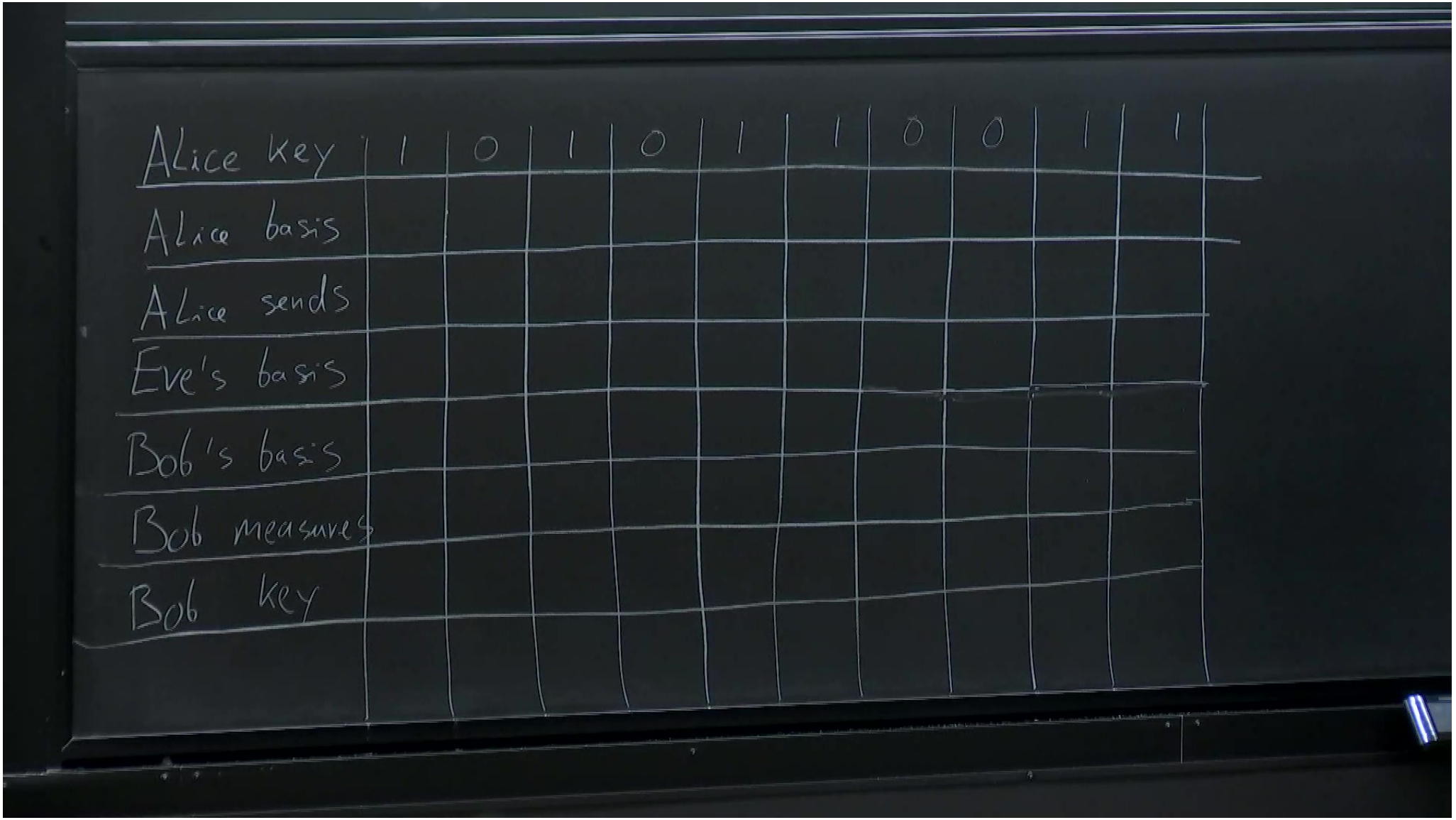
Title: Quantum Information Lecture - 230329

