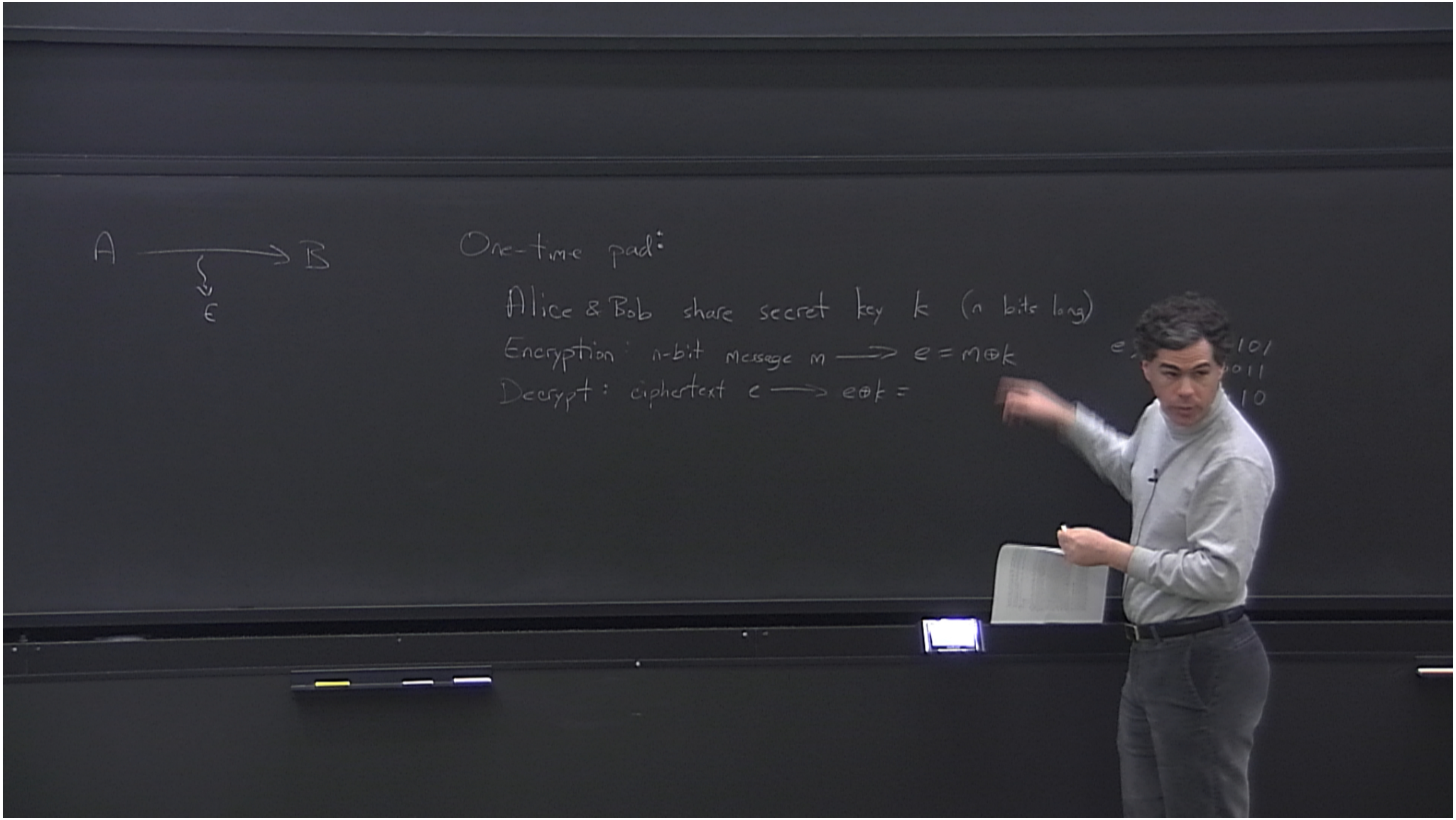
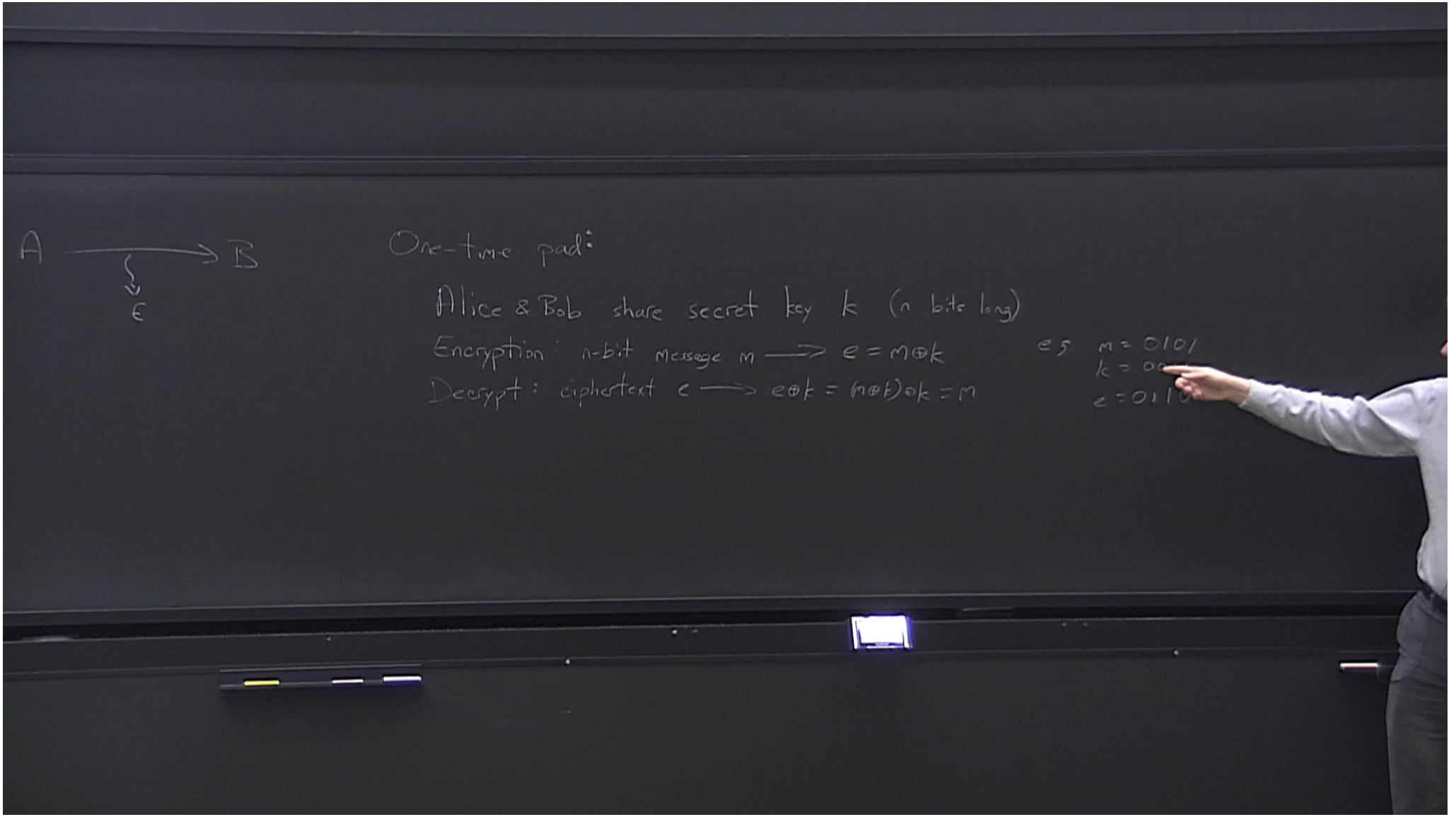
Title: Quantum Information Review-12

