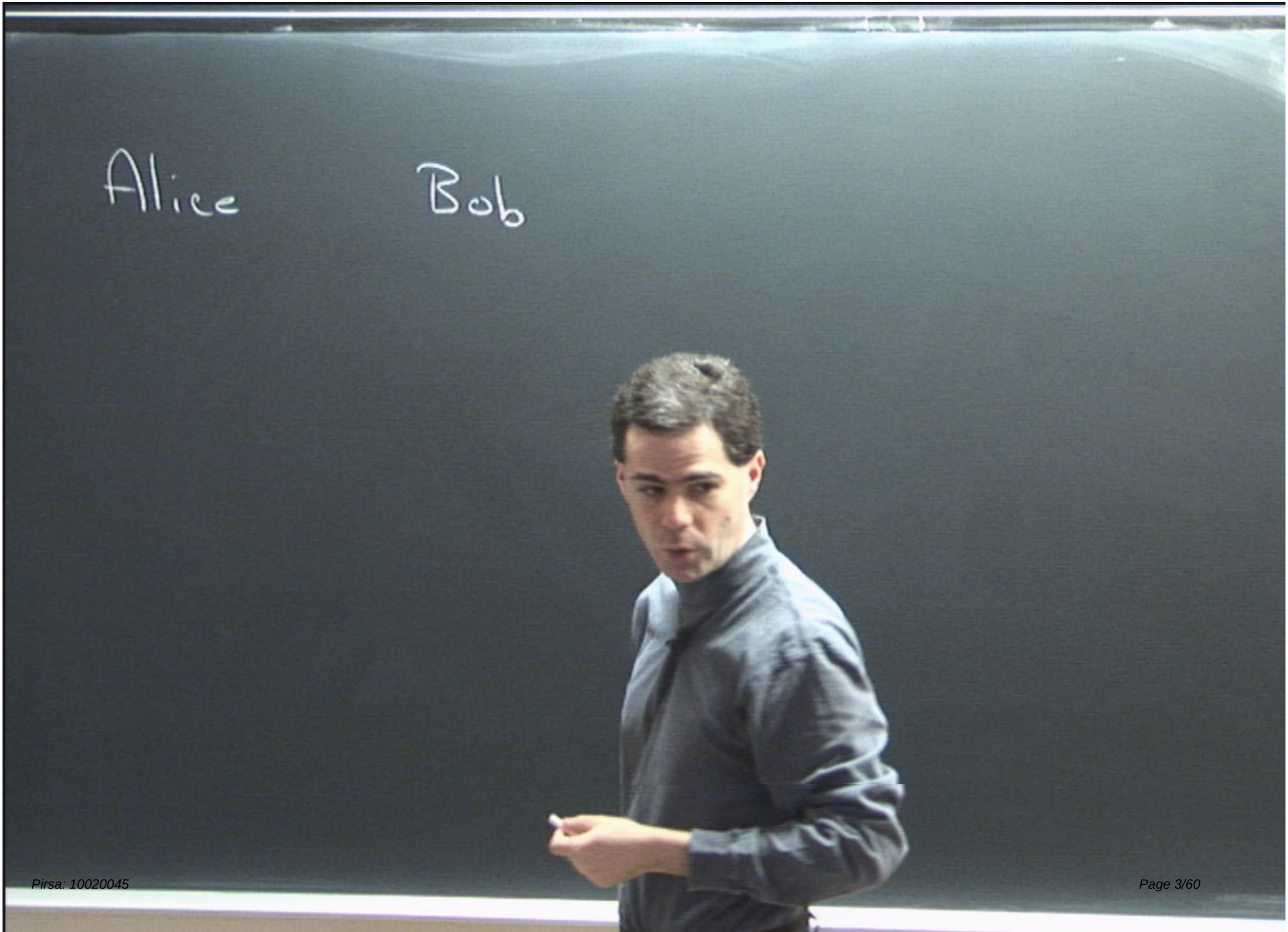
Title: Quantum Information - Review (PHYS 635) - Lecture 11

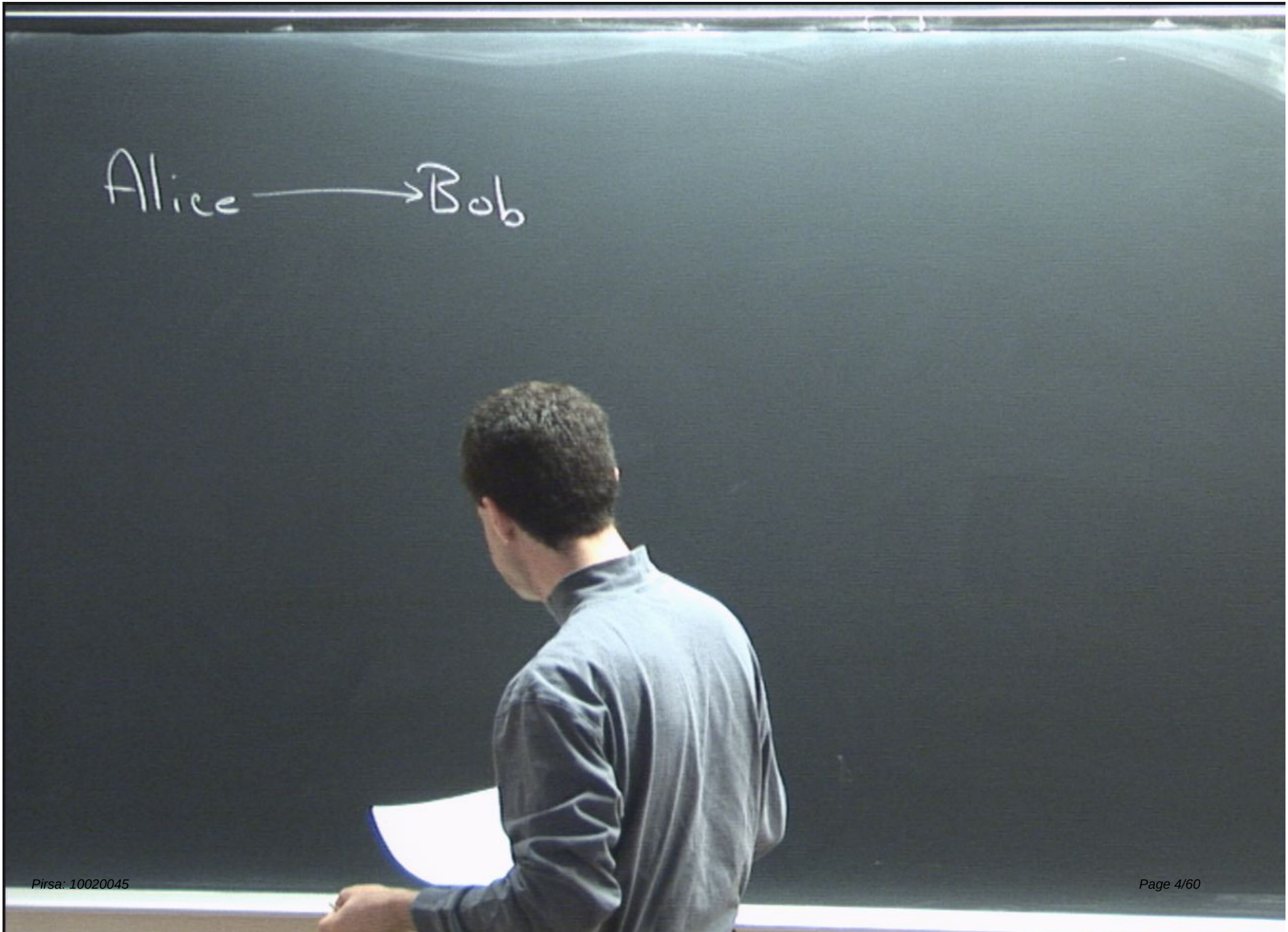
Date: Feb 08, 2010 09:00 AM

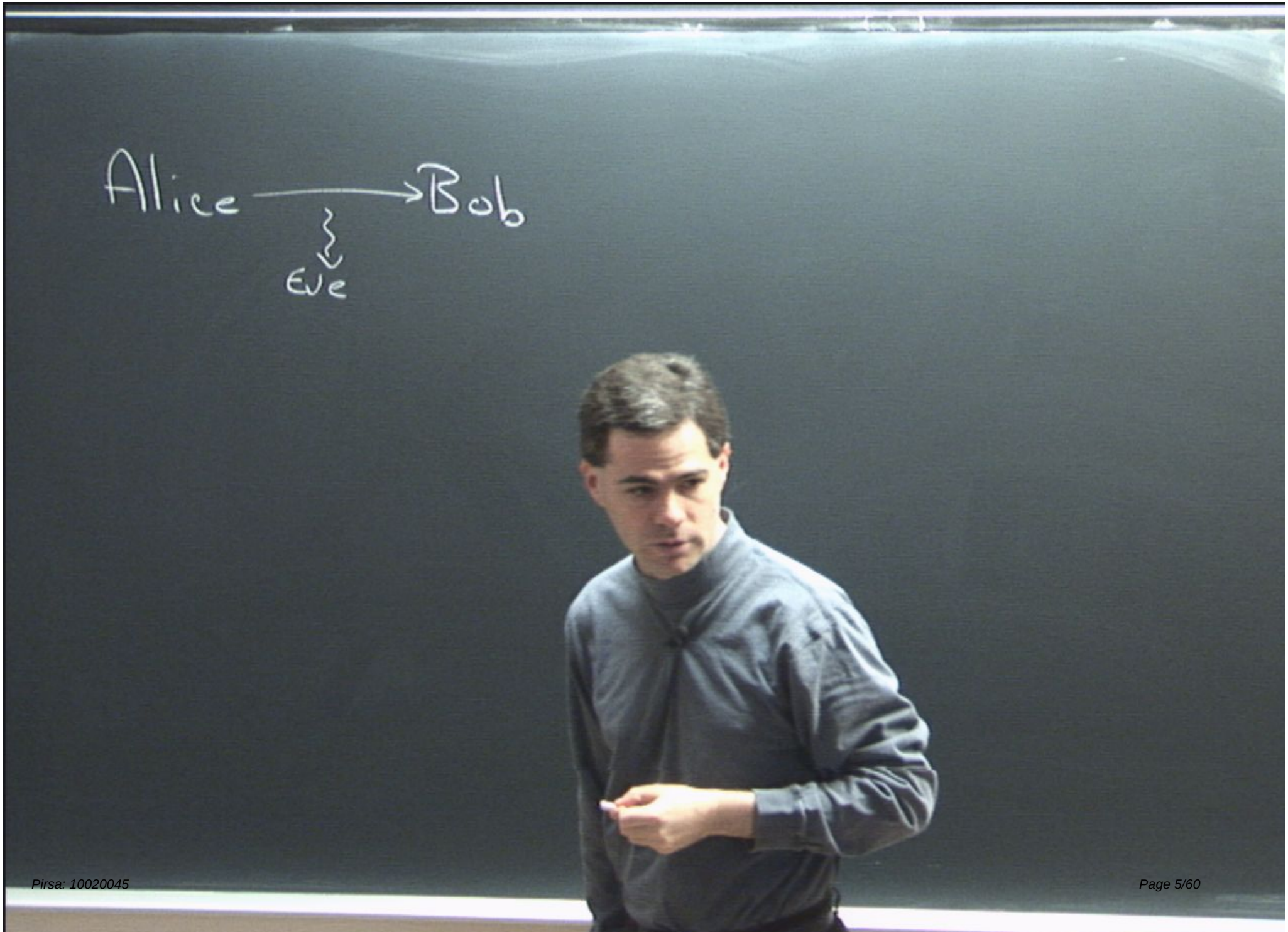
URL: http://pirsa.org/10020045

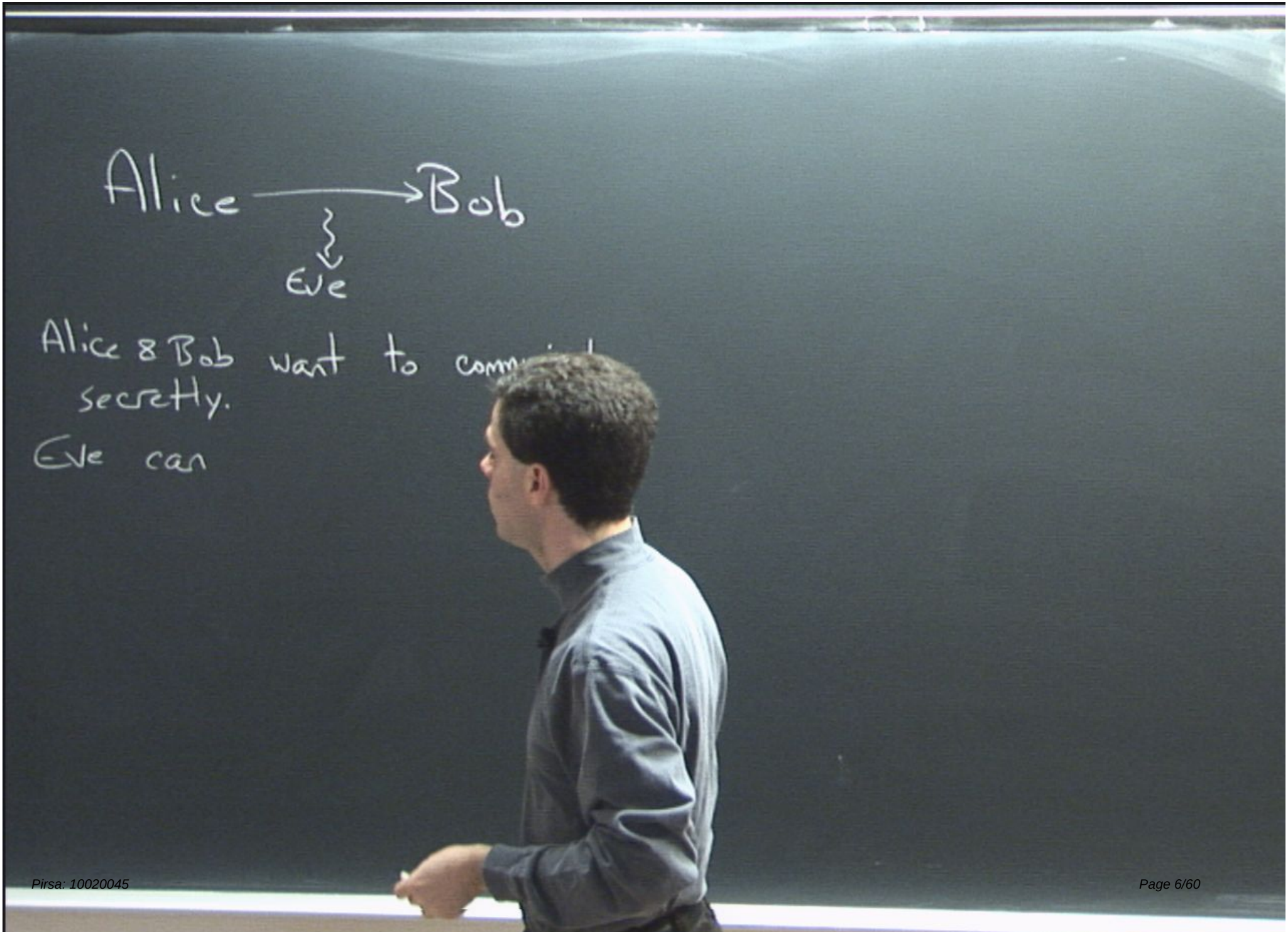
Abstract:

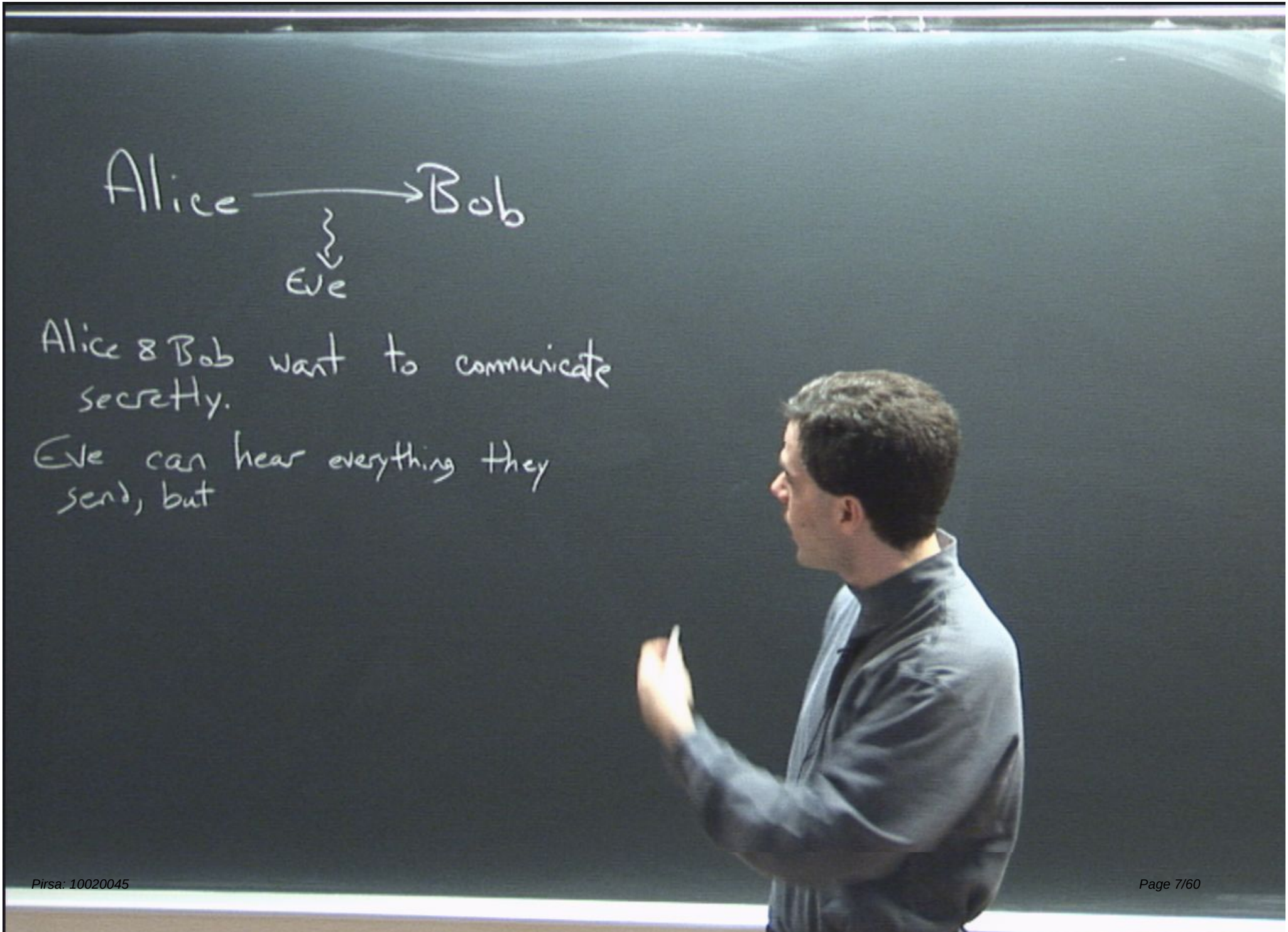

perimeter scholars
international

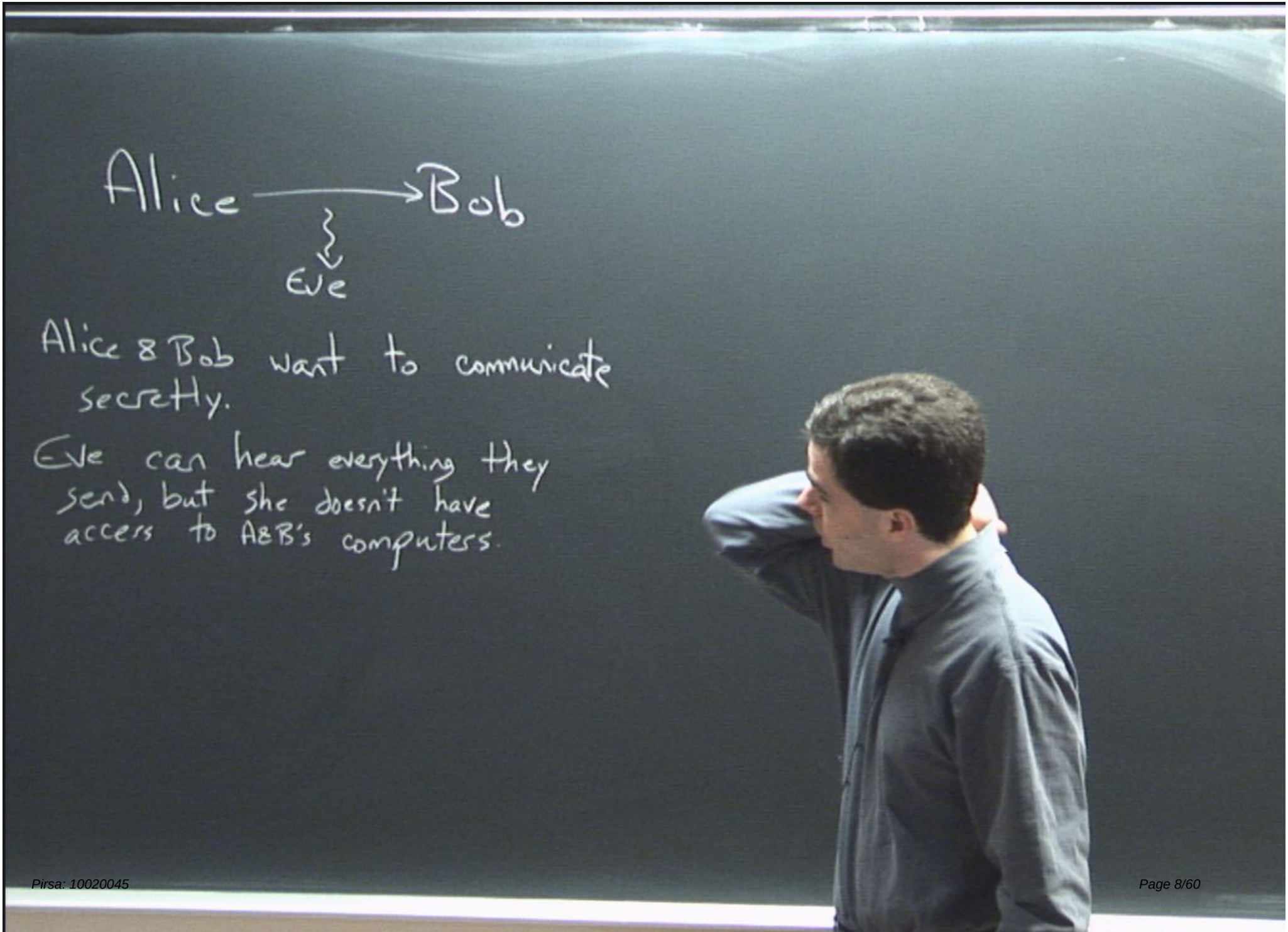

Alice
Bob

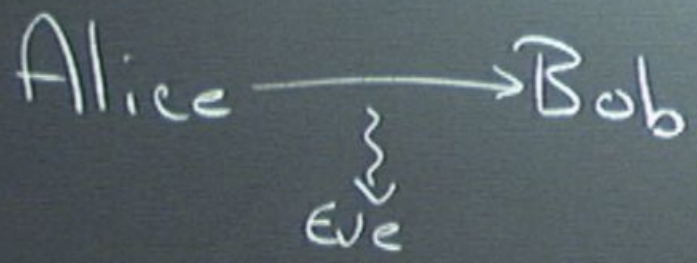

Alice
Bob


Alice
Bob
Eve


Alice
Bob
Eve
Alice & Bob want to
secretly.
Eve can


Alice
Bob
Eve
Alice & Bob want to communicate secretly.
Eve can hear everything they send, but

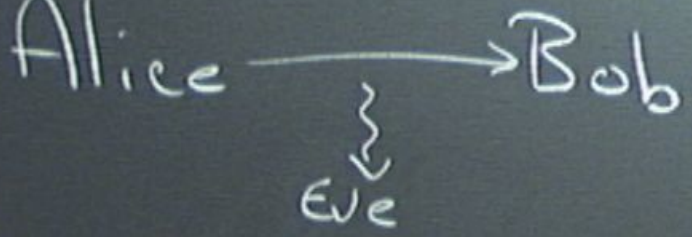

Alice
Bob
Eve
Alice & Bob want to communicate secretly.
Eve can hear everything they send, but she doesn't have access to A&B's computers.



Alice & Bob want to communicate secretly.

Eve can hear everything they send, but she doesn't have access to A&B's computers.

One-time pad:

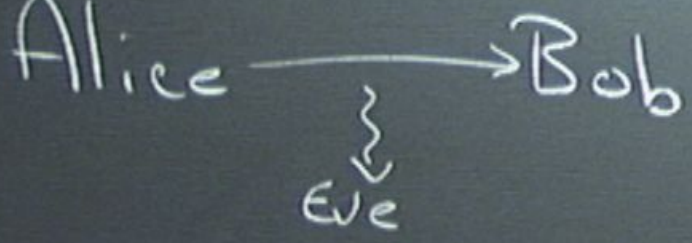


Alice & Bob want to communicate secretly.

Eve can hear everything they send, but she doesn't have access to A&B's computers.

One-time pad:

Alice & Bob share a long private key k (a string of random bits)



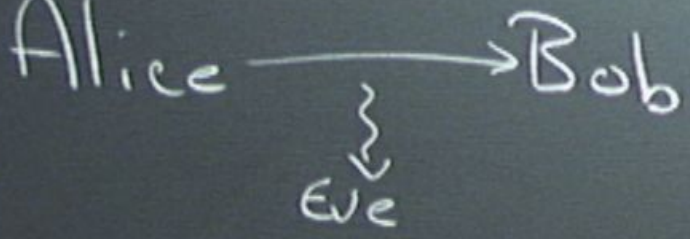
Alice & Bob want to communicate secretly.

Eve can hear everything they send, but she doesn't have access to A&B's computers.

One-time pad:

Alice & Bob share a long private key k (a string of random bits)

Alice converts her message to a string of bits



Alice & Bob want to communicate secretly.

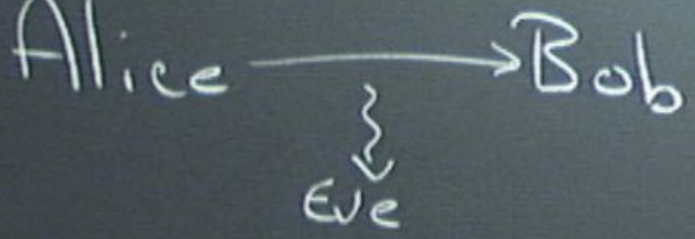
Eve can hear everything they send, but she doesn't have access to A&B's computers.

One-time pad:

Alice & Bob share a long private key k (a string of random bits)

Alice converts her message to a string of bits m

Sends $e = m \oplus k$ (bitwise XOR)



lice & Bob want to communicate secretly.

ve can hear everything they send, but she doesn't have accers to A&B's computers.

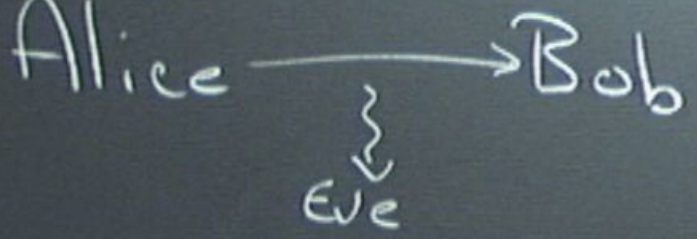
One-time pad:

Alice & Bob share a long private key k (a string of random bits)

Alice converts her message to a string of bits m

Sends $e = m \oplus k$ (bitwise XOR)

Bob decodes $e \oplus k = (m \oplus k) \oplus k = m$



lice & Bob want to communicate secretly.

ve can hear everything they send, but she doesn't have accers to A&B's computers.

One-time pad:

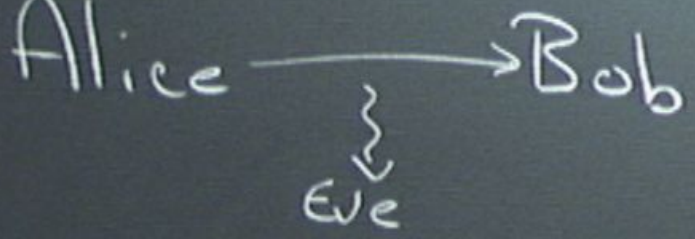
Alice & Bob share a long private key k (a string of random bits)

Alice converts her message to a string of bits m

Sends $e = m \oplus k$ (bitwise XOR)

Bob decodes $e \oplus k = (m \oplus k) \oplus k = m$

But Eve doesn't know k, so to her each bit looks completely random.



lice & Bob want to communicate secretly.

ve can hear everything they send, but she doesn't have acces to A&B's computers.

One-time pad:

Alice & Bob share a long private key k (a string of random bits)

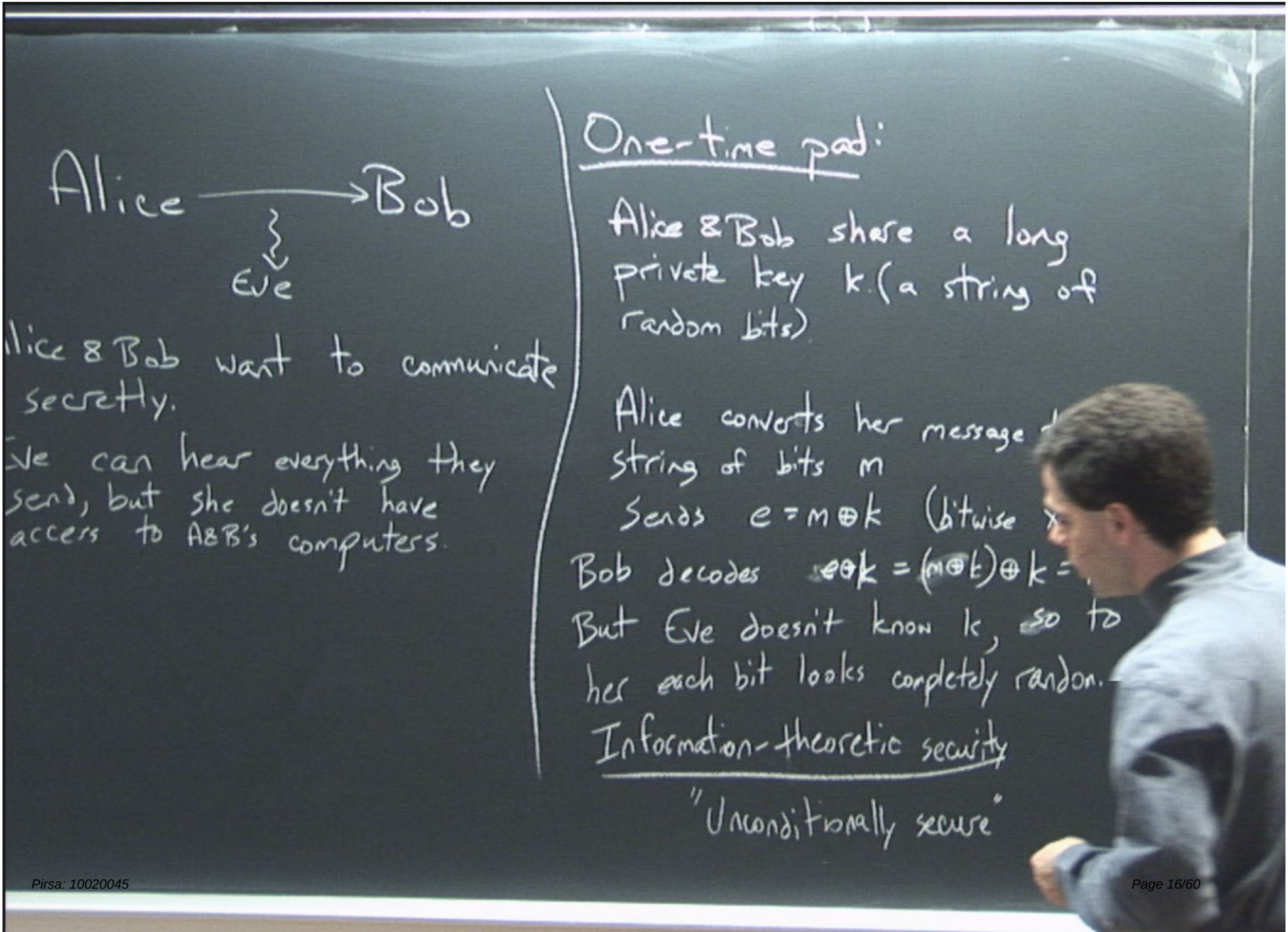
Alice converts her message to a string of bits m

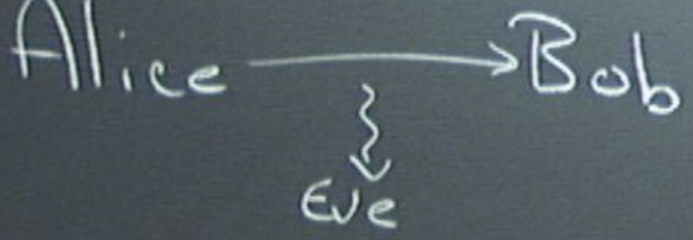
Sends $e = m \oplus k$ (bitwise XOR)

Bob decodes $e \oplus k = (m \oplus k) \oplus k = m$

But Eve doesn't know k, so to her each bit looks completely random.

Information-theoretic security


Alice
Bob
Eve
lice & Bob want to communicate secretly.
Ve can hear everything they send, but she doesn't have acces to A&B's computers.
One-time pad:
Alice & Bob share a long private key k (a string of random bits)
Alice converts her message
string of bits m
Sends e = m ⊕ k (bitwise
Bob decodes e⊕k = (m⊕k)⊕k =
But Eve doesn't know k, so to her each bit looks completely random.
Information-theoretic security
"Unconditionally secure"



Alice & Bob want to communicate secretly.

Eve can hear everything they send, but she doesn't have access to A&B's computers.

