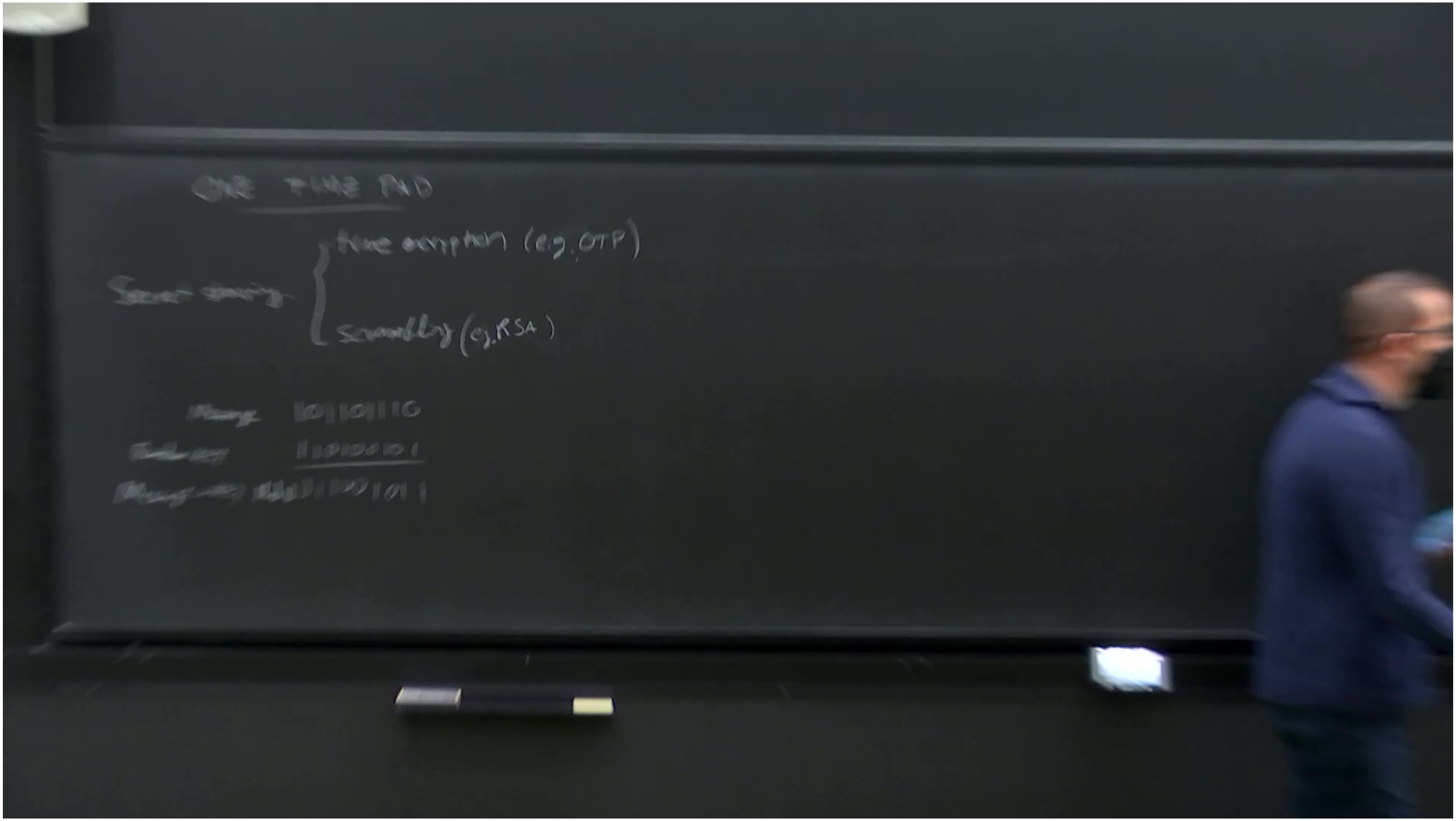
Title: Quantum Information 2021/2022

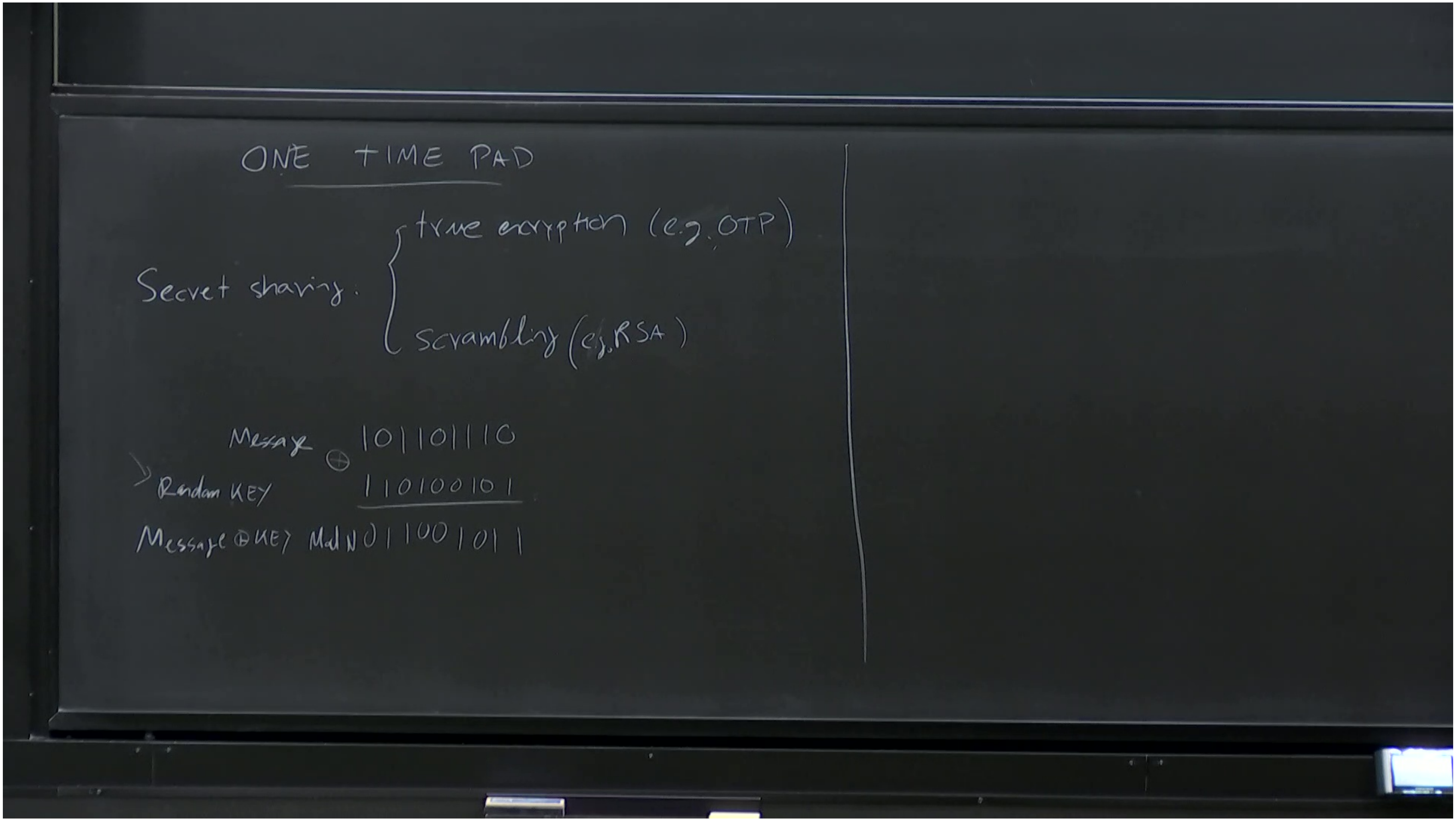
Speakers: Eduardo Martin-Martinez, Philippe Allard Guerin

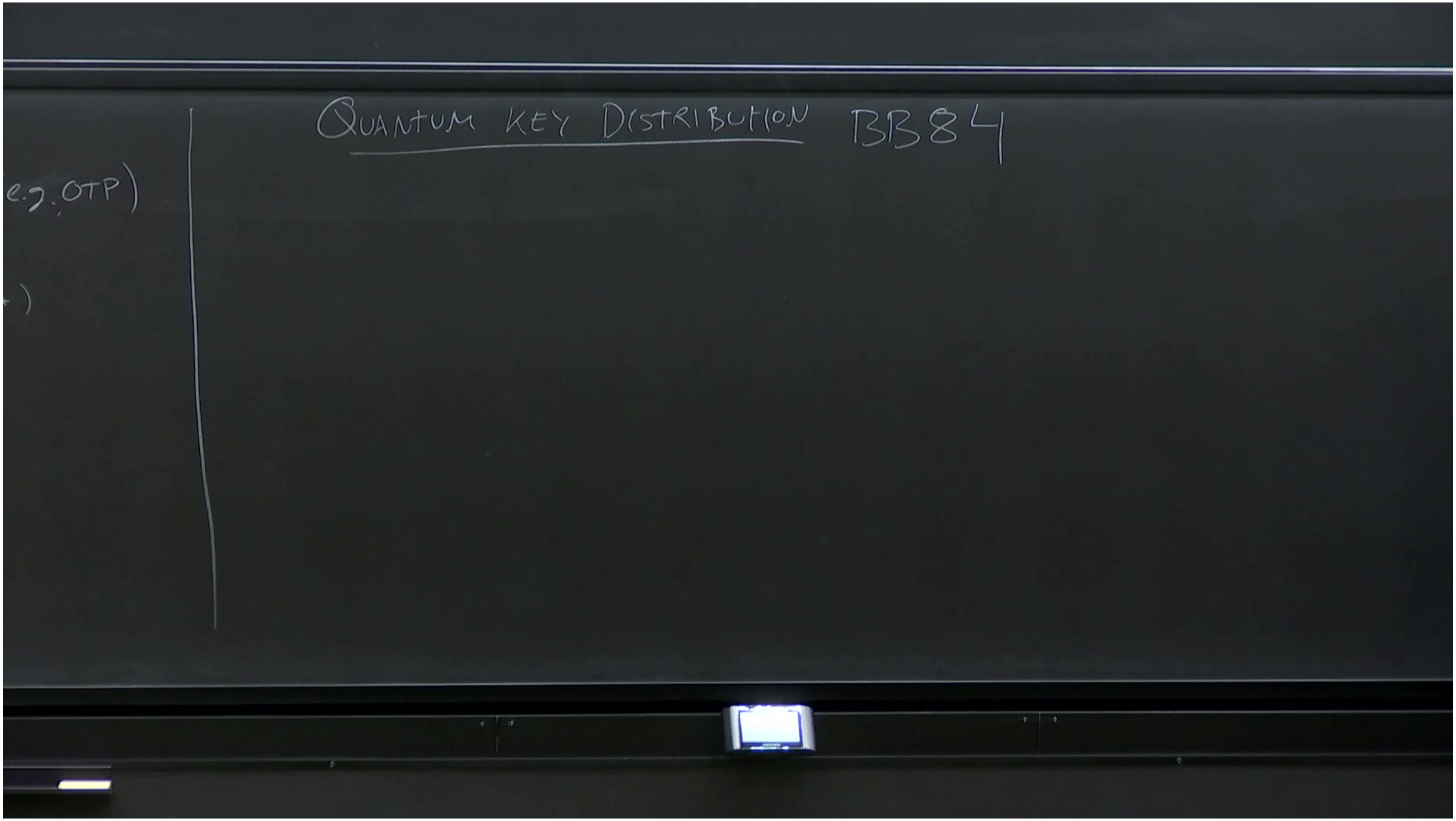
Collection: Quantum Information 2021/2022