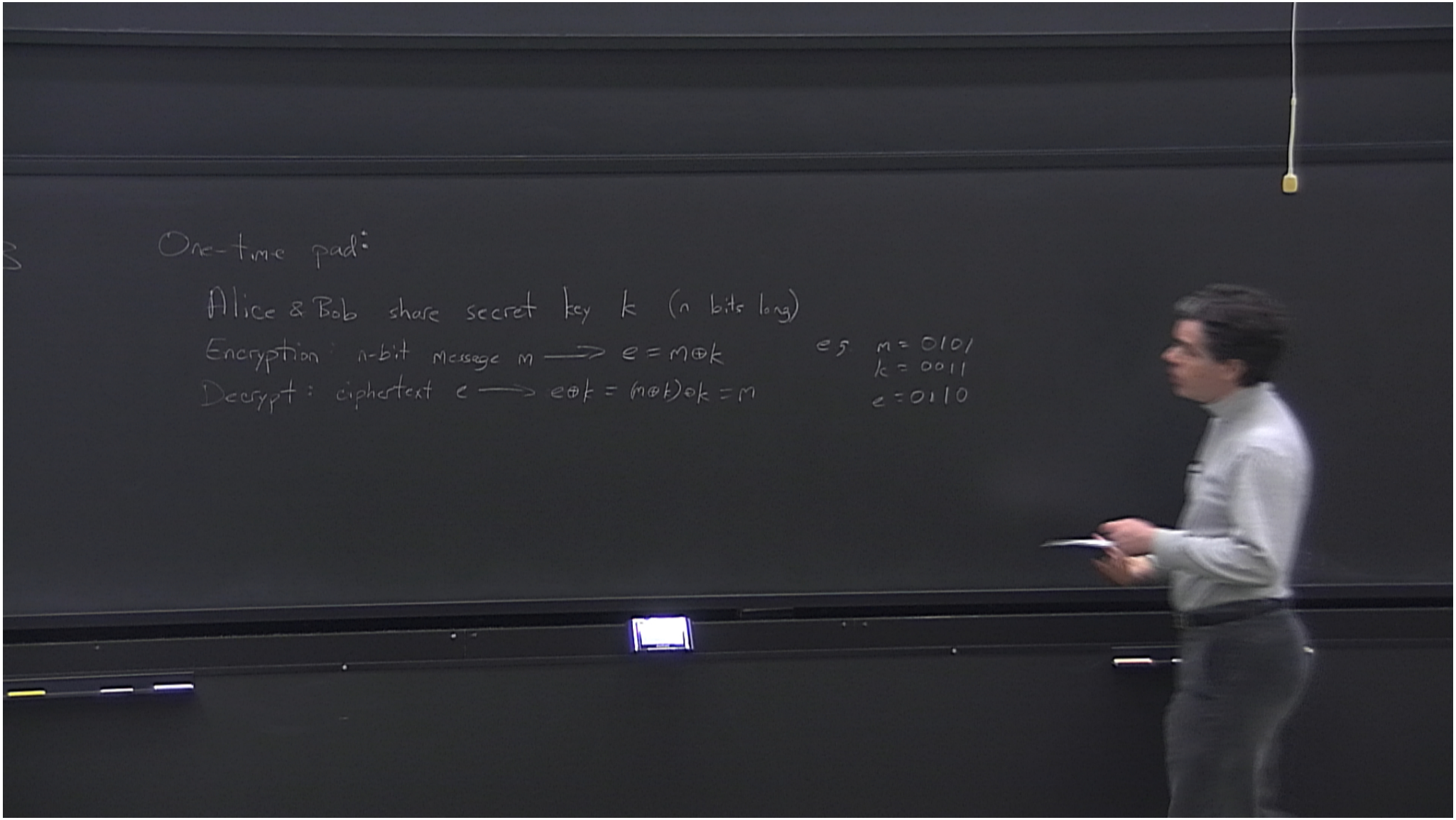
Date: Mar 04, 2015 11:30 AM

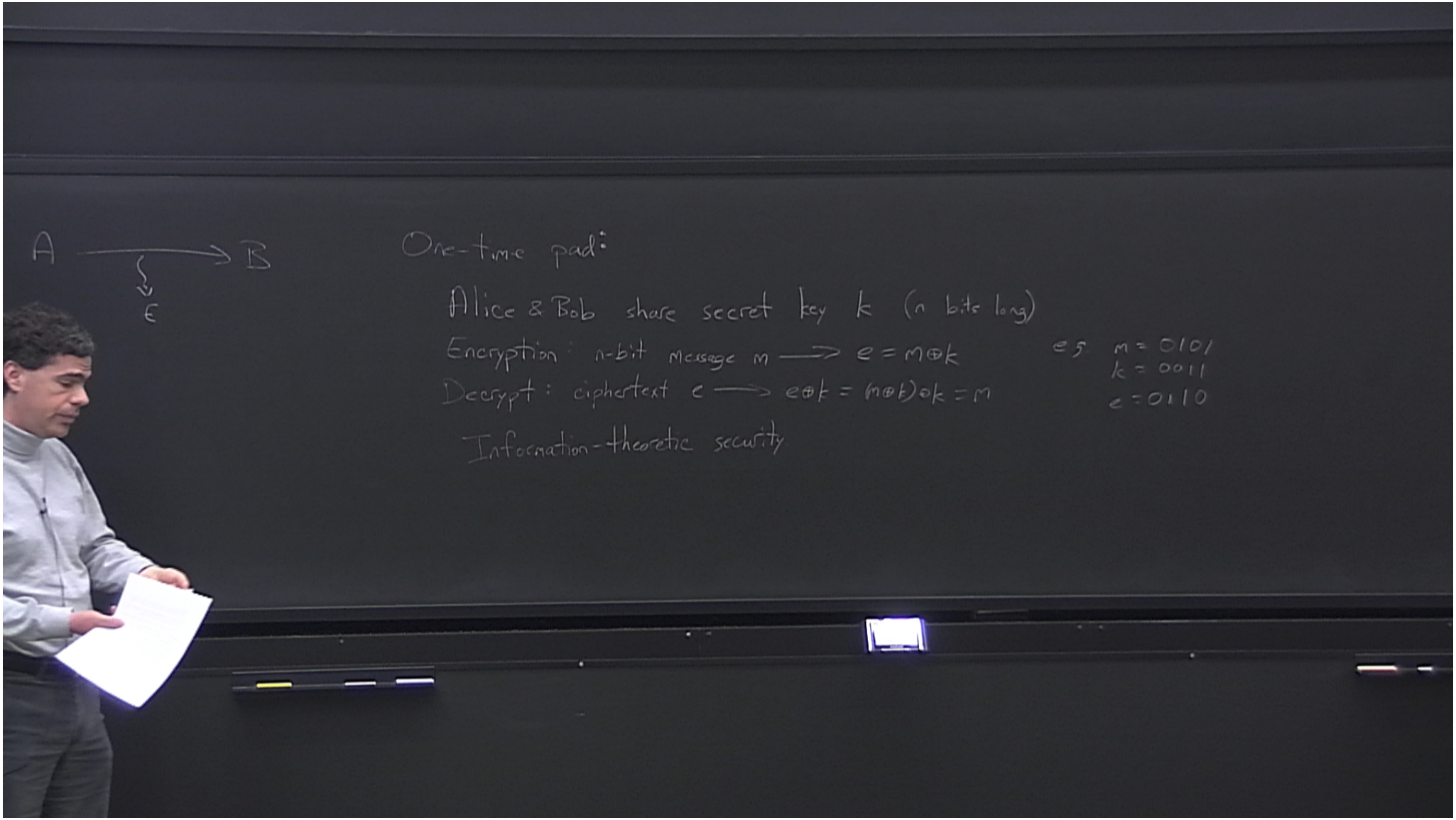
URL: http://pirsa.org/15030015

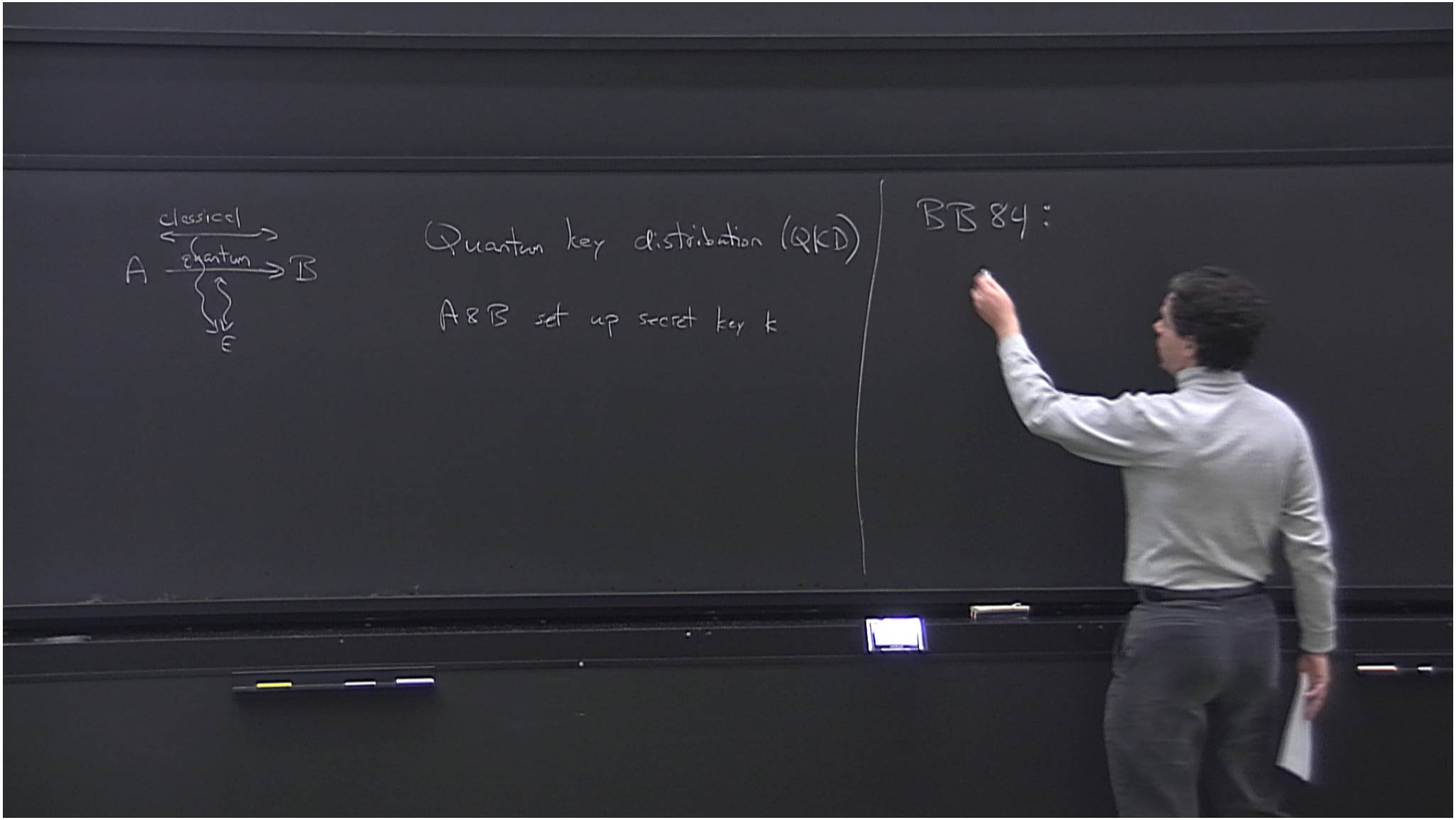
Abstract:

