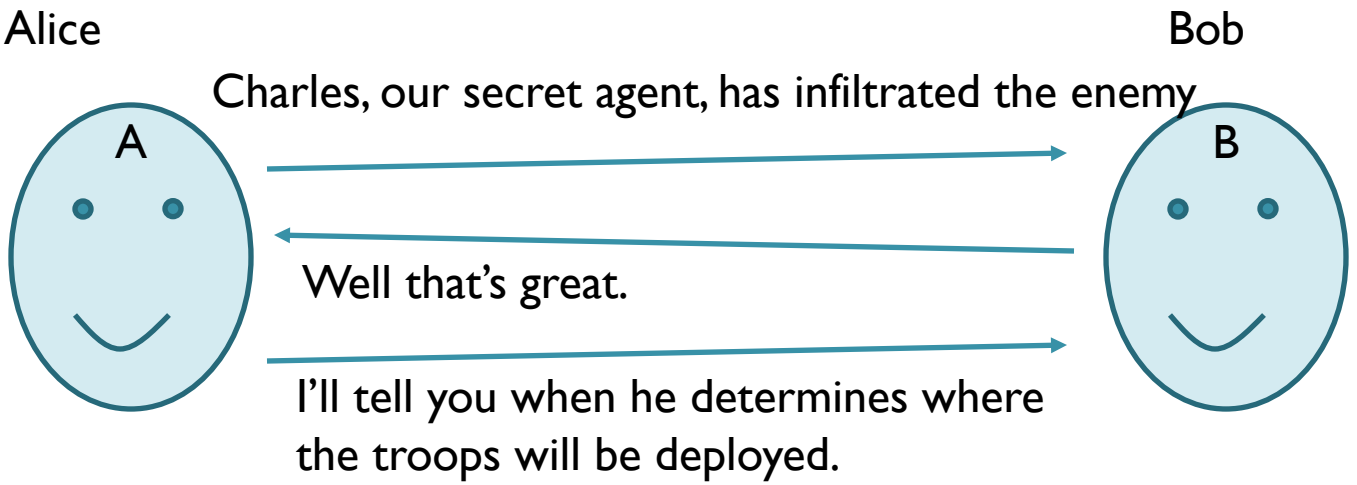
Alice and Bob live in different places.
But they can talk to each other over the phone.
They can also send a few qubits back and forth to each other over the quantum phone.

Introducing Alice and Bob



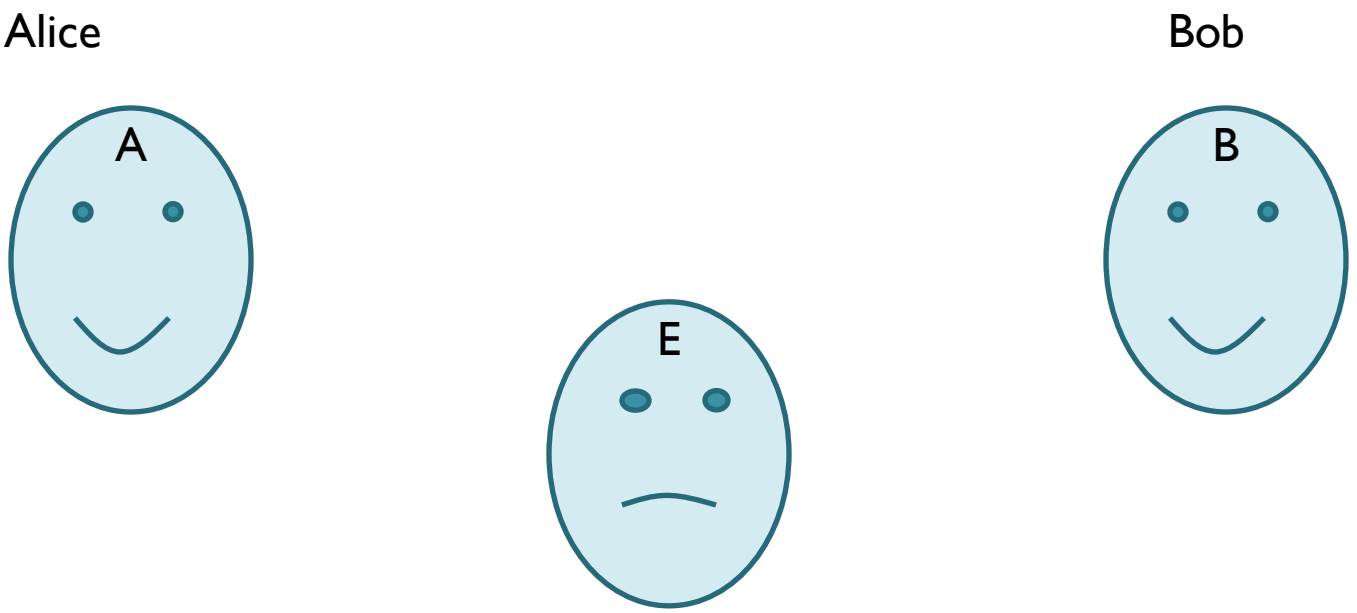
Sometimes Alice and Bob discuss sensitive topics.
They would not like their conversations to become public.