One-time pad:

Alice & Bob share a long private key k (a string of random bits)

Alice converts her message to a string of bits m

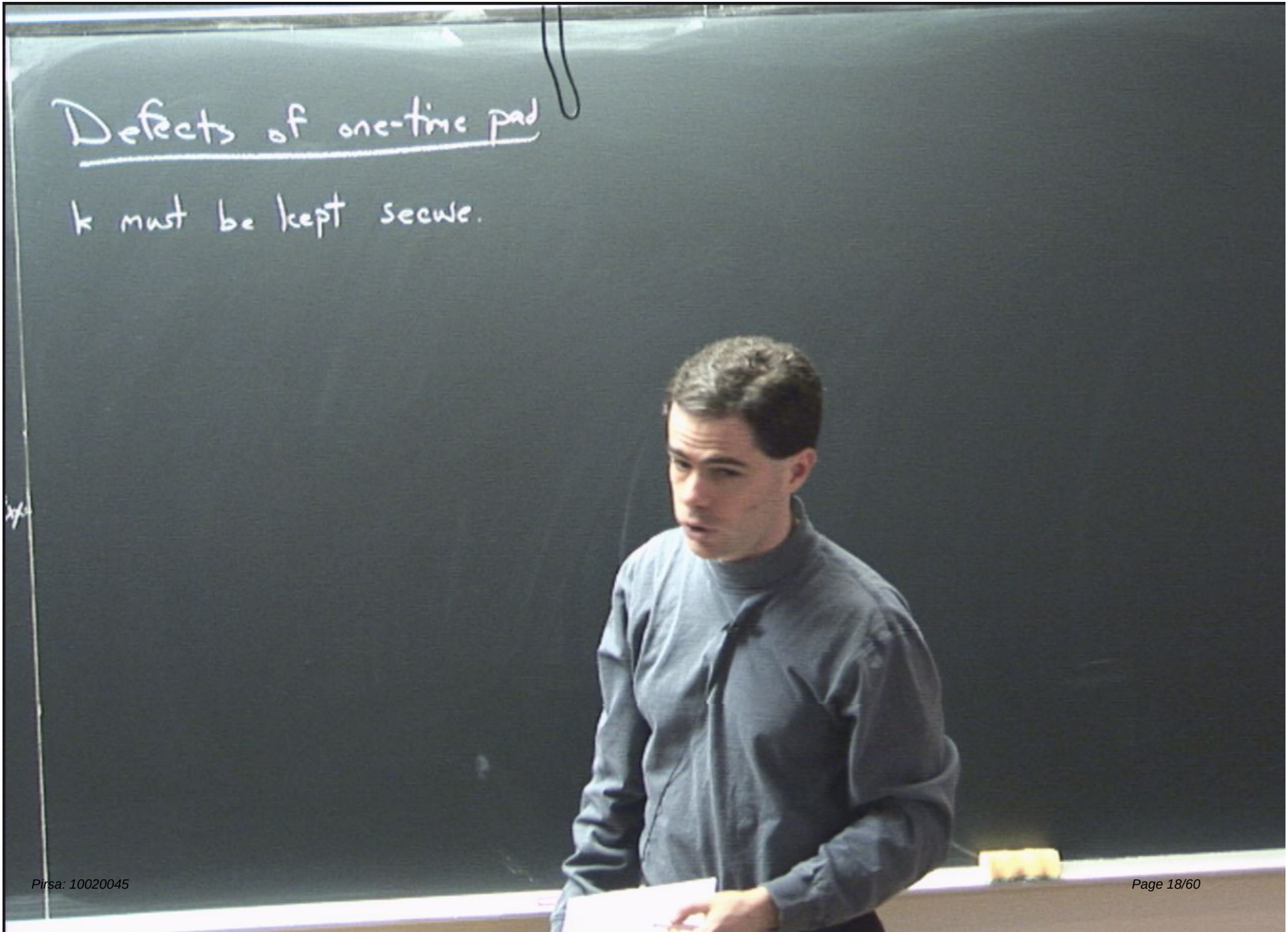
Sends $e = m \oplus k$ (bitwise XOR) "ciphertext"

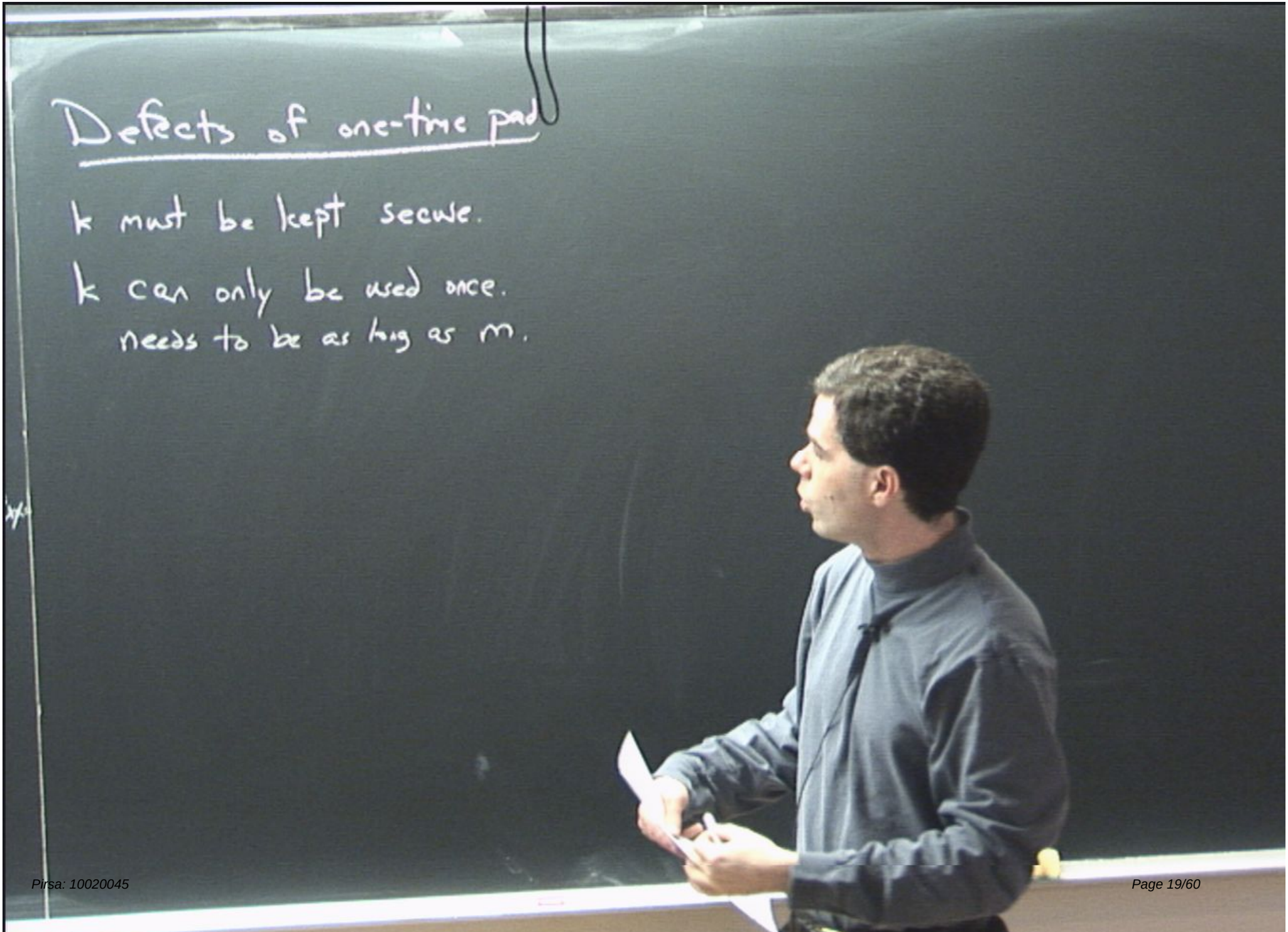
Bob decodes $e \oplus k = (m \oplus k) \oplus k = m$

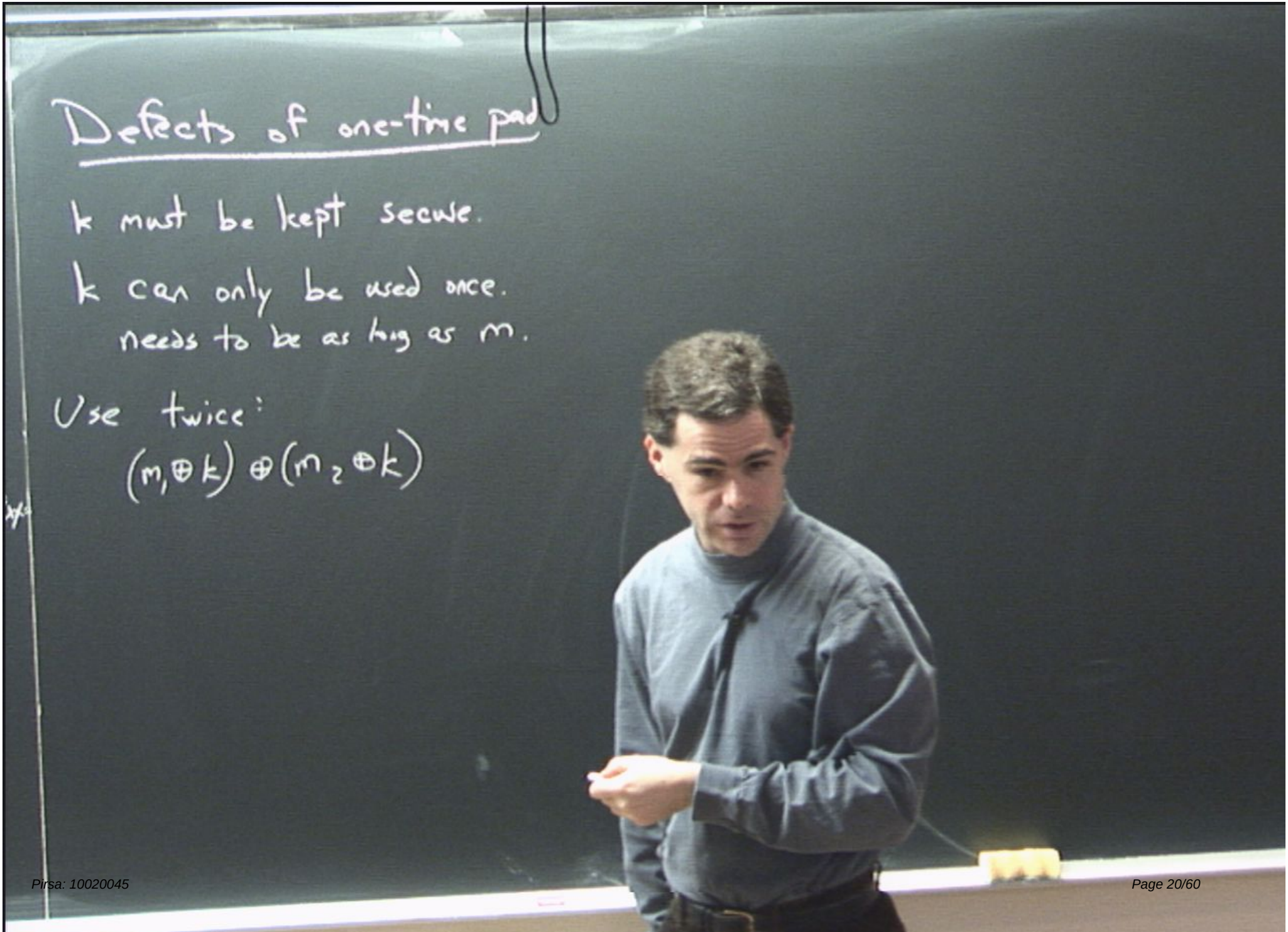
But Eve doesn't know k, so to her each bit looks completely random.

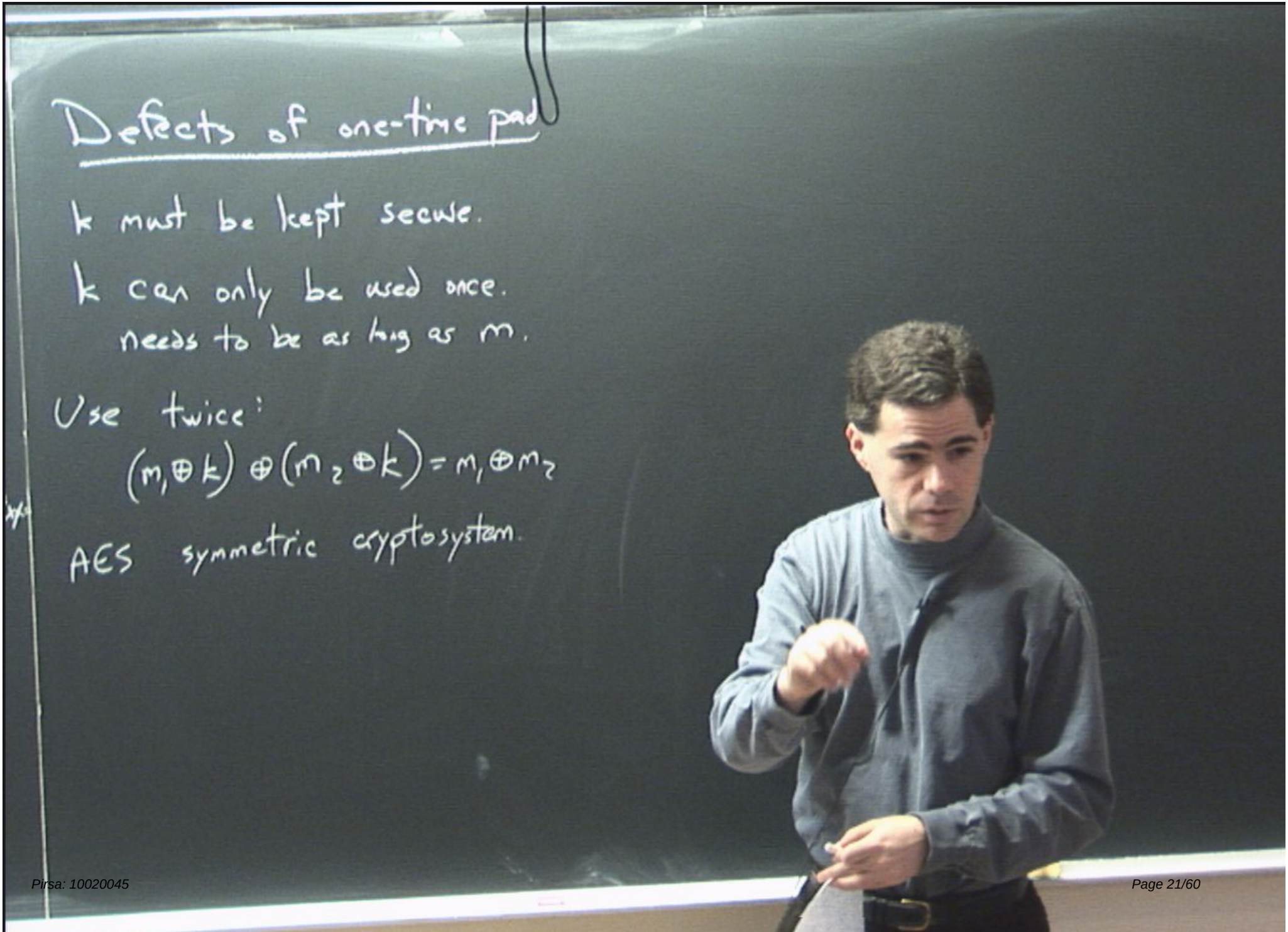
Information-theoretic security

"Unconditionally secure"


Defects of one-time pad
k must be kept secure.


Defects of one-time pad
k must be kept secure.
k can only be used once.
needs to be as long as m.


Defects of one-time pad
k must be kept secure.
k can only be used once.
needs to be as long as m.
Use twice:
$(m_1 \oplus k) \oplus (m_2 \oplus k)$


Defects of one-time pad
k must be kept secure.
k can only be used once.
needs to be as long as m.
Use twice:
$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$
AES symmetric cryptosystem.

Defects of one-time pad

k must be kept secure.

k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)

Defects of one-time pad

k must be kept secure.

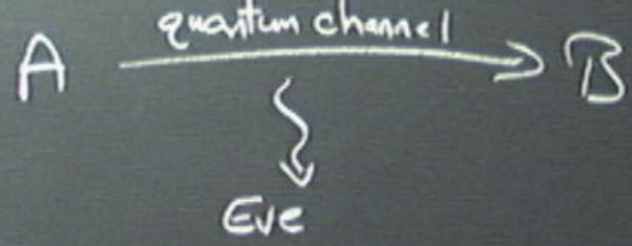
k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



Defects of one-time pad

k must be kept secure.

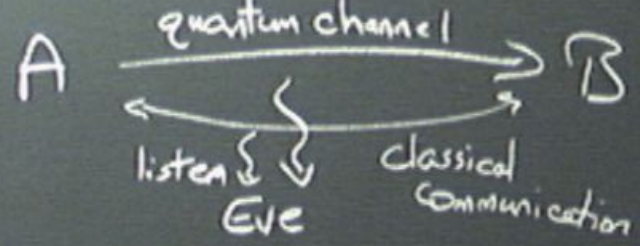
k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



(1) Alice generate N pairs of random bits (a_i, r_i) $i = 1, \ldots, N$

Defects of one-time pad

k must be kept secure.

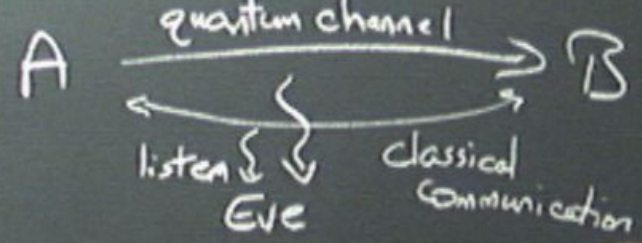
k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



(1) Alice generate .f
random bits $(a_i, r_i$,N

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

Defects of one-time pad

k must be kept secure.

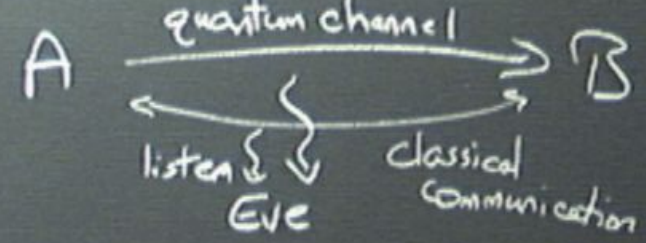
k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



(1) Alice generate N pairs of random bits (a_i, r_i) $i = 1, \ldots$

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

(2)

Defects of one-time pad

k must be kept secure.

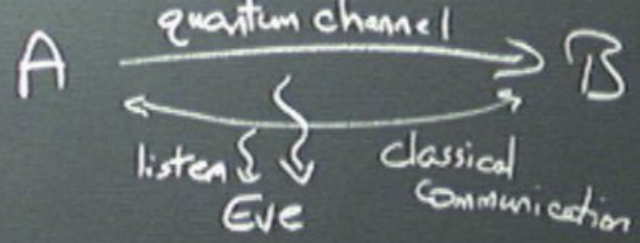
k can only be used once.
needs to be as long as m.

Use twice:

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



(1) Alice generate N pairs of random bits (a_i, r_i) $i = 1, \ldots, N$

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

(2) Alice sends the corresponding qubits to Bob for each i.

Defects of one-time pad

k must be kept secure.

k can only be used once.
needs to be as long as m.

Use twice:

$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

AES symmetric cryptosystem.

Quantum key distribution (QKD)

(1) Alice generate N pairs of random bits (a_i, r_i) $i = 1, \ldots, N$

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

(2) Alice sends the corresponding qubits to Bob for each i.

