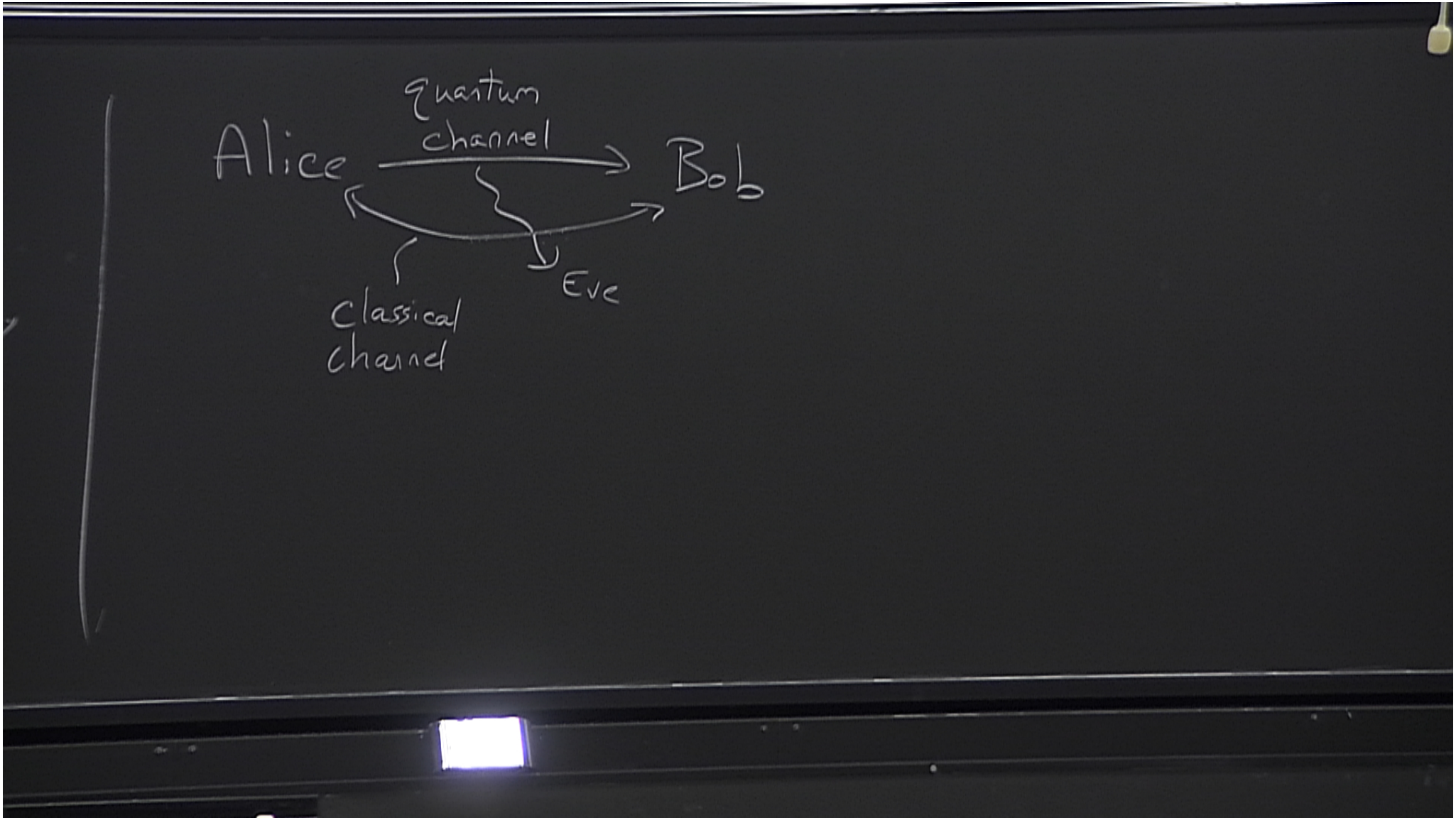
Title: Quantum Information (Review) - Lecture 14

Date: Mar 02, 2012 10:15 AM

URL: http://www.pirsa.org/12030001

Abstract:


Quantum
channel
Alice
Bob
Eve
Classical
channel

BB84

① Alice generates N random bit pairs (a_i, r_i)

② Alice prepares qubits determined by each pair & sends the qubits to Bob

a_i	r_i	state
0	0	$\|0\rangle$
0	1	$\|1\rangle$

a_i	r_i	state
1	0	$\|+\rangle$
1	1	$\|-\rangle$

BB84

① Alice generates N random bit pairs (a_i, r_i)

② Alice prepares qubits determined by each pair & sends the qubits to Bob

a_i	r_i	state
0	0	$\|0\rangle$
0	1	$\|1\rangle$

a_i	r_i	state
1	0	$\|+\rangle$
1	1	$\|-\rangle$

③ Bob chooses N random bases b_i & measures qubit i in basis b_i, getting result s_i

BB84

① Alice generates N random bit pairs (a_i, r_i)

② Alice prepares qubits determined by each pair & sends the qubits to Bob

a_i	r_i	state
0	0	$\|0\rangle$
0	1	$\|1\rangle$

a_i	r_i	state
1	0	$\|+\rangle$
1	1	$\|-\rangle$

③ Bob chooses N random bases b_i & measures qubit i in basis b_i, getting result s_i

④ Alice & Bob announce a_i & b_i over classical channel (but <u>not</u> r_i & s_i).

If $a_i = b_i$, keep bit i;

If $a_i \neq b_i$, throw away bit i;

Have about $\sim N/2$ bits left.

0	|	|1⟩	|	|1→⟩

Have about 1/2 bits left.

Suppose Eve measures qubits as they are sent.

E.g.: She might choose a basis & measure in that basis, then send state on to Bob

But Eve might measure in wrong basis

If Alice sends |0⟩, but Eve chooses |±⟩ basis Eve gets |+⟩

But Eve might measure in wrong basis

If Alice sends $|0\rangle$, but Eve chooses $|\pm\rangle$ basis Eve gets $|+\rangle$, sends that to Bob. If Bob measures in $|0\rangle/|1\rangle$ basis, Bob's outcome is random & is wrong 50% of the time

Eve's attempt to learn about the key introduces errors.

(3) Bob chooses N random bases b_i & measures qubit i

(5) Alice & Bob choose a rando

is wrong 50% of the time

③ Bob chooses N random bases b_i & measures qubit i in basis b_i, getting result s_i

④ Alice & Bob announce a_i & b_i over classical channel (but not r_i & s_i).

If $a_i = b_i$, keep bit i;