Introducing Alice and Bob



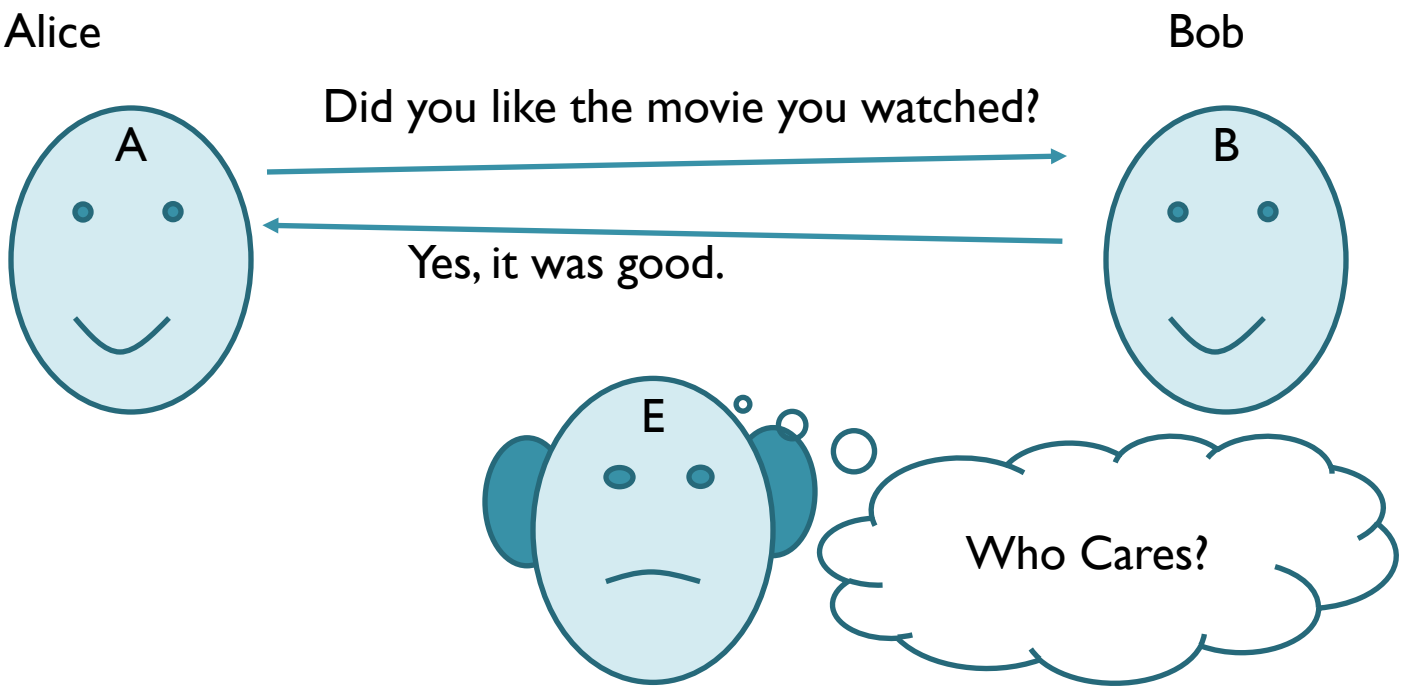
Sometimes Alice and Bob discuss **very** sensitive topics.
It could be dangerous (e.g., for Charles) if their conversations became public.

Introducing Eve



Eve is a powerful eavesdropper. She can listen in to any telephone call.

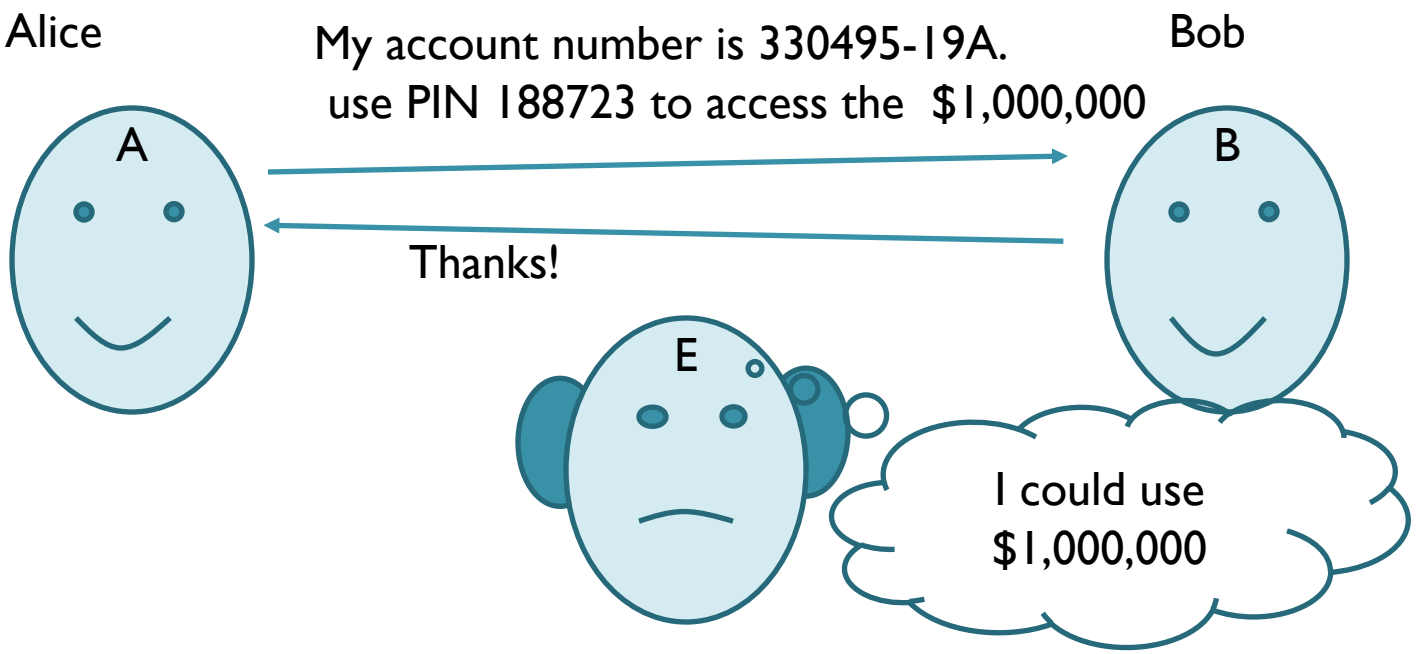
Introducing Eve



Eve is a powerful eavesdropper. She can listen in to any telephone call.