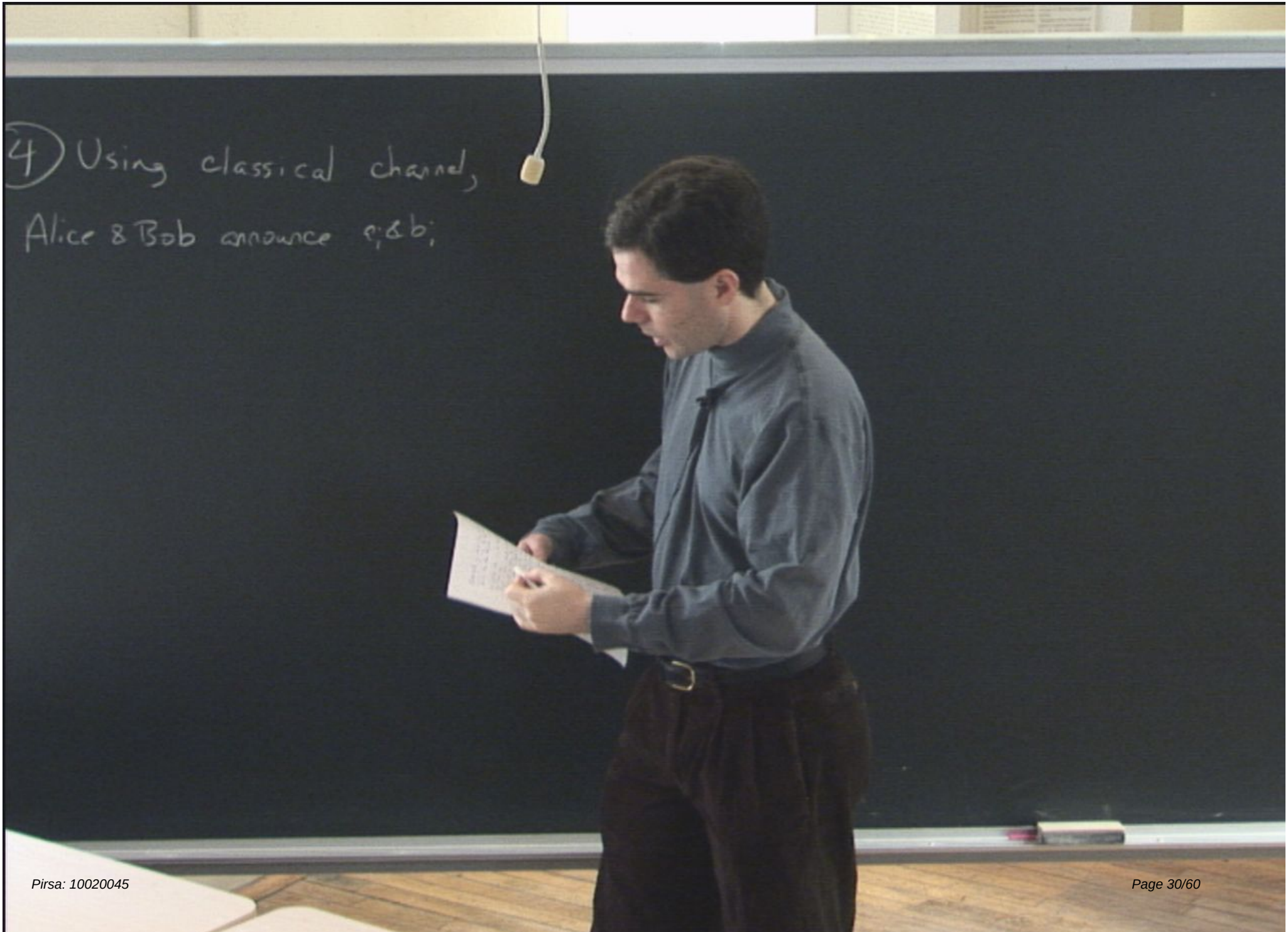
(3) Bob chooses a random basis for each qubit & measures it in that basis.

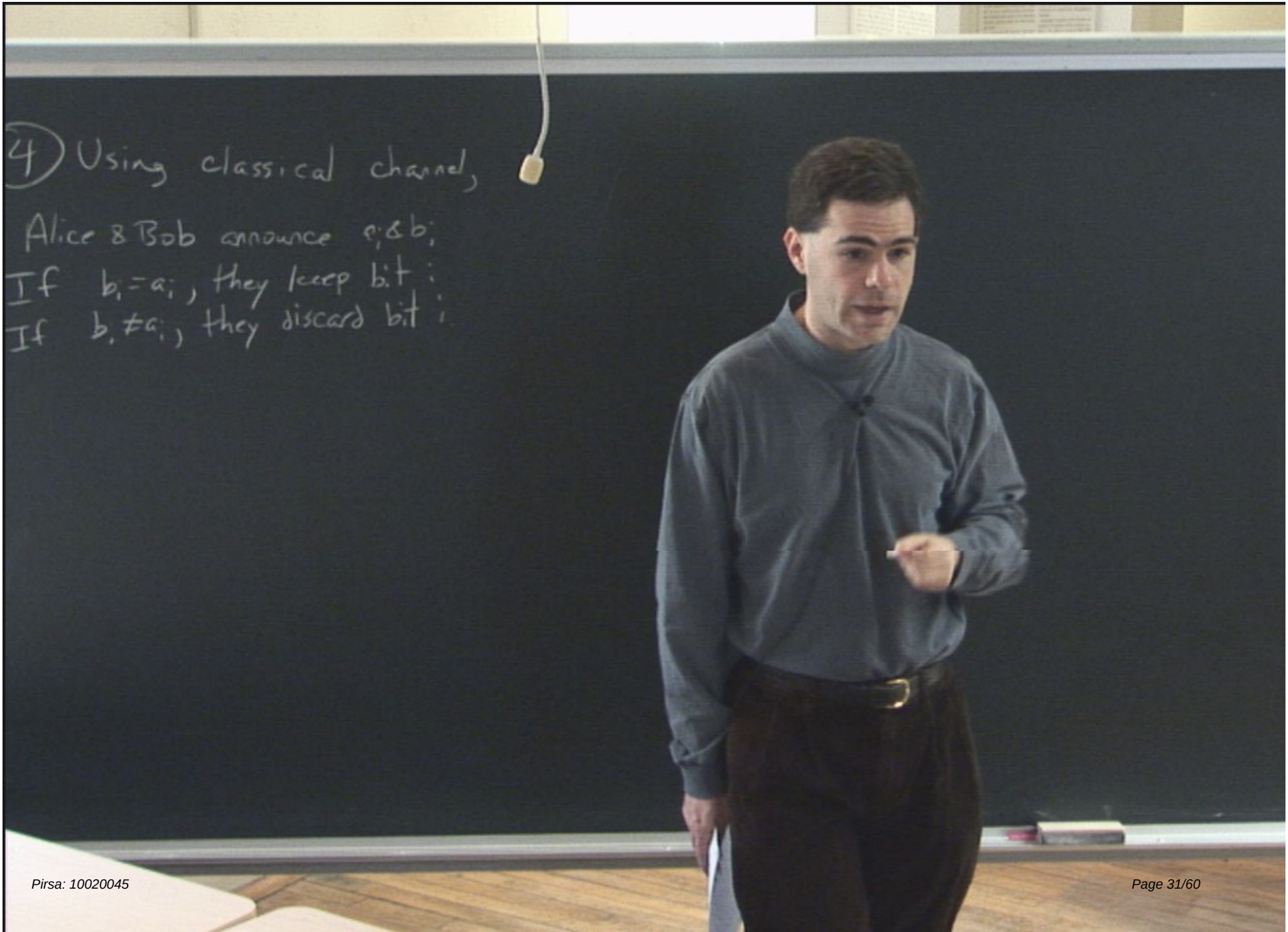
① Alice generate N pairs
random bits (a_i, r_i) $i = 1, \ldots$

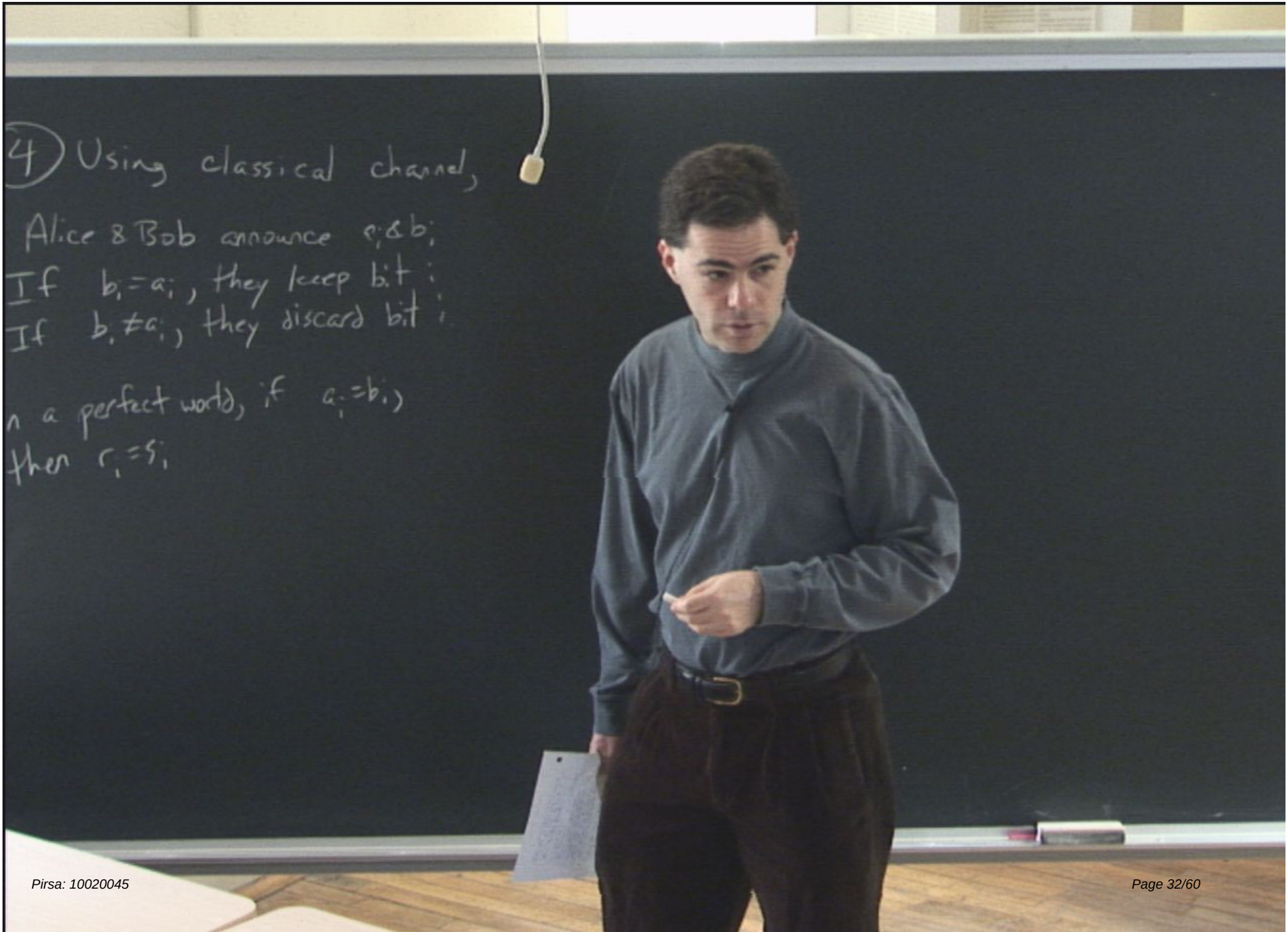
a_i	r_i	
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle = \|0\rangle + \|1\rangle$
1	1	$\|-\rangle = \|0\rangle - \|1\rangle$