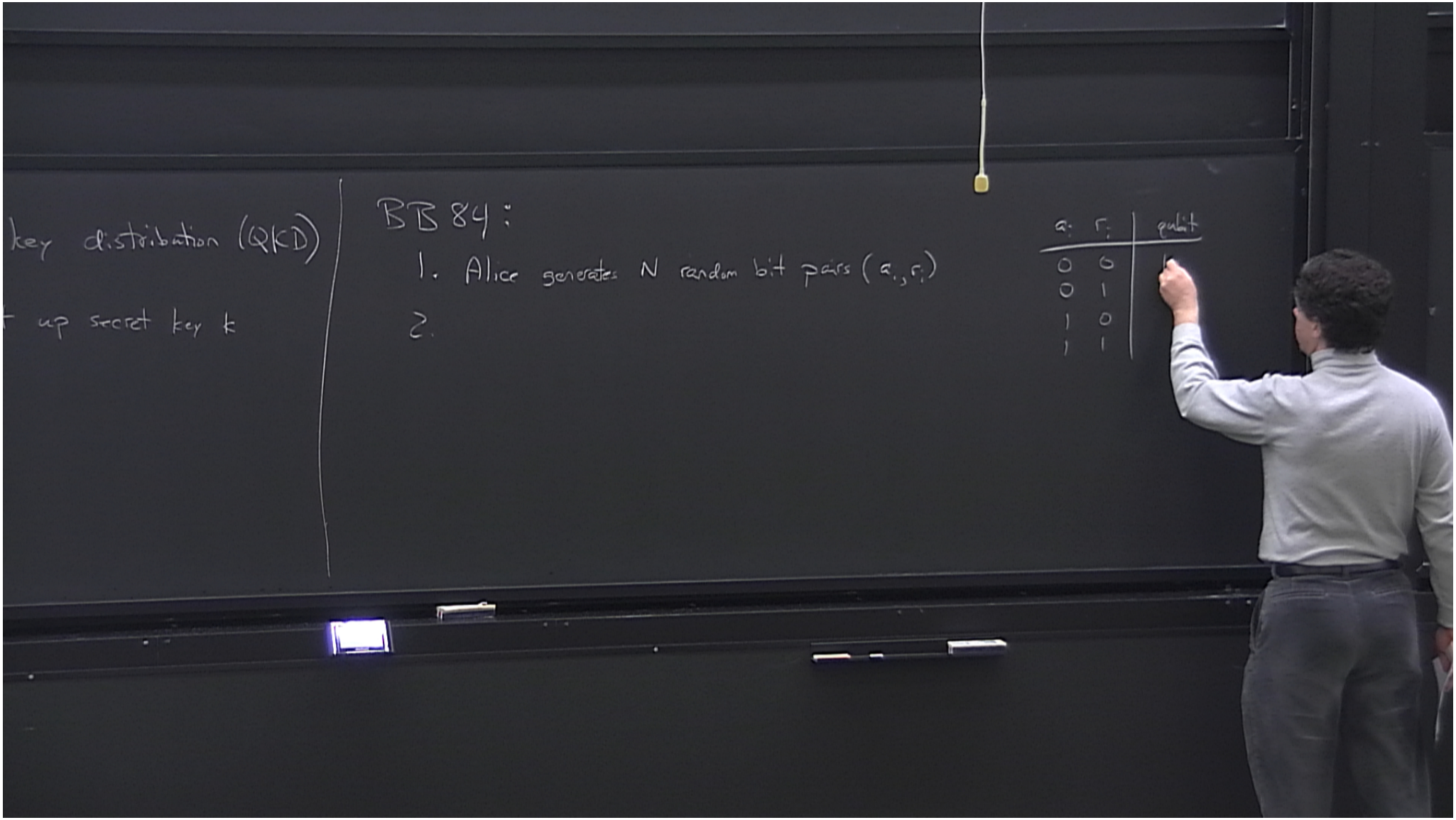

A
B
E
One-time pad:
Alice & Bob share secret key k (n bits long)
Encryption: n-bit message m ⟶ e = m⊕k
Decrypt: ciphertext e ⟶ e⊕k =

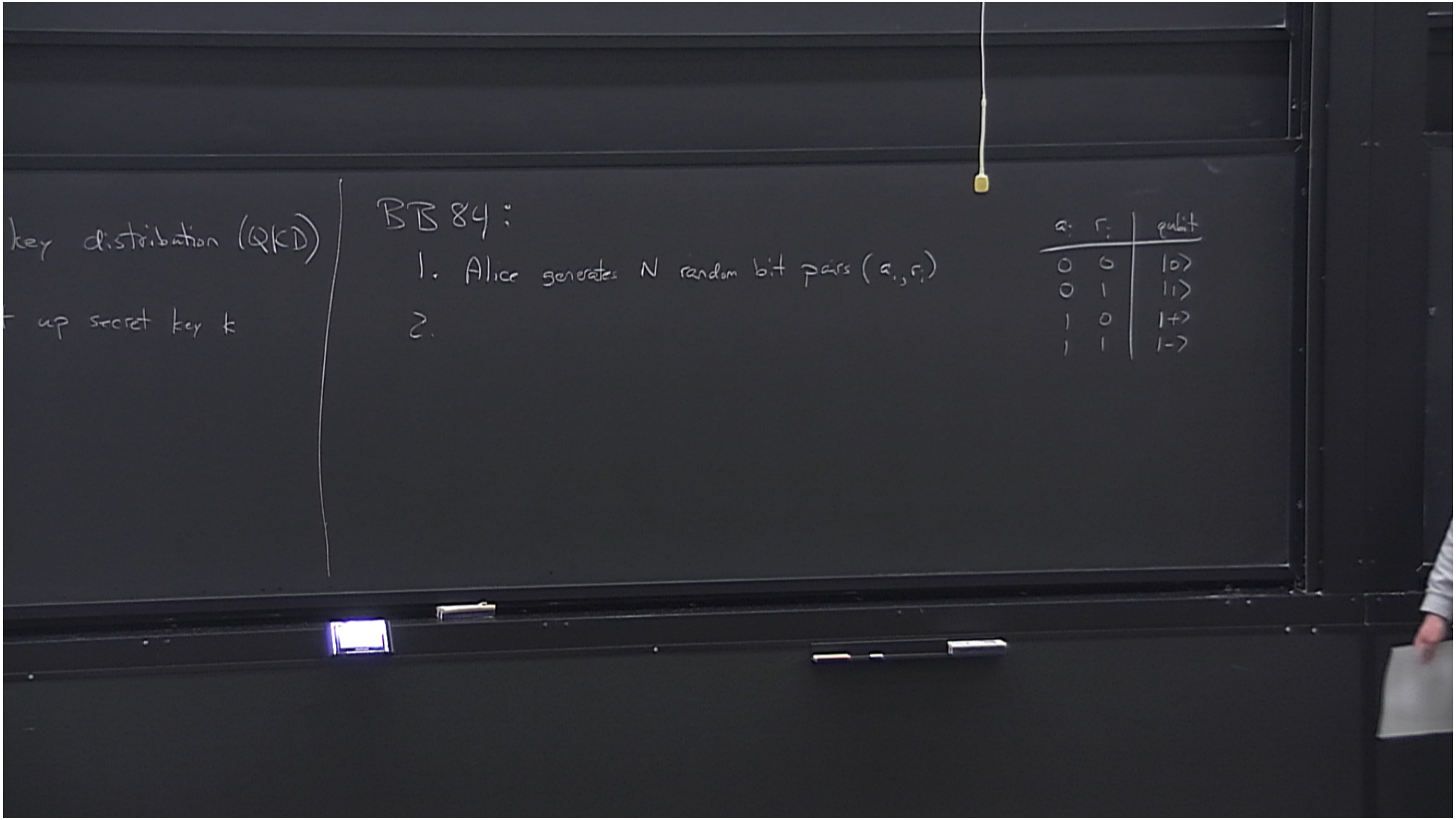

A
B
e
One-time pad:
Alice & Bob share secret key k (n bits long)
Encryption: n-bit message m → e = m⊕k
Decrypt: ciphertext e → e⊕k = (m⊕k)⊕k = m
eg m = 0101
k = 0
e = 0 1