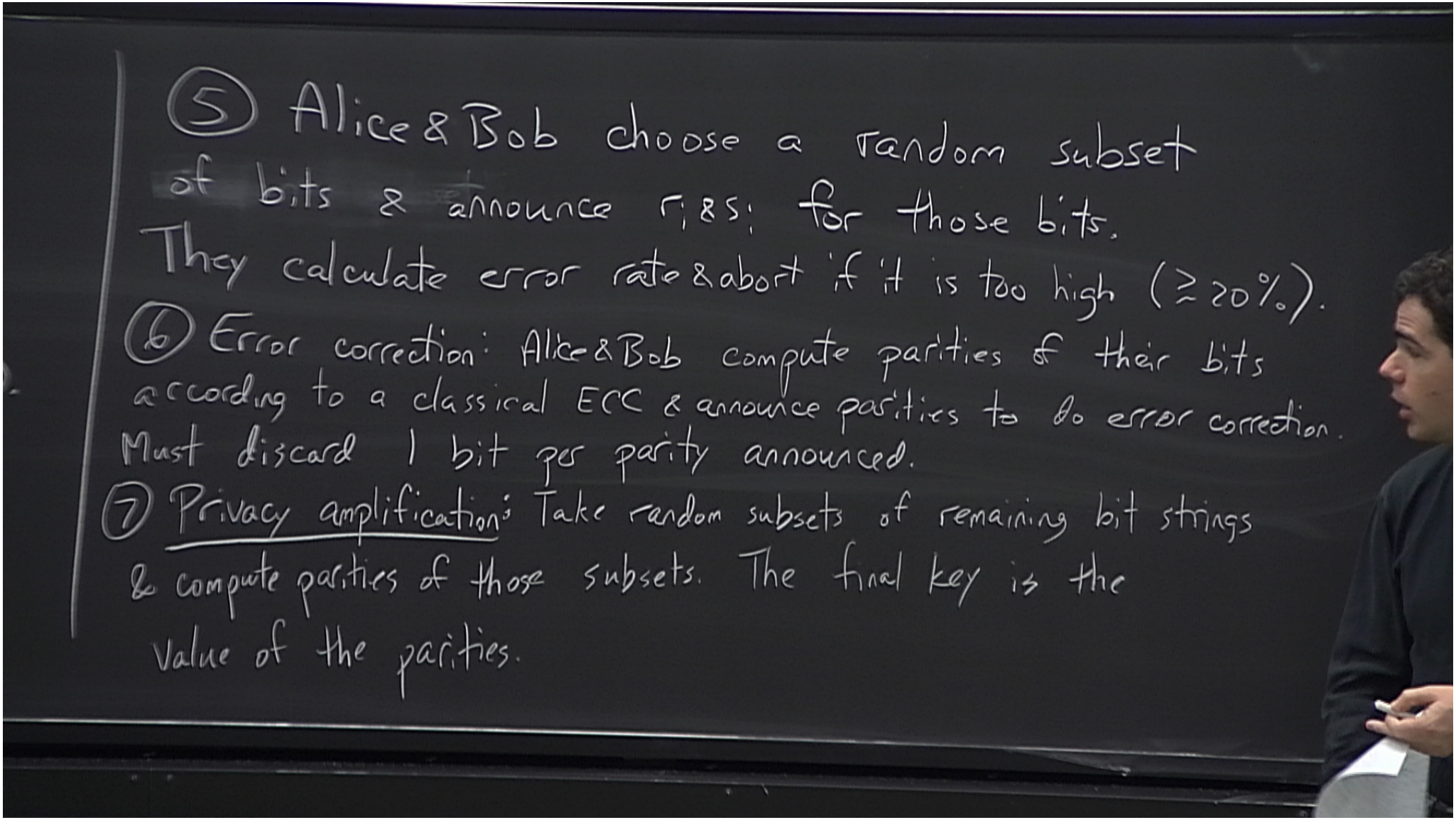
If $a_i \neq b_i$, throw away bit i;