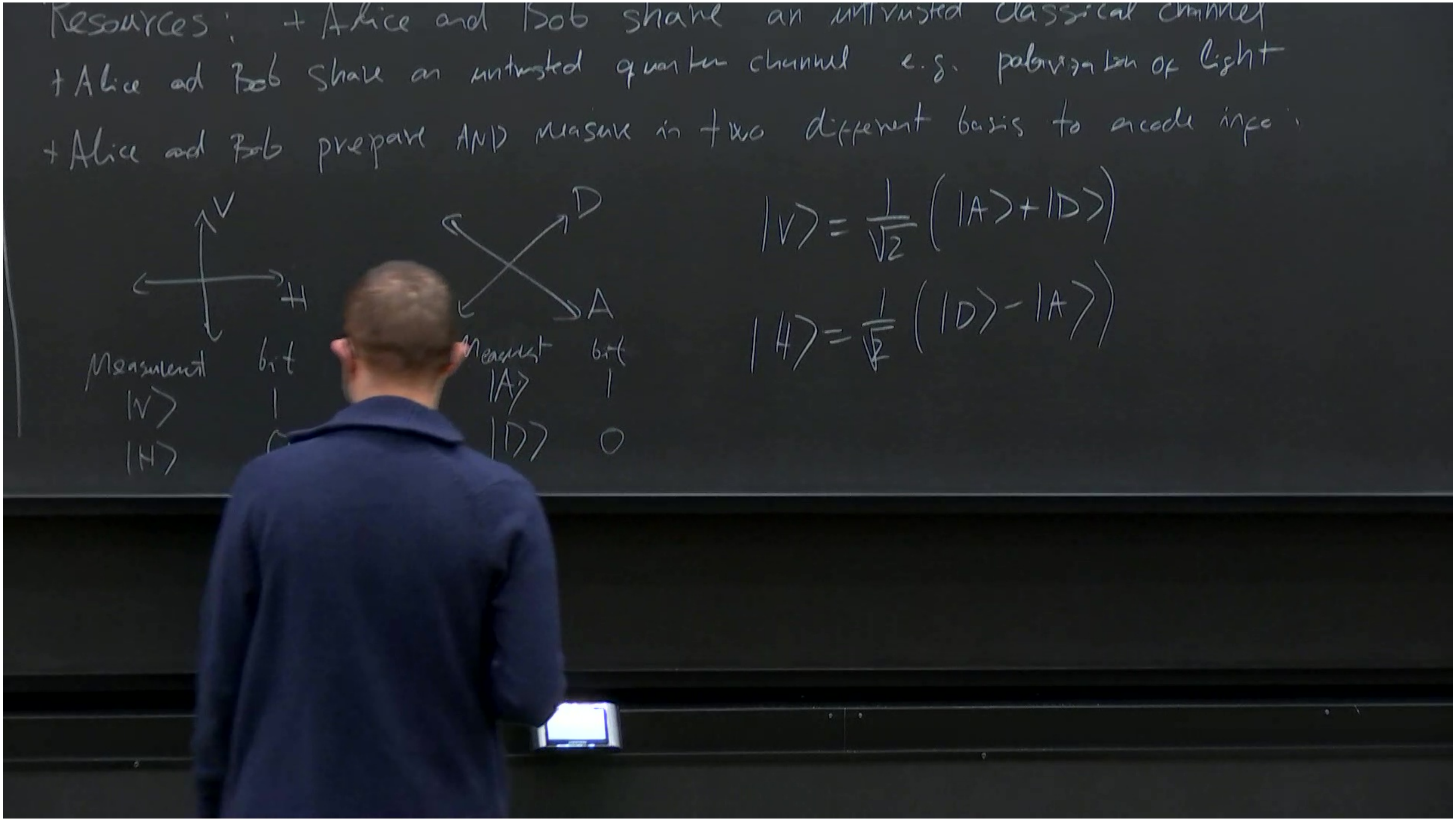
Date: March 28, 2022 - 9:00 AM

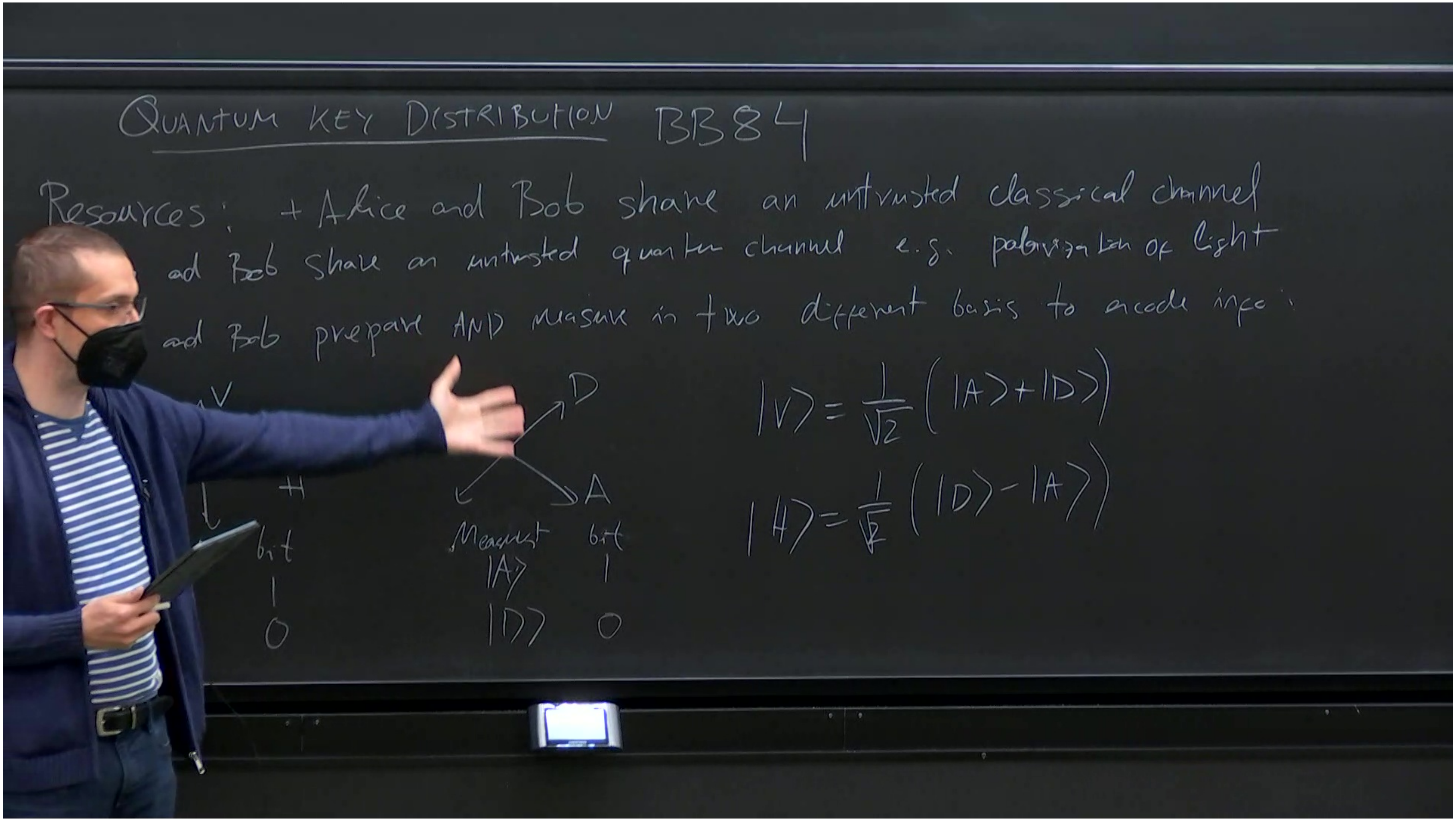
URL: https://pirsa.org/22030080


(e.g. OTP)
(e.g. RSA)


ONE TIME PAD
Secret sharing:
true encryption (e.g. OTP)
scrambling (e.g. RSA)
Message 101101110
⊕
Random KEY 110100101
Message ⊕ KEY Mod N 011001011


QUANTUM KEY DISTRIBUTION BB84
e.g. OTP)


Resources: + Alice and Bob share an untrusted classical channel
+ Alice and Bob share an untrusted quantum channel e.g. polarization of light
+ Alice and Bob prepare AND measure in two different basis to encode info:
V
H
D
A
Measurement bit
|V> 1
|H>
|A> 1
|D> 0
|V> = 1/√2 (|A> + |D>)
|H> = 1/√2 (|D> - |A>)


QUANTUM KEY DISTRIBUTION BB84
Resources: + Alice and Bob share an untrusted classical channel
and Bob share an untrusted quantum channel e.g. polarization of light
and Bob prepare AND measure in two different basis to encode info:
D
A
bit
1
0
Measurement bit
|A⟩ 1
|D⟩ 0
|V⟩ = 1/√2 (|A⟩ + |D⟩)
|H⟩ = 1/√2 (|D⟩ − |A⟩)

1. Alice generates a key — 1010110011

2. Alice generates a sequence of bases to prepare — + × + + × + + × + ×

3. Alice encodes the key in the quantum state of qubit — V D V H A V H D V A

4. Alice sends the qubits through the quantum channel — + + × + × × + × × +
   Bob receives the qubits and selects a basis to measure randomly to retrieve the key — 1

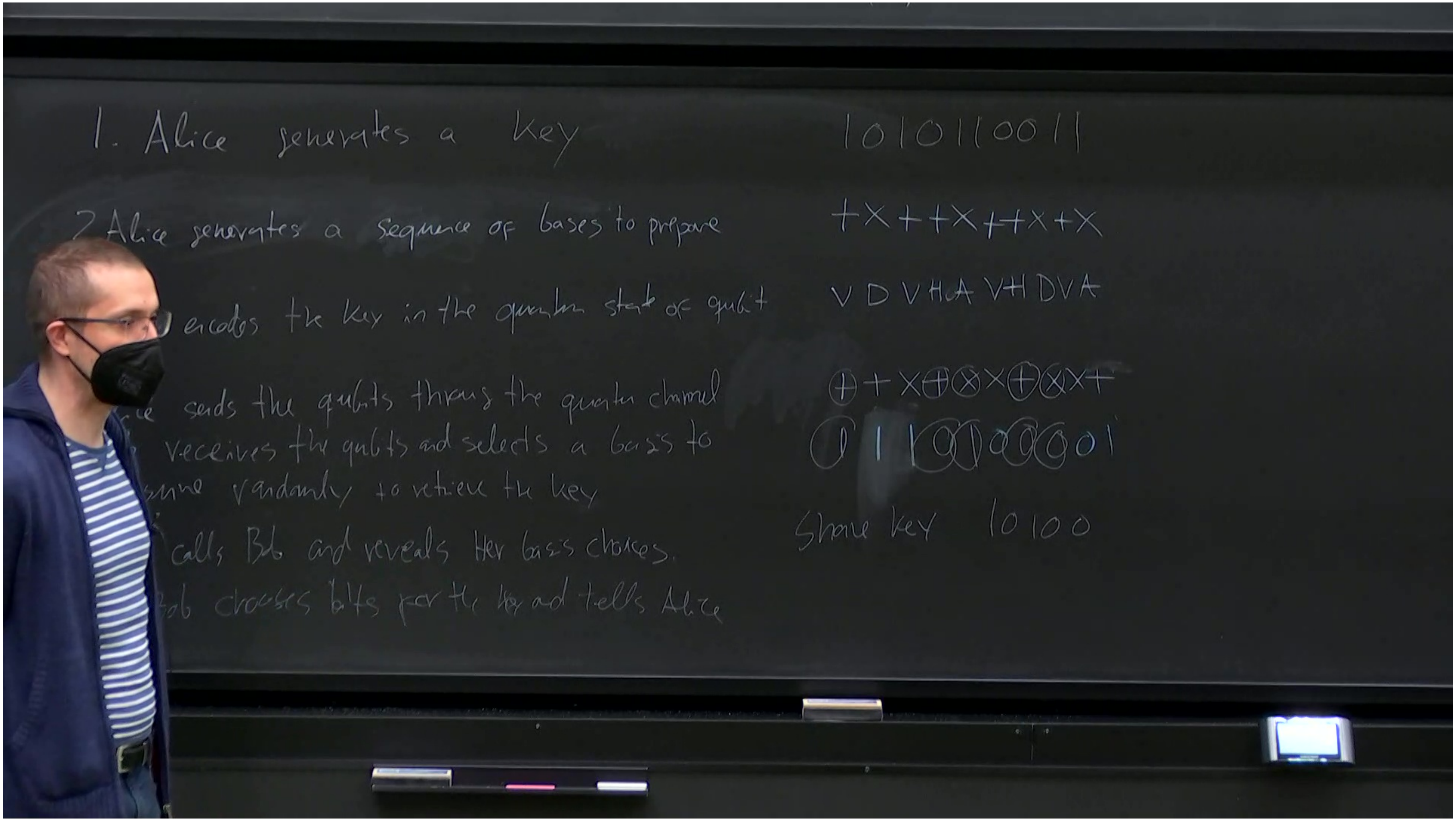
1. Alice generates a key — 1010110011

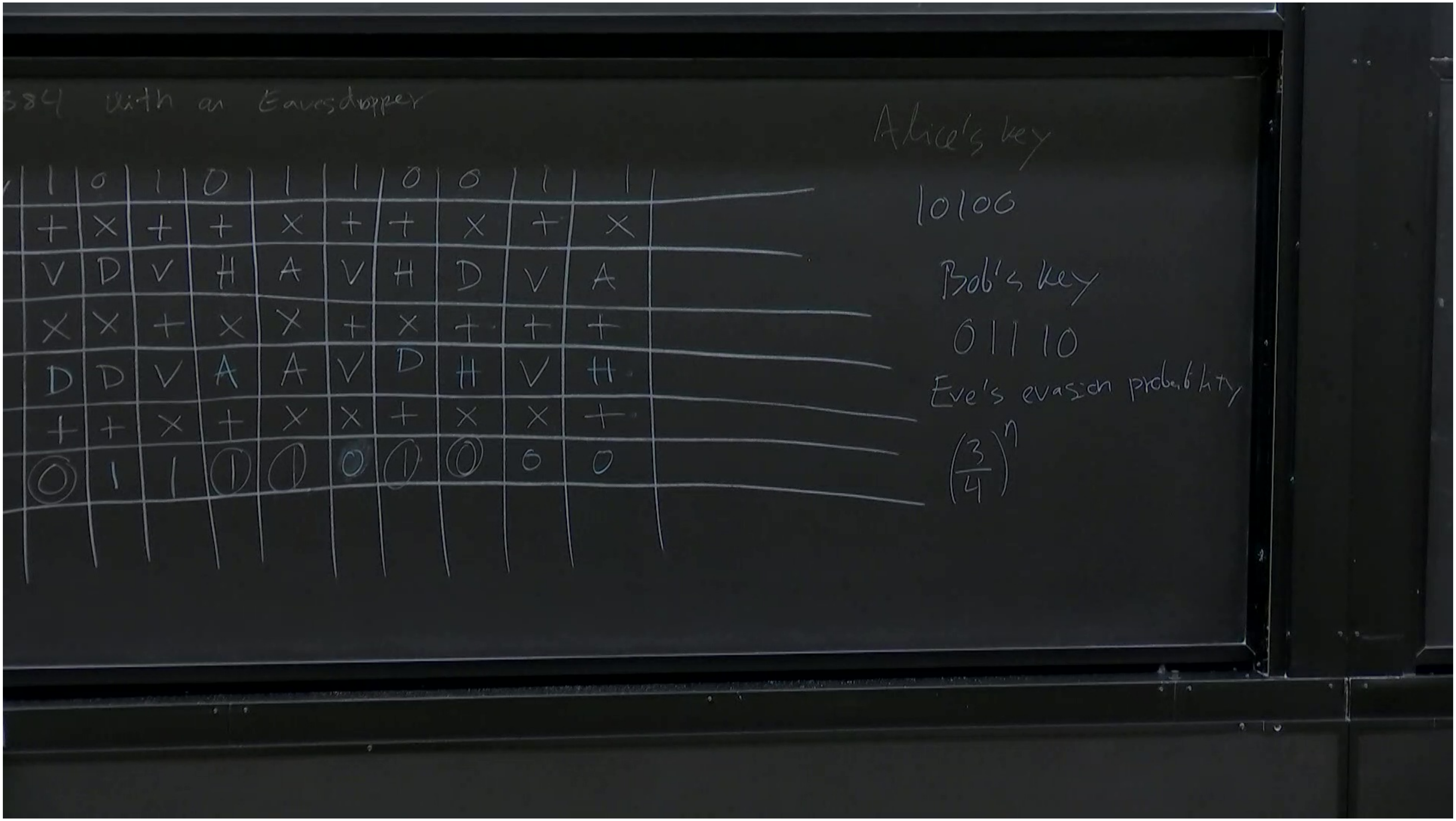
2. Alice generates a sequence of bases to prepare — + × + + × + + × + ×