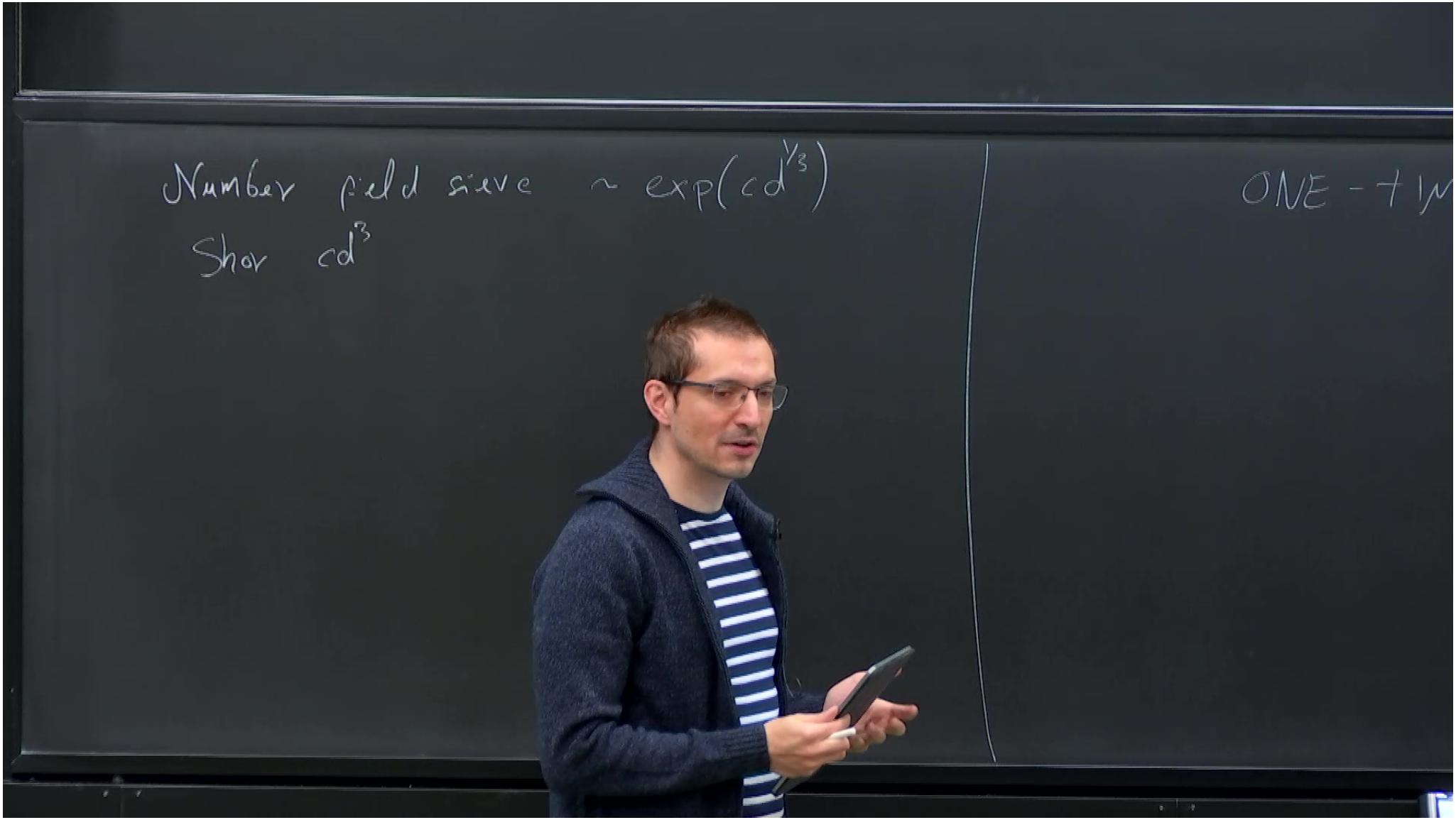
Speakers: Eduardo Martin-Martinez

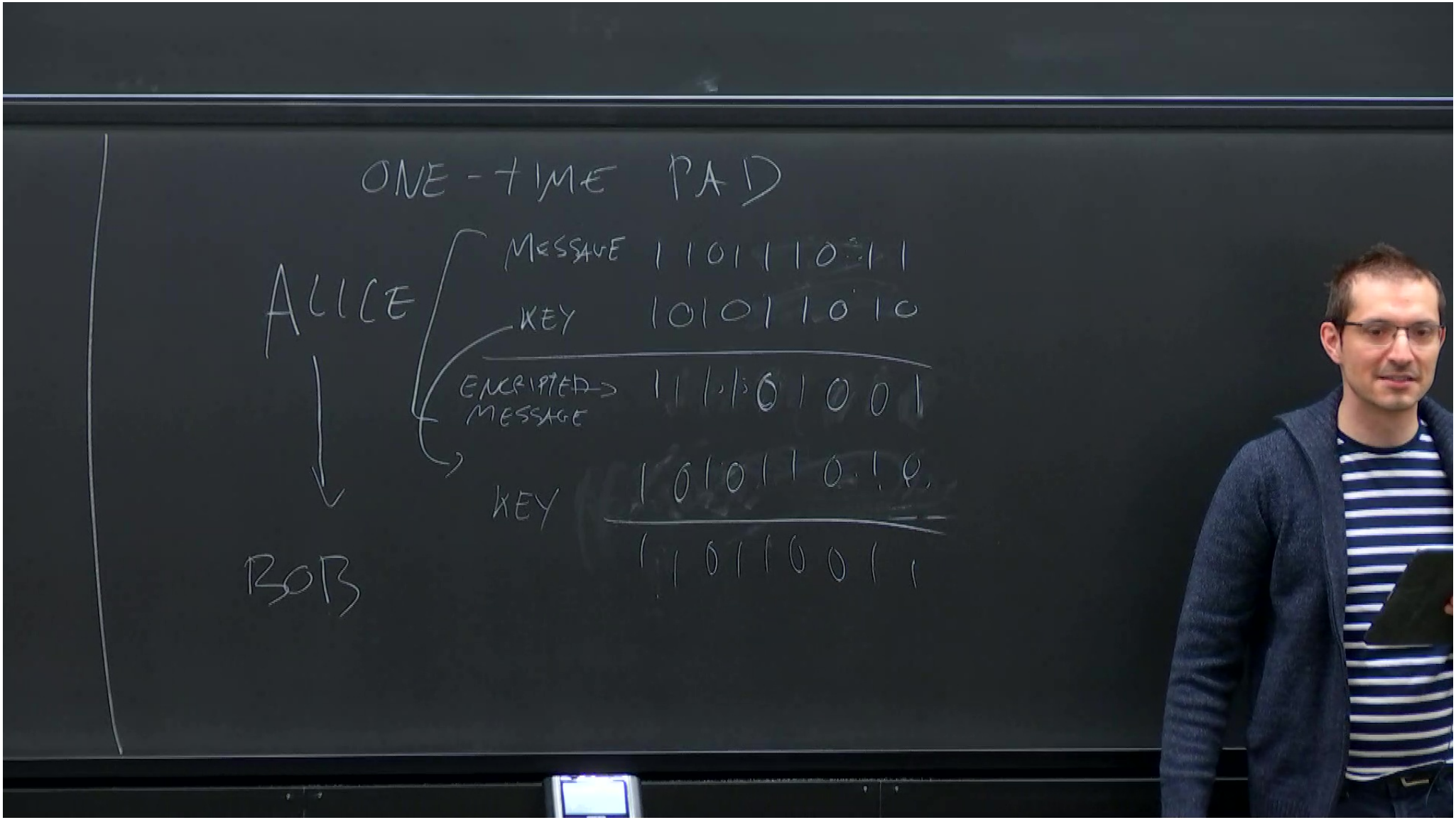
Collection: Quantum Information (2022/2023)