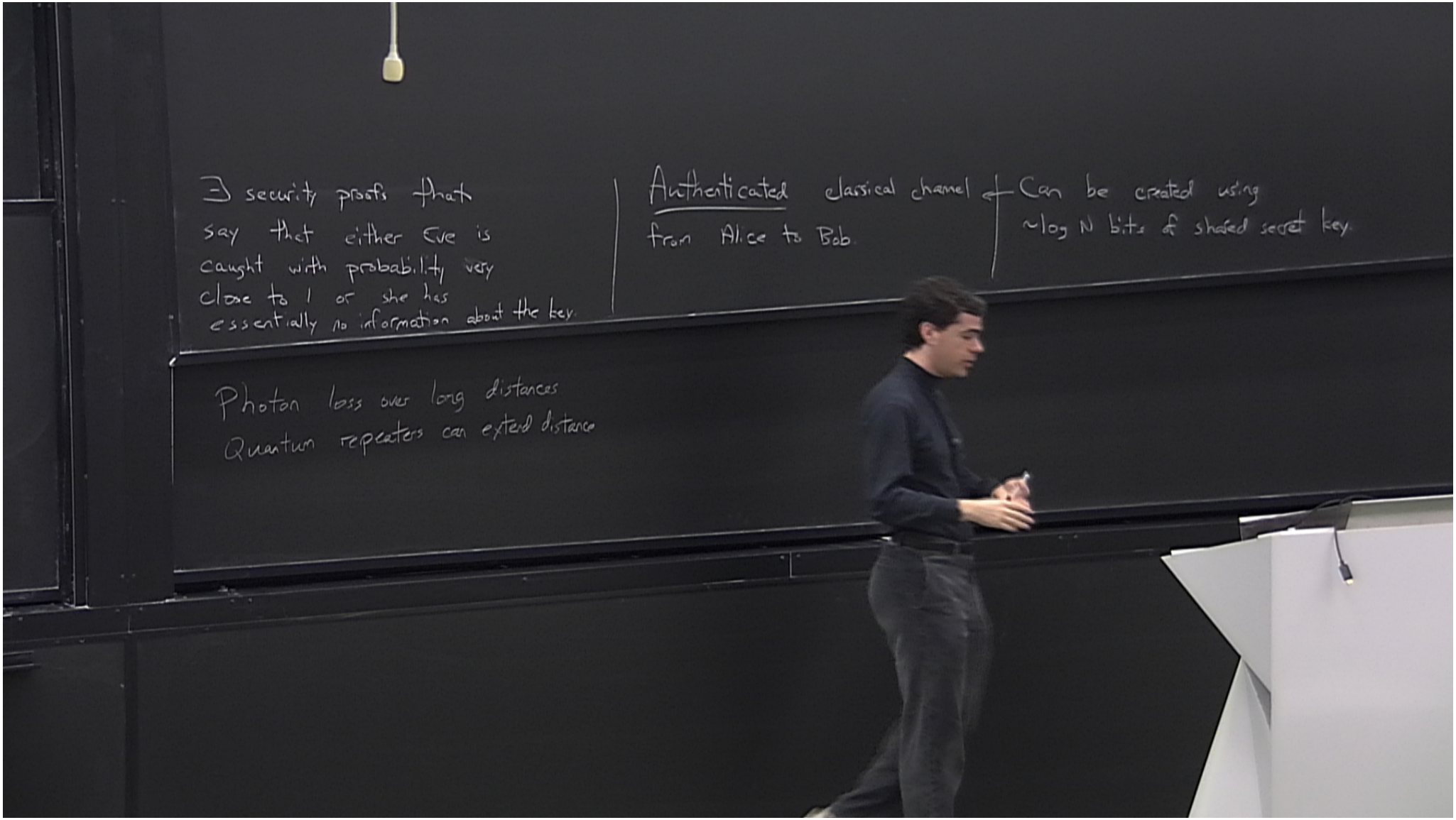
Have about $\sim N/2$ bits left

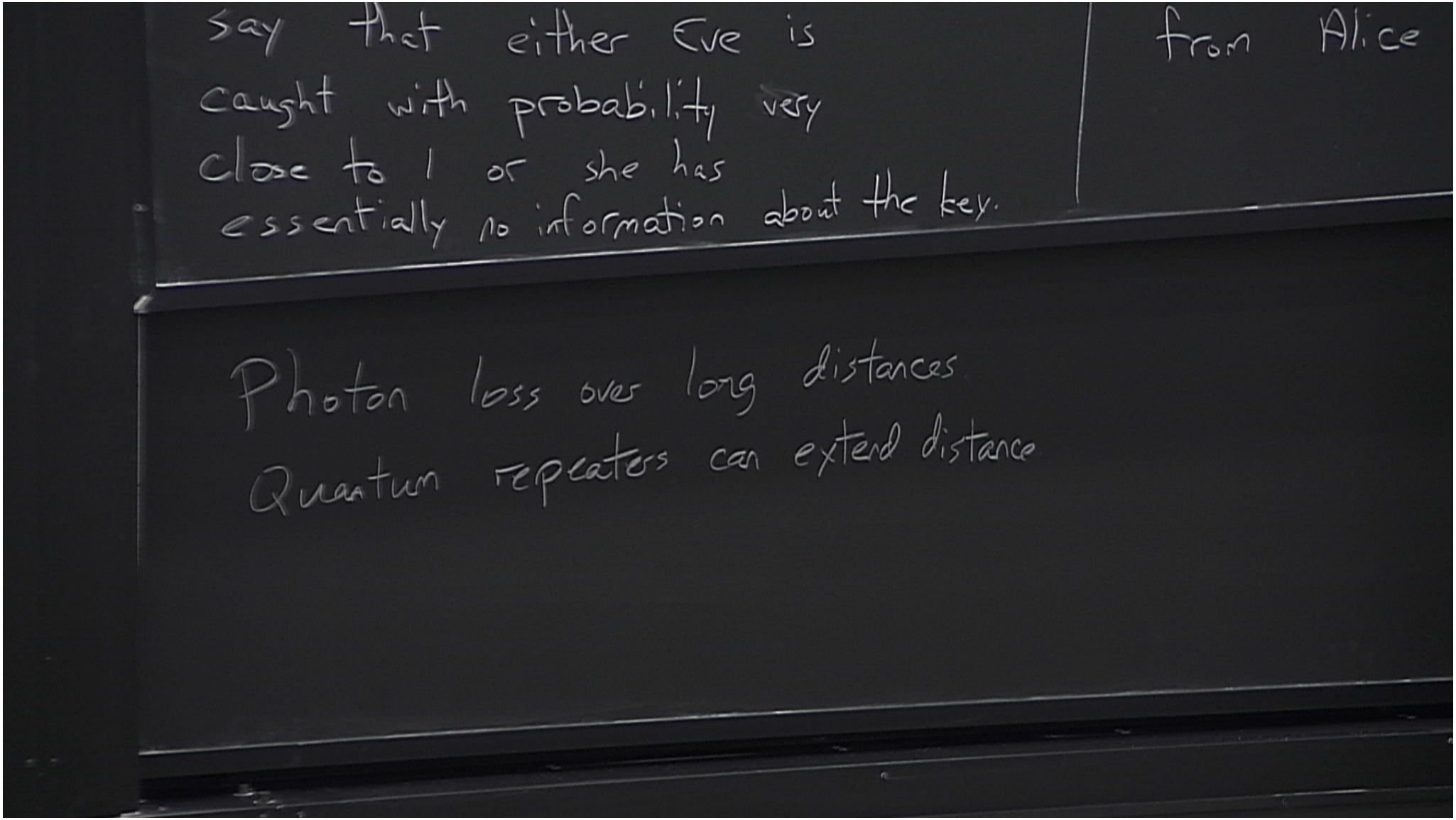
⑤ Alice & Bob choose a random subset of bits & announce r_i & s_i for those bits. They calculate error rate & abort if it is too high ($\geq 20\%$).