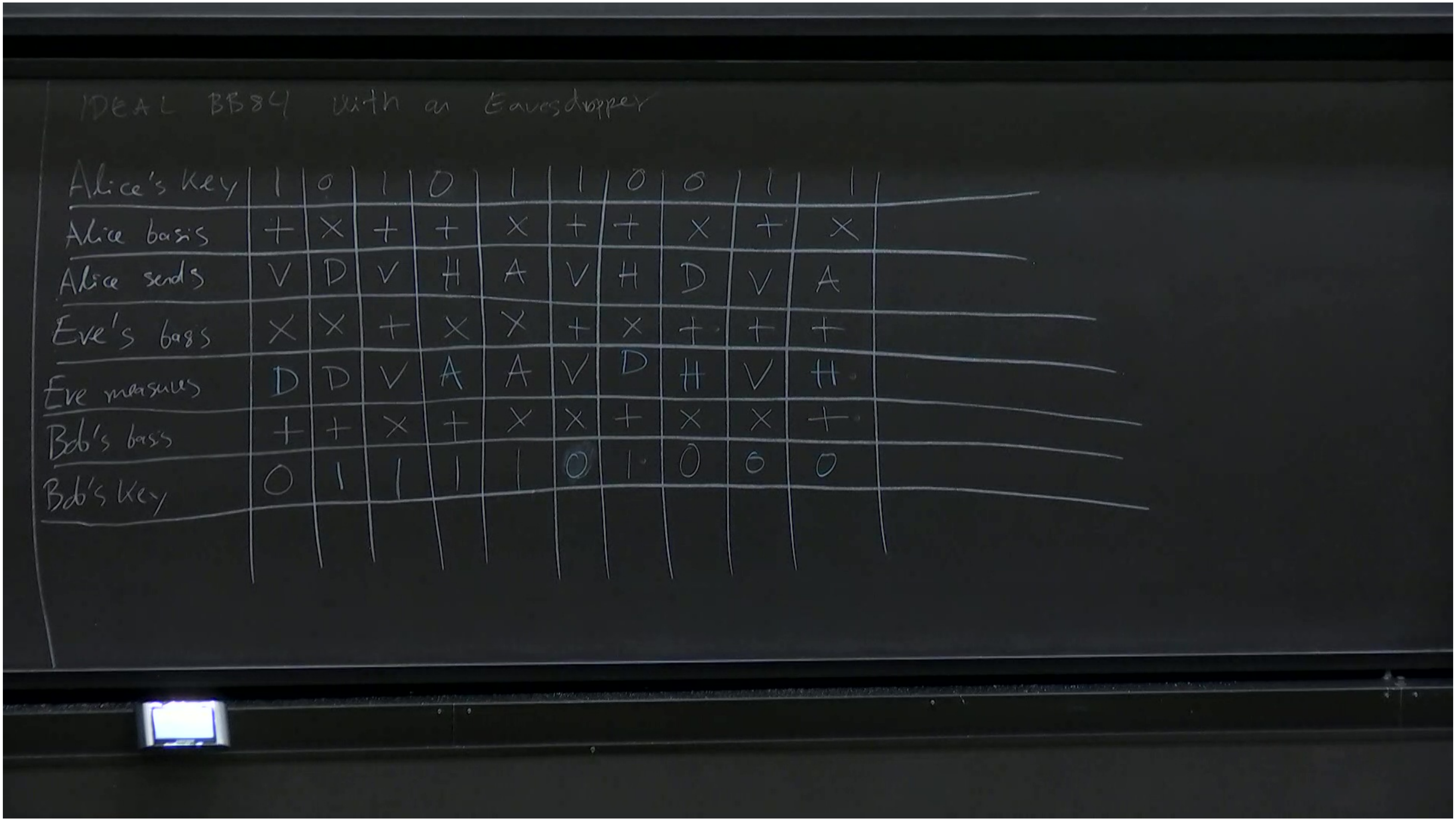
3. Alice encodes the key in the quantum state of qubit — V D V H A V H D V A

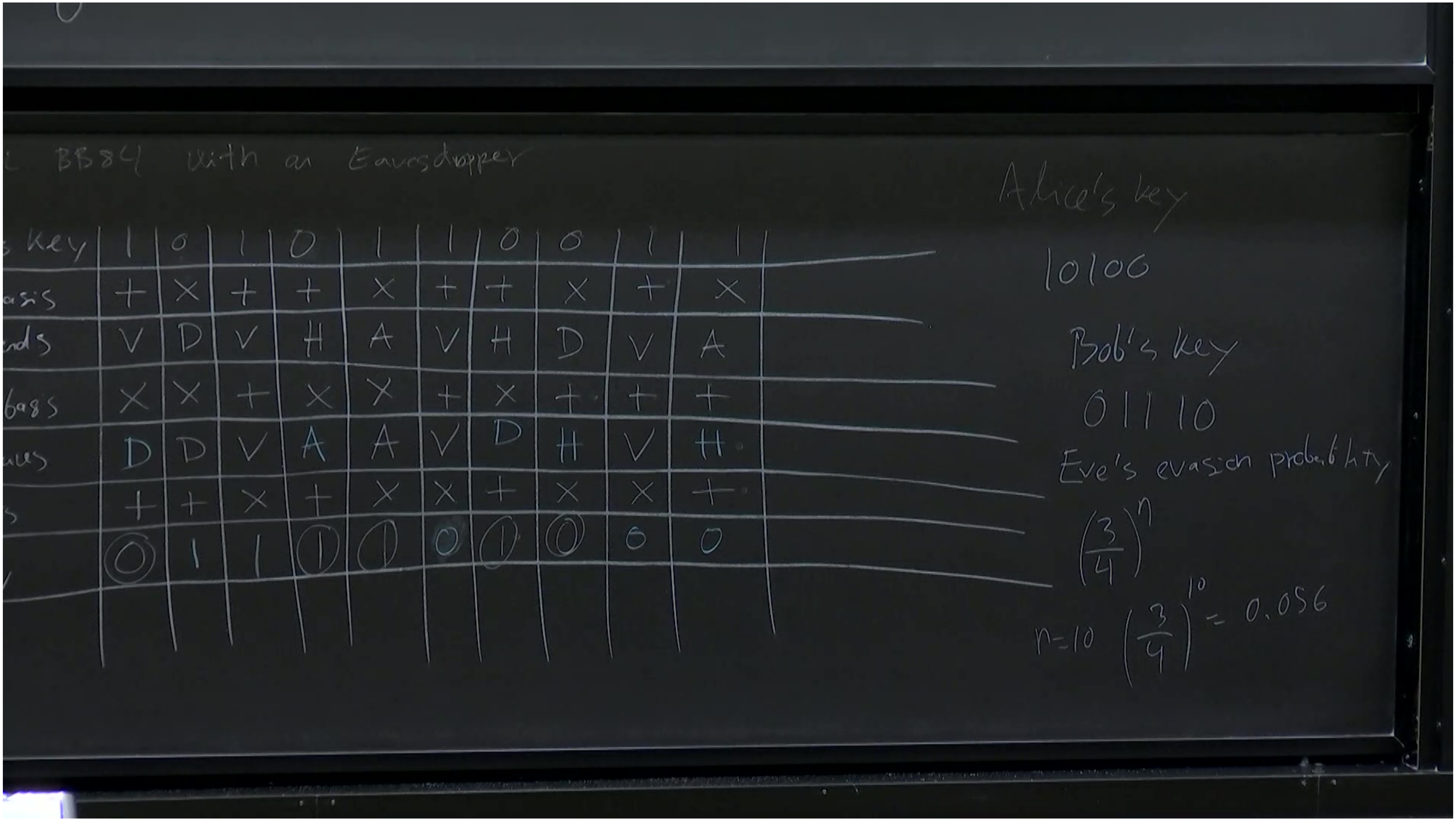
4. Alice sends the qubits through the quantum channel. Bob receives the qubits and selects a basis to measure randomly to retrieve the key — + + × + × × + × × +