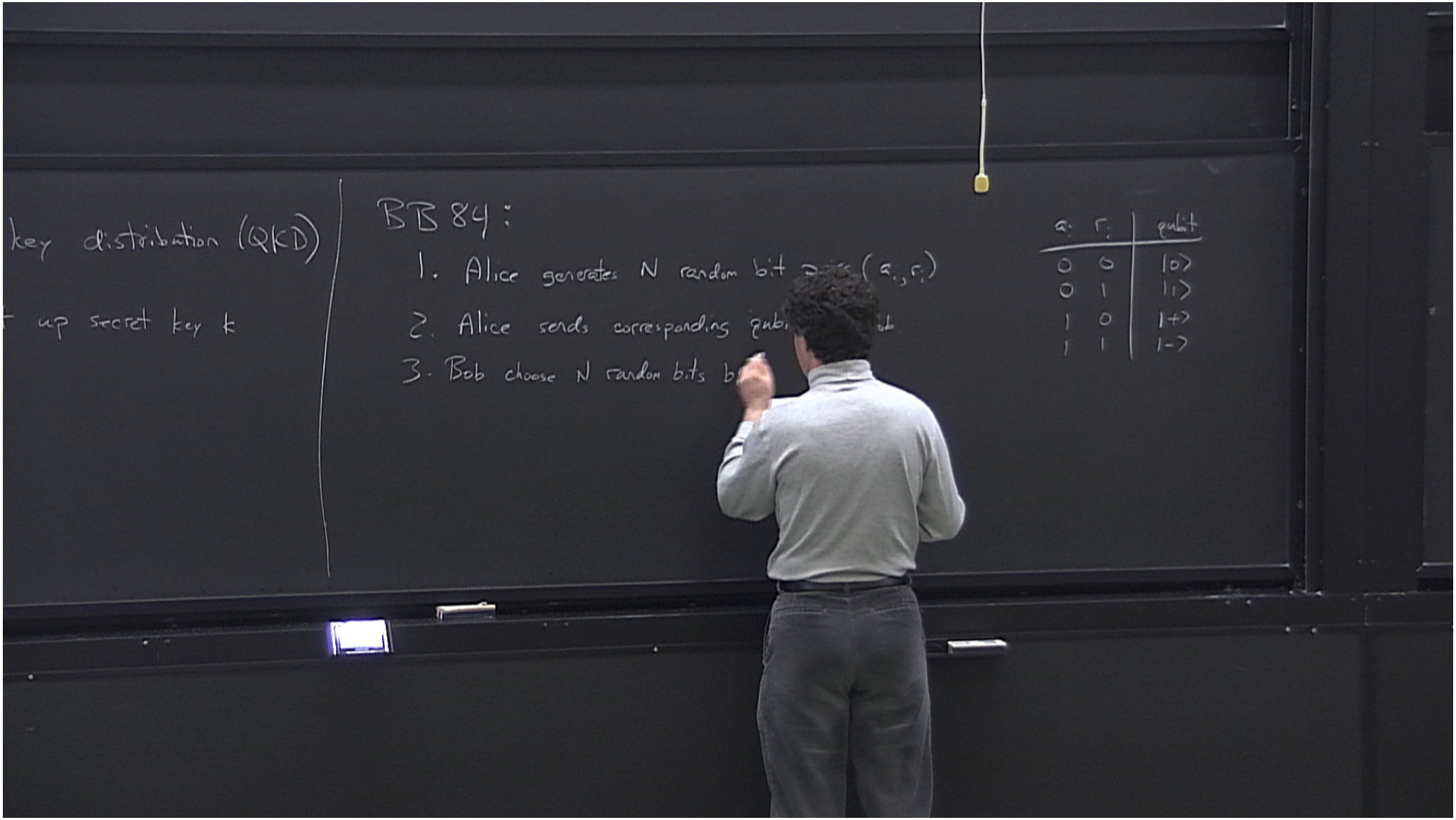

One-time pad:
Alice & Bob share secret key k (n bits long)
Encryption: n-bit message m ⟶ e = m⊕k
Decrypt: ciphertext e ⟶ e⊕k = (m⊕k)⊕k = m
eg m = 0101
k = 0011
e = 0110

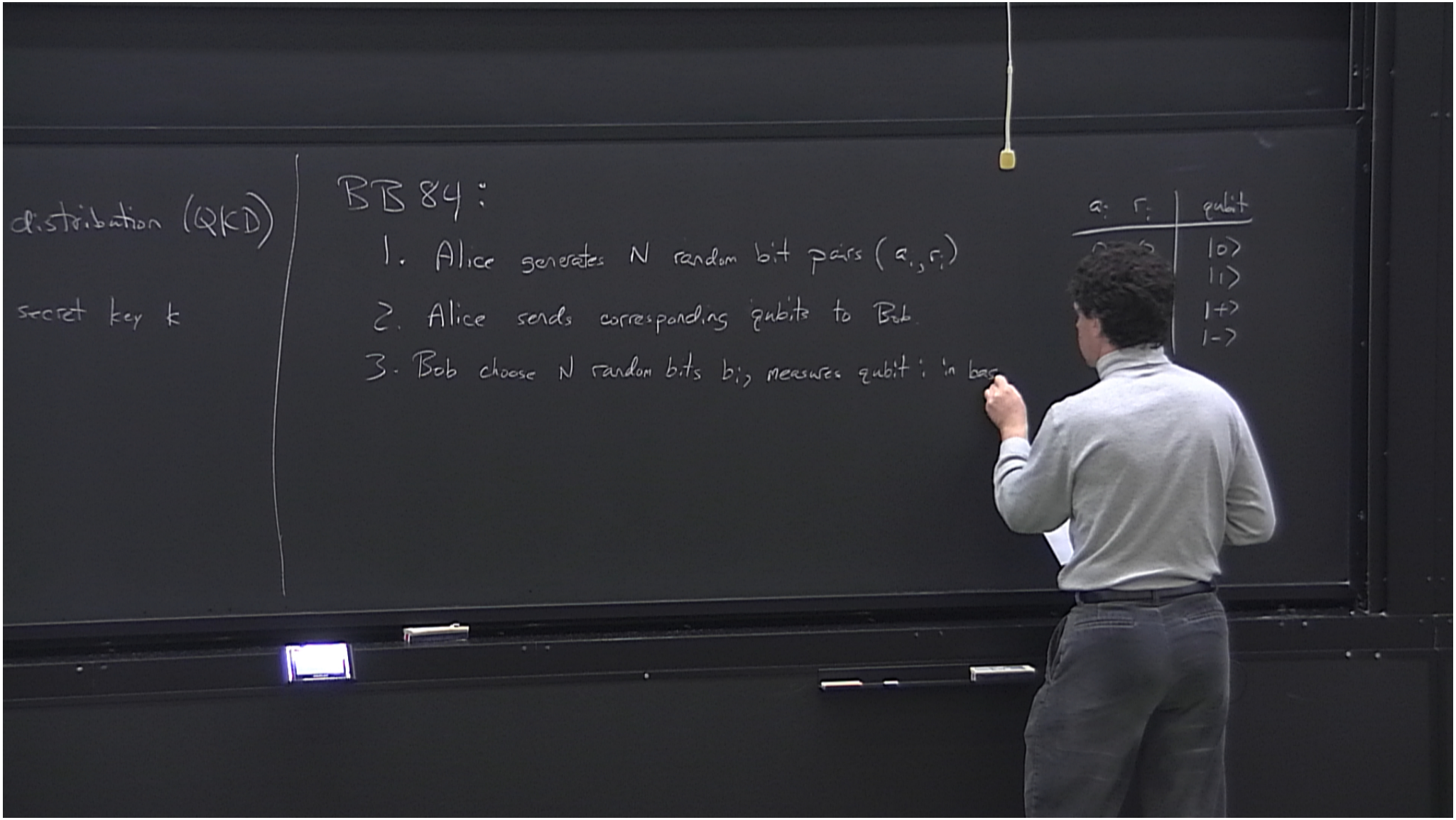

A
B
E
One-time pad:
Alice & Bob share secret key k (n bits long)
Encryption: n-bit message m → e = m⊕k
Decrypt: ciphertext e → e⊕k = (m⊕k)⊕k = m
Information-theoretic security
eg m = 0101
k = 0011
e = 0110