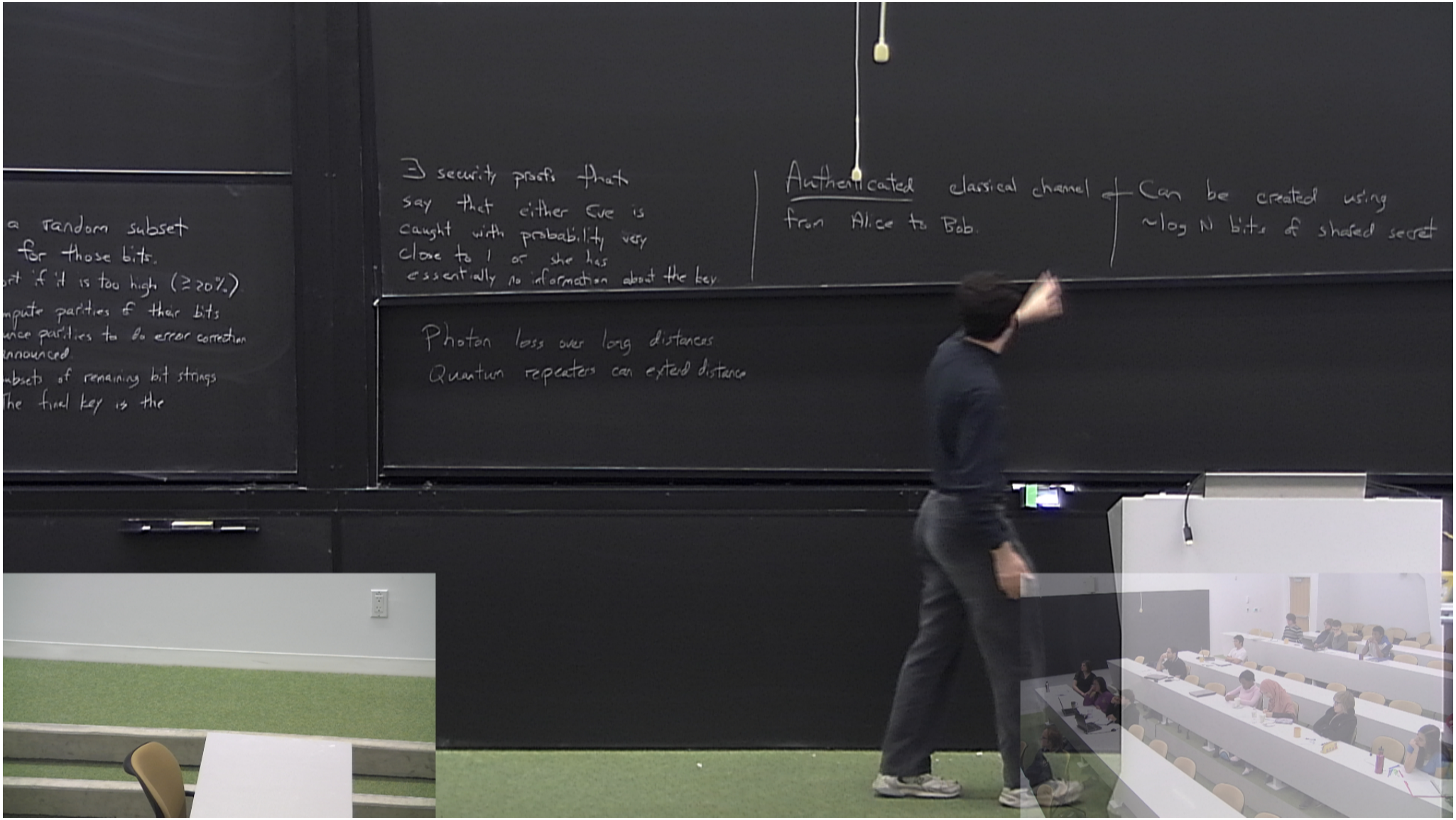
⑥ Error correction: Alice & Bob compute parities of their bits according to a classical ECC & announce parities to do error correction. Must discard 1 bit per parity announced.