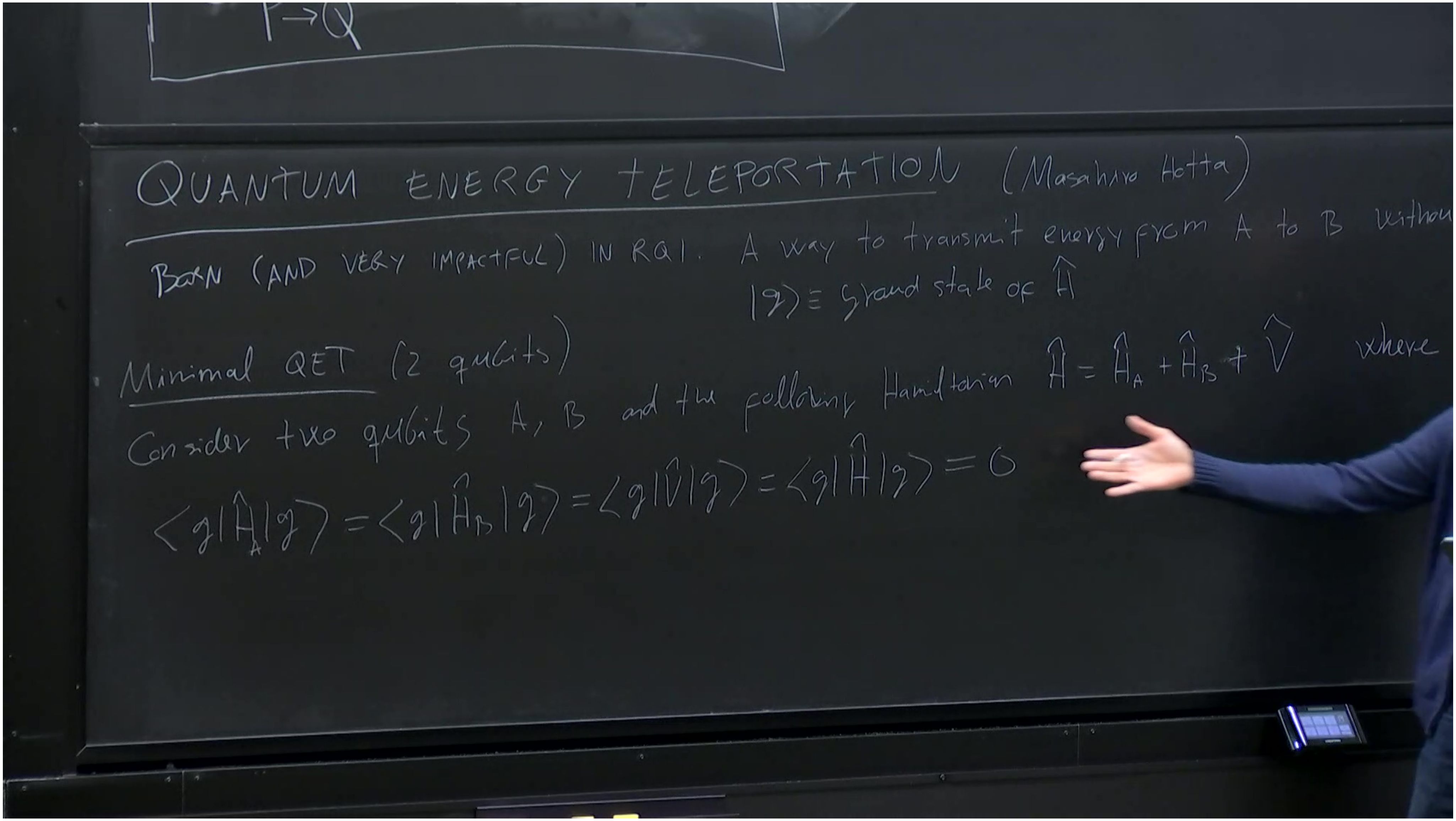
1 1

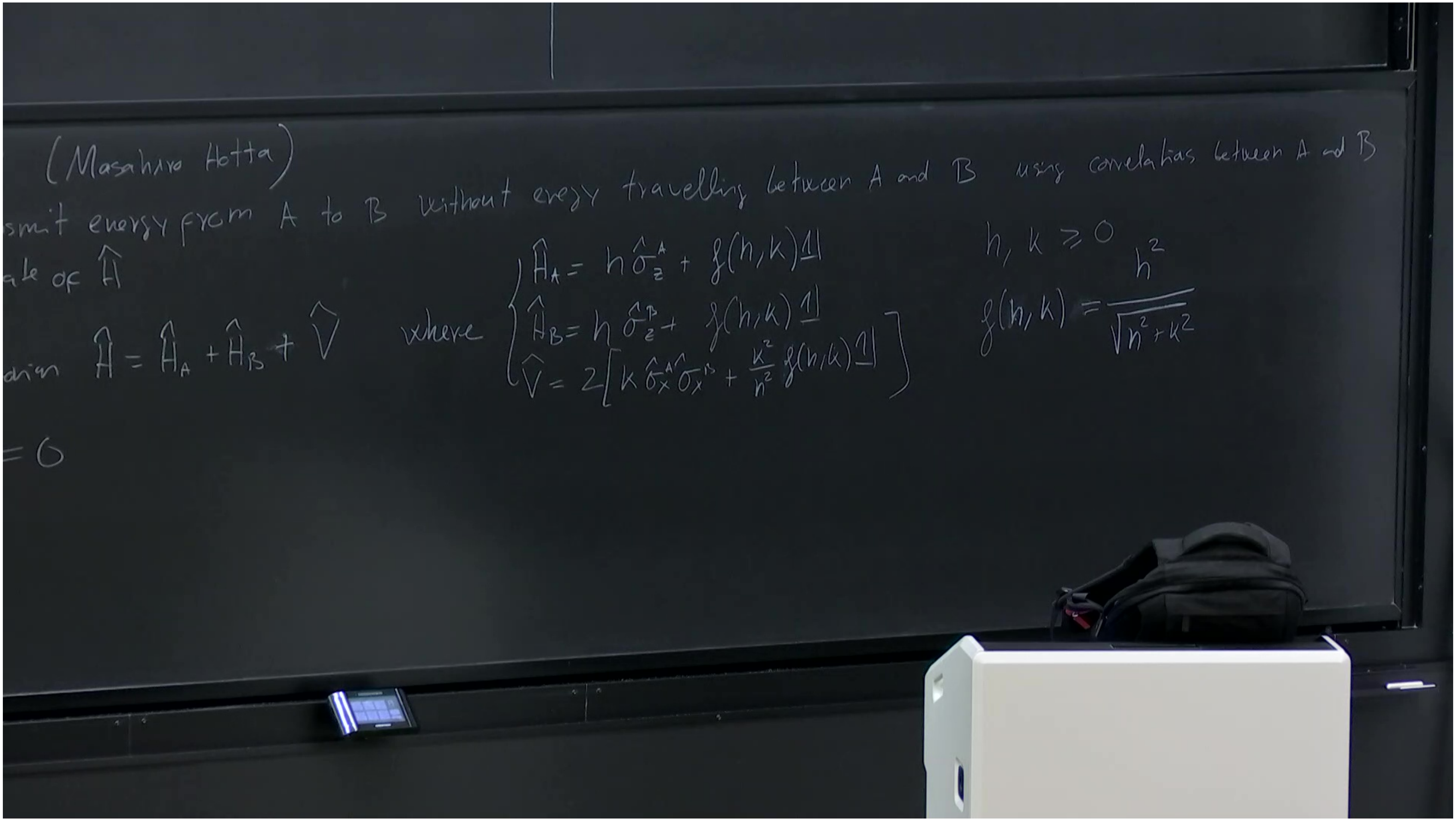

1. Alice generates a key
1010110011
2 Alice generates a sequence of bases to prepare
+×++×++×+×
V D V H A V H D V A
encodes the key in the quantum state of qubit
sends the qubits through the quantum channel
receives the qubits and selects a basis to
randomly to retrieve the key
calls Bob and reveals her basis choices.
Bob chooses bits for the key and tells Alice
Share key 10100

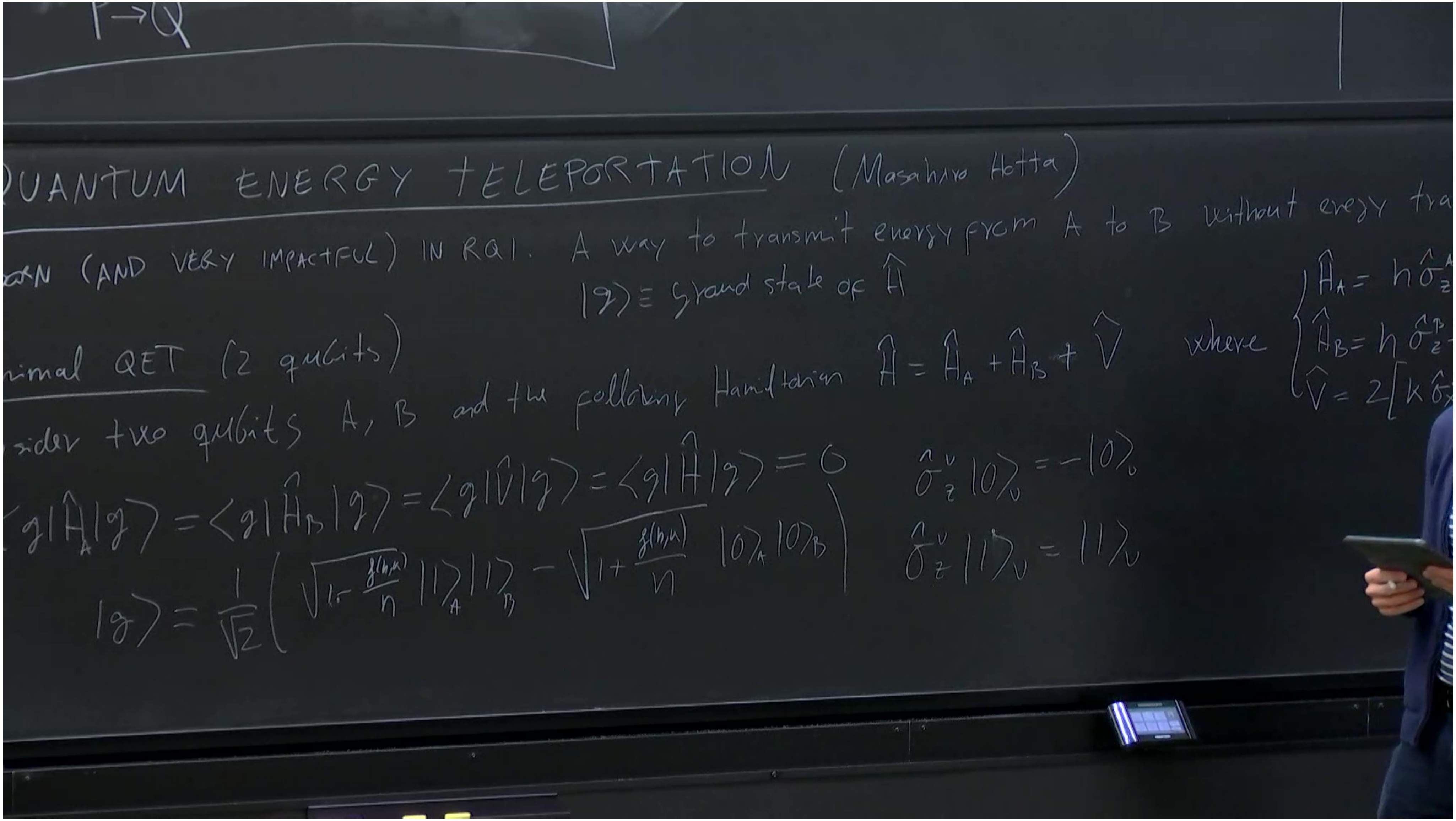

With an Eavesdropper
Alice's key
10100
Bob's key
01110
Eve's evasion probability
(3/4)^n

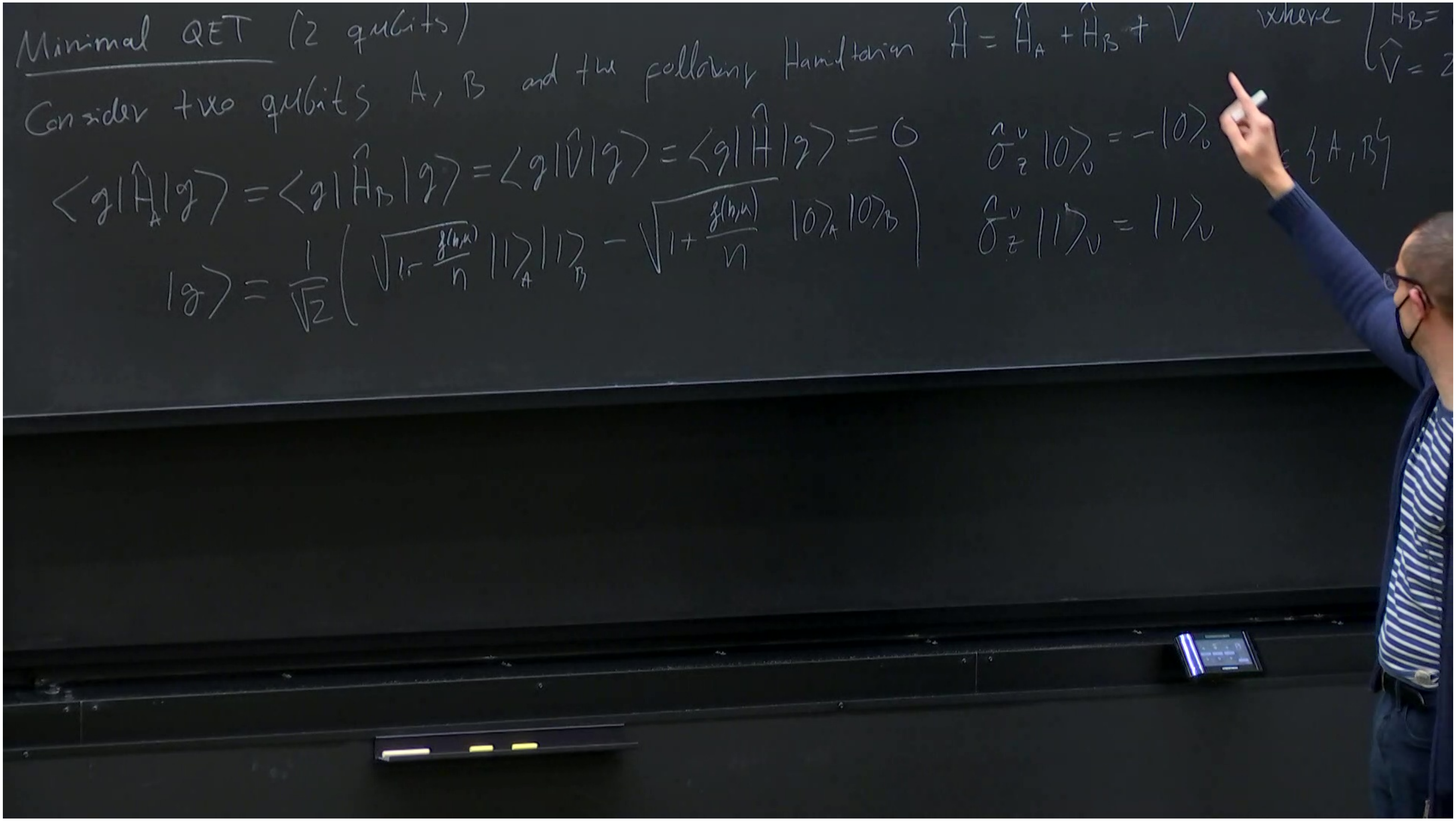

IDEAL BB84 with an Eavesdropper
Alice's key | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1
Alice basis | + | × | + | + | × | + | + | × | + | ×
Alice sends | V | D | V | H | A | V | H | D | V | A
Eve's basis | × | × | + | × | × | + | × | + | + | +
Eve measures | D | D | V | A | A | V | D | H | V | H
Bob's basis | + | + | × | + | × | × | + | × | × | +
Bob's Key | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0

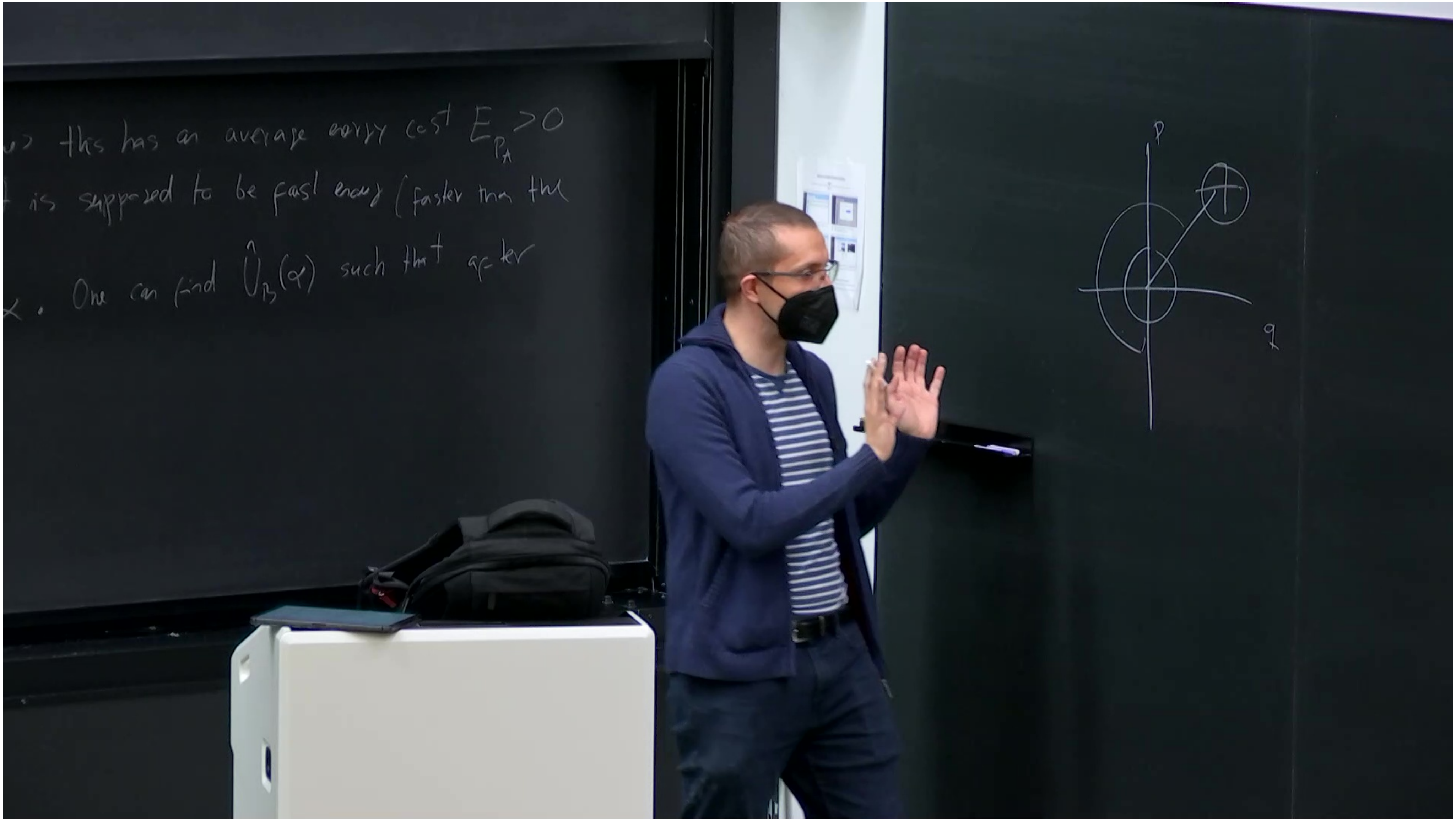

BB84 with an Eavesdropper
key 1 0 1 0 1 1 0 0 1 1
+ × + + × + + × + ×
V D V H A V H D V A
× × + × × + × + + +
D D V A A V D H V H
+ + × + × × + × × +
0 1 1 1 1 0 1 0 0 0
Alice's key
10100
Bob's key
01110
Eve's evasion probability
(3/4)^n
n=10 (3/4)^10 = 0.056