Sometimes this is no big deal.

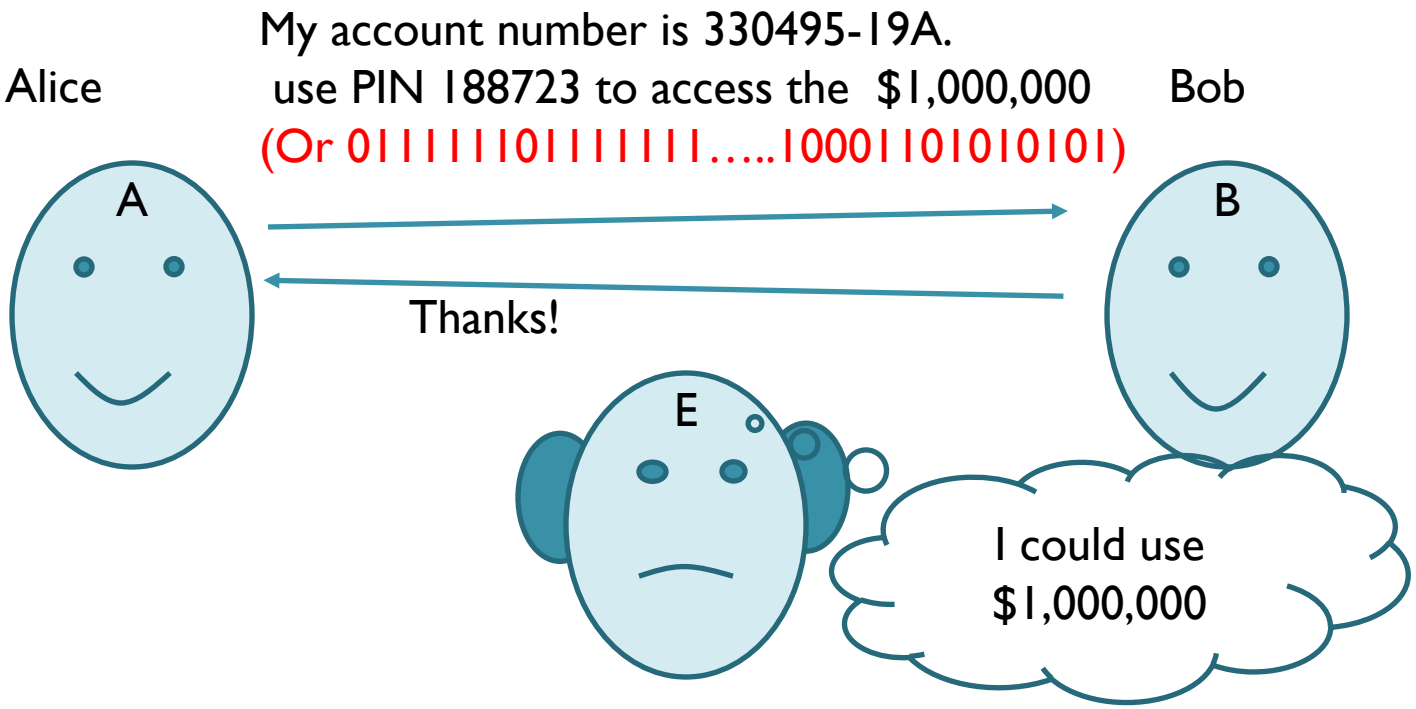
Introducing Eve



Eve is a powerful eavesdropper. She can listen in to any telephone call.

Other times it is a big problem.

Introducing Eve



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

Random binary string

Assume x is a n-bit string (Alice's message), and r is a uniformly randomly chosen n-bit string. Let $y = x \oplus r$. If Eve learns y, what information can she get about x?