classical
quantum
A
B
E
Quantum key distribution (QKD)
A & B set up secret key k
BB 84:


key distribution (QKD)
up secret key k
BB84:
1. Alice generates N random bit pairs (a_i, r_i)
2.
a_i r_i | qubit
0 0
0 1
1 0
1 1


key distribution (QKD)
up secret key k
BB84:
1. Alice generates N random bit pairs (a_i, r_i)
2.
a_i r_i | qubit
0 0 | |0>
0 1 | |1>
1 0 | |+>
1 1 | |->
Pirsa: 15030015
Page 8/25


key distribution (QKD)
up secret key k
BB84:
1. Alice generates N random bit
2. Alice sends corresponding
3. Bob choose N random bits
a_i r_i | qubit
0 0 | |0>
0 1 | |1>
1 0 | |+>
1 1 | |->
Alice


distribution (QKD)
secret key k
BB84:
1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i; measures qubit i in bas
a_i r_i | qubit
|0>
|1>
|+>
|->
Pirsa: 15030015
Page 10/25

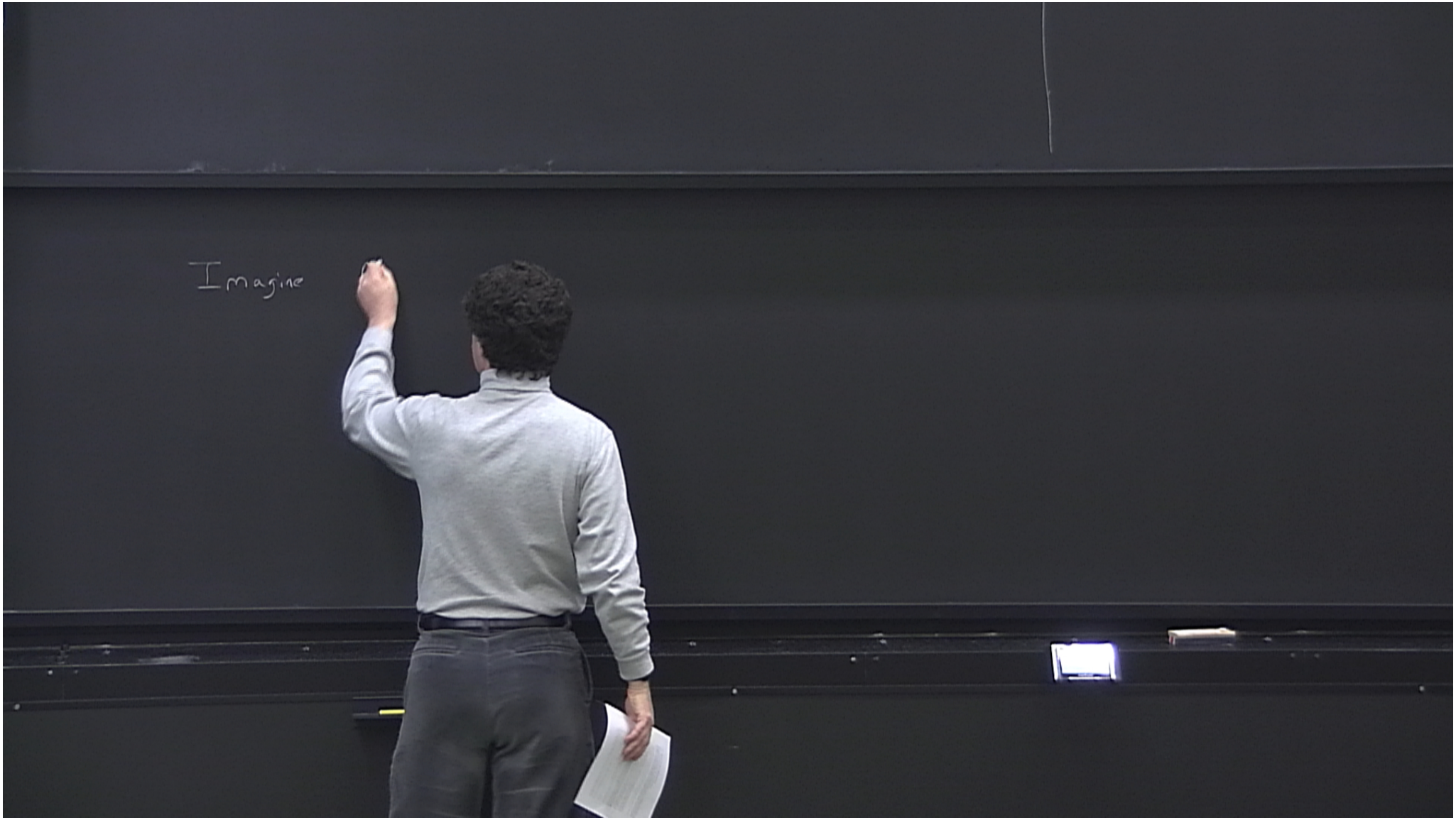
distribution (QKD)

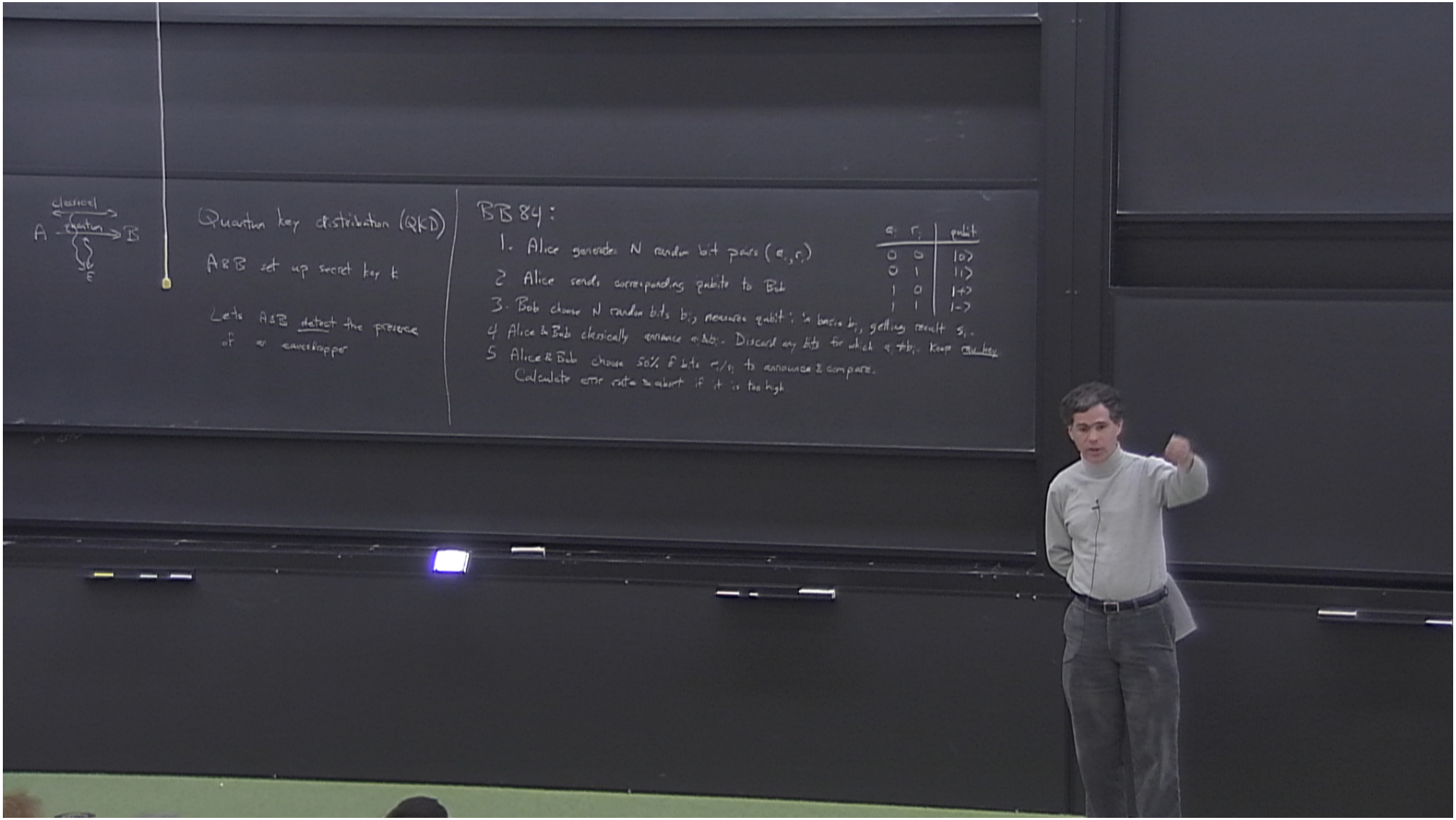
secret key k

BB84:

1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i; measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep <u>rest key</u>.