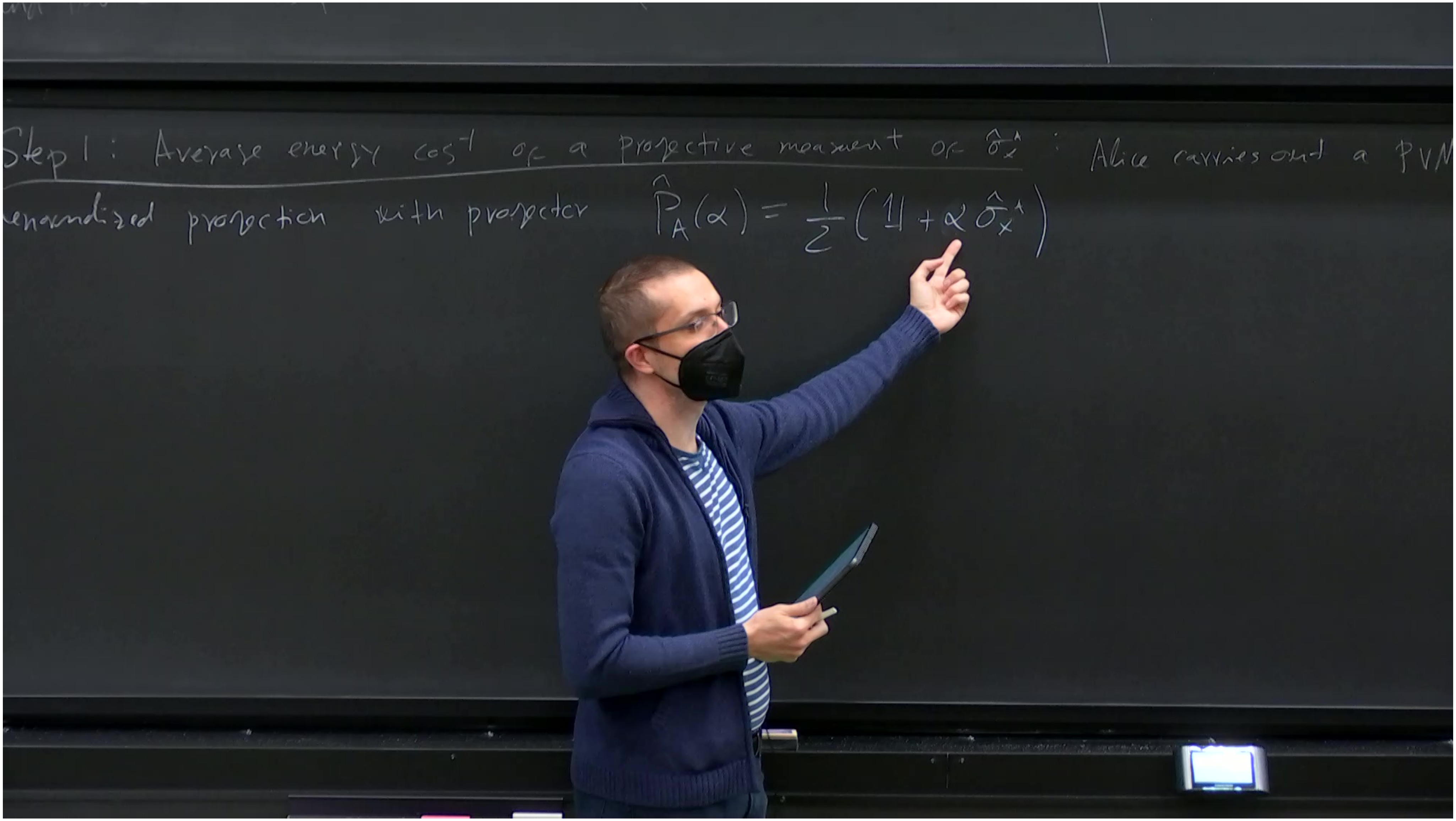

P→Q
QUANTUM ENERGY TELEPORTATION (Masahiro Hotta)
BORN (AND VERY IMPACTFUL) IN RQI. A way to transmit energy from A to B withou
|g⟩ ≡ ground state of Ĥ
Minimal QET (2 qubits)
Consider two qubits A, B and the following Hamiltonian Ĥ = Ĥ_A + Ĥ_B + V̂ where
⟨g|Ĥ_A|g⟩ = ⟨g|Ĥ_B|g⟩ = ⟨g|V̂|g⟩ = ⟨g|Ĥ|g⟩ = 0

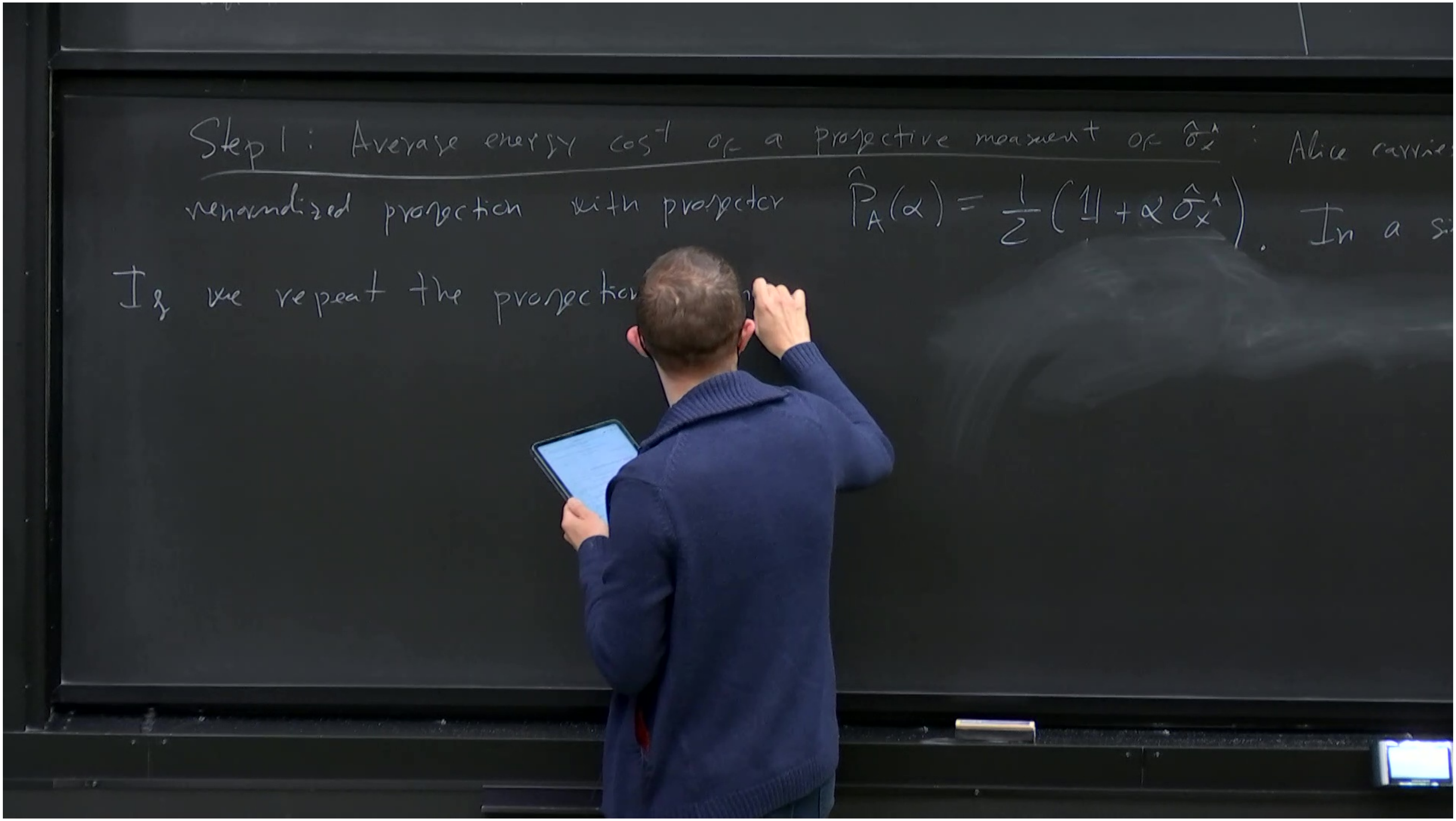

(Masahiro Hotta)
smit energy from A to B without energy travelling between A and B using correlations between A and B
ate of Ĥ
nian Ĥ = Ĥ_A + Ĥ_B + V̂ where
Ĥ_A = h σ̂_z^A + f(h,k) 1
Ĥ_B = h σ̂_z^B + f(h,k) 1
V̂ = 2[k σ̂_x^A σ̂_x^B + k²/h² f(h,k) 1]
h, k ≥ 0
f(h,k) = h² / √(h² + k²)
= 0

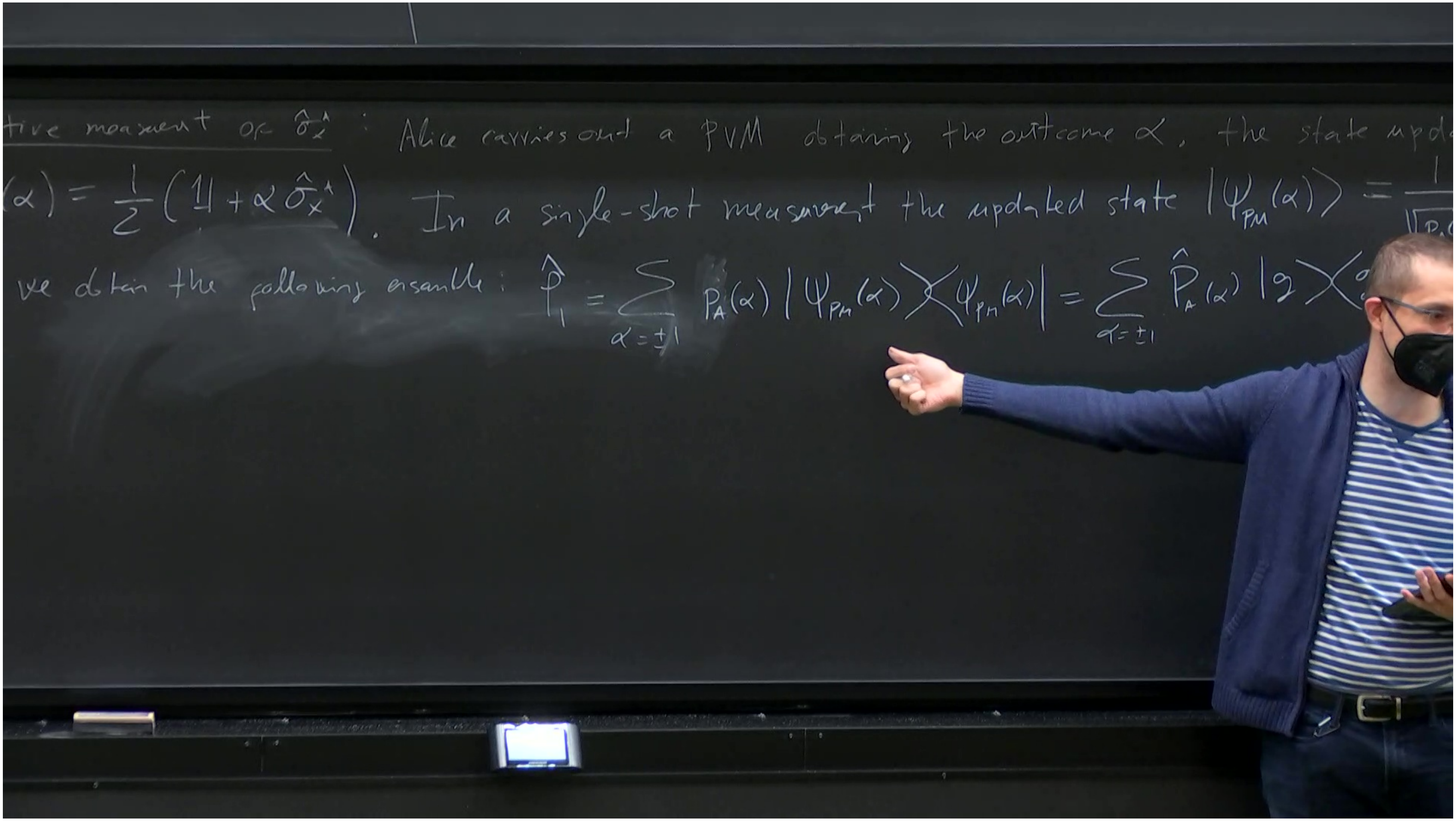

P→Q
QUANTUM ENERGY TELEPORTATION (Masahiro Hotta)
(AND VERY IMPACTFUL) IN RQI. A way to transmit energy from A to B without energy tra
|g⟩ ≡ ground state of Ĥ
imal QET (2 qubits)
sider two qubits A, B and the following Hamiltonian Ĥ = Ĥ_A + Ĥ_B + V̂ where
Ĥ_A = h σ̂_z^A
Ĥ_B = h σ̂_z^B
V̂ = 2[k σ̂_x
⟨g|Ĥ_A|g⟩ = ⟨g|Ĥ_B|g⟩ = ⟨g|V̂|g⟩ = ⟨g|Ĥ|g⟩ = 0
σ̂_z^ν |0⟩_ν = −|0⟩_ν
σ̂_z^ν |1⟩_ν = |1⟩_ν
|g⟩ = 1/√2 (√(1 − g(h,k)/h) |1⟩_A |1⟩_B − √(1 + g(h,k)/h) |0⟩_A |0⟩_B)