A) She can learn the whole bit string x

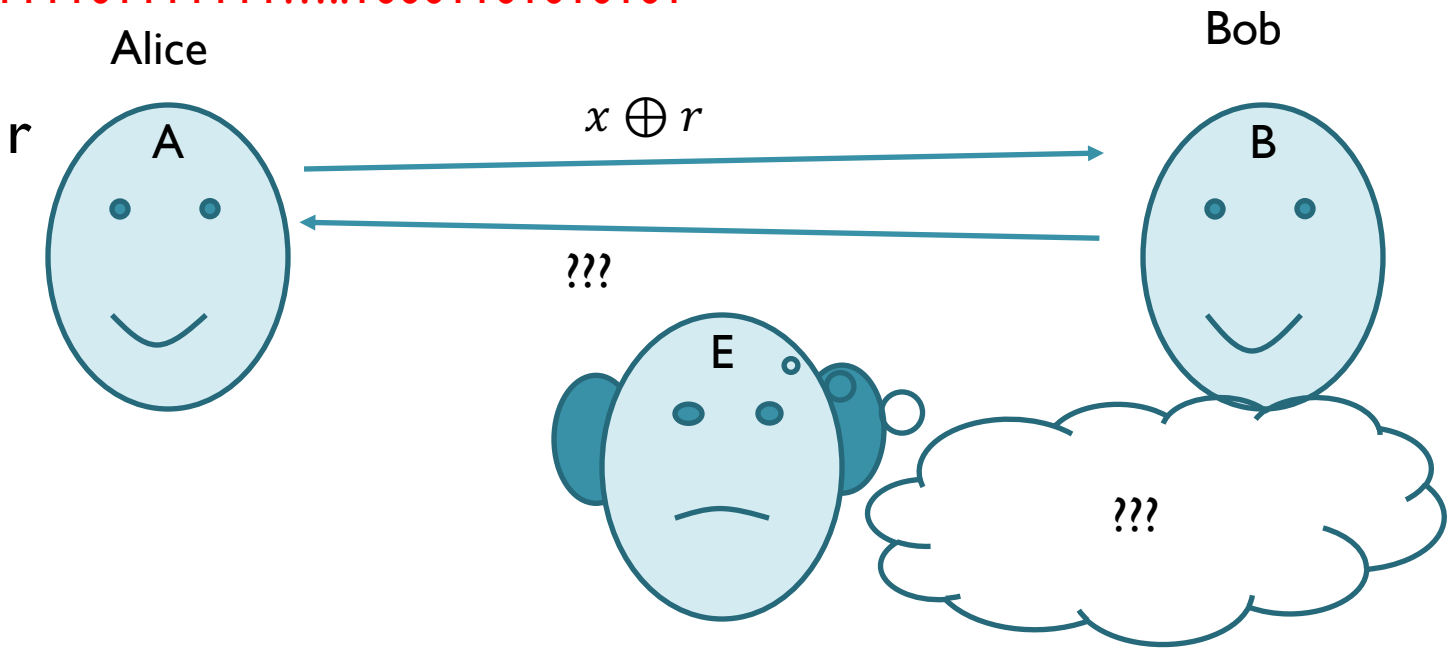
B)No information whatsoever

C) She can learn the first bit of x

D) It depends on what x is

Random strings

My account number is 330495-19A.
use PIN 188723 to access the $1,000,000
x= 0111111011111111…..1000110101010101



- 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!

- Bob can also not learn anything though :(

XOR for days

Assume x and r are a n-bit strings. What is $y = x \oplus r \oplus r$?