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


Imagine


classical
A
quantum
B
E
Quantum key distribution (QKD)
A & B set up secret key k
Lets A&B detect the presence of an eavesdropper
BB84:
1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4 Alice & Bob classically announce a_i ? b_i. Discard any bits for which a_i ≠ b_i. Keep raw key.
5 Alice & Bob choose 50% of bits r_i/s_i to announce & compare.
Calculate error rate & abort if it is too high
a_i r_i | qubit
0 0 | |0>
0 1 | |1>
1 0 | |+>
1 1 | |->
Pirsa: 15030015
Page 13/25

...ntum key distribution (QKD)

...B set up secret key k

...s A&B detect the presence
or eavesdropper

BB84:

1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob.
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce a_i & b_i. Discard any bits for which $a_i \neq b_i$. Keep rem key
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare

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

...ntum key distribution (QKD)

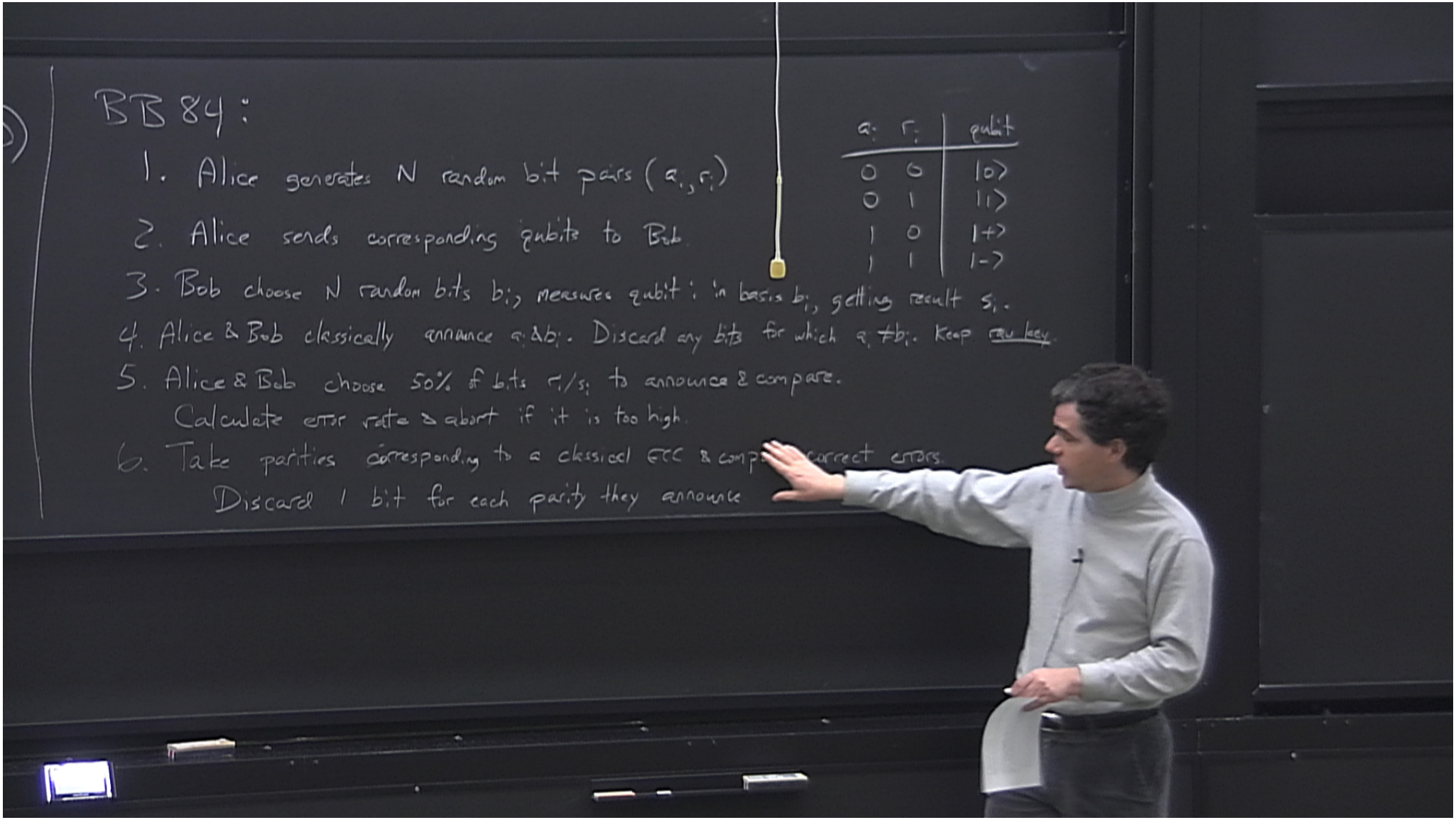
...B set up secret key k

...is A&B detect the presence
or eavesdropper

BB84:

1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i; measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce a_i & b_i. Discard any bits for which $a_i \neq b_i$. Keep rem key
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

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


BB84:
1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i; measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep rest key.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & comp correct errors.
Discard 1 bit for each parity they announce
a_i r_i | qubit
0 0 | $|0\rangle$
0 1 | $|1\rangle$
1 0 | $|+\rangle$
1 1 | $|-\rangle$

BB84:

1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep <u>raw key</u>.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

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

BB84:

1. Alice generates N random bit pairs (a_i, r_i)
2. Alice sends corresponding qubits to Bob
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep <u>raw key</u>.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

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

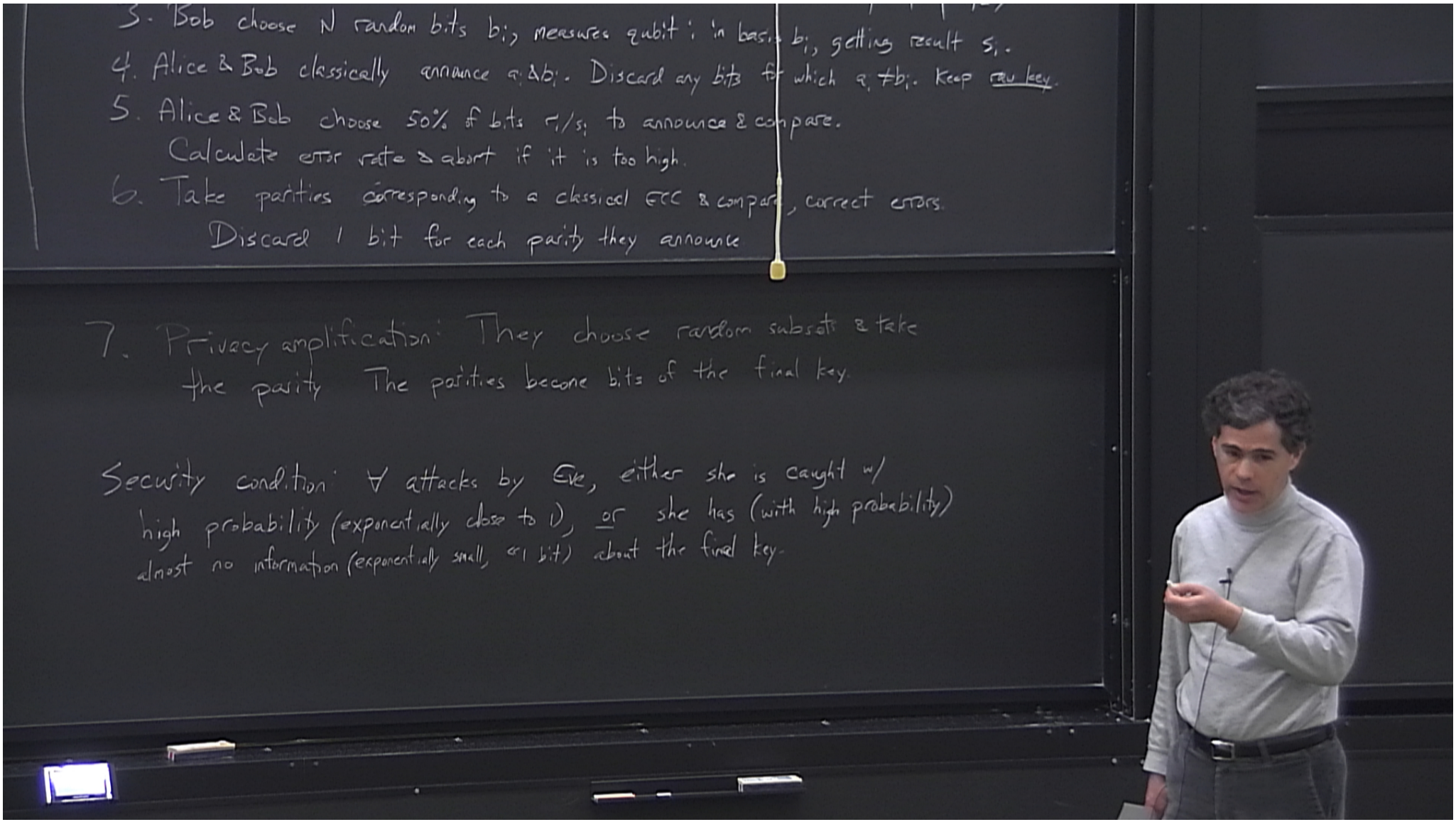
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep raw key.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