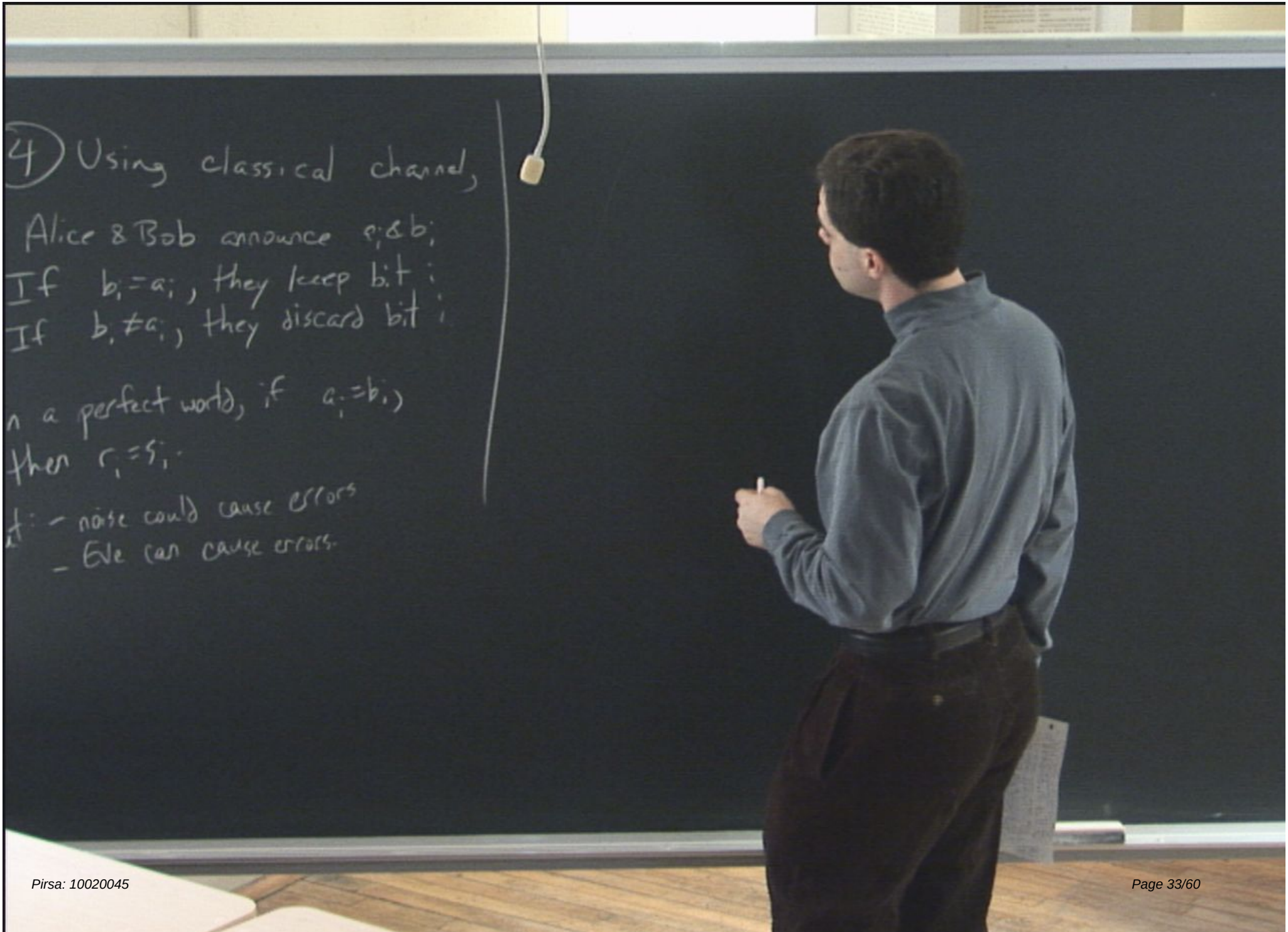
② Alice se
corresponding
to Bob fo

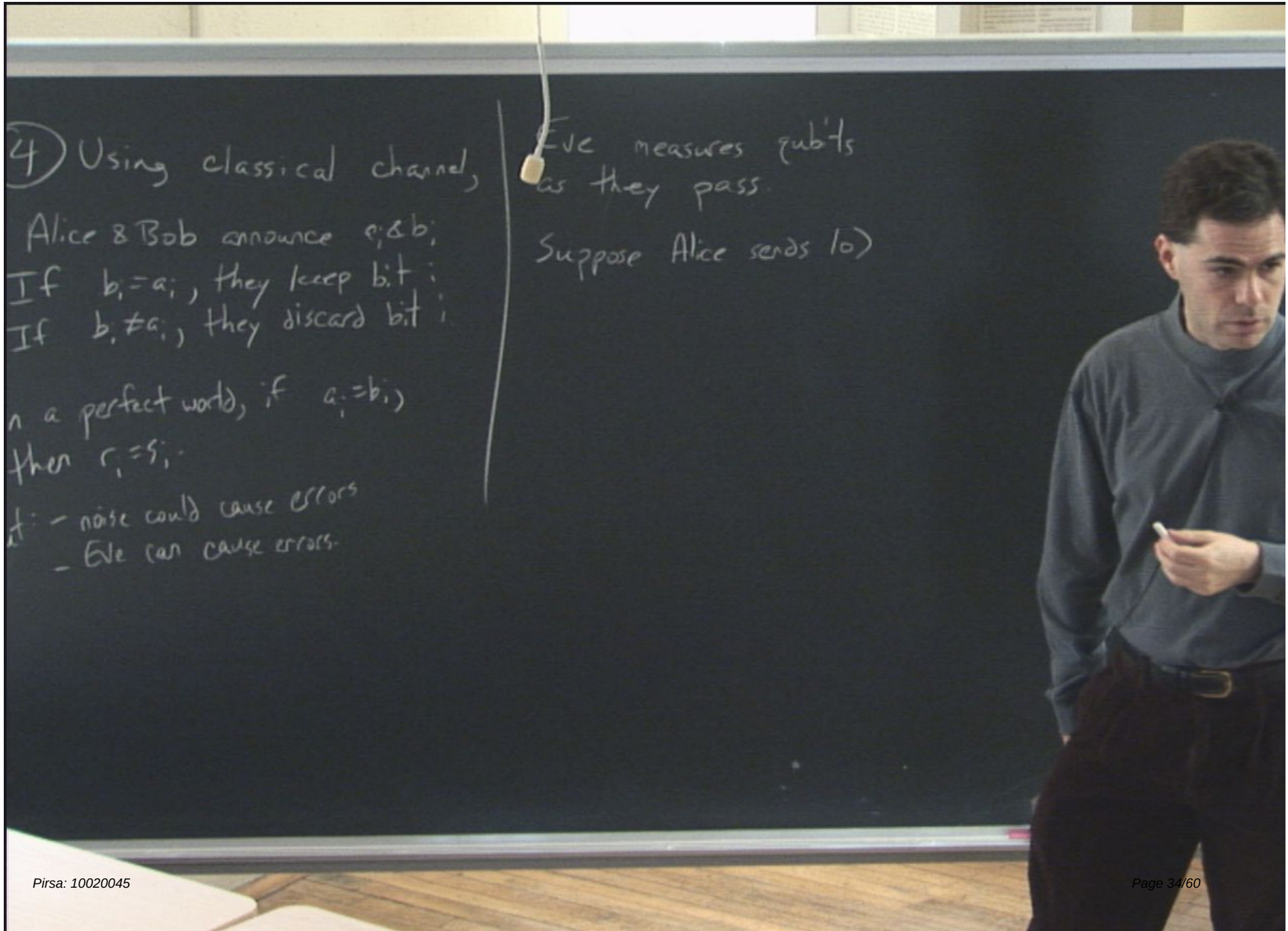
③ Bob chooses
for each qubit

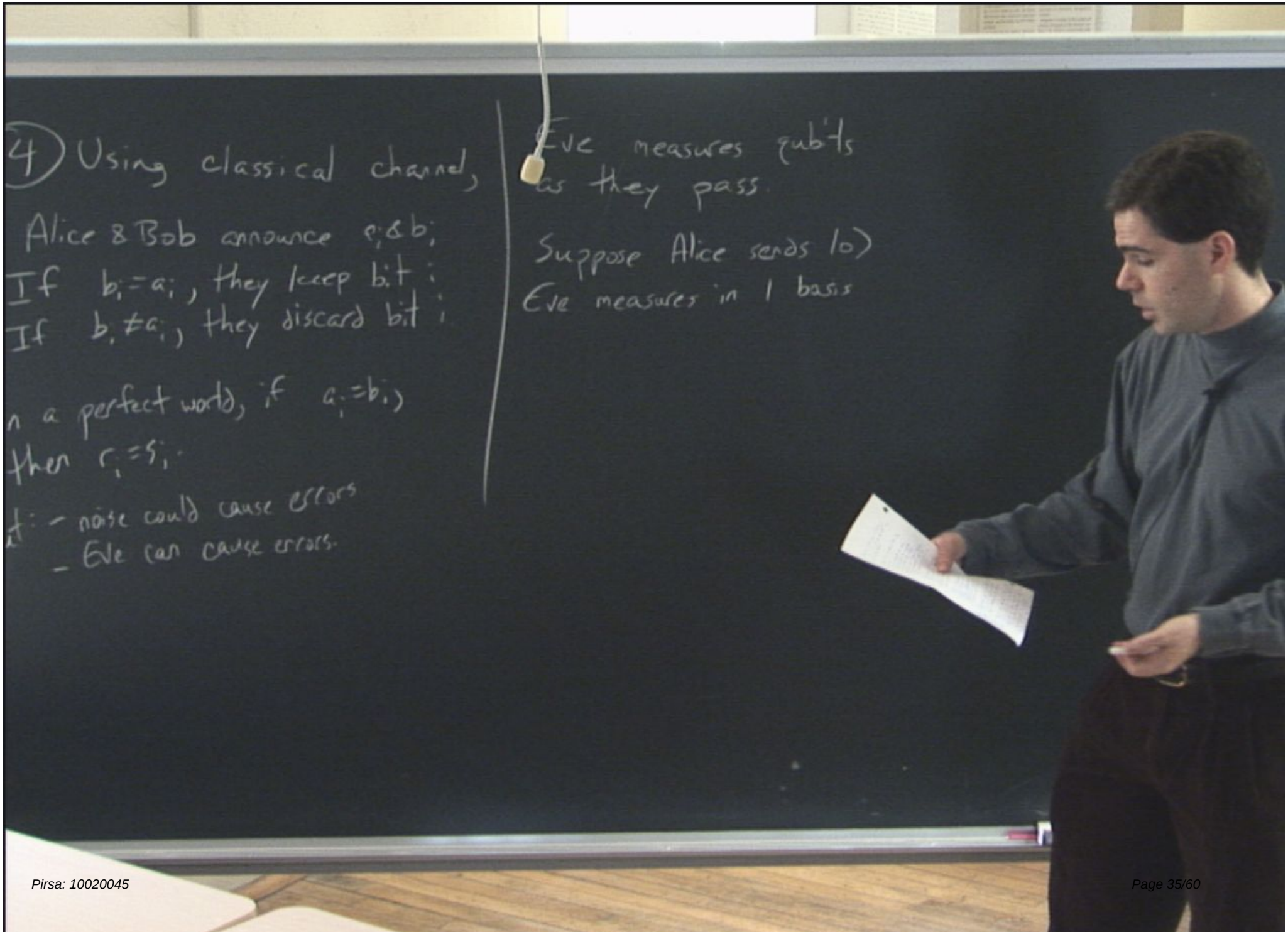

(4) Using classical channel,
Alice & Bob announce a; & b;

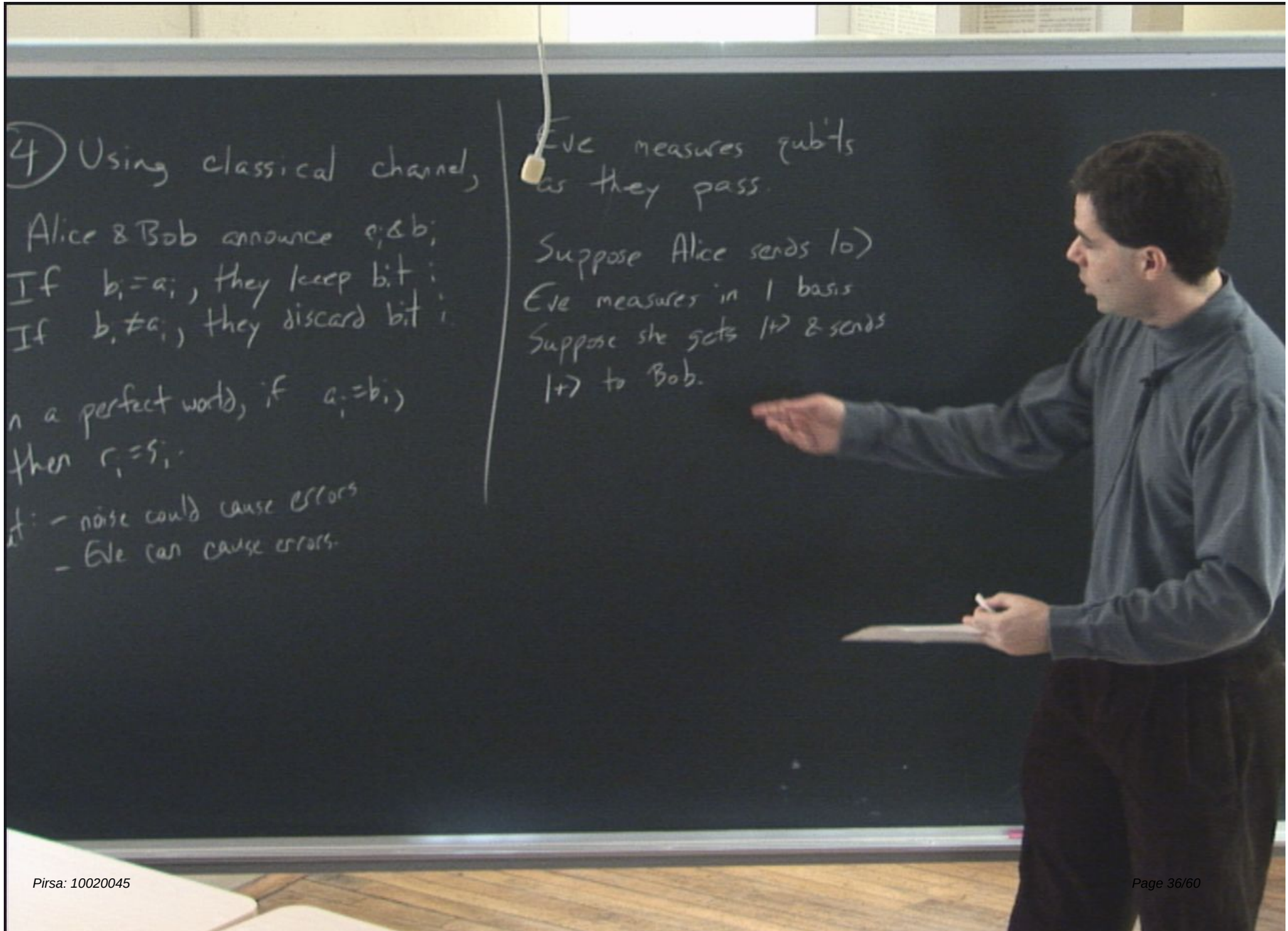

4) Using classical channel,
Alice & Bob announce a_i & b_i
If $b_i = a_i$, they keep bit i
If $b_i \neq a_i$, they discard bit i

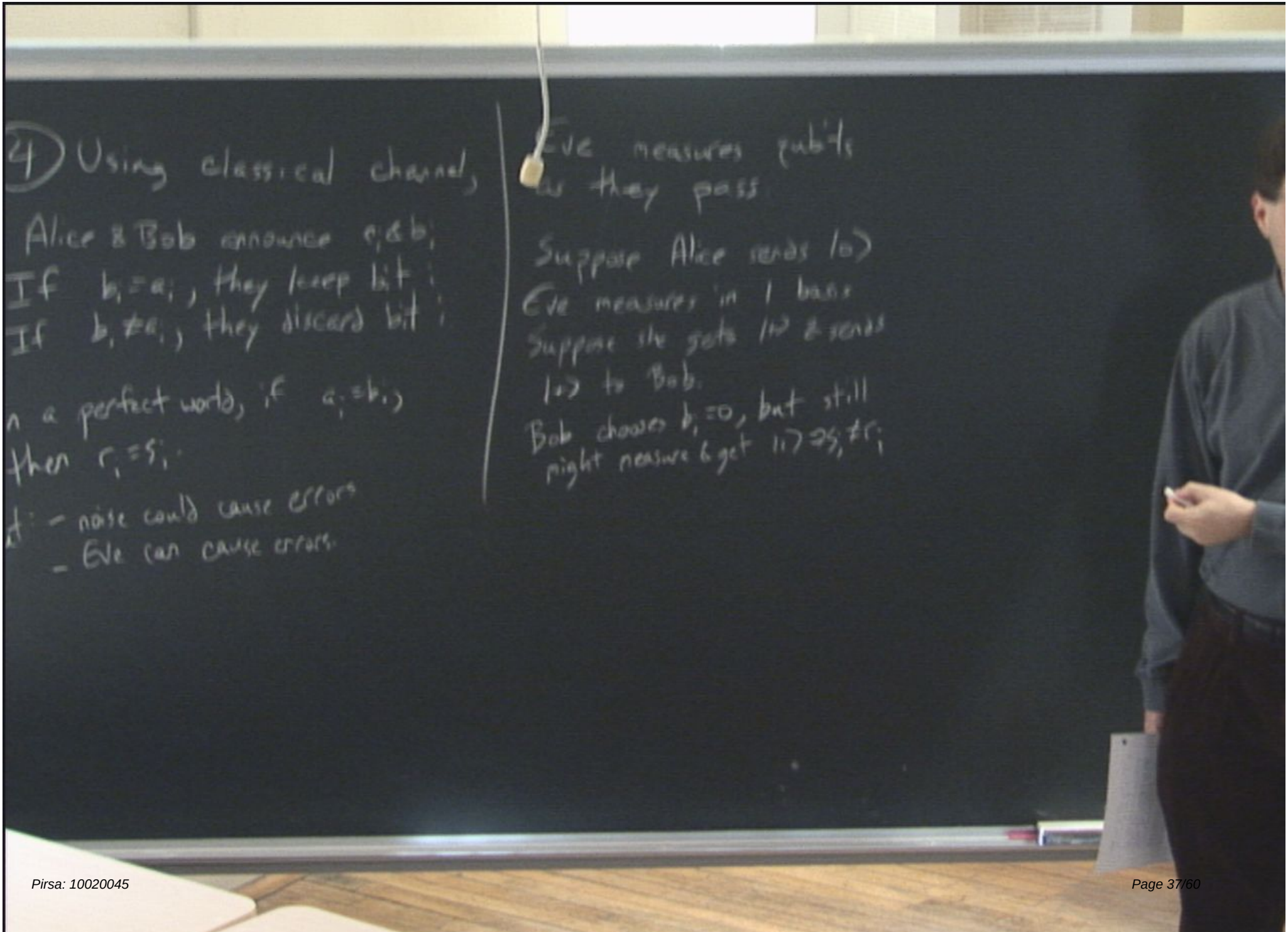

(4) Using classical channel,
Alice & Bob announce r_i & b_i
If $b_i = a_i$, they keep bit i
If $b_i \neq a_i$, they discard bit i
n a perfect world, if $a_i = b_i$)
then $r_i = s_i$

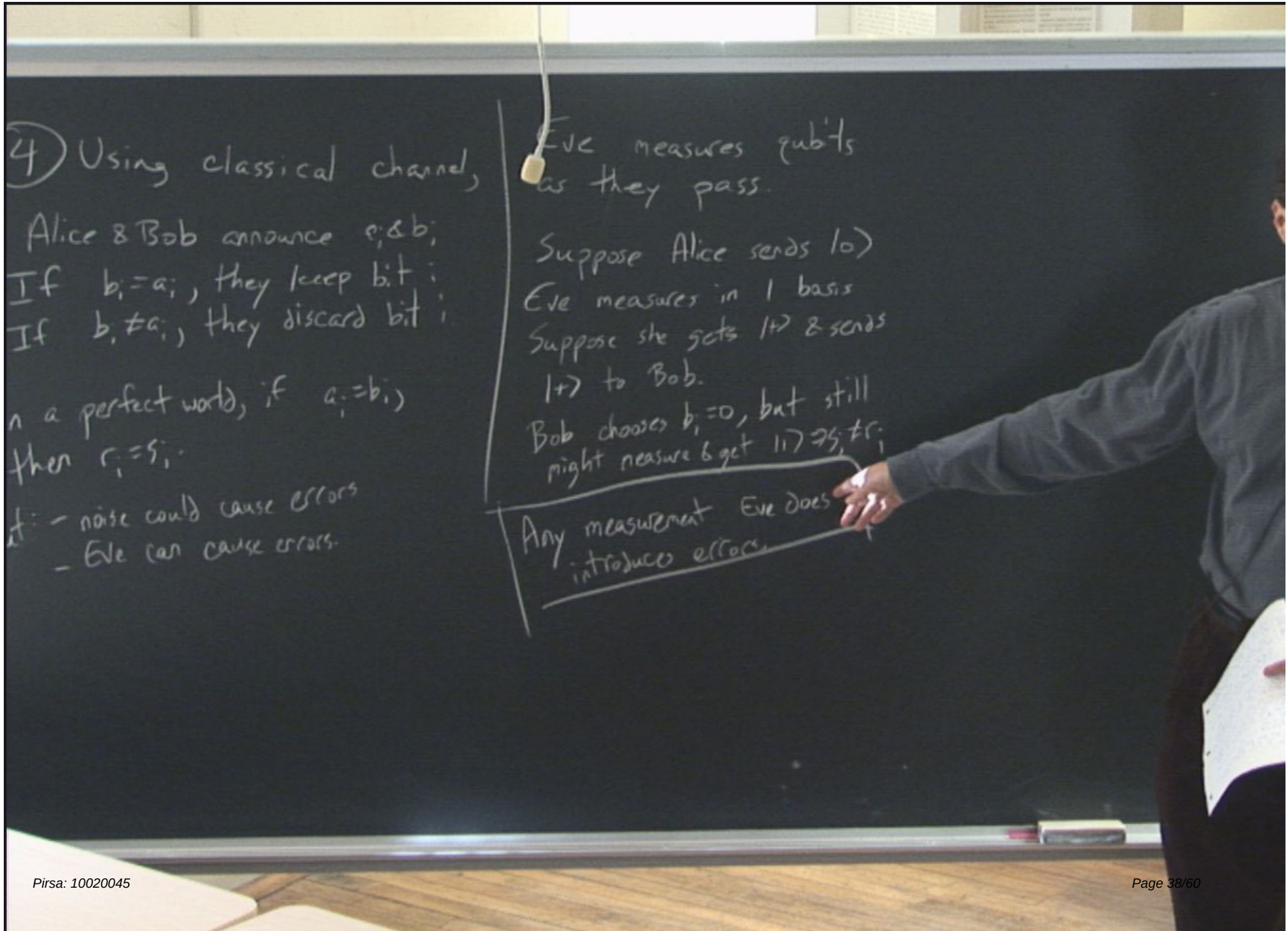

(4) Using classical channel,
Alice & Bob announce s_i & b_i
If $b_i = a_i$, they keep bit i
If $b_i \neq a_i$, they discard bit i
n a perfect world, if $a_i = b_i$)
then $r_i = s_i$
t: - noise could cause errors
- Eve can cause errors.