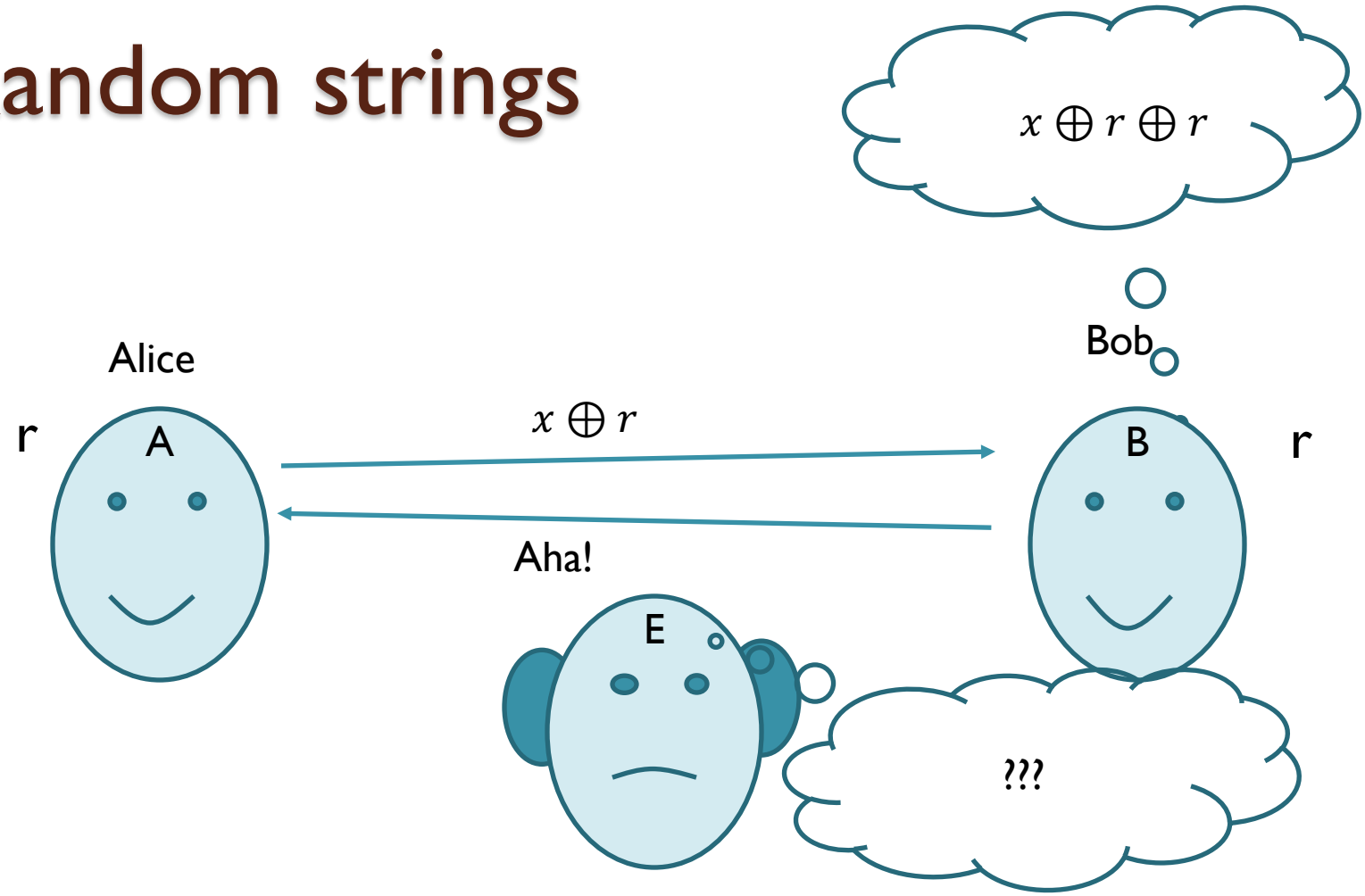
A) r

B) x

C) A random n-bit string

D) the all-0 string

Random strings



- 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

- Clasically, the problem seems the same as exchanging the secret message safely.
- Quantumly, Alice and Bob can safely share a random string r and detect if any eavesdropping happens.
- BB84 Protocol (Bennet-Brassard)

The Protocol

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

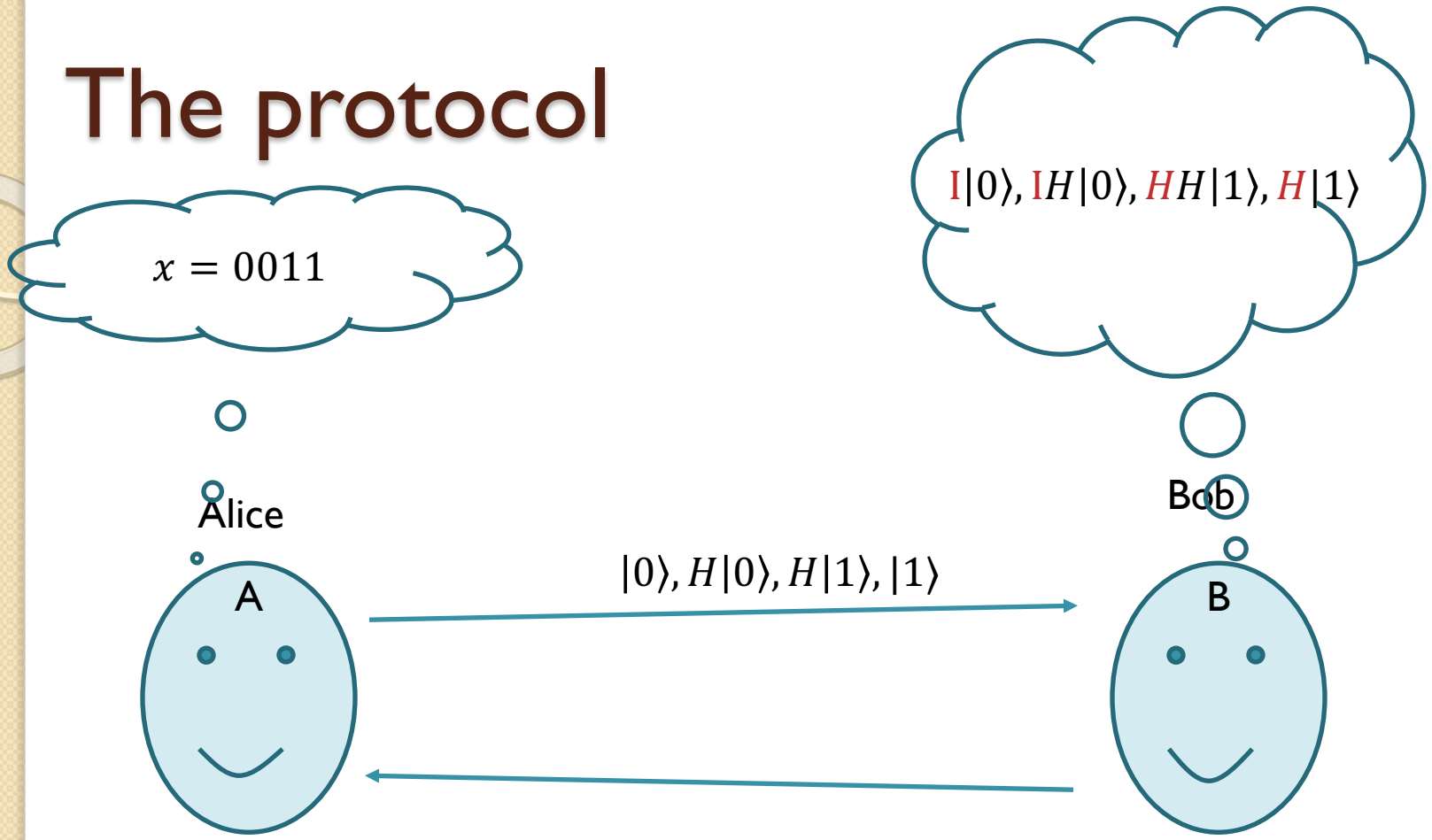
- When she wants to send the bit 1, she randomly sends