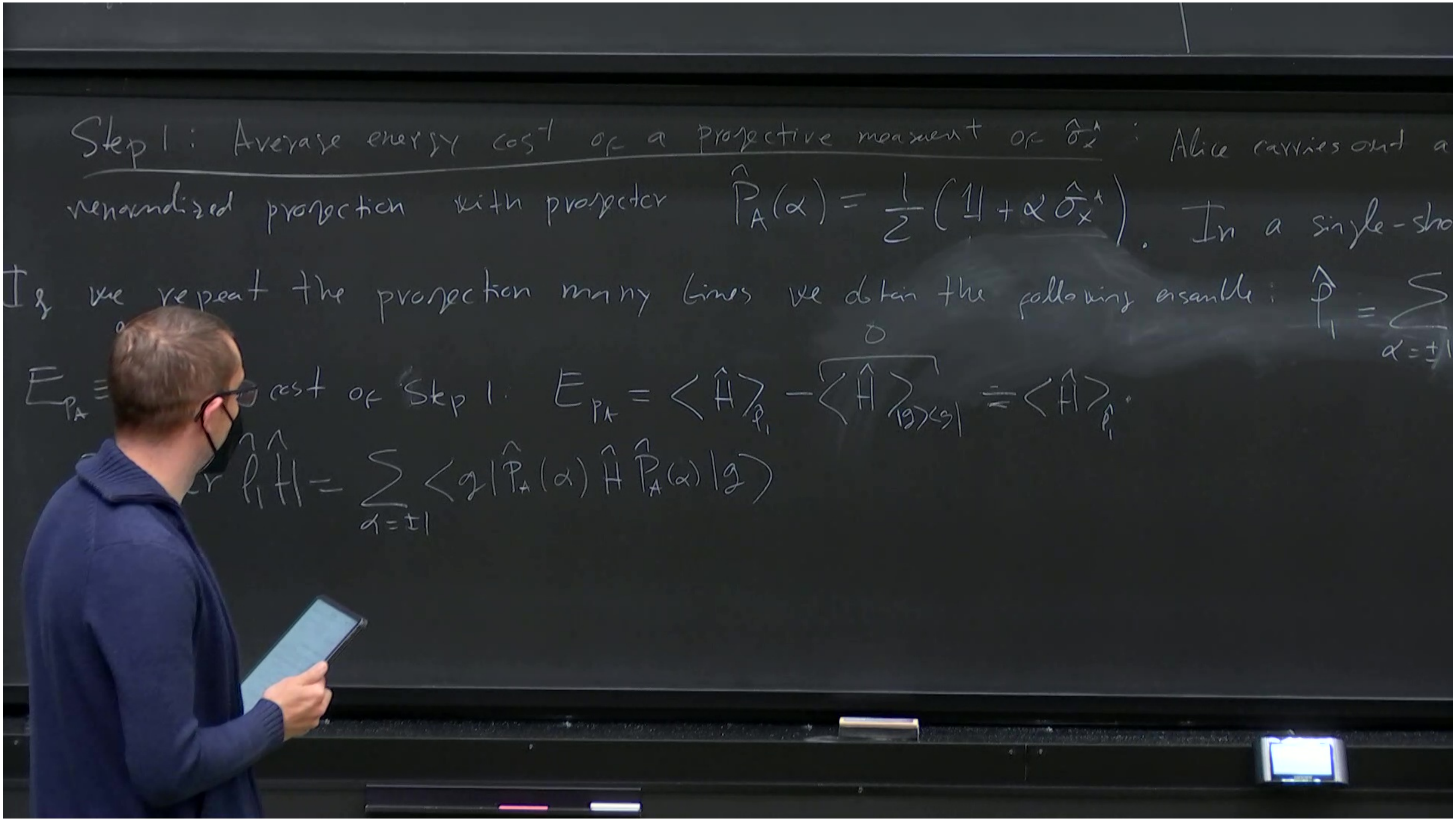

Minimal QET (2 qubits)
Consider two qubits A, B and the following Hamiltonian $\hat{H} = \hat{H}_A + \hat{H}_B + \hat{V}$ where
$\hat{H}_B =$
$\hat{V} = 2$
$\langle g|\hat{H}_A|g\rangle = \langle g|\hat{H}_B|g\rangle = \langle g|\hat{V}|g\rangle = \langle g|\hat{H}|g\rangle = 0$
$\hat{\sigma}_z^{\nu}|0\rangle_\nu = -|0\rangle_\nu$
$\hat{\sigma}_z^{\nu}|1\rangle_\nu = |1\rangle_\nu$
$\nu \in \{A, B\}$
$|g\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{1-\frac{g(h,k)}{n}}|1\rangle_A|1\rangle_B - \sqrt{1+\frac{g(h,k)}{n}}|0\rangle_A|0\rangle_B\right)$

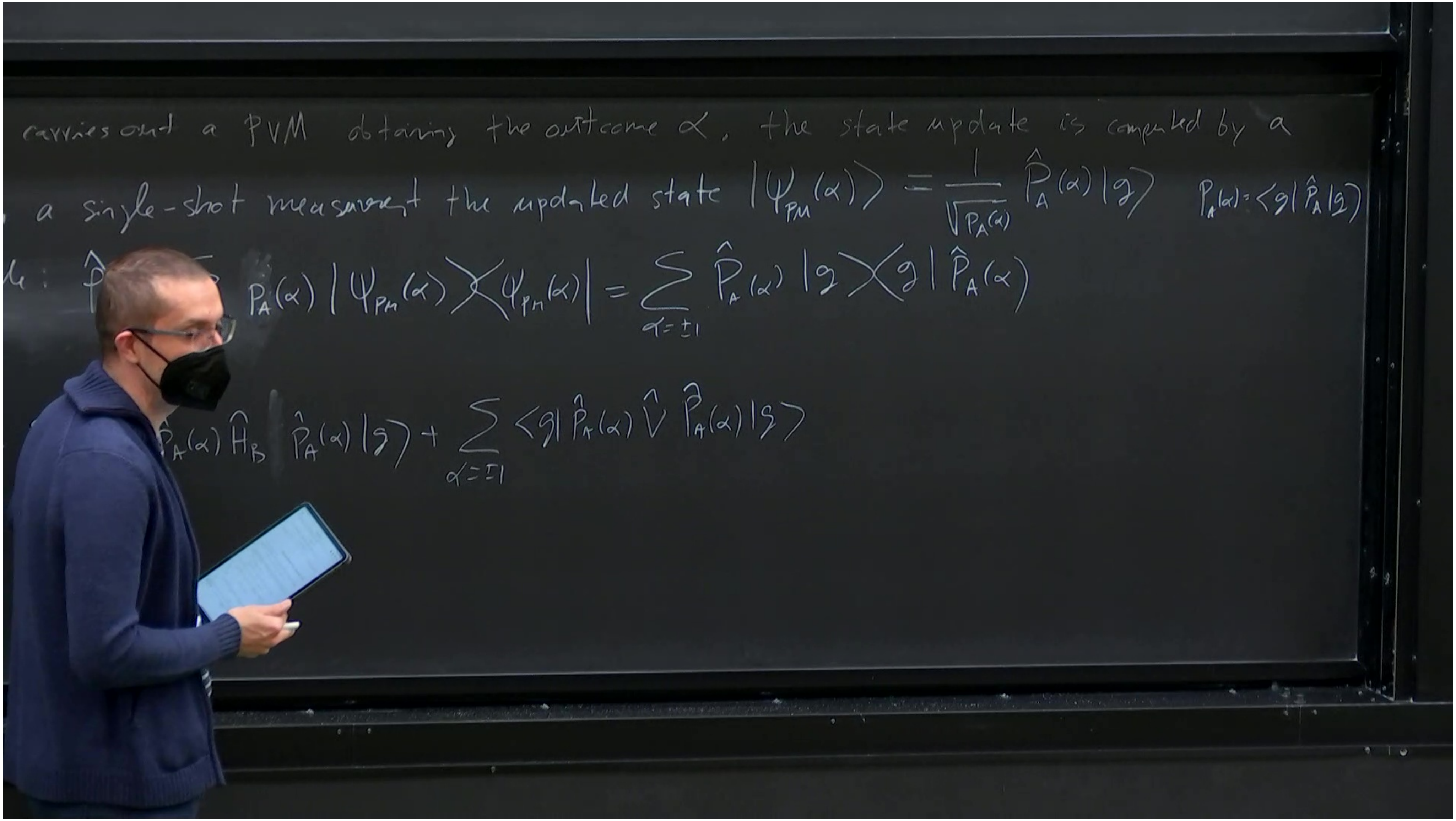

this has an average energy cost $E_{P_A} > 0$
is supposed to be fast enough (faster than the
One can find $\hat{U}_B(\alpha)$ such that after
p
q


Step 1: Average energy cost of a projective measurement of $\hat{\sigma}_x^A$: Alice carries out a PV
enormalized projection with projector $\hat{P}_A(\alpha) = \frac{1}{2}(\mathbb{1} + \alpha\,\hat{\sigma}_x^A)$


Step 1: Average energy cost of a projective measurement of sigma hat x^A : Alice carries
renormalized projection with projector P hat A(α) = 1/2 (1 + α sigma hat x^A). In a
If we repeat the projection


tive measurement of $\hat{\sigma}_x^A$: Alice carries out a PVM obtaining the outcome α, the state upd
$(\alpha) = \frac{1}{2}\left(\mathbb{1} + \alpha\,\hat{\sigma}_x^A\right)$. In a single-shot measurement the updated state $|\psi_{PM}(\alpha)\rangle =$
we obtain the following ensemble: $\hat{\rho}_1 = \sum_{\alpha=\pm1} P_A(\alpha)\,|\psi_{PM}(\alpha)\rangle\langle\psi_{PM}(\alpha)| = \sum_{\alpha=\pm1} \hat{P}_A(\alpha)\,|g\rangle\langle$


Step 1: Average energy cost of a projective measurement of $\hat{\sigma}_x^A$: Alice carries out a
renormalized projection with projector $\hat{P}_A(\alpha) = \frac{1}{2}(\mathbb{1} + \alpha\hat{\sigma}_x^A)$. In a single-sho
If we repeat the projection many times we obtain the following ensemble: $\hat{\rho}_1 = \sum_{\alpha=\pm1}$
$E_{P_A} \equiv$ cost of Step 1: $E_{P_A} = \langle \hat{H} \rangle_{\rho_1} - \langle \hat{H} \rangle_{|g\rangle\langle g|} = \langle \hat{H} \rangle_{\rho_1}$
$\hat{\rho}_1 \hat{H} = \sum_{\alpha=\pm1} \langle g | \hat{P}_A(\alpha) \hat{H} \hat{P}_A(\alpha) | g \rangle$


carries out a PVM obtaining the outcome α, the state update is computed by a
a single-shot measurement the updated state |ψ_PM(α)⟩ = 1/√p_A(α) P̂_A(α)|g⟩
p_A(α) = ⟨g| P̂_A |g⟩
p_A(α) |ψ_PM(α)⟩⟨ψ_PM(α)| = Σ_{α=±1} P̂_A(α) |g⟩⟨g| P̂_A(α)
P̂_A(α) Ĥ_B P̂_A(α) |g⟩ + Σ_{α=±1} ⟨g| P̂_A(α) V̂ P̂_A(α) |g⟩

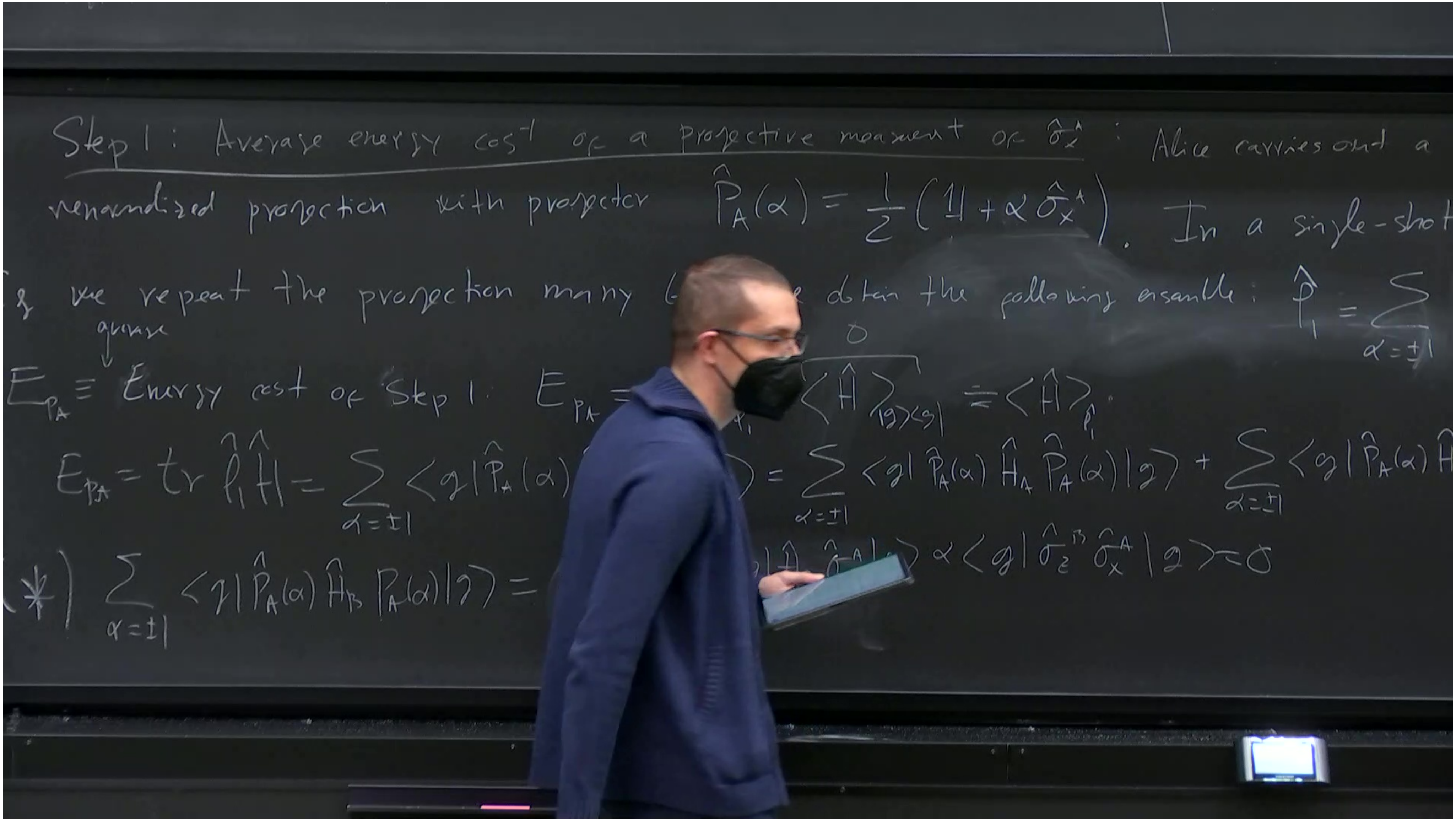
cost of a projective measurement of $\hat{\sigma}_\alpha^A$: Alice carries out a PVM obtaining the outcome