7. Privacy amplification: They choose random subsets & take the parity. The parities become bits of the final key.

3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep raw key.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

7. Privacy amplification: They choose random subsets & take the parity. The parities become bits of the final key.

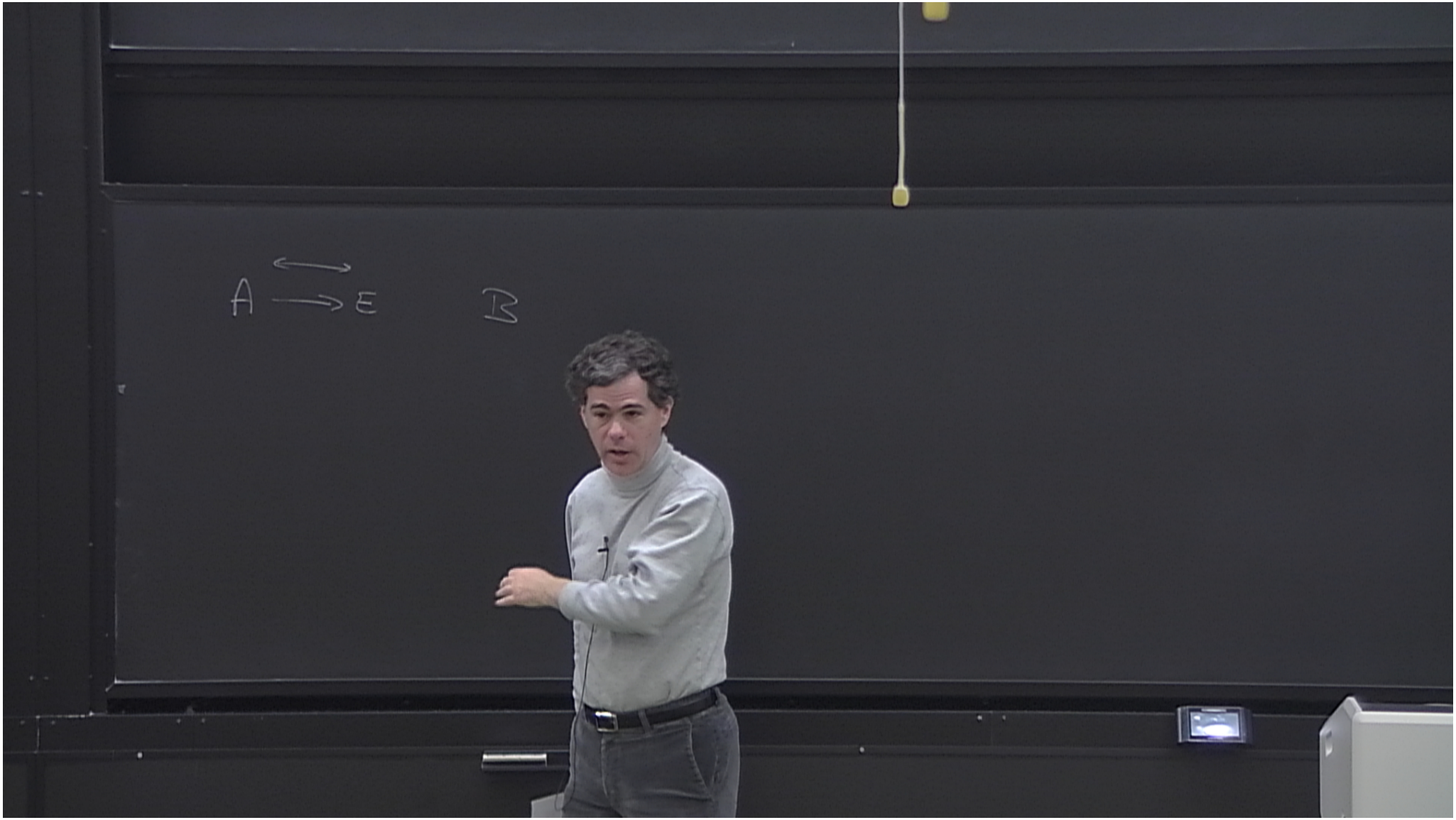
Security condition: $\forall$ attacks by Eve, either she is caught w/ high probability (exponentially close to 1), or she has (with high probability) almost no information (exponentially small, $\ll 1$ bit) about the final key.