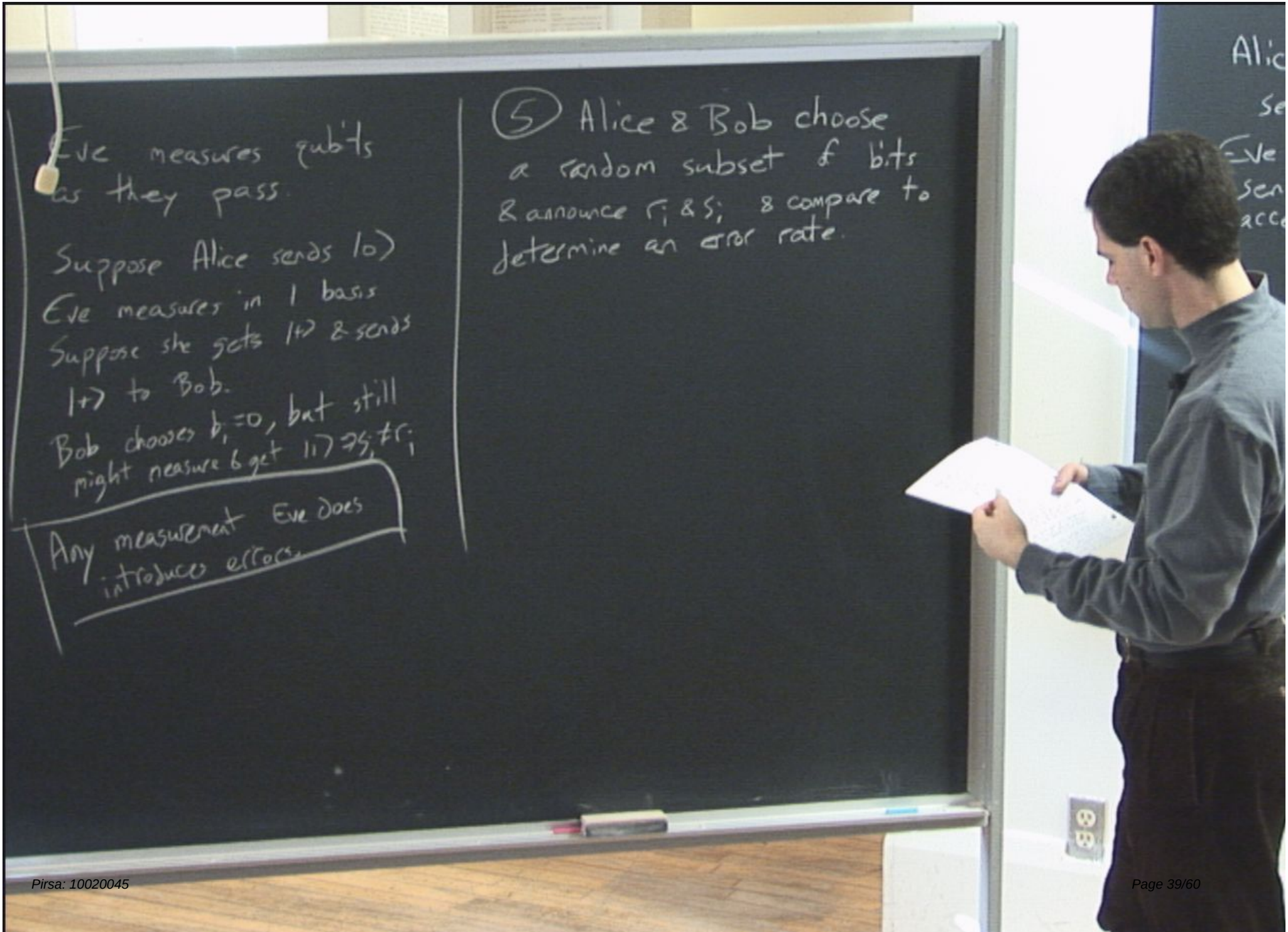

(4) Using classical channel,
Alice & Bob announce e_i & b_i
If $b_i = a_i$, they keep bit i
If $b_i \neq a_i$, they discard bit i
n a perfect world, if $a_i = b_i$)
then $r_i = s_i$
t: - noise could cause errors
- Eve can cause errors.
Eve measures qubits
as they pass.
Suppose Alice sends 1o)

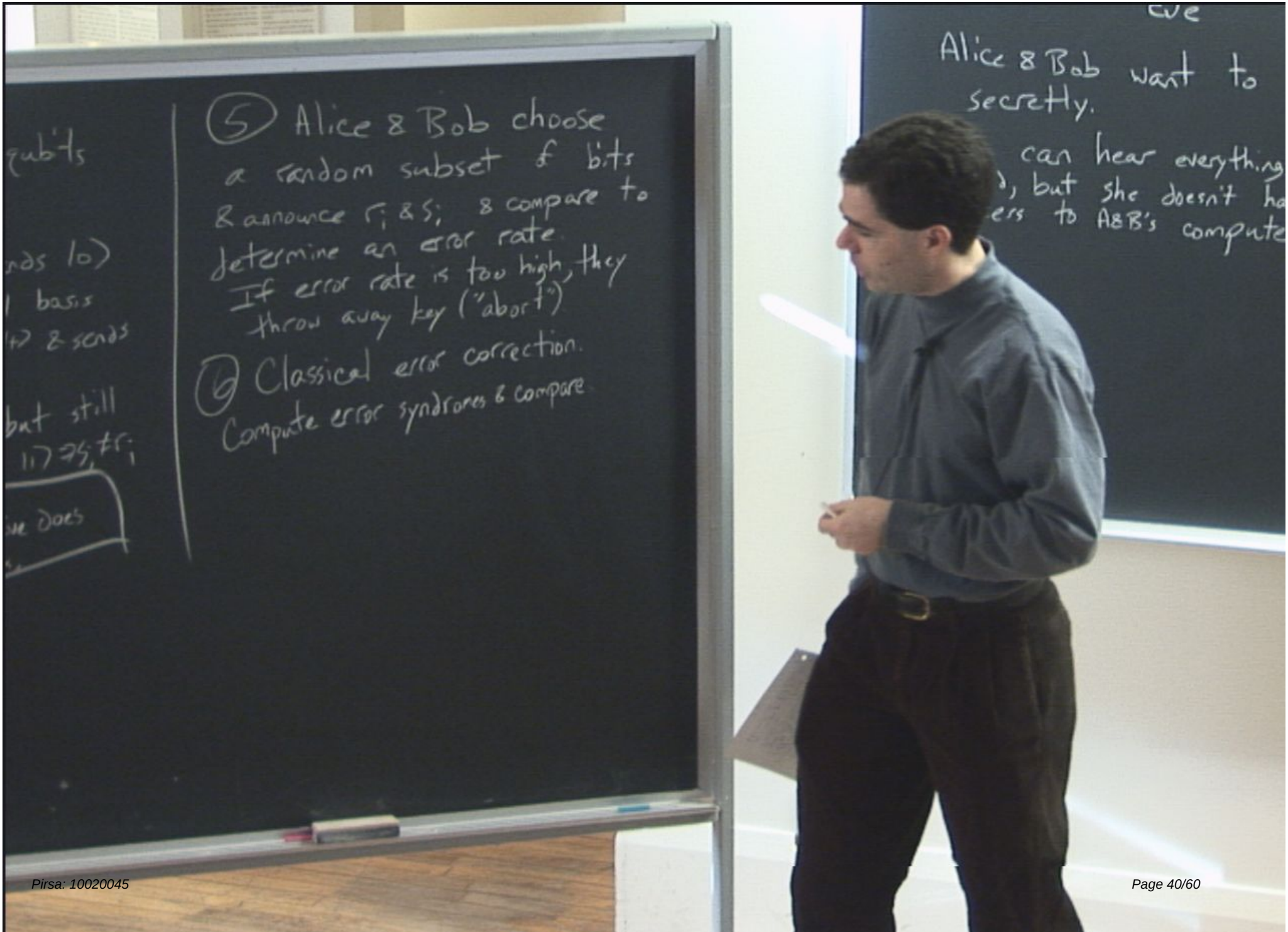

(4) Using classical channel,
Alice & Bob announce a_i & b_i;
If $b_i = a_i$, they keep bit i;
If $b_i \neq a_i$, they discard bit i;
n a perfect world, if $a_i = b_i$,
then $r_i = s_i$.
t: - noise could cause errors
- Eve can cause errors.
Eve measures qubits
as they pass.
Suppose Alice sends |0⟩
Eve measures in I basis

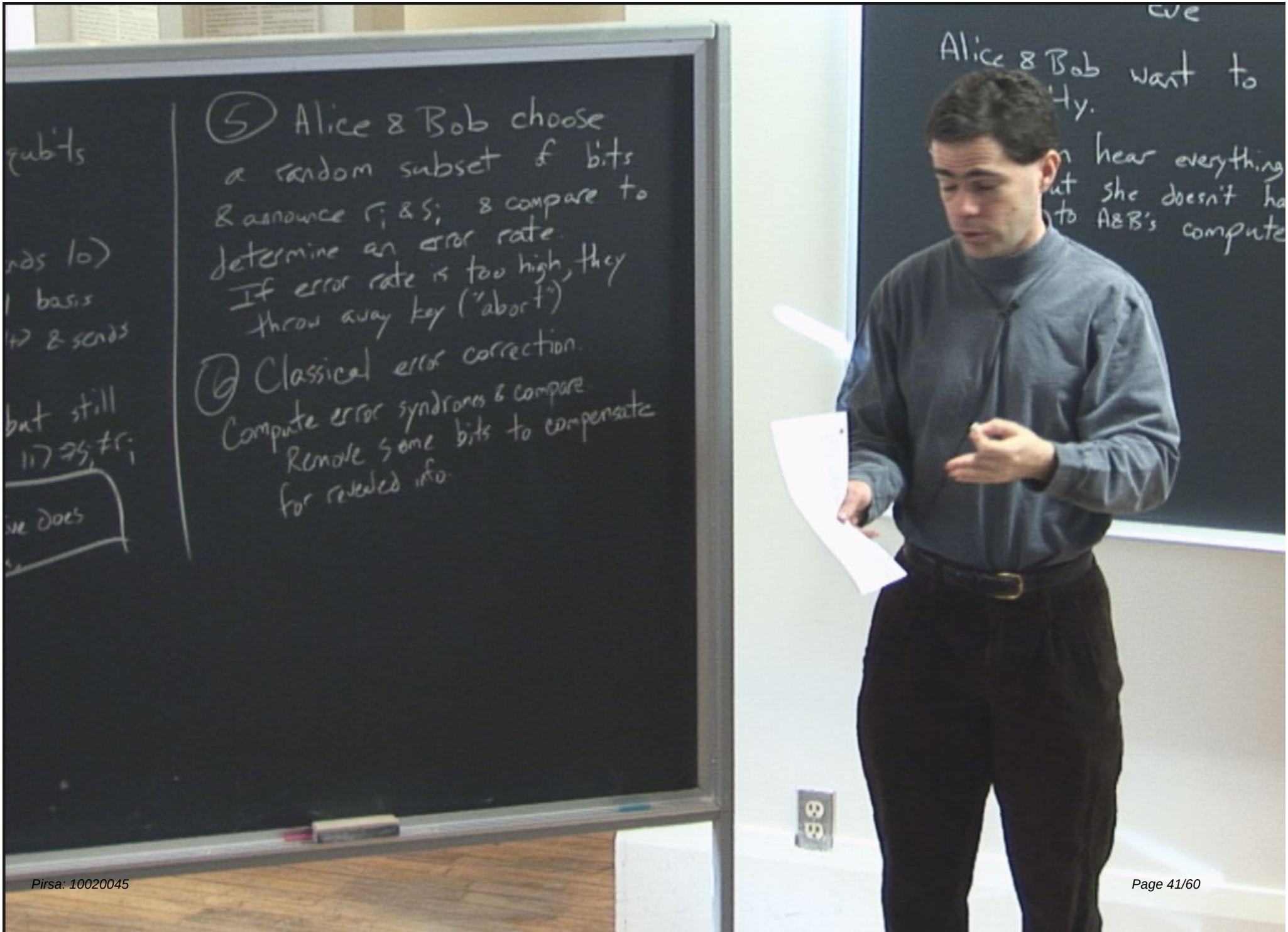

(4) Using classical channel,
Alice & Bob announce a_i & b_i
If $b_i = a_i$, they keep bit i
If $b_i \neq a_i$, they discard bit i
In a perfect world, if $a_i = b_i$
then $r_i = s_i$
But: - noise could cause errors
- Eve can cause errors.
Eve measures qubits
as they pass.
Suppose Alice sends $|0\rangle$
Eve measures in I basis
Suppose she gets $|+\rangle$ & sends
$|+\rangle$ to Bob.

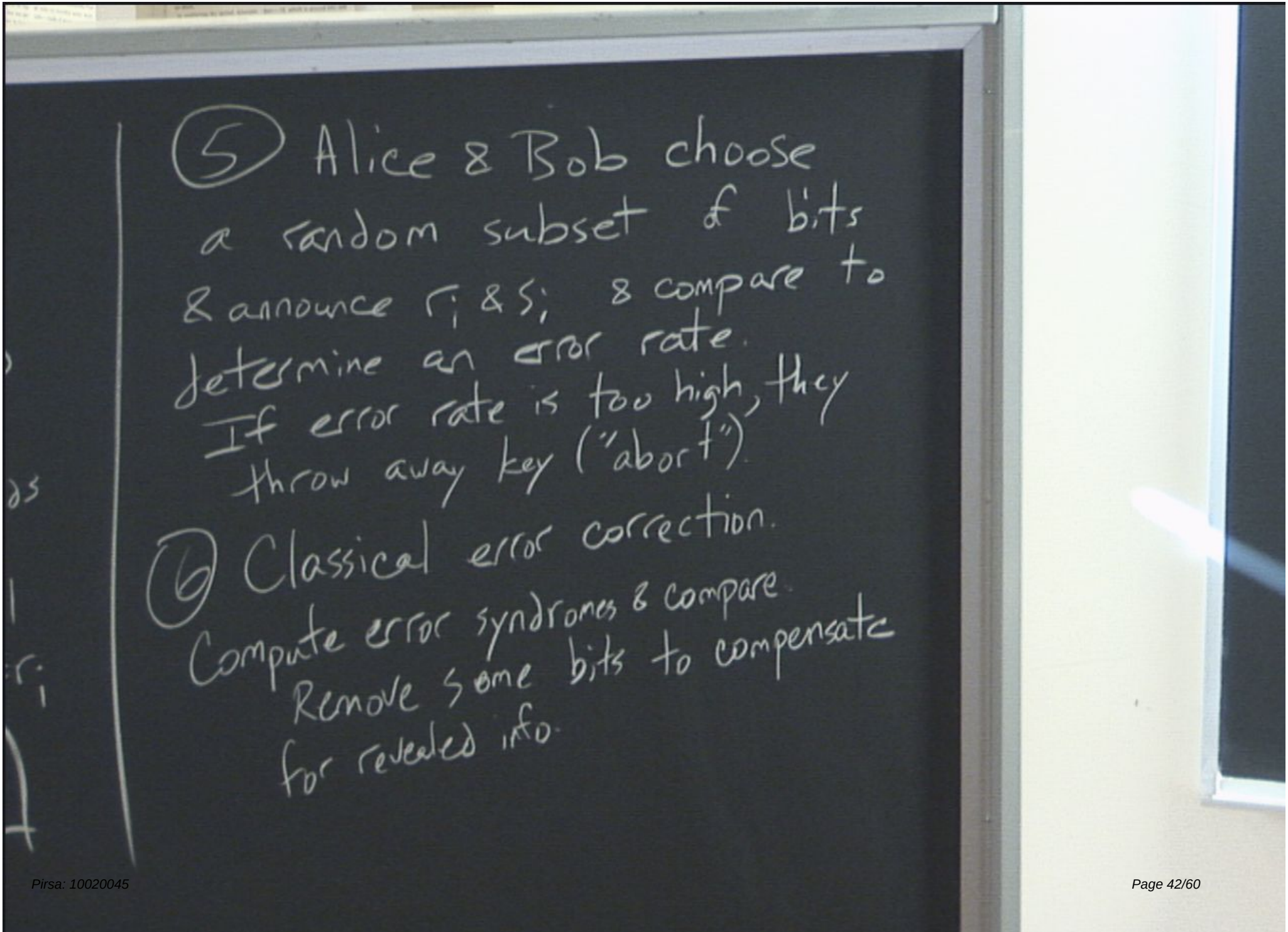

(4) Using classical channel,
Alice & Bob announce a_i & b_i;
If $b_i = a_i$, they keep bit;
If $b_i \neq a_i$, they discard bit;
In a perfect world, if $a_i = b_i$,
then $r_i = s_i$;
- noise could cause errors
- Eve can cause errors.
Eve measures qubits
as they pass
Suppose Alice sends $|0\rangle$
Eve measures in I basis
Suppose she gets $|0\rangle$ & sends
$|0\rangle$ to Bob.
Bob chooses $b_i = 0$, but still
might measure 0 get $|1\rangle \Rightarrow s_i \neq r_i$

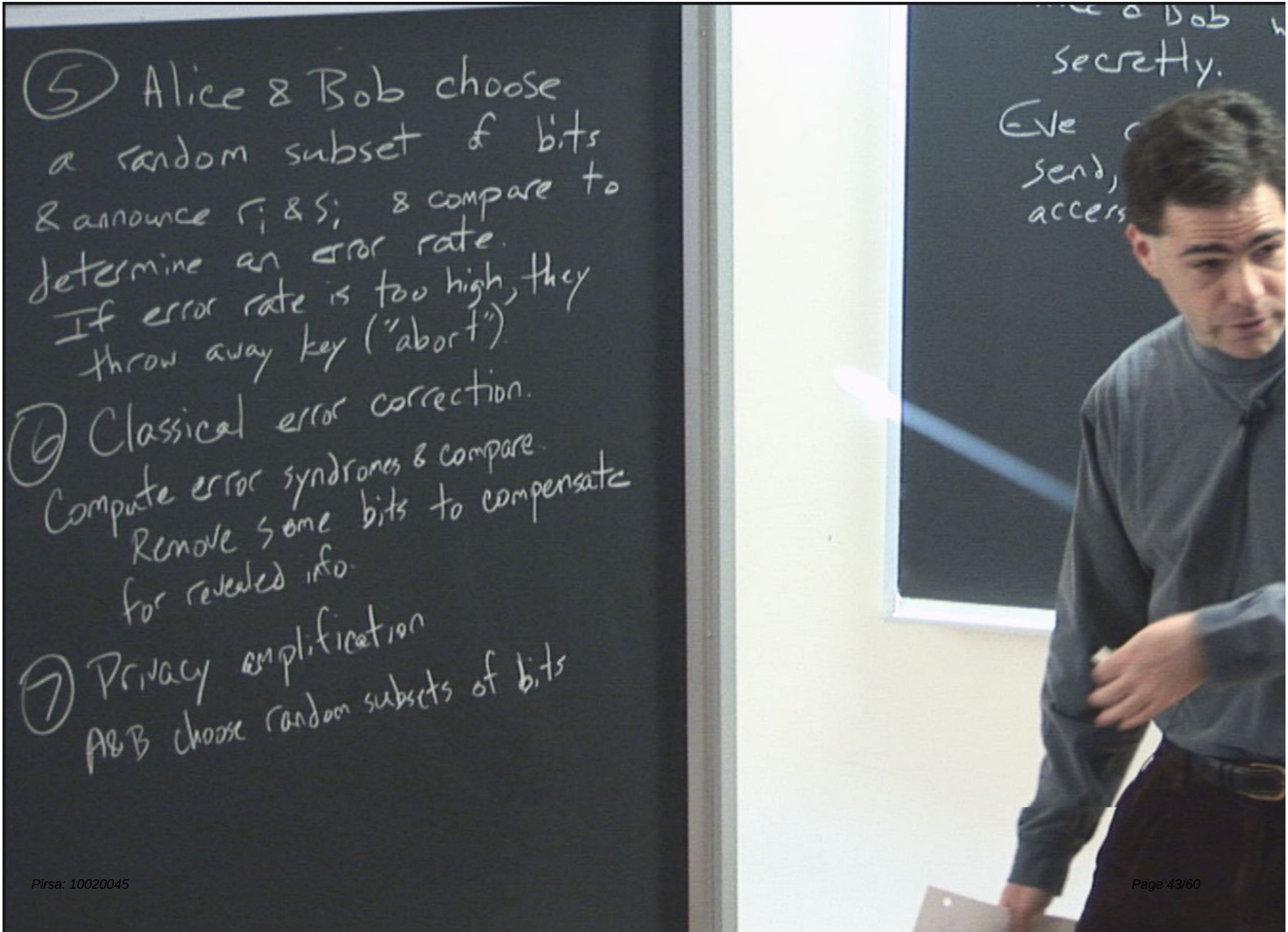

(4) Using classical channel,
Alice & Bob announce a_i & b_i;
If $b_i = a_i$, they keep bit i;
If $b_i \neq a_i$, they discard bit i;
n a perfect world, if $a_i = b_i$)
then $r_i = s_i$.
t: - noise could cause errors
- Eve can cause errors.
Eve measures qubits as they pass.
Suppose Alice sends $|0\rangle$
Eve measures in I basis
Suppose she gets $|+\rangle$ & sends $|+\rangle$ to Bob.
Bob chooses $b_i = 0$, but still might measure & get $|-\rangle$, $s_i \neq r_i$
Any measurement Eve does introduces errors.