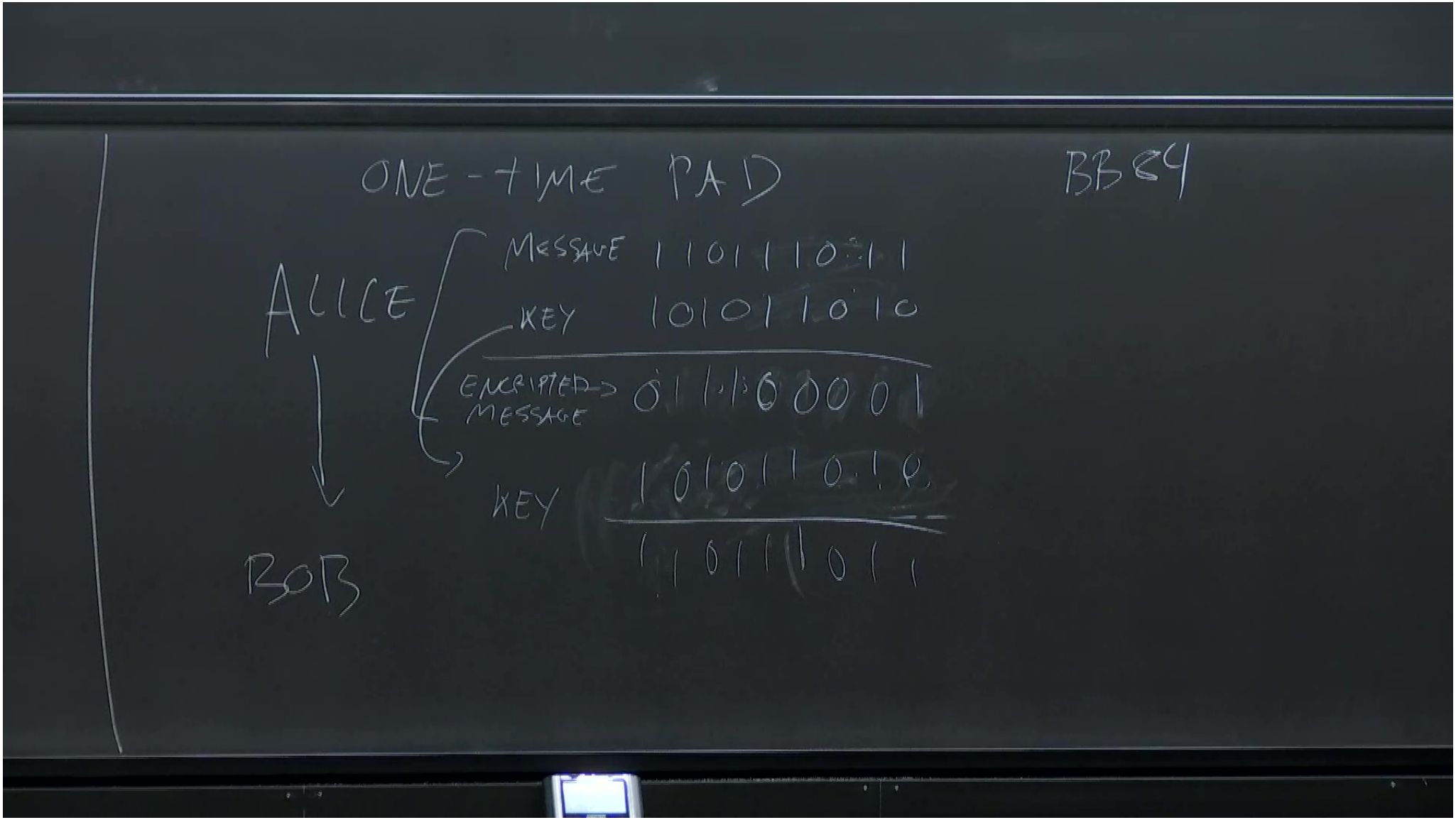
Date: March 29, 2023 - 9:00 AM

URL: https://pirsa.org/23030013


Alice key
1 0 1 0 1 1 0 0 1 1
Alice basis
Alice sends
Eve's basis
Bob's basis
Bob measures
Bob key