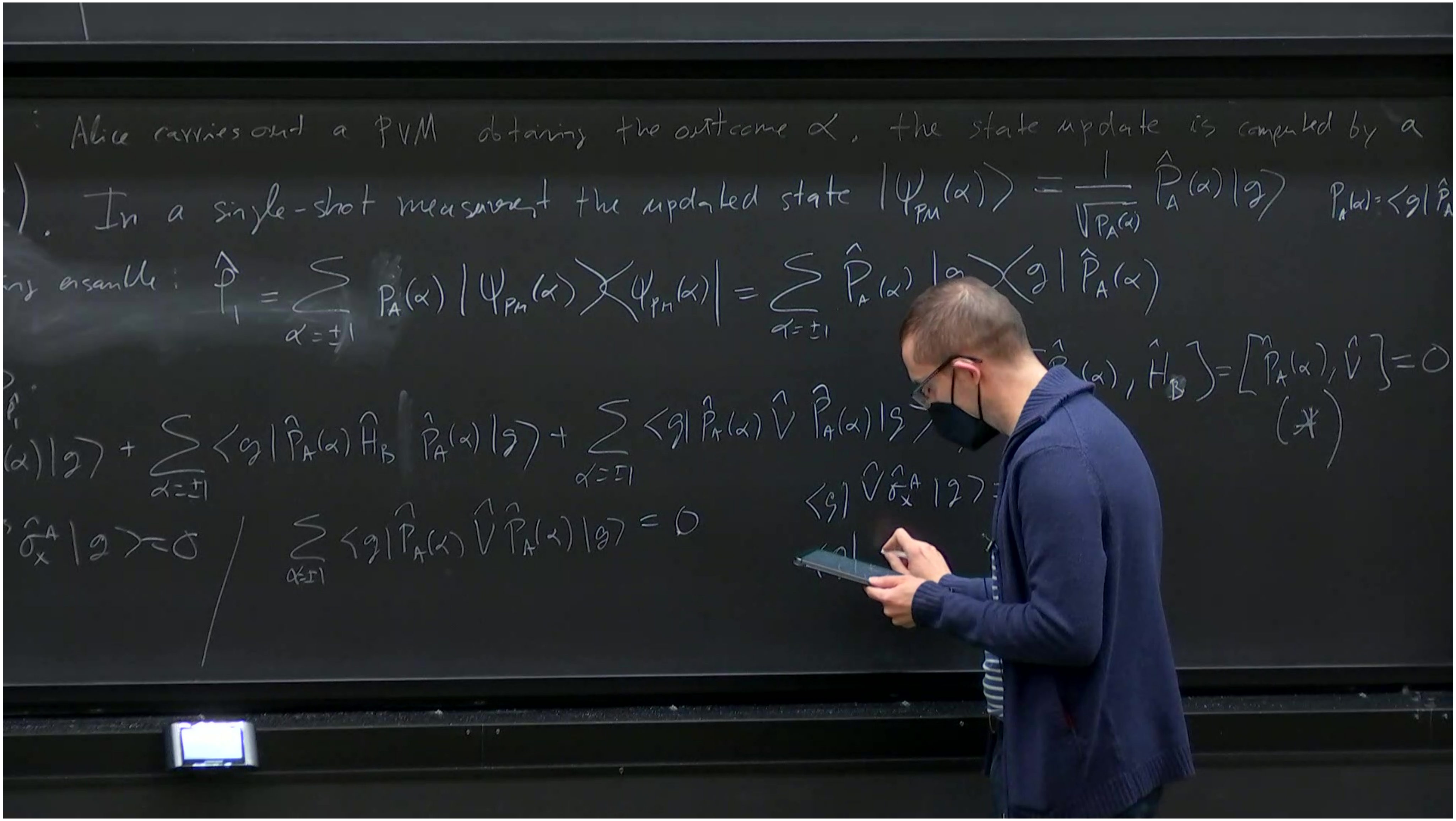
with projector $\hat{P}_A(\alpha) = \frac{1}{2}(\mathbb{1} + \alpha\,\hat{\sigma}_x^A)$. In a single-shot measurement the updated st

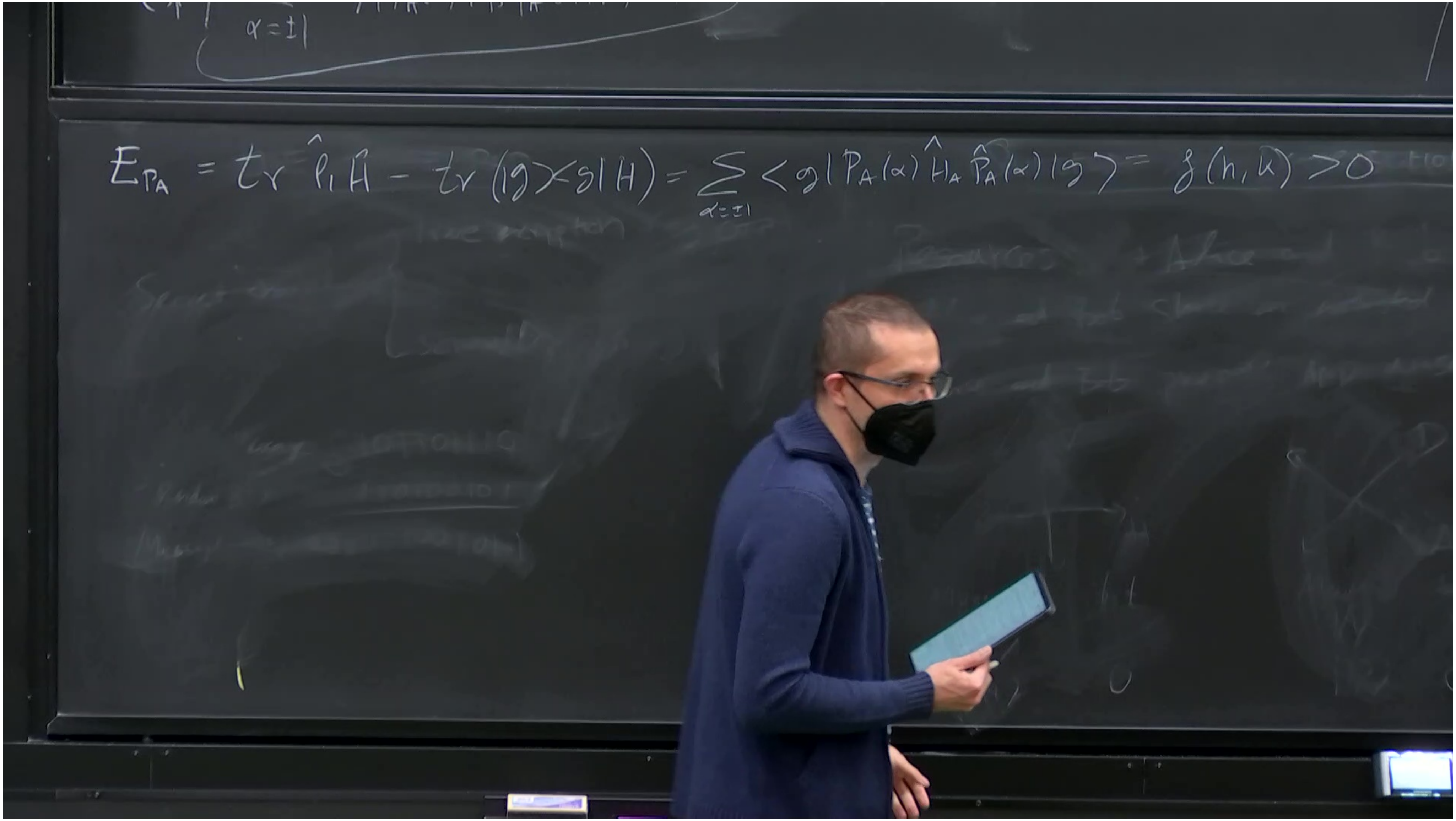
ction many times we obtain the following ensemble: $\hat{\rho}_1 = \sum_{\alpha=\pm1} P_A(\alpha)\,|\psi_{PM}(\alpha)\rangle\langle\psi_{PM}(\alpha)| = \sum_{\alpha=}$

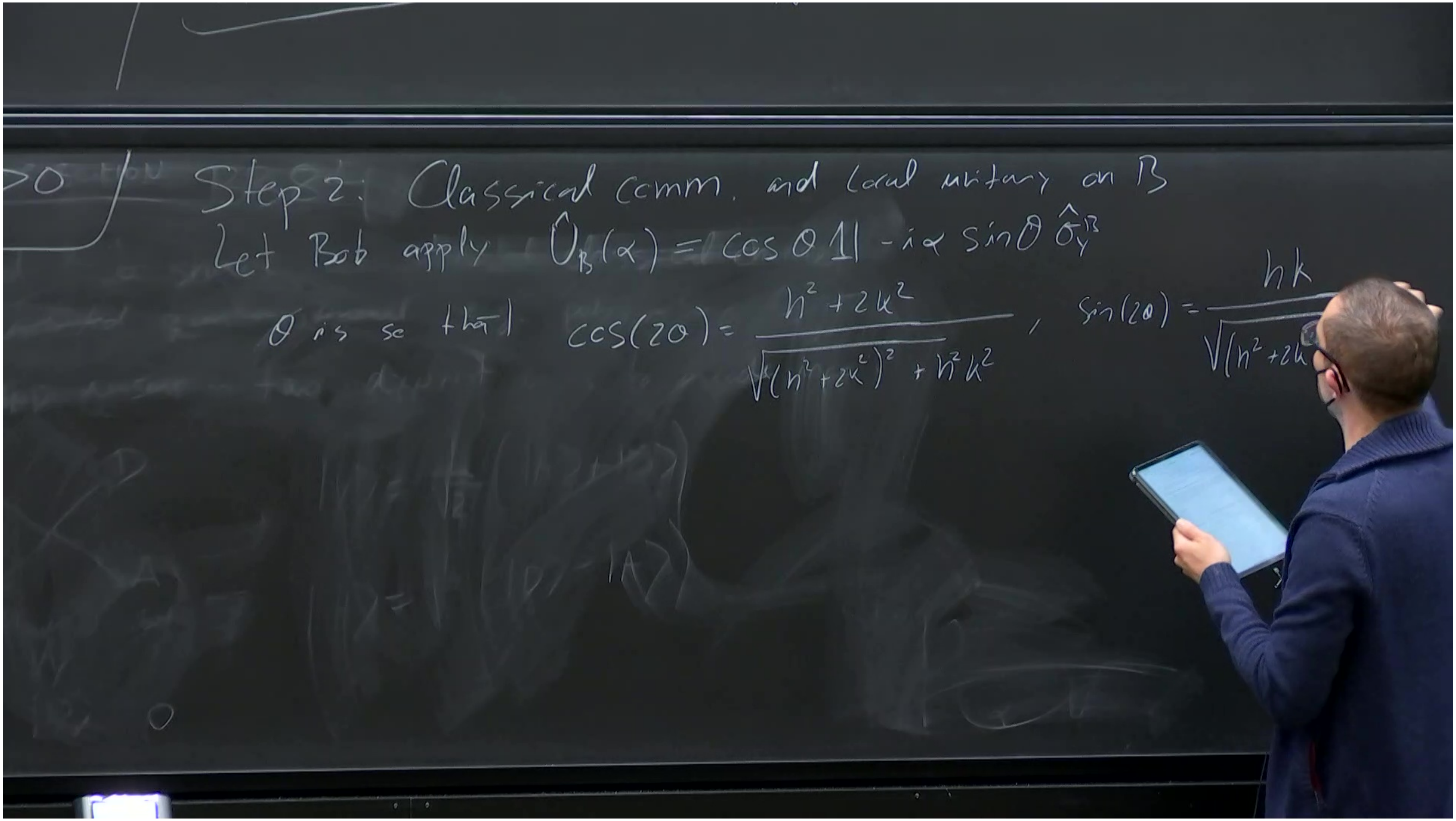
1. $E_{P_A} = \langle \hat{H} \rangle_{\rho_1} - \overbrace{\langle \hat{H} \rangle_{|g\rangle\langle g|}}^{0} \doteq \langle \hat{H} \rangle_{\rho_1}$.