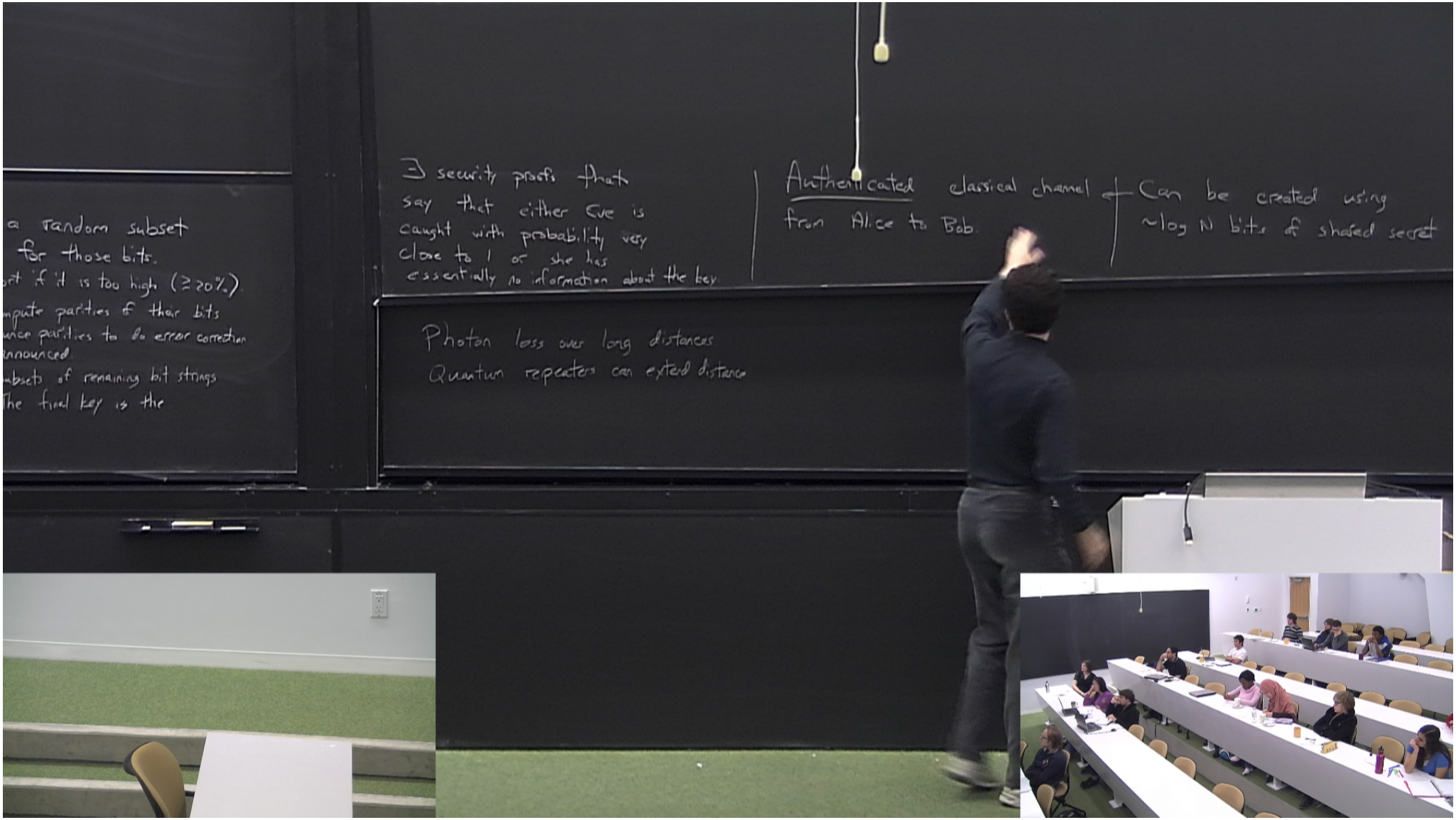
⑦ Privacy amplification: Take random subsets of remaining bit strings & compute parities of those subsets. The final key is the value of the parities.


(5) Alice & Bob choose a random subset of bits & announce r_i & s_i for those bits. They calculate error rate & abort if it is too high ($\gtrsim 20\%$).
(6) Error correction: Alice & Bob compute parities of their bits according to a classical ECC & announce parities to do error correction. Must discard 1 bit per parity announced.
(7) Privacy amplification: Take random subsets of remaining bit strings & compute parities of those subsets. The final key is the value of the parities.


3 security proofs that say that either Eve is caught with probability very close to 1 or she has essentially no information about the key.
Authenticated classical channel from Alice to Bob.
Can be created using ~log N bits of shared secret key.
Photon loss over long distances
Quantum repeaters can extend distance


say that either Eve is
caught with probability very
close to 1 or she has
essentially no information about the key.
from Alice
Photon loss over long distances
Quantum repeaters can extend distance


a random subset
for those bits.
if it is too high (≥ 20%)
mpute parities of their bits
nce parities to do error correction
announced.
ubsets of remaining bit strings
The final key is the
3 security proofs that
say that either Eve is
caught with probability very
close to 1 or she has
essentially no information about the key
Photon loss over long distances
Quantum repeaters can extend distance
Authenticated classical channel
from Alice to Bob.
Can be created using
~log N bits of shared secret


a random subset
for those bits.
ort if it is too high (≥ 20%)
mpute parities of their bits
nce parities to do error correction
announced
ubsets of remaining bit strings
The final key is the
3 security proofs that
say that either Eve is
caught with probability very
close to 1 or she has
essentially no information about the key
Authenticated classical channel from Alice to Bob
Can be created using
~log N bits of shared secret
Photon loss over long distances
Quantum repeaters can extend distance