Number field sieve ~ exp(cd^1/3)
Shor cd^3
ONE - 1/


ONE-TIME PAD
ALICE
MESSAGE 1101110111
KEY 1010110110
ENCRIPTED MESSAGE 1111101001
KEY 1010110110
BOB
1101100111

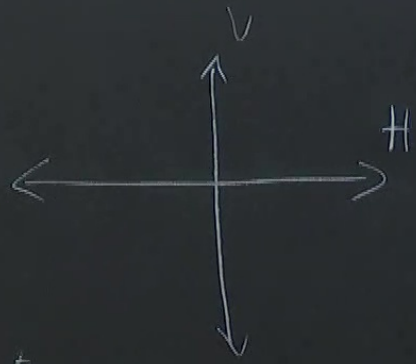

ONE-TIME PAD
BB84
ALICE
MESSAGE 1101110111
KEY 1010110110
ENCRIPTED MESSAGE -> 0111000101
KEY 1010110110
BOB
1101110111

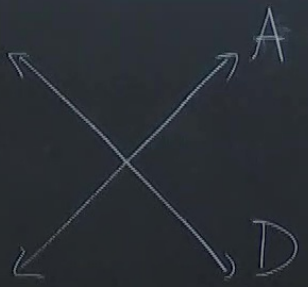
BB84

Alice and Bob have two choices of basis

$$|V\rangle = \frac{1}{\sqrt{2}}\left(|A\rangle + |D\rangle\right)$$

$$|H\rangle = \frac{1}{\sqrt{2}}\left(|D\rangle - |A\rangle\right)$$





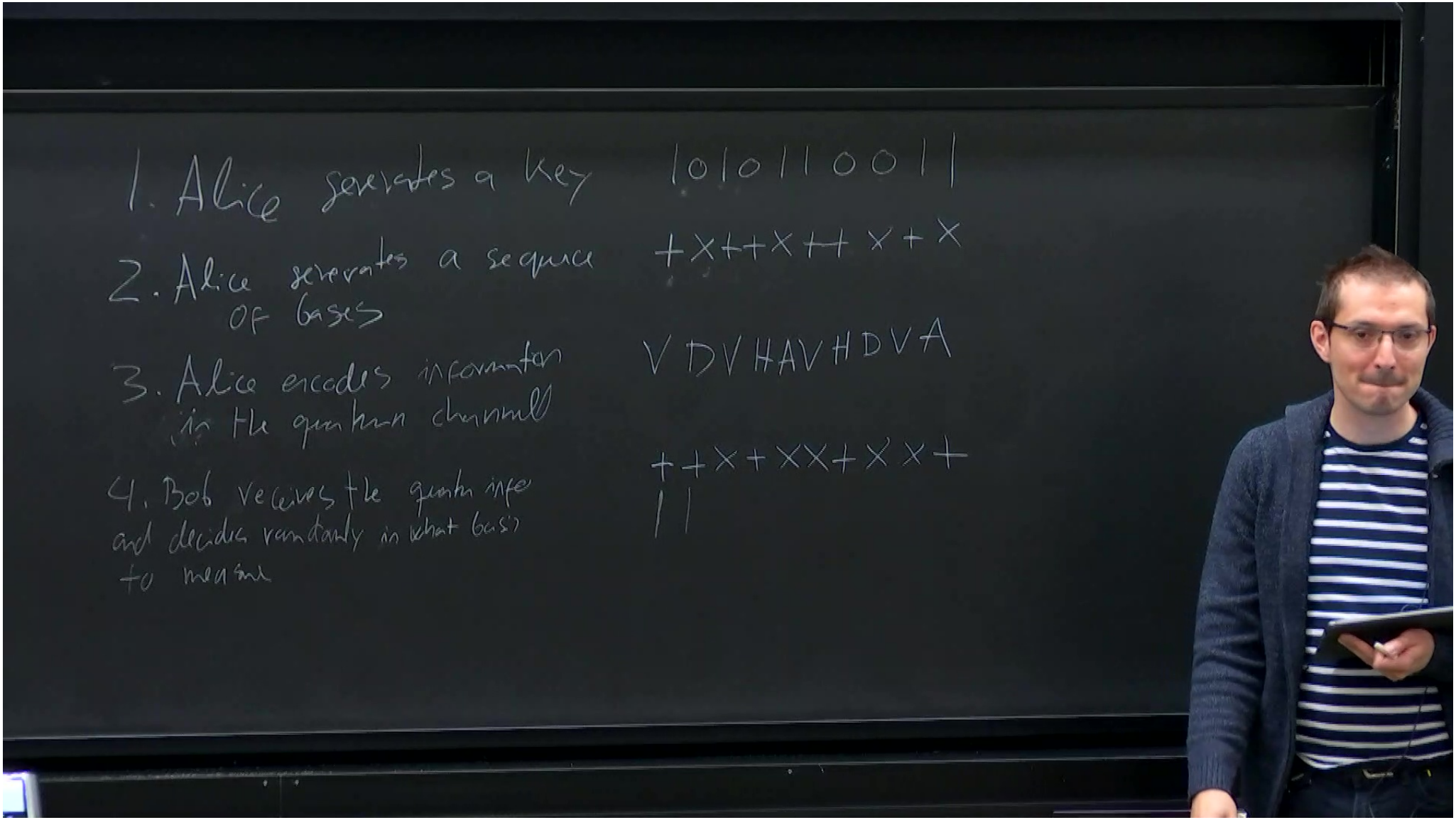
Encoding:

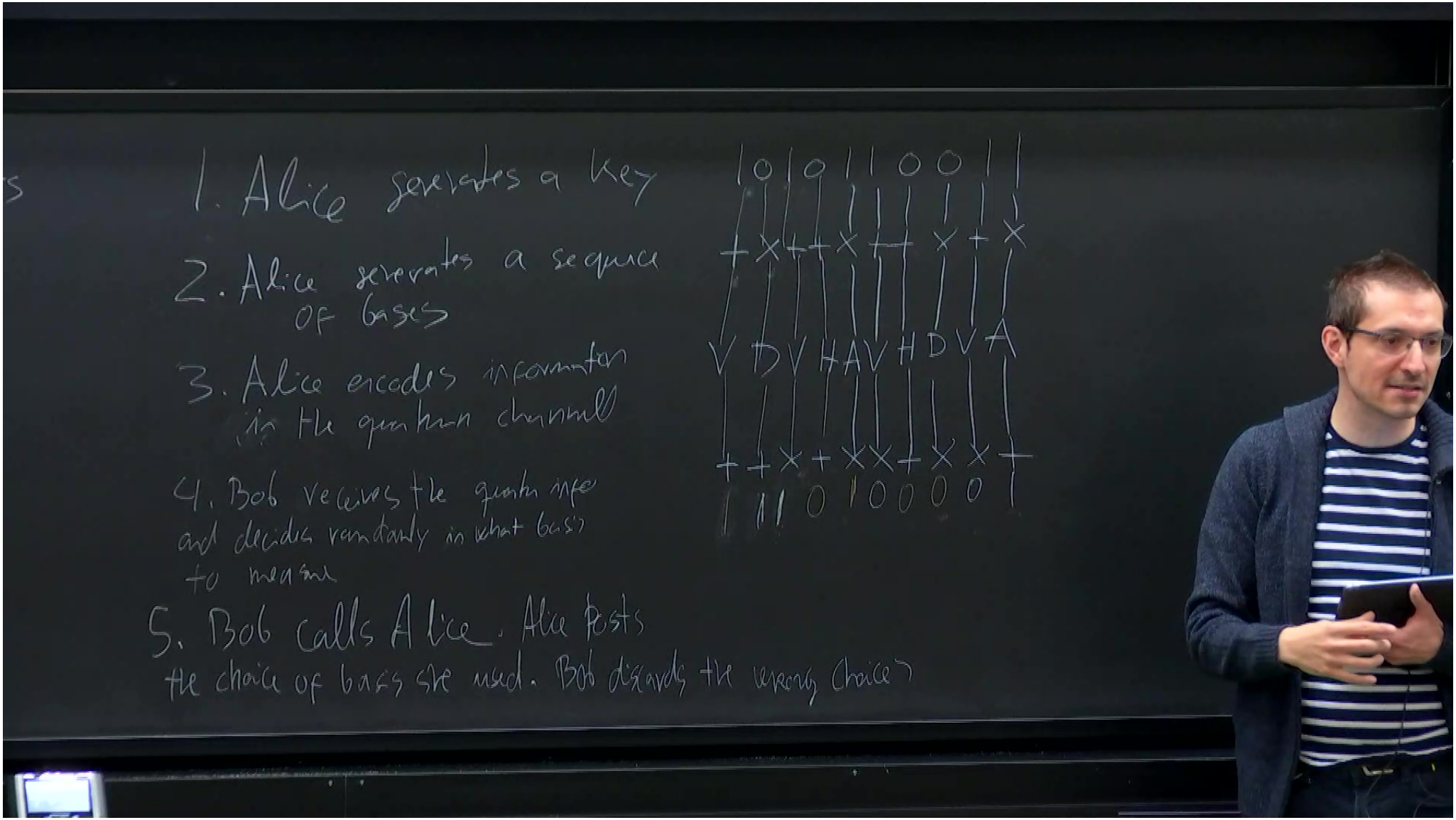
$|V\rangle \leftrightarrow 1$

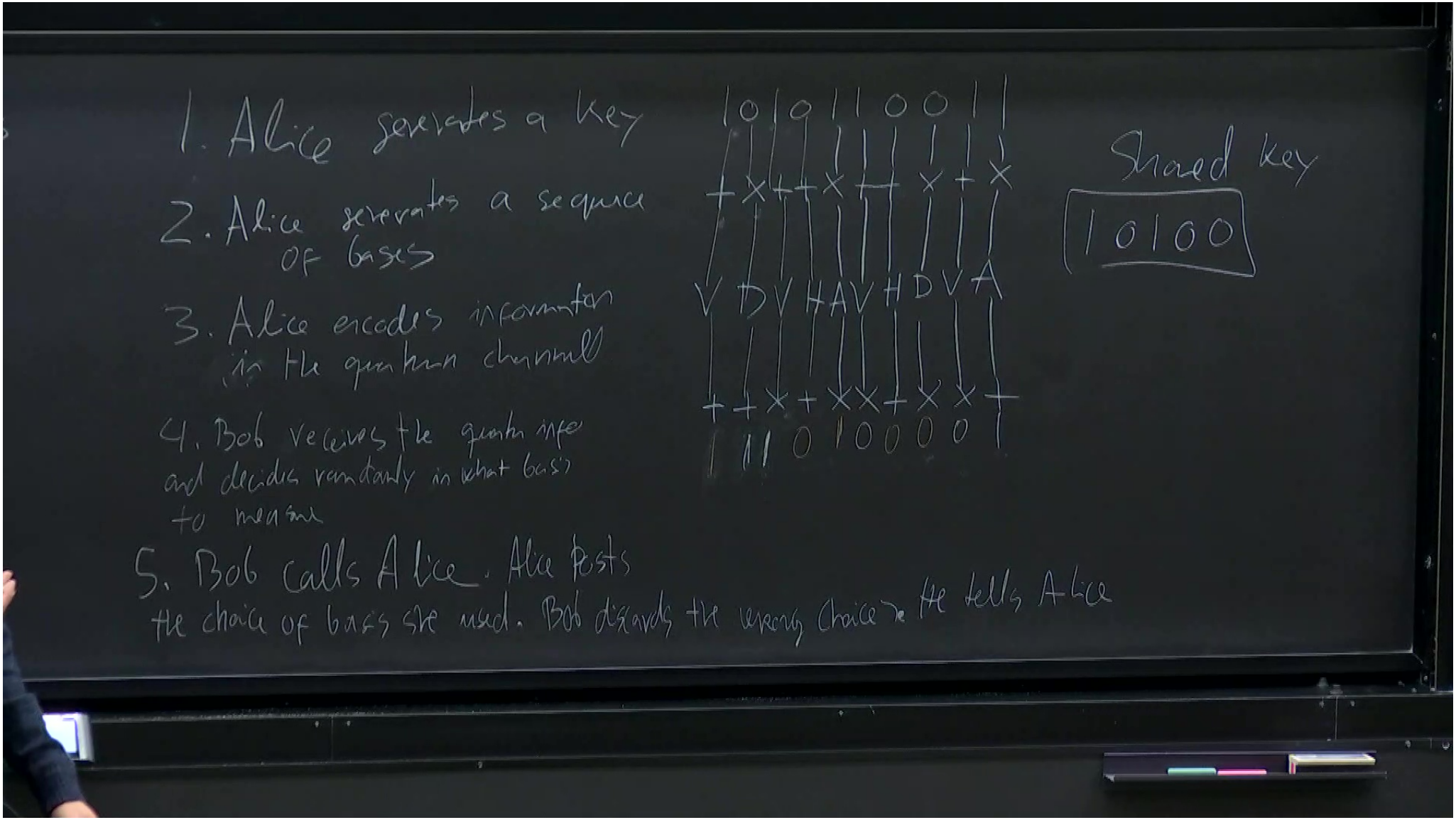
$|H\rangle \leftrightarrow 0$

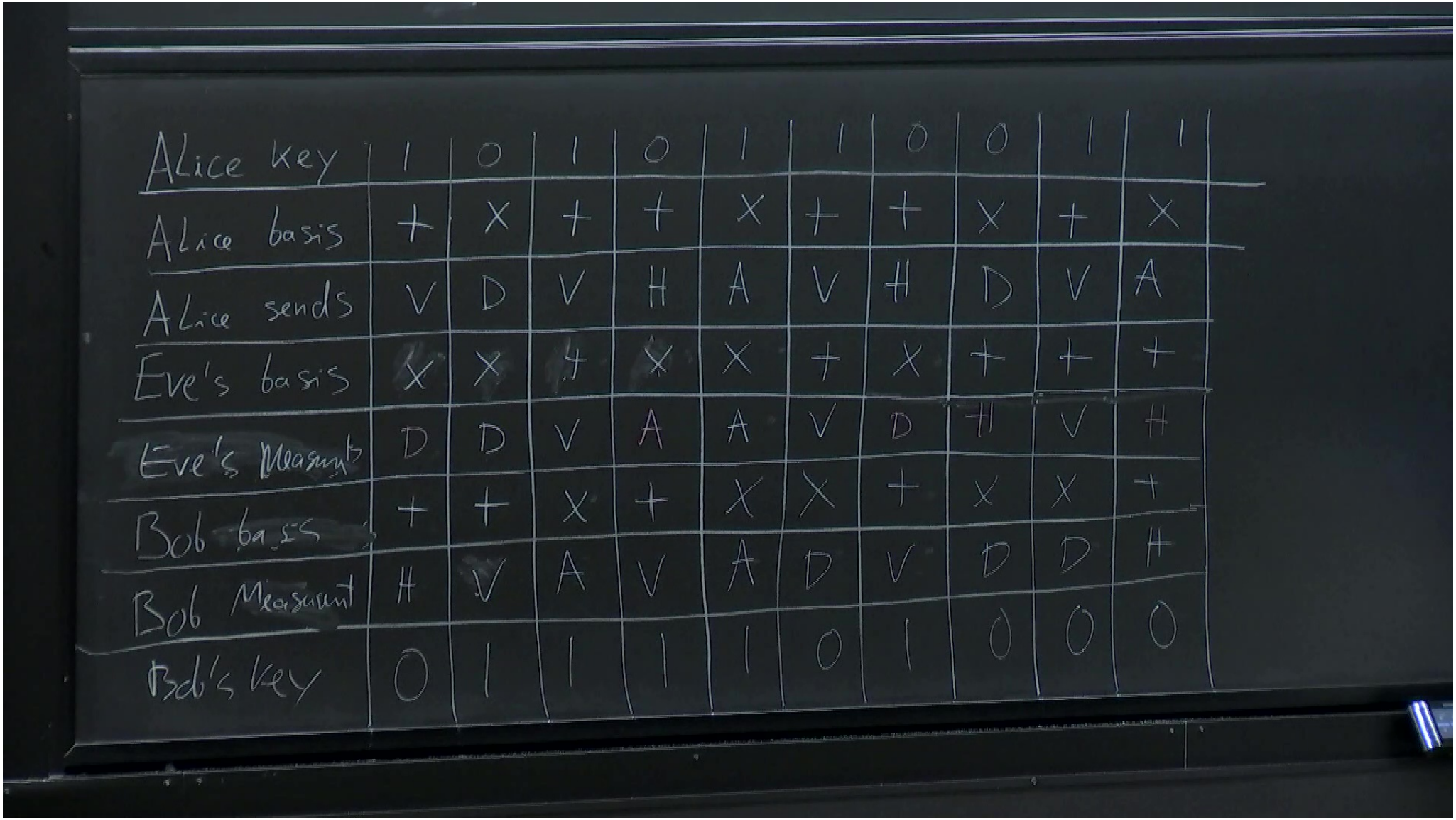
$|A\rangle \leftrightarrow 1$

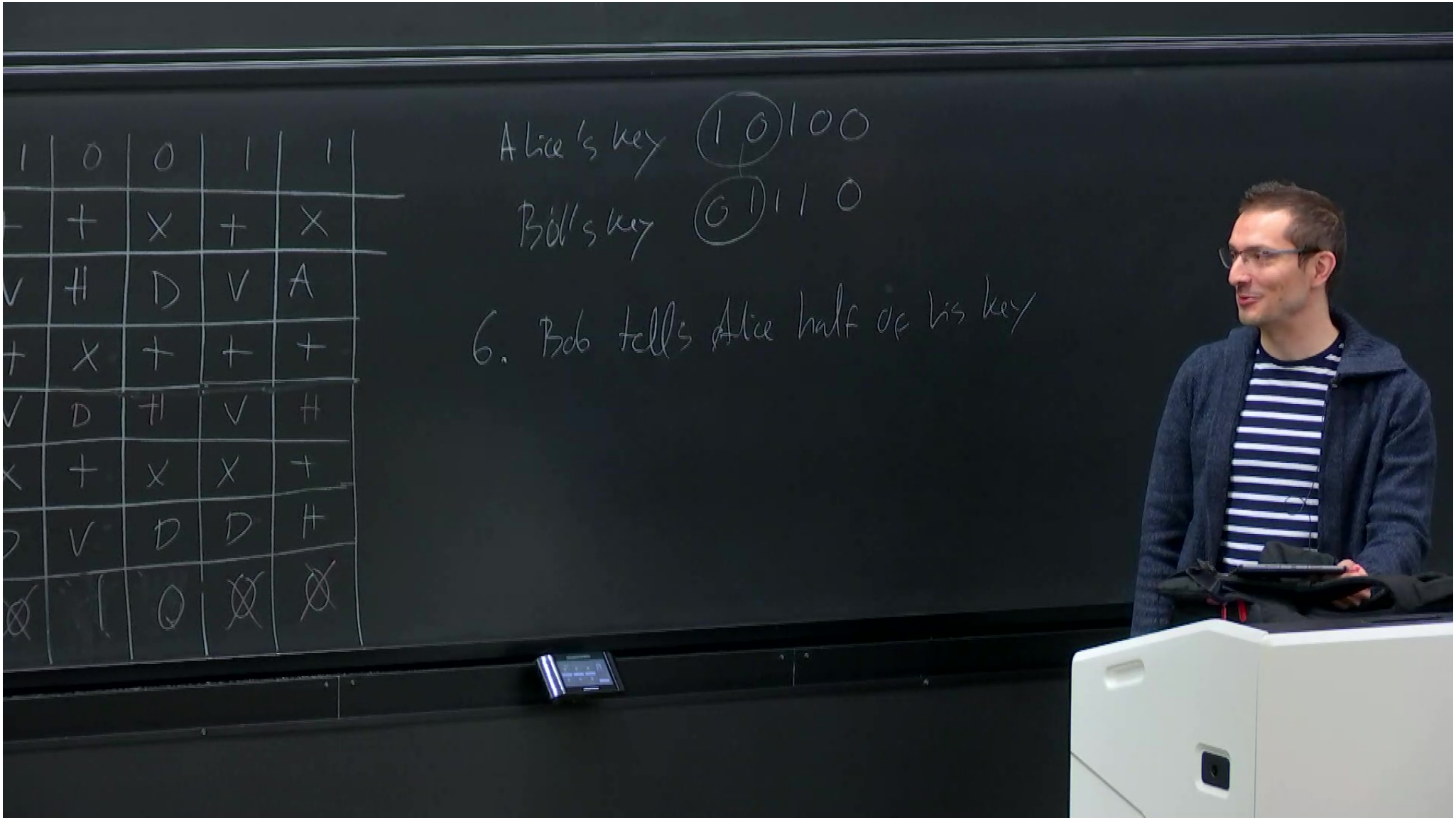
$|D\rangle \leftrightarrow 0$

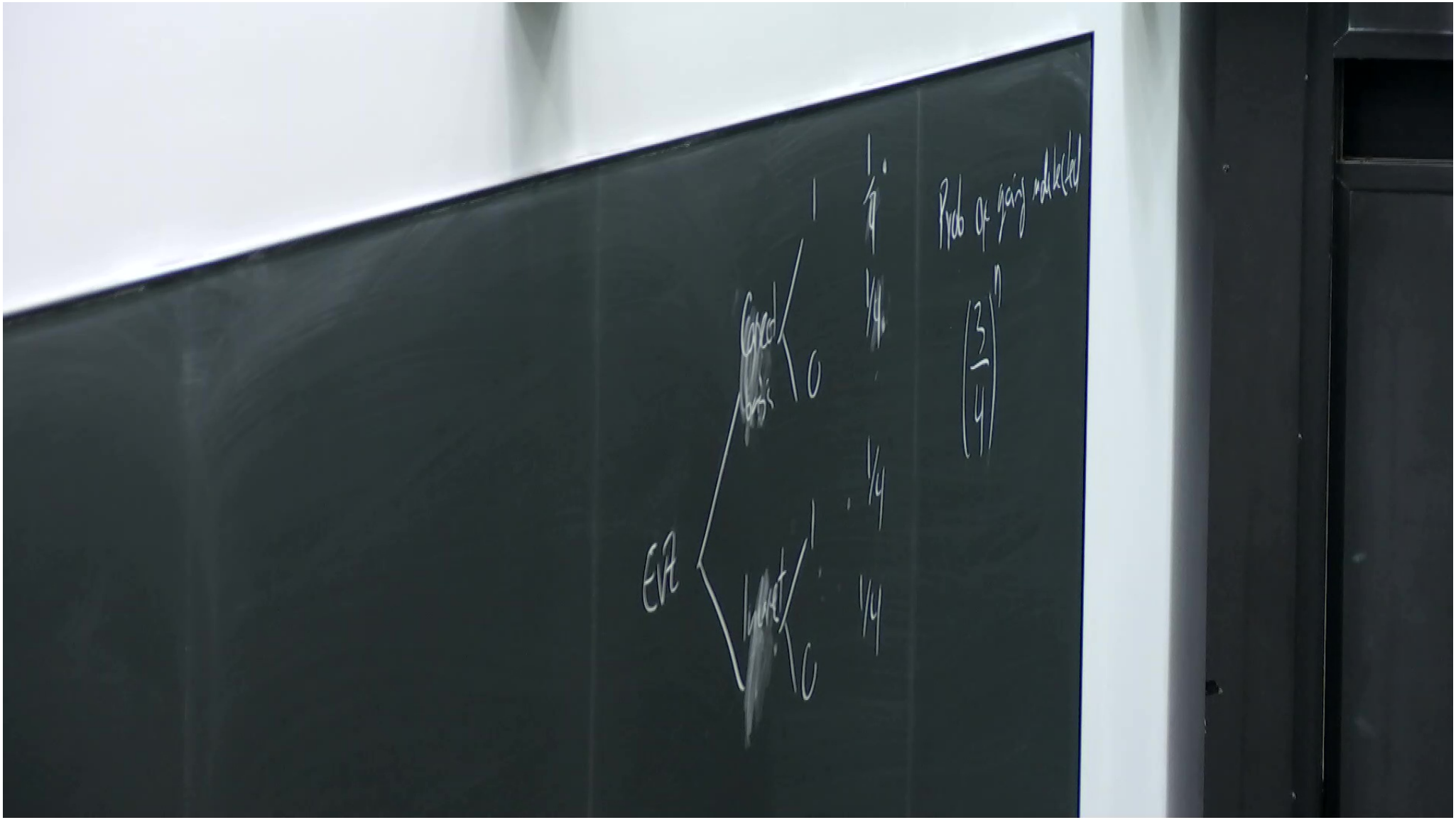

1. Alice generates a key
|0|0|1|1|0|0|1|1|
2. Alice generates a sequence of bases
+X++X++X+X
3. Alice encodes information in the quantum channel
V D V H A V H D V A