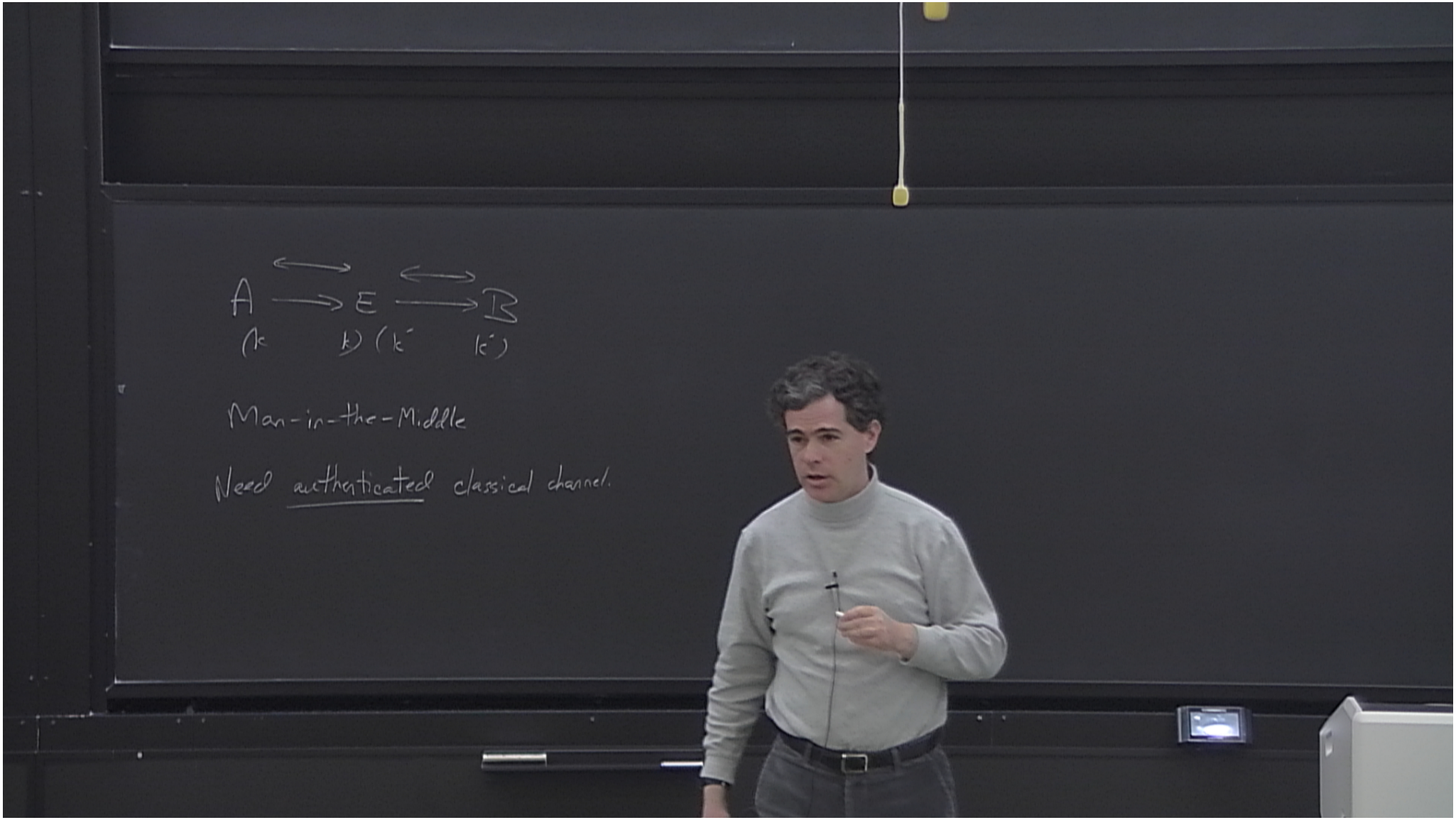


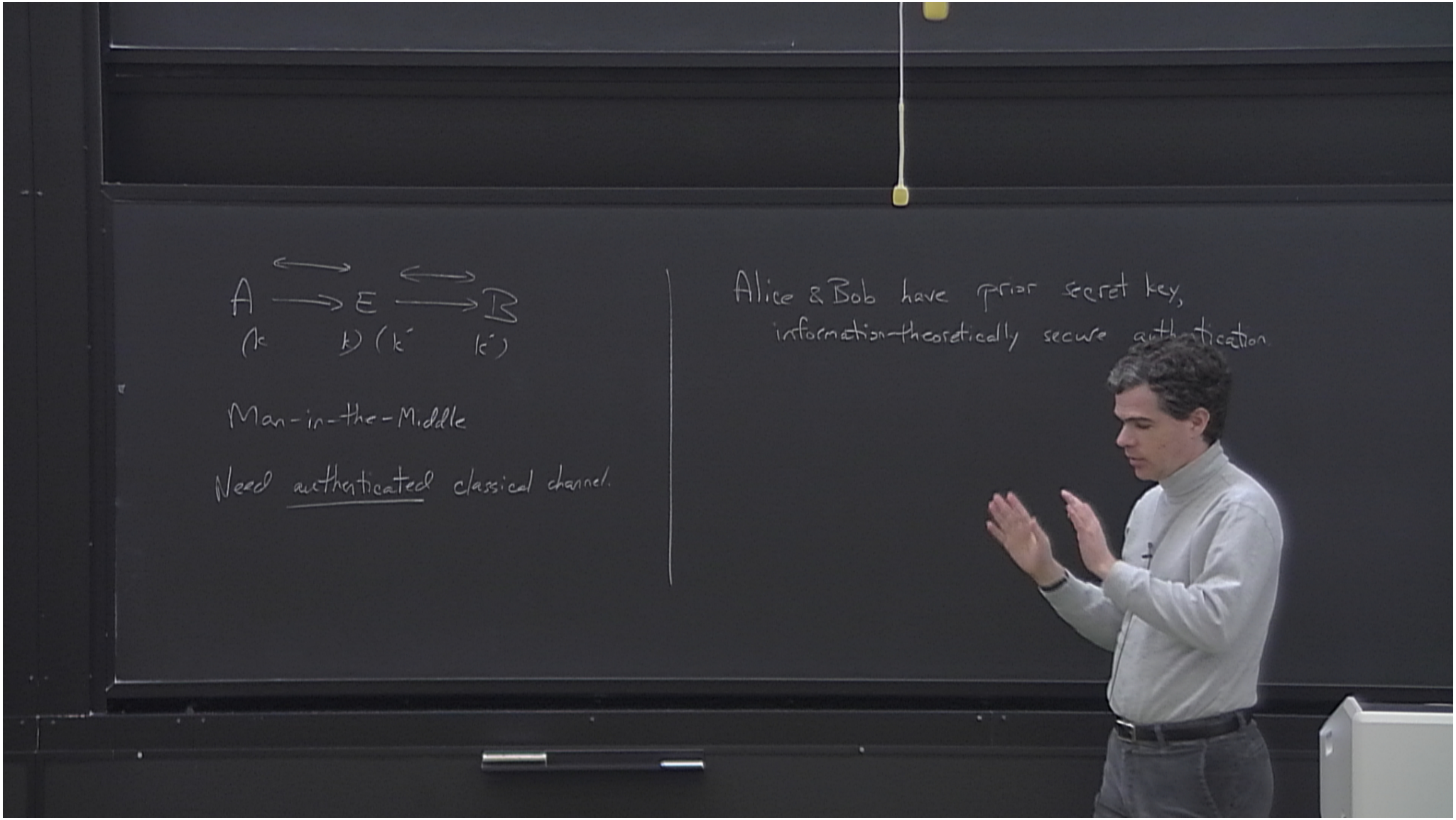
3. Bob choose N random bits b_i, measures qubit i in basis b_i, getting result s_i.
4. Alice & Bob classically announce $a_i \& b_i$. Discard any bits for which $a_i \neq b_i$. Keep raw key.
5. Alice & Bob choose 50% of bits r_i / s_i to announce & compare.
   Calculate error rate & abort if it is too high.
6. Take parities corresponding to a classical ECC & compare, correct errors.
   Discard 1 bit for each parity they announce

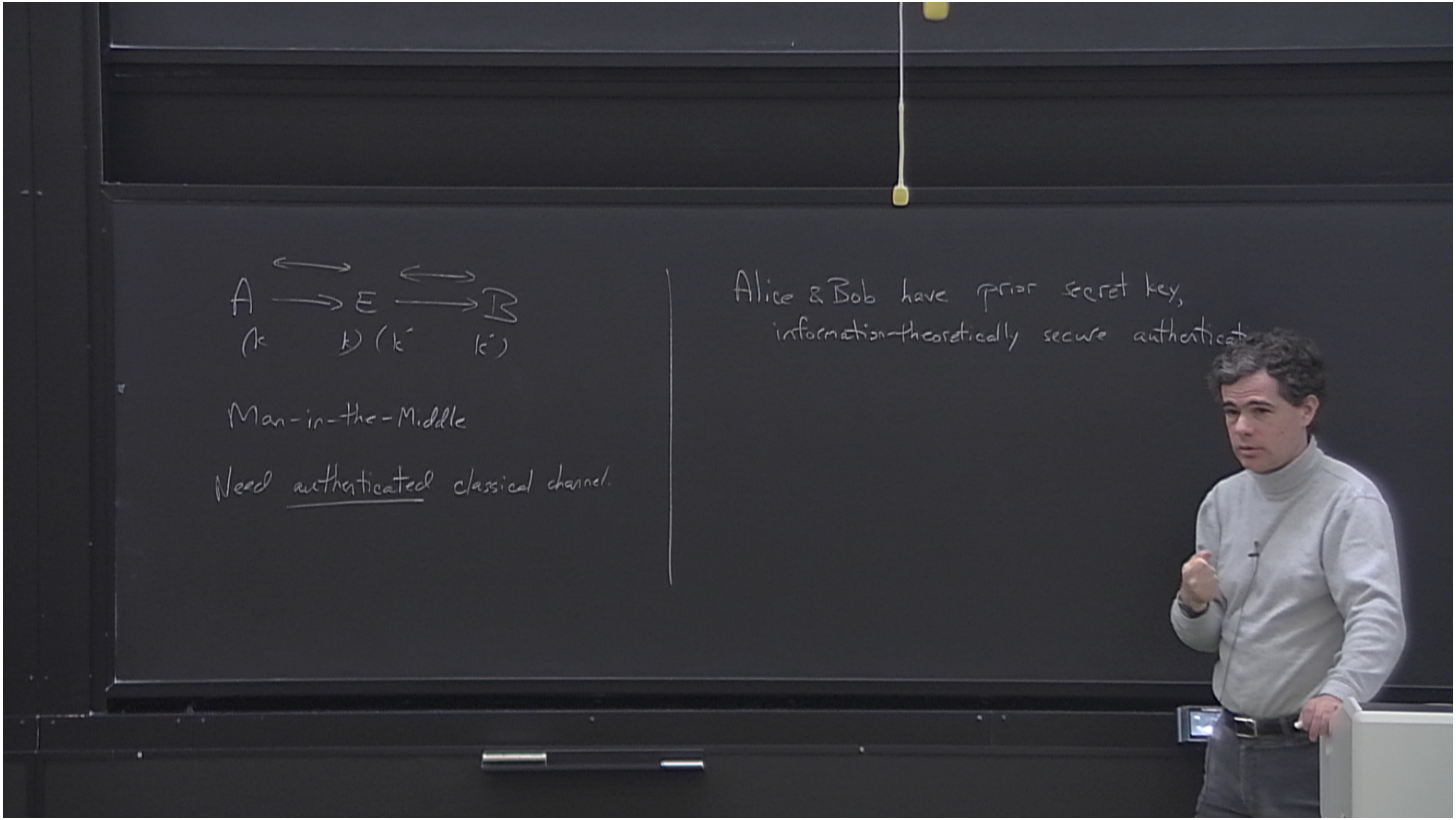
7. Privacy amplification: They choose random subsets & take the parity. The parities become bits of the final key.

Security condition: $\forall$ attacks by Eve, either she is caught w/ high probability (exponentially close to 1), or she has (with high probability) almost no information (exponentially small, $\ll 1$ bit) about the final key.


A
E
B


A
E
B
(k
k) (k'
k')
Man-in-the-Middle
Need authenticated classical channel.


A
E
B
(k k) (k' k')
Man-in-the-Middle
Need authenticated classical channel.
Alice & Bob have prior secret key,
information-theoretically secure authentication.


A
E
B
(k k) (k' k')
Man-in-the-Middle
Need authenticated classical channel.
Alice & Bob have prior secret key,
information-theoretically secure authentica