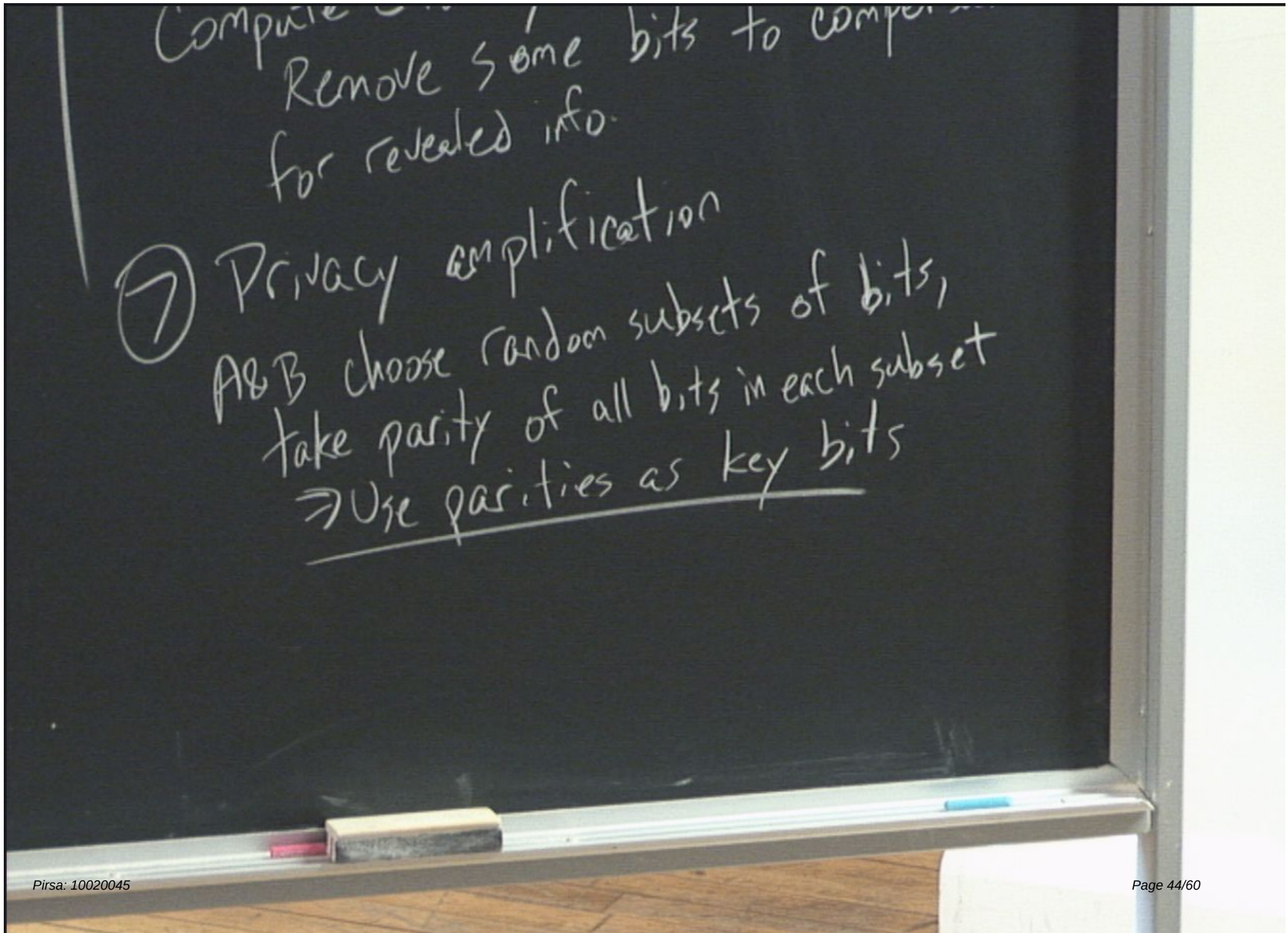

Eve measures qubits as they pass.
Suppose Alice sends |0⟩
Eve measures in I basis
Suppose she gets |+⟩ & sends |+⟩ to Bob.
Bob chooses $b_i = 0$, but still might measure 6 get $1/7 = s_i \neq r_i$
Any measurement Eve does introduces errors.
(5) Alice & Bob choose a random subset of bits & announce r_i & s_i & compare to determine an error rate.


qubits
basis
& sends
but still
Alice does
(5) Alice & Bob choose a random subset of bits & announce r_i & s_i & compare to determine an error rate. If error rate is too high, they throw away key ("abort")
(6) Classical error correction. Compute error syndromes & compare.
Alice & Bob want to secretly.
can hear everything
but she doesn't ha
ers to A&B's compute


qubits
basis
but still
(5) Alice & Bob choose
a random subset of bits
& announce r_i & s_i & compare to
determine an error rate.
If error rate is too high, they
throw away key ("abort")
(6) Classical error correction.
Compute error syndromes & compare
Remove some bits to compensate
for revealed info.
Alice & Bob want to
hear everything
she doesn't
A&B's


(5) Alice & Bob choose
a random subset of bits
& announce r_i & s_i & compare to
determine an error rate.
If error rate is too high, they
throw away key ("abort")
(6) Classical error correction.
Compute error syndromes & compare.
Remove some bits to compensate
for revealed info.


(5) Alice & Bob choose
a random subset of bits
& announce r_i & s_i & compare to
determine an error rate.
If error rate is too high, they
throw away key ("abort")
(6) Classical error correction.
Compute error syndromes & compare.
Remove some bits to compensate
for revealed info.
(7) Privacy amplification
A&B choose random subsets of bits
secretly.
Eve
send,
acces


Remove some bits to compen
for revealed info.
⑦ Privacy amplification
A & B choose random subsets of bits,
take parity of all bits in each subset
⇒ Use parities as key bits

Defects of one-time pad

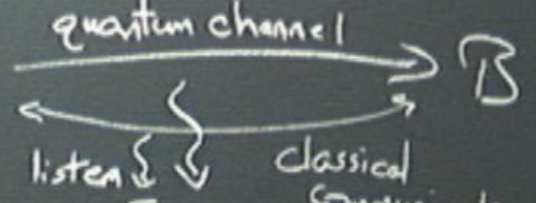
k must be kept secure.

k can only be used once.
needs to be as long as m.

se twice:
$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



BB84 " Bennett Brassard

(1) Alice generate N pairs of
random bits (a_i, r_i) $i = 1, \ldots$

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

(2) Alice sends
corresponding
to Bob

(3) Bob ch
for each
if that

Defects of one-time pad

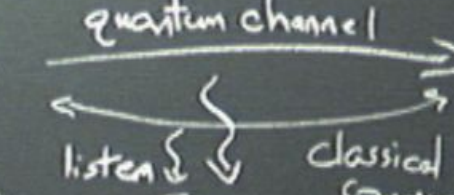
k must be kept secure.

k can only be used once.
needs to be as long as m.

se twice:
$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

AES symmetric cryptosystem.

Quantum key distribution (QKD)



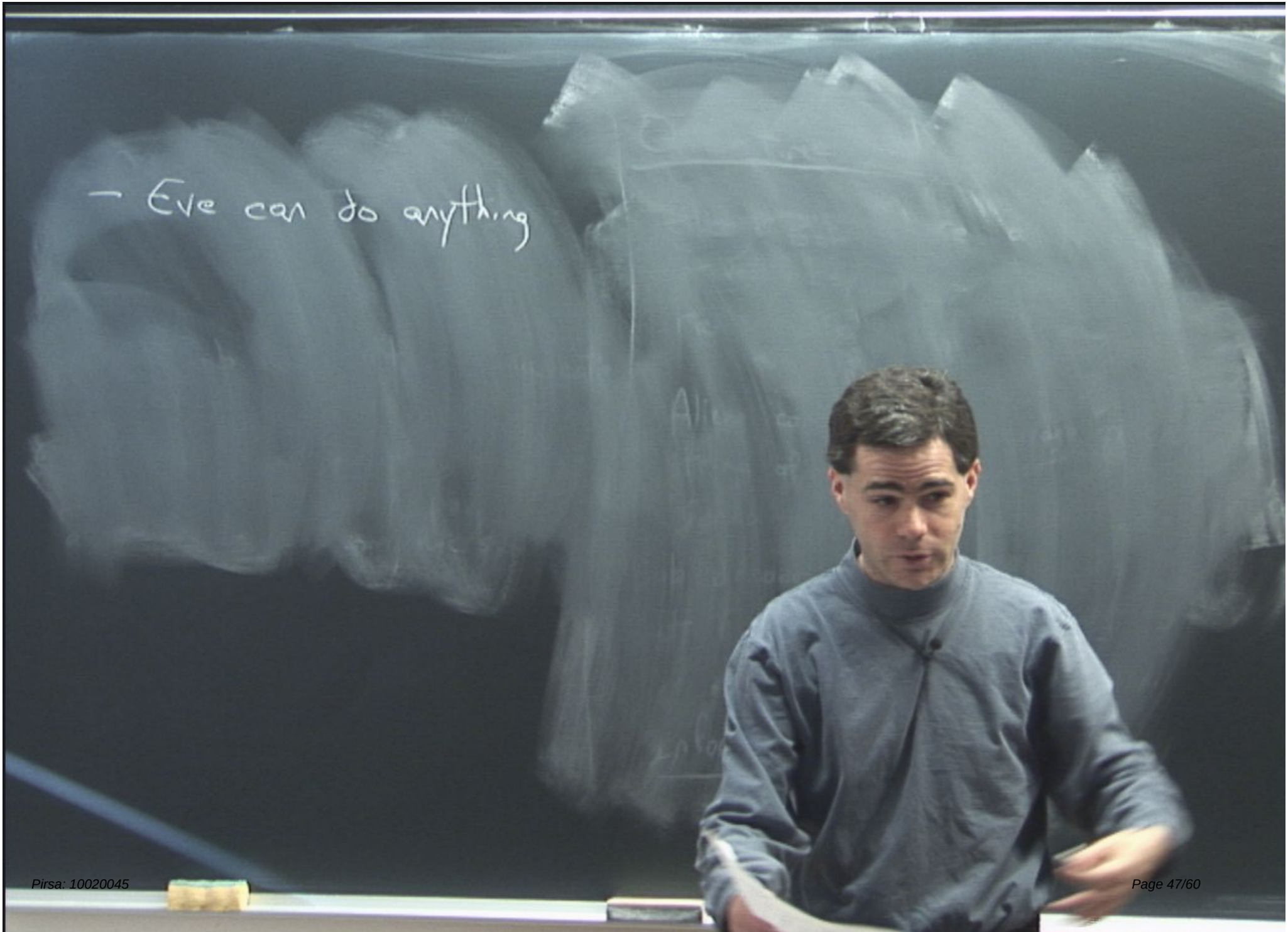
BB84 "Bennett Brassard 1984"

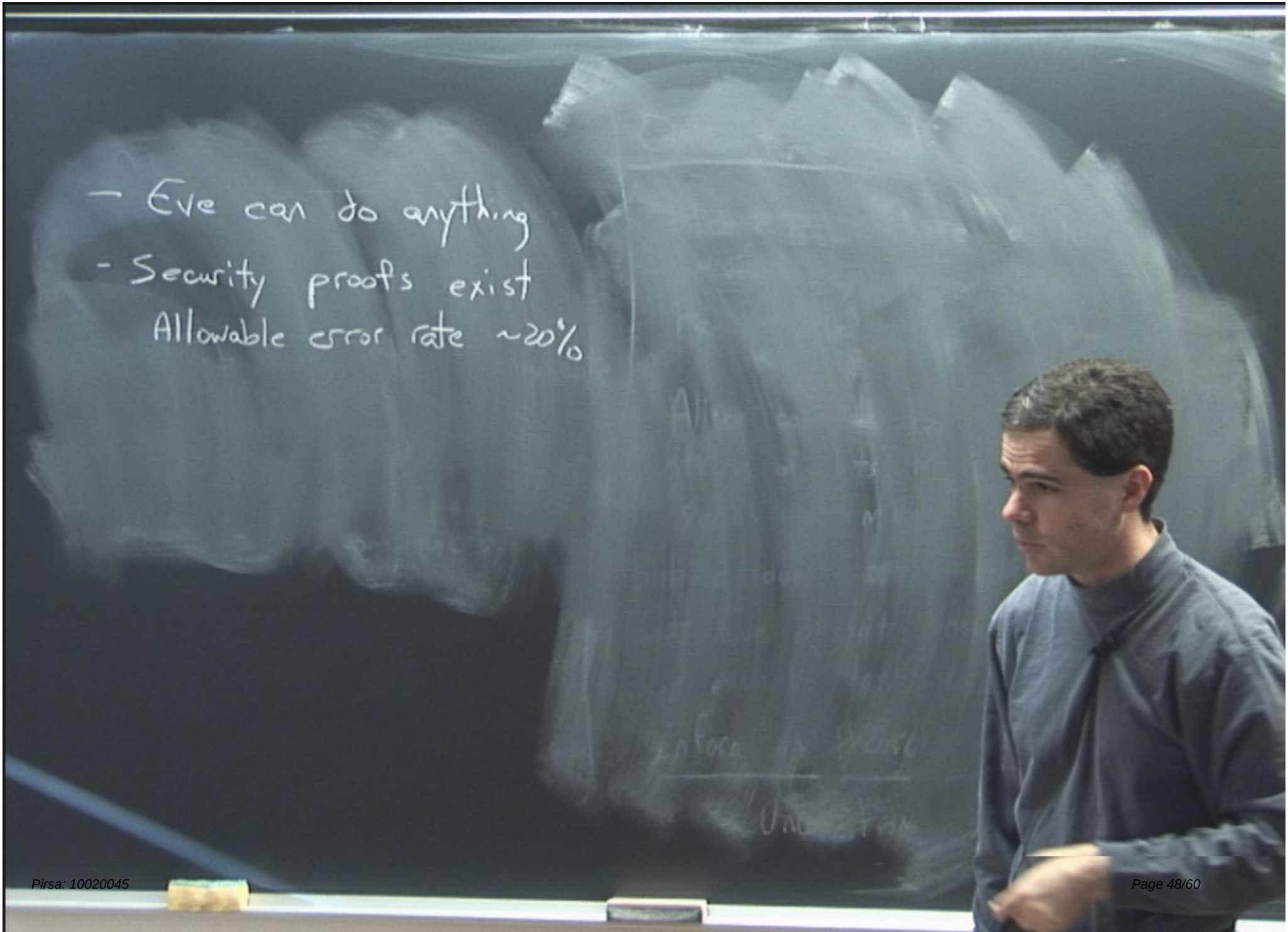
(1) Alice generate N pairs of random bits (a_i, r_i) $i = 1, \ldots, N$

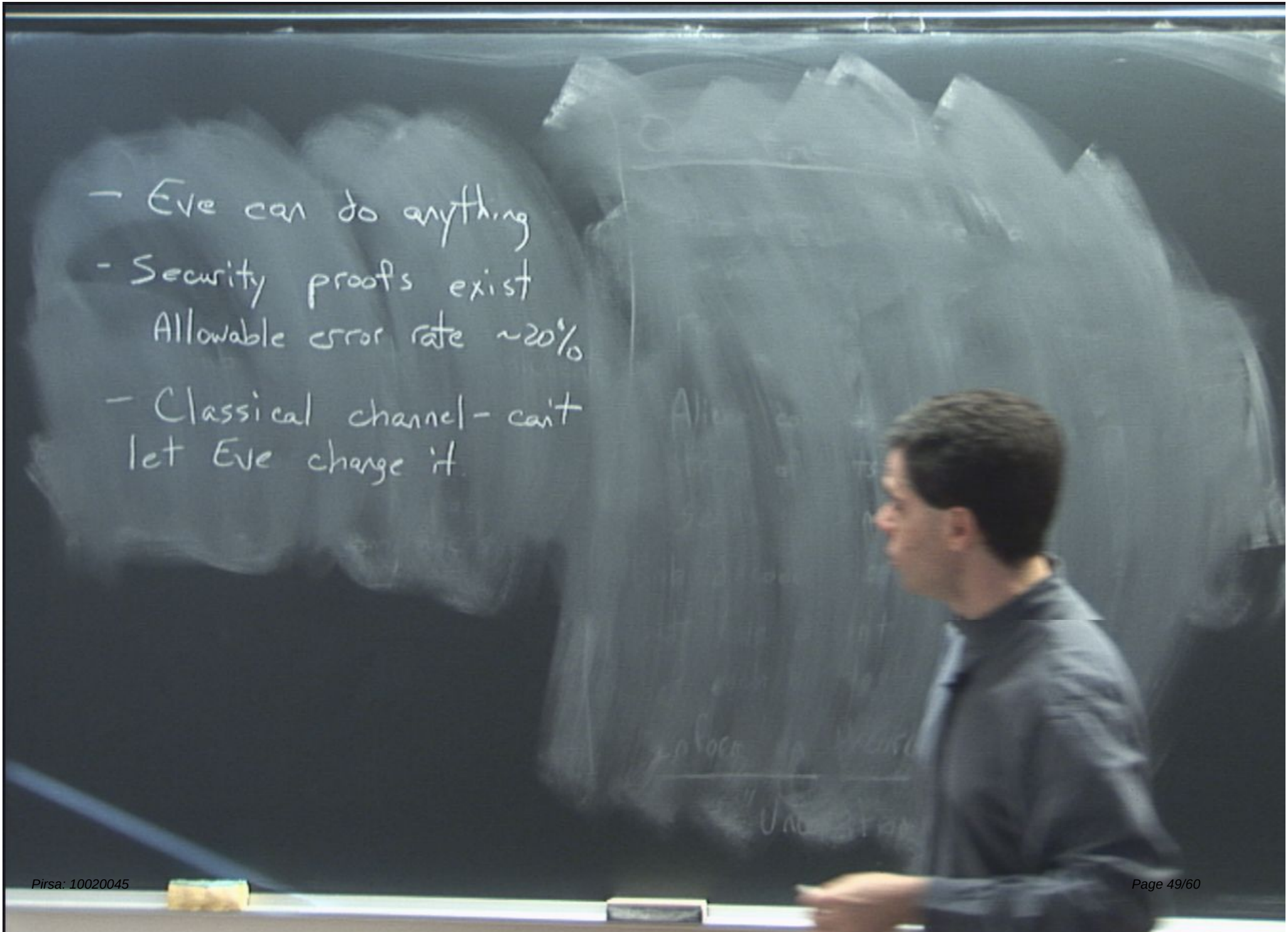
a_i	r_i	
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle = \|0\rangle + \|1\rangle$
1	1	$\|-\rangle = \|0\rangle - \|1\rangle$