4. Bob receives the quantum info and decides randomly in what basis to measure
+ + X + X X + X X +
| |


1. Alice generates a key
2. Alice generates a sequence of bases
3. Alice encodes information in the quantum channel
4. Bob receives the quantum info and decides randomly in what basis to measure
5. Bob calls Alice. Alice posts the choice of bases she used. Bob discards the wrong choices


1. Alice generates a key
2. Alice generates a sequence of bases
3. Alice encodes information in the quantum channel
4. Bob receives the quantum info and decides randomly in what basis to measure
5. Bob calls Alice. Alice tells the choice of basis she used. Bob discards the wrong choice & he tells Alice
1 0 1 0 0 1 1 0 0 1 1
Shared key
1 0 1 0 0


Alice key 1 0 1 0 1 1 0 0 1 1
Alice basis + X + + X + + X + X
Alice sends V D V H A V H D V A
Eve's basis X X + X X + X + + +
Eve's Measmt D D V A A V D H V H
Bob basis + + X + X X + X X +
Bob Measmt H V A V A D V D D H
Bob's key 0 1 1 1 1 0 1 0 0 0


1 0 0 1 1
+ X + X
H D V A
X + + +
D H V H
+ X X +
V D D H
Alice's key 1 0 1 0 0
Bob's key 0 1 1 1 0
6. Bob tells Alice half of his key


EVZ
1/4
1/4
1/4
1/4
Prob of going undetected
(3/4)^n

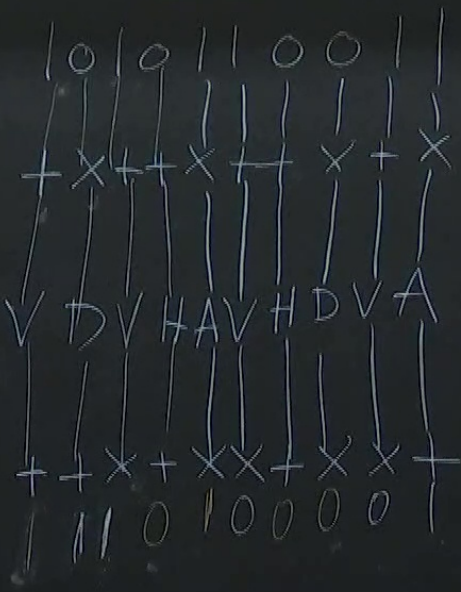
1. Alice generates a key

2. Alice generates a sequence of bases

3. Alice encodes information in the quantum channel

4. Bob receives the quantum info and decides randomly in what basis to measure

5. Bob calls Alice. Alice tests the choice of bases she used. Bob discards the wrong choice & he tells Alice



Shared key

1 0 1 0 0