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

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

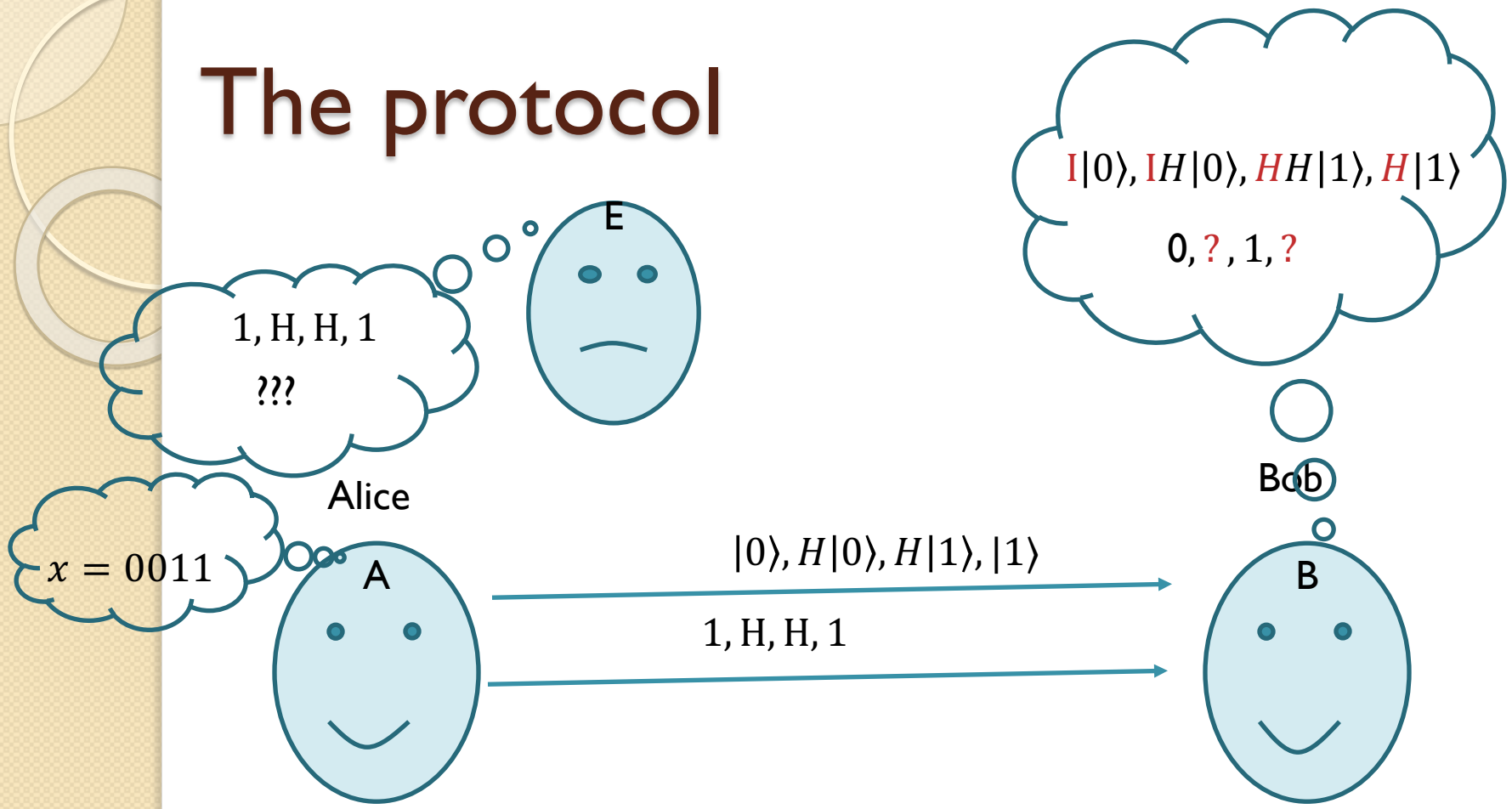
to apply either I (type I measurement) or H (type H measurement) to the qubit and then measure in the standard basis.

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.

How many bits?

Assume Alice wants to send k random bits, so she sends k qubits to Bob and they follow the protocol described above.
For how many of those k bits (in expectation) does Bob learn the actual value of Alice's original choice of bit she wanted to send?