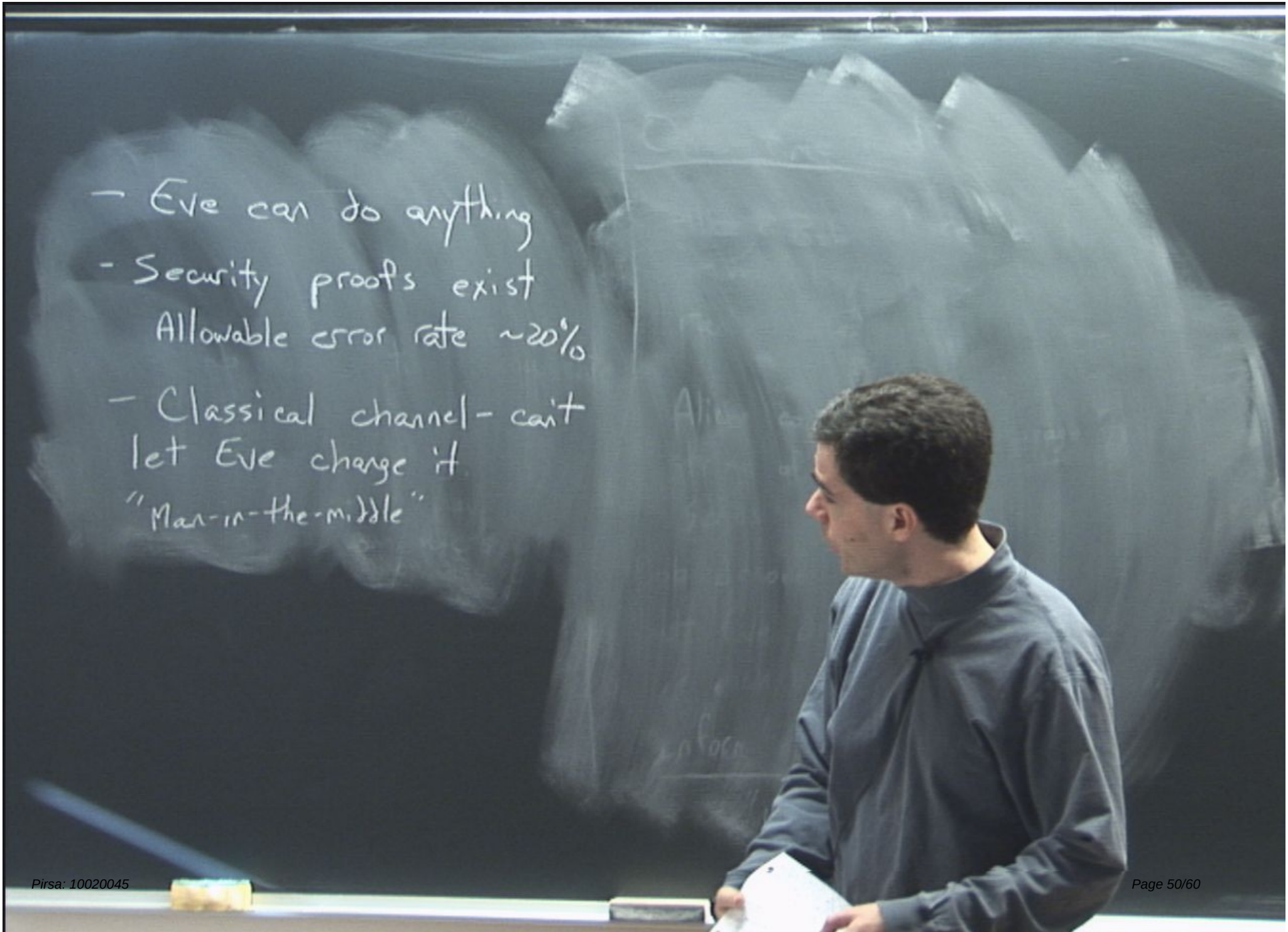
(2) Alice sends the corresponding qubits to Bob for each i.

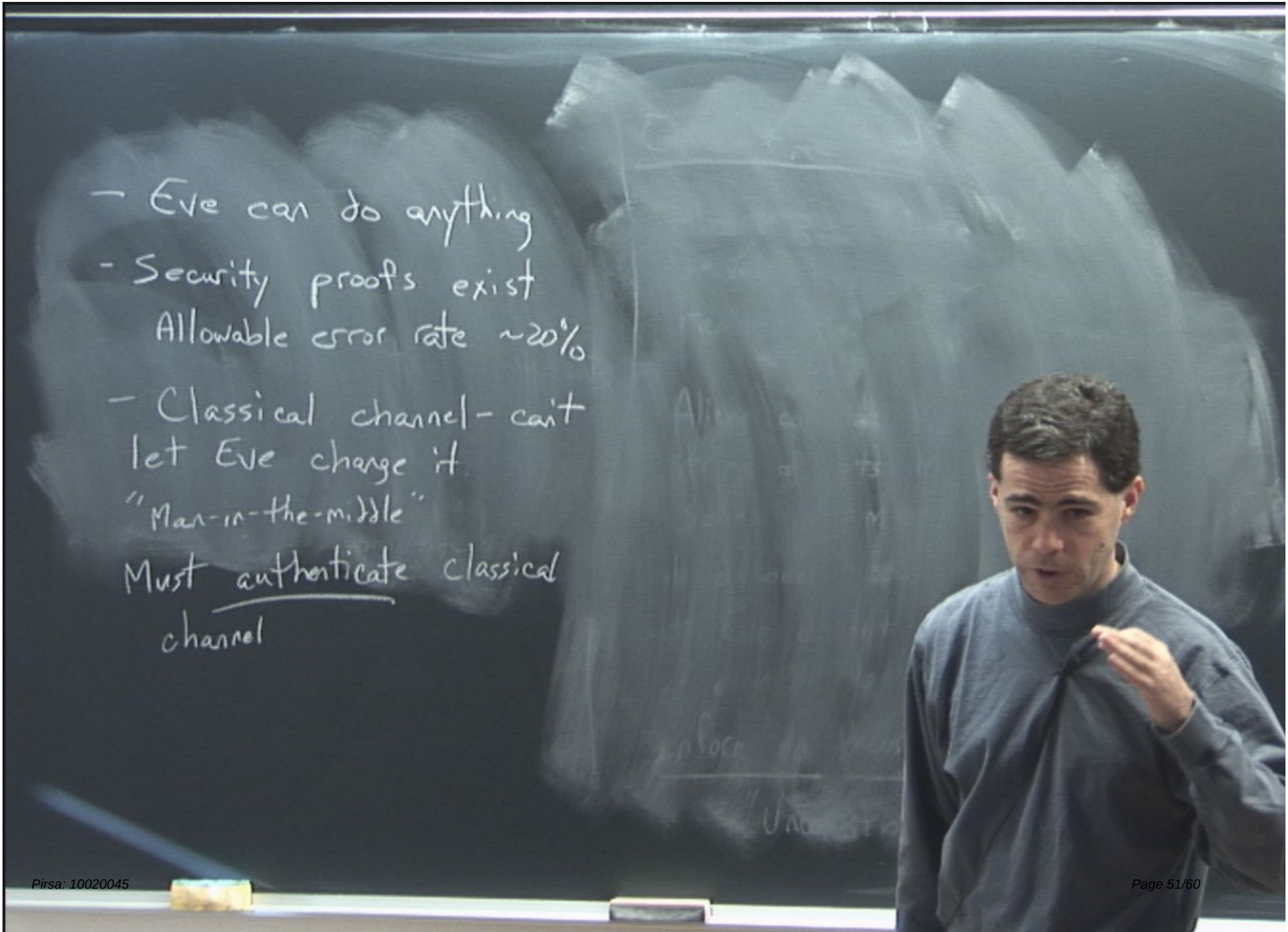
(3) Bob chooses a random basis for each qubit & measures it in that basis — gets s_i

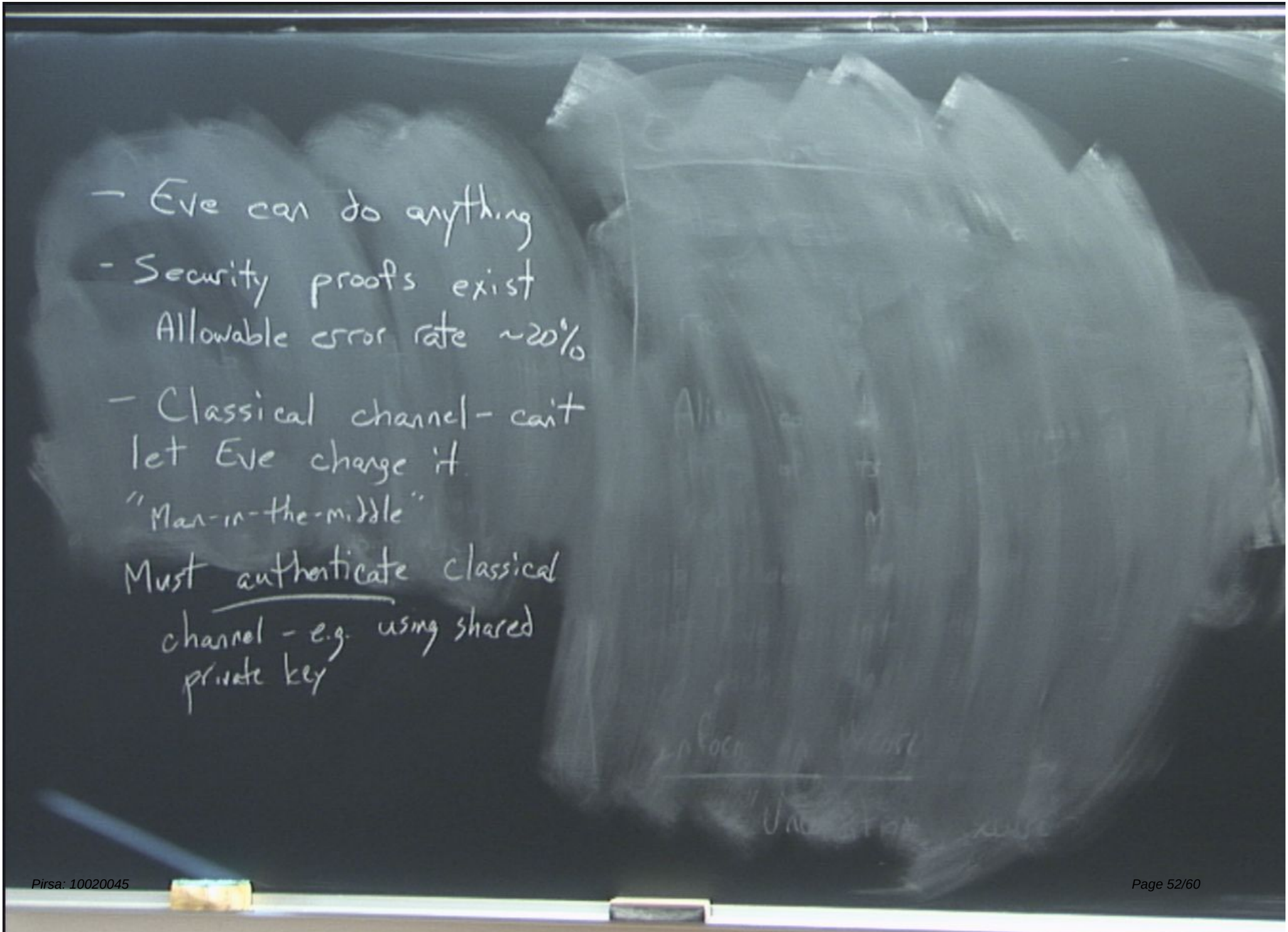

– Eve can do anything

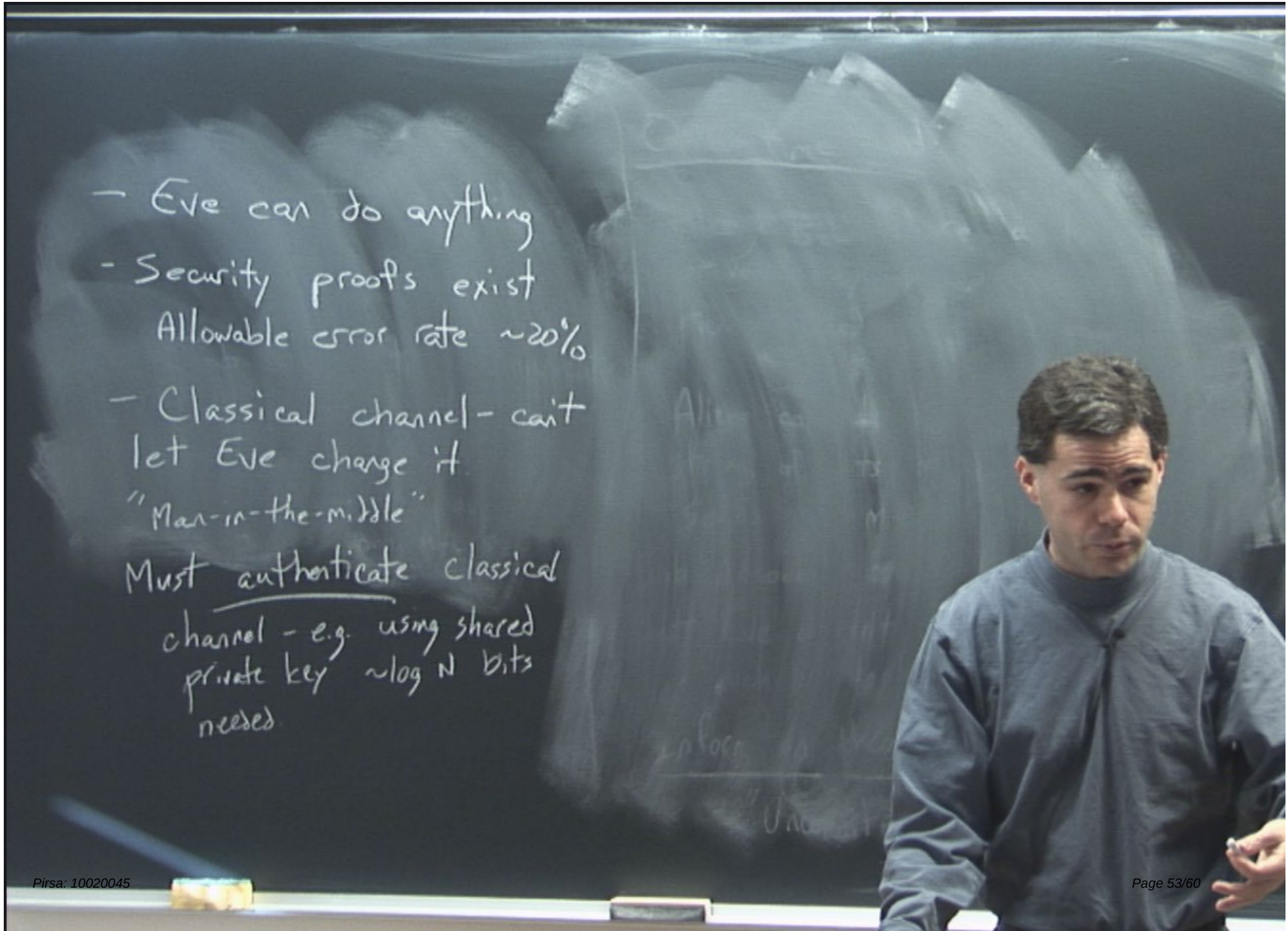

- Eve can do anything
- Security proofs exist
Allowable error rate ~20%


- Eve can do anything
- Security proofs exist
Allowable error rate ~20%
- Classical channel - can't let Eve change it


- Eve can do anything
- Security proofs exist
Allowable error rate ~20%
- Classical channel - can't let Eve change it
"Man-in-the-middle"


- Eve can do anything
- Security proofs exist
Allowable error rate ~20%
- Classical channel - can't let Eve change it
"Man-in-the-middle"
Must authenticate classical channel


- Eve can do anything
- Security proofs exist
Allowable error rate ~20%
- Classical channel - can't let Eve change it
"Man-in-the-middle"
Must authenticate classical channel - e.g. using shared private key


- Eve can do anything
- Security proofs exist
Allowable error rate ~20%
- Classical channel - can't let Eve change it
"Man-in-the-middle"
Must authenticate classical channel - e.g. using shared private key ~log N bits needed

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Frequently use weak coherent states

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Frequently use weak coherent states
  $p \approx 0.1 \Rightarrow$ 90% no photons
  10% 1 photon
  ~1% 32 photons
- Loss in channel & dete[illegible] low efficiency (~5-15%)

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Frequently use weak coherent states
  $p \approx 0.1 \Rightarrow$ 90% no photons
  10% 1 photon
  ~1% 32 photons
- Loss in channel & detectors have low efficiency (~5-15%)

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
  Need to account for imperfection
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Frequently use weak coherent state
  $p \approx 0.1 \Rightarrow$ 90% no photons
  10% 1 photon
  ~1% 32 photons
- Loss in channel & detectors have lo efficiency (~5-15%)

- Eve can do anything
- Security proofs exist
  Allowable error rate ~20%
  Need to account for imperfections
- Classical channel - can't let Eve change it
  "Man-in-the-middle"

Must authenticate classical channel - e.g. using shared private key ~log N bits needed

QKD experimentally
photons through optical fibers
through open air

- Frequently use weak coherent states
  $p \approx 0.1 \Rightarrow$ 90% no photons
  10% 1 photon
  ~1% 32 photons
- Loss in channel & detectors have low efficiency (~5-15%)
- Range limit ~100 km