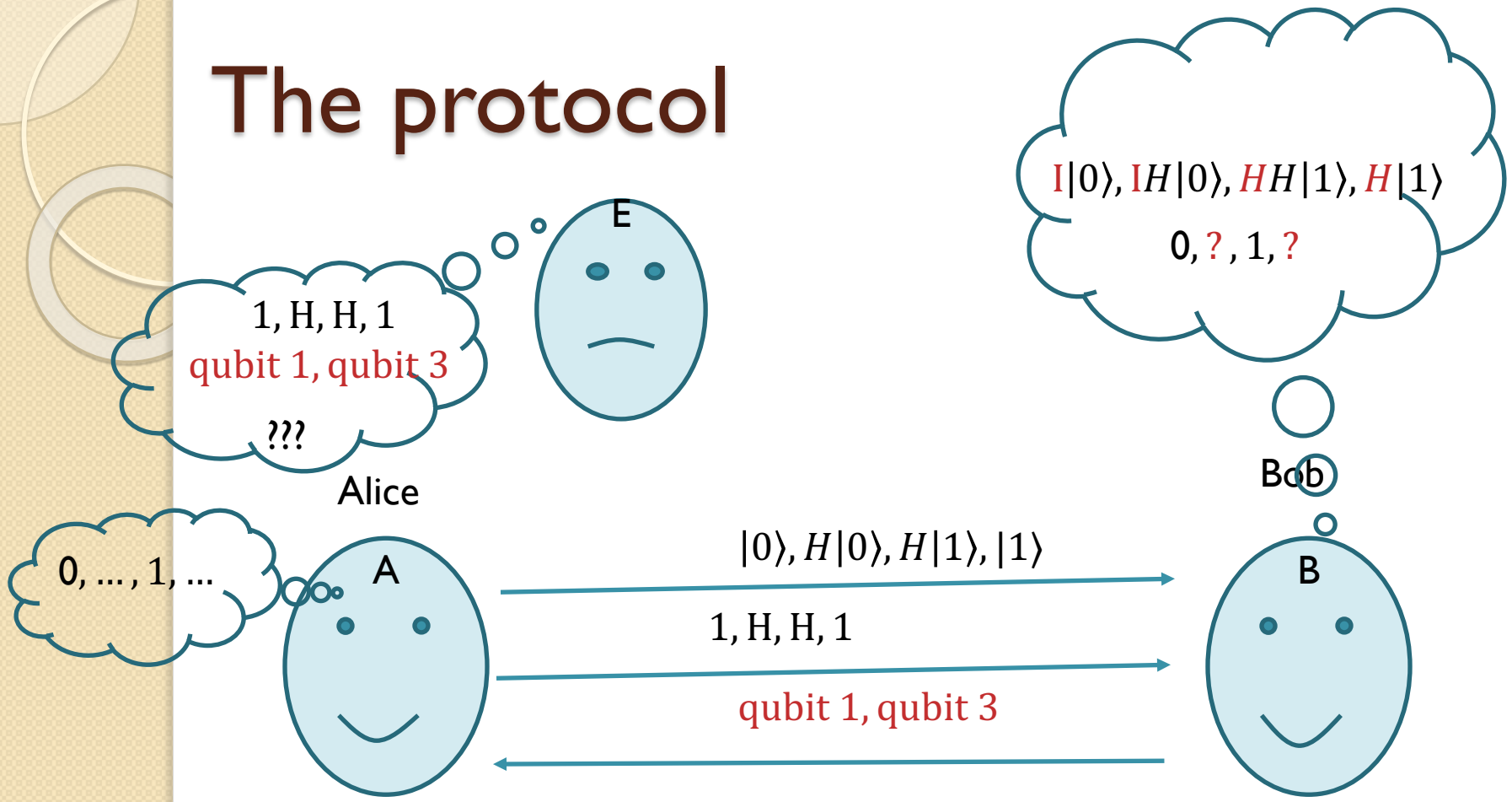
A) k

B) $\frac{k}{2}$

C) 0

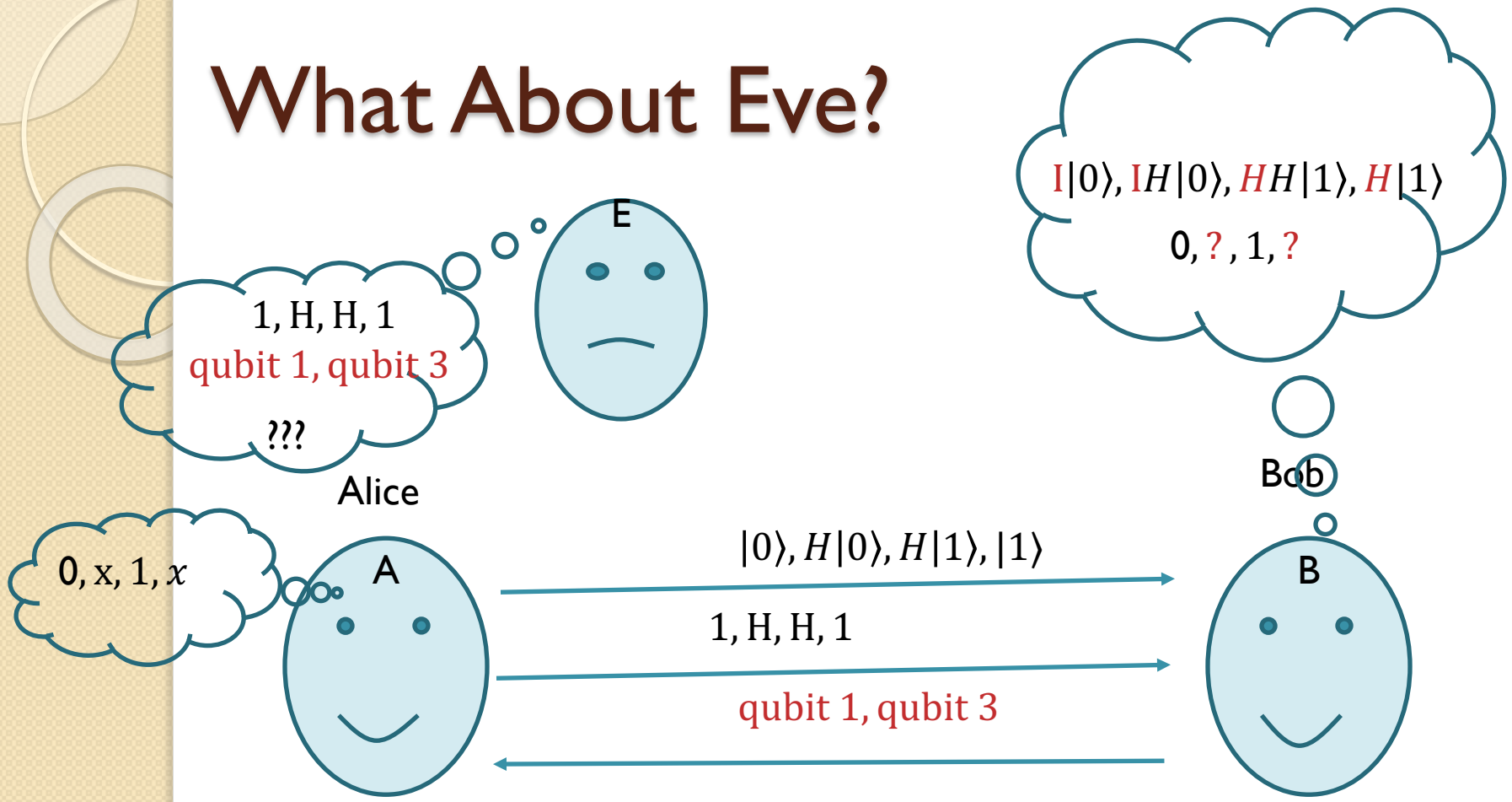
D) $\frac{k}{4}$

The protocol



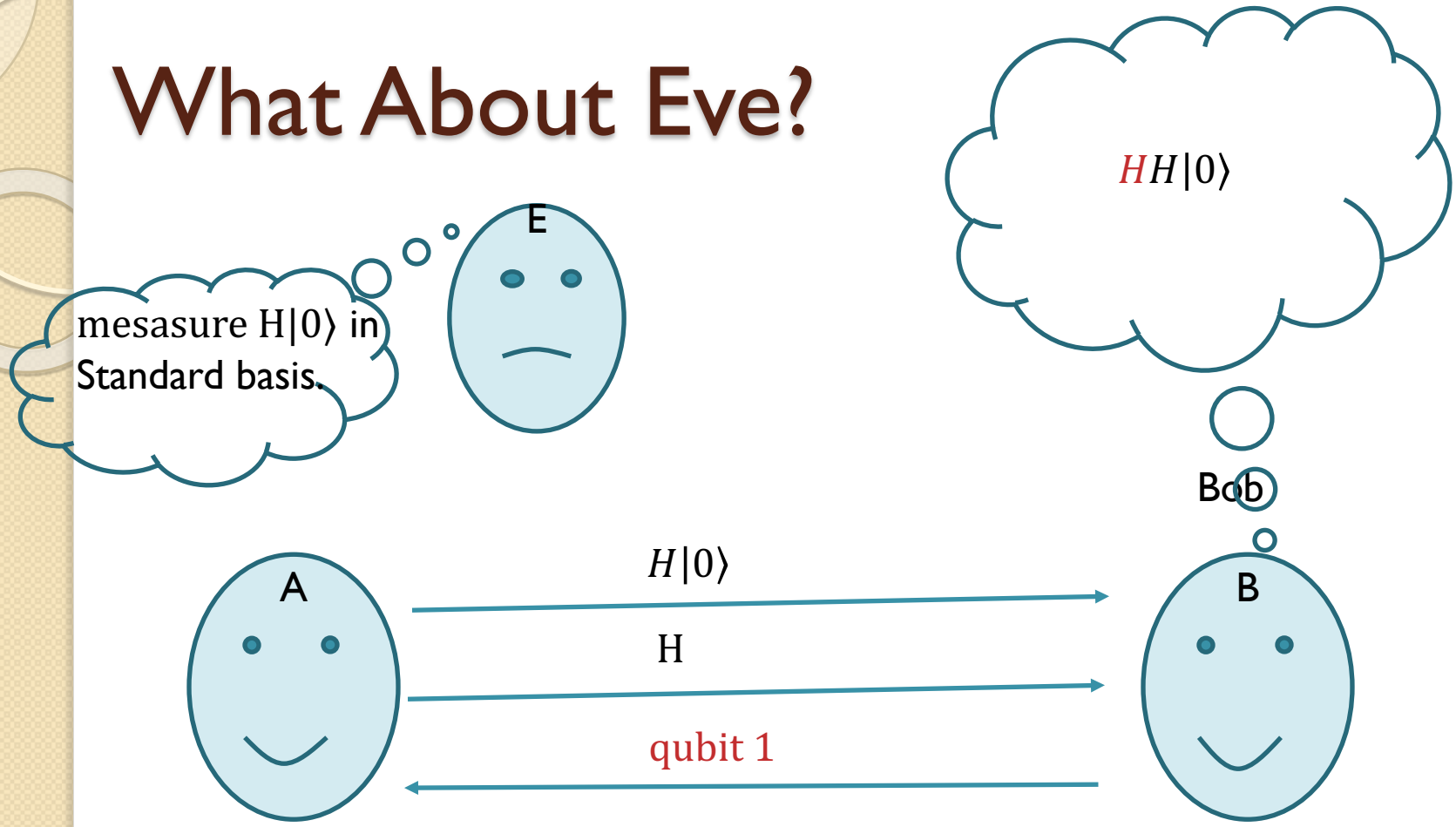
- If both Alice and Bob chose type I or they both chose type H, then their respective bits agree after Bob measures.
- How do they know which bits agree?
- Alice sends Bob over an insecure channel, which qubits were type I and type H.
- Bob tells Alice over an insecure channel for which qubits did their choices agree.
- Those (approximately half) of the bits are identical random bits between Alice and Bob, and they discard the rest. One time codepad!

What About Eve?



- The reason Alice randomly varies the type (I,H) of qubit she sends to Bob is to provide security against Eve.
- If, say Alice and Bob agreed that all qubits will be type-I, and Eve learned this, she could directly measure in the standard basis without affecting the state of the qubit, proceed to send it to Bob, and thus learn the random string as well undetected.
- Nothing in the protocol will give Bob a clue that Eve was listening.

What About Eve?



- With BB84, the best Eve can do is, like Bob, to make random type I or type H measurements.
- This reveals her presence.
- For the example of 1-qubit above, Alice and Bob are supposed to have identical bits.
- If Eve randomly measures, Bob will get $|0\rangle$ only half the time.
- They can check that by sacrificing some of the supposedly identical random bits.