$g|\hat{P}_A(\alpha)\,\hat{H}\,\hat{P}_A(\alpha)|g\rangle = \sum_{\alpha=\pm1} \langle g|\hat{P}_A(\alpha)\,\hat{H}_A\,\hat{P}_A(\alpha)|g\rangle + \sum_{\alpha=\pm1} \langle g|\hat{P}_A(\alpha)\,\hat{H}_B\,\hat{P}_A(\alpha)|g\rangle + \sum_{\alpha=\pm1} \langle g|\hat{P}_A(\alpha)\,\hat{V}$


Step 1: Average energy cost of a projective measurement of σ̂ₓᴬ : Alice carries out a
renormalized projection with projector P̂_A(α) = 1/2 (𝟙 + α σ̂ₓᴬ). In a single-shot
If we repeat the projection many times we obtain the following ensemble: ρ̂₁ = Σ α=±1
E_PA ≡ average Energy cost of Step 1. E_PA = ⟨Ĥ⟩|g⟩⟨g| ≐ ⟨Ĥ⟩ρ̂₁
E_PA = tr ρ̂₁ Ĥ = Σ α=±1 ⟨g| P̂_A(α) = Σ α=±1 ⟨g| P̂_A(α) Ĥ_A P̂_A(α) |g⟩ + Σ α=±1 ⟨g| P̂_A(α) Ĥ
(*) Σ α=±1 ⟨g| P̂_A(α) Ĥ_B P̂_A(α) |g⟩ = α ⟨g| σ̂_z^B σ̂ₓᴬ |g⟩ = 0


Alice carries out a PVM obtaining the outcome α, the state update is computed by a
In a single-shot measurement the updated state |ψ_PM(α)⟩ = 1/√P_A(α) P̂_A(α)|g⟩ P_A(α) = ⟨g|P̂_A
ensemble: ρ̂_1 = Σ_{α=±1} P_A(α) |ψ_PM(α)⟩⟨ψ_PM(α)| = Σ_{α=±1} P̂_A(α)|g⟩⟨g|P̂_A(α)
[P̂_A(α), Ĥ_B] = [P̂_A(α), V̂] = 0
(*)
(α)|g⟩ + Σ_{α=±1} ⟨g|P̂_A(α) Ĥ_B P̂_A(α)|g⟩ + Σ_{α=±1} ⟨g|P̂_A(α) V̂ P̂_A(α)|g⟩
⟨g| V̂ σ̂_x^A |g⟩
σ̂_x^A |g⟩ = 0
Σ_{α=±1} ⟨g|P̂_A(α) V̂ P̂_A(α)|g⟩ = 0

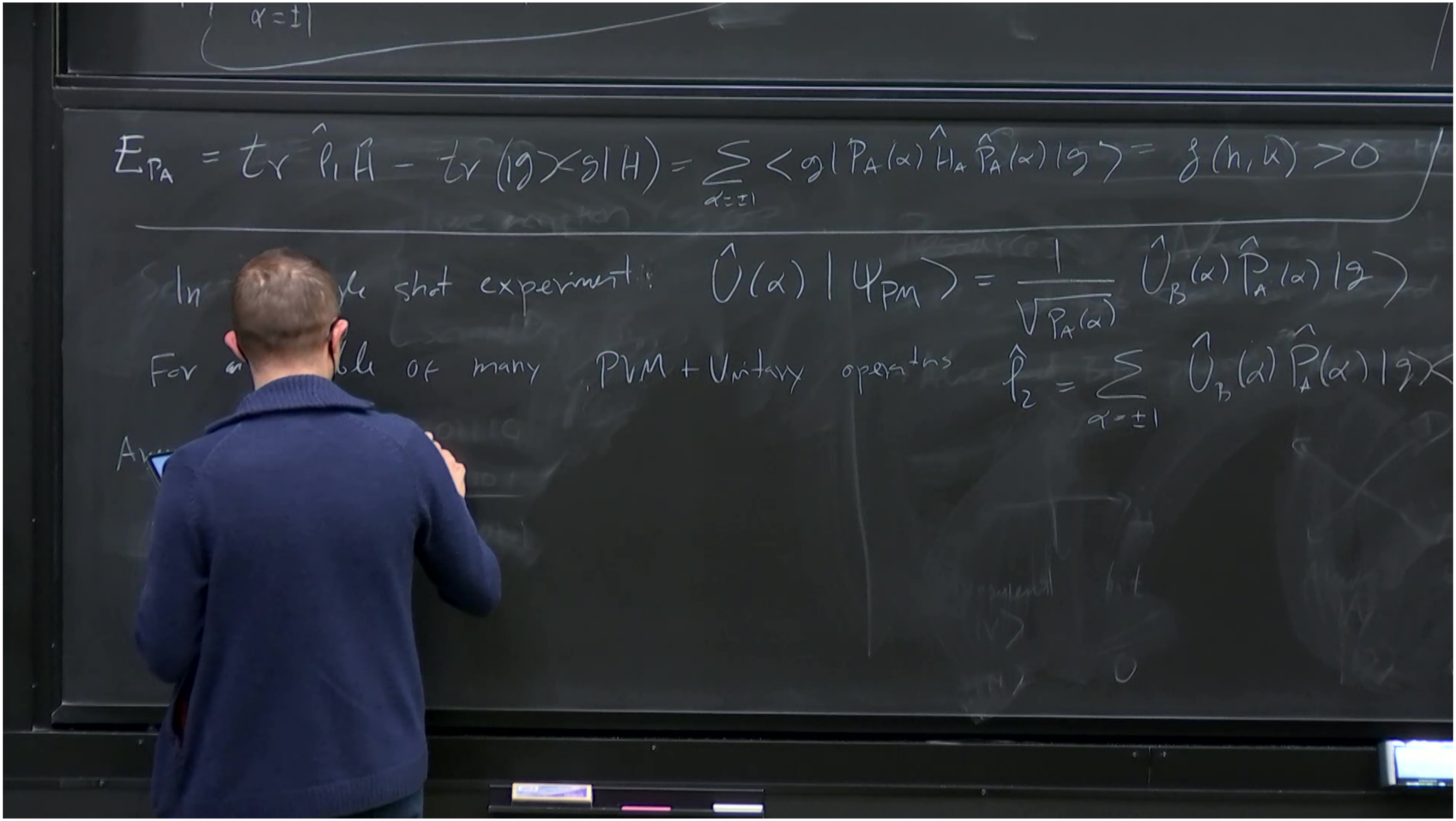

E_{P_A} = tr ρ̂_1 Ĥ − tr(|g⟩⟨g| H) = Σ_{α=±1} ⟨g| P_A(α) Ĥ_A P̂_A(α) |g⟩ = f(h, k) > 0


Step 2: Classical comm. and local unitary on B
Let Bob apply $\hat{U}_B(\alpha) = \cos\theta\, \mathbb{1} - i\alpha \sin\theta\, \hat{\sigma}_y^B$
θ is so that $\cos(2\theta) = \frac{h^2+2k^2}{\sqrt{(h^2+2k^2)^2 + h^2k^2}}$, $\sin(2\theta) = \frac{hk}{\sqrt{(h^2+2k}}$

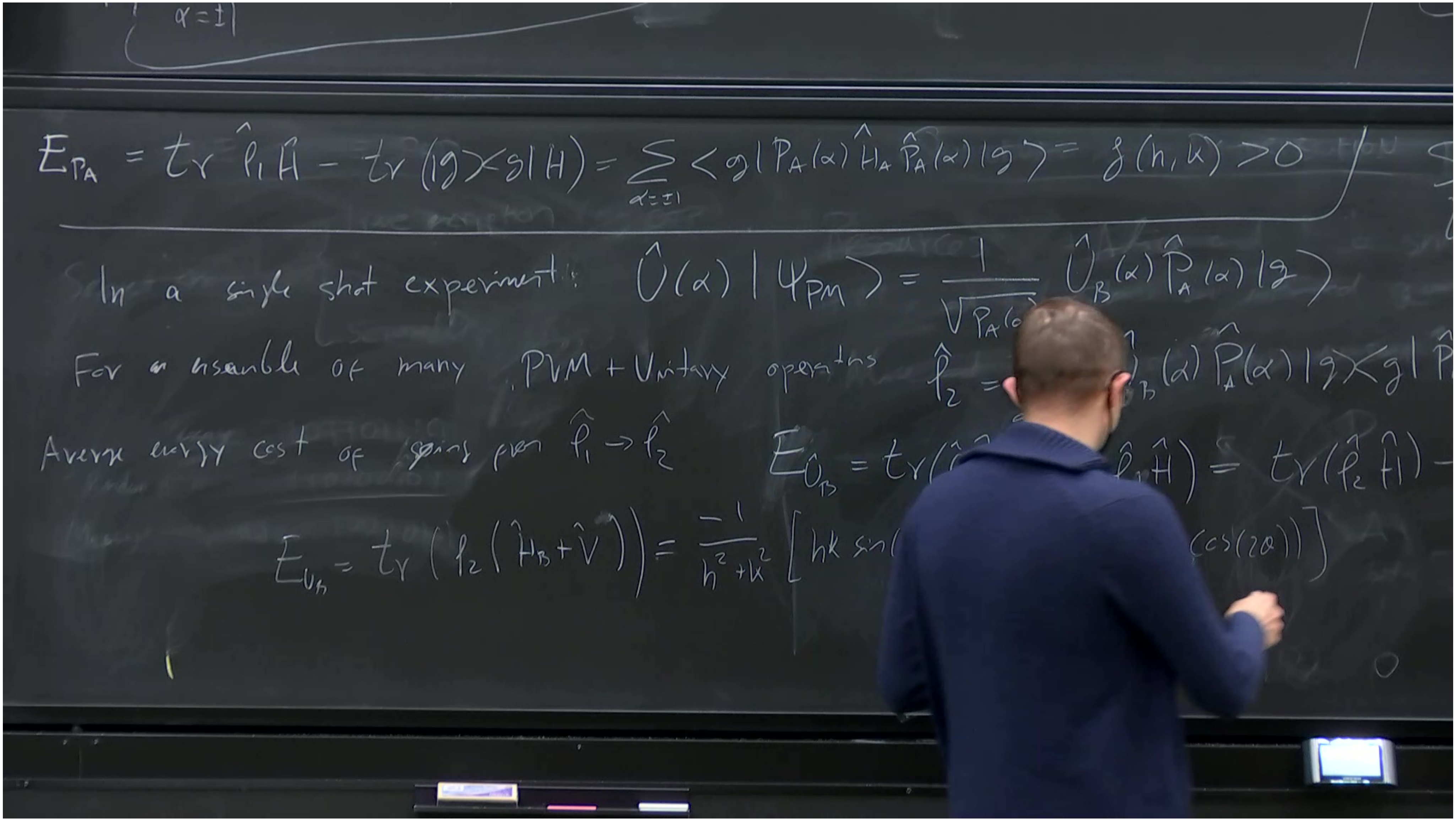
Step 2: Classical comm. and local unitary on B

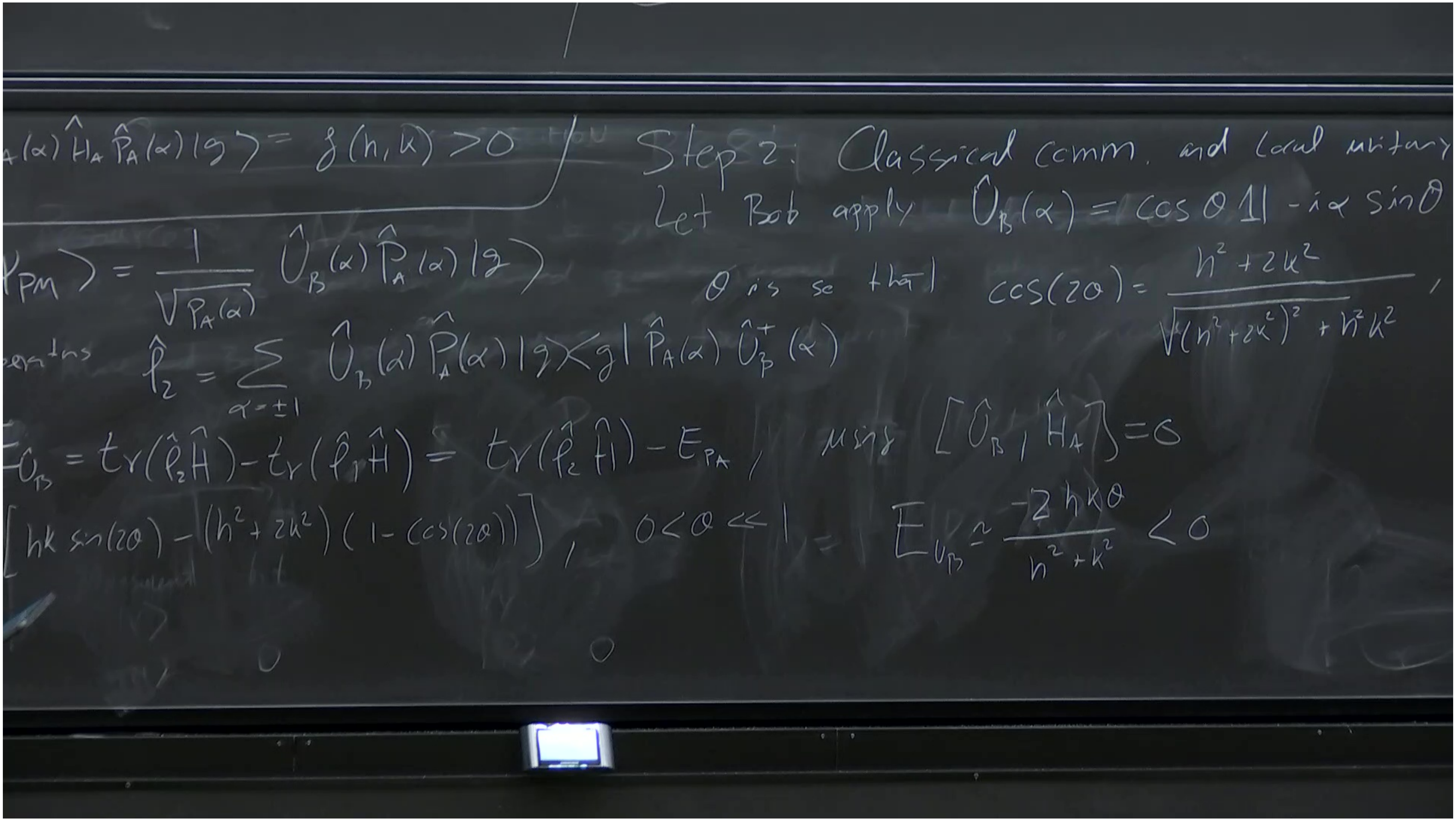
Let Bob apply $\hat{U}_B(\alpha) = \cos\theta \, \mathbb{1} - i\alpha \sin\theta \, \hat{\sigma}_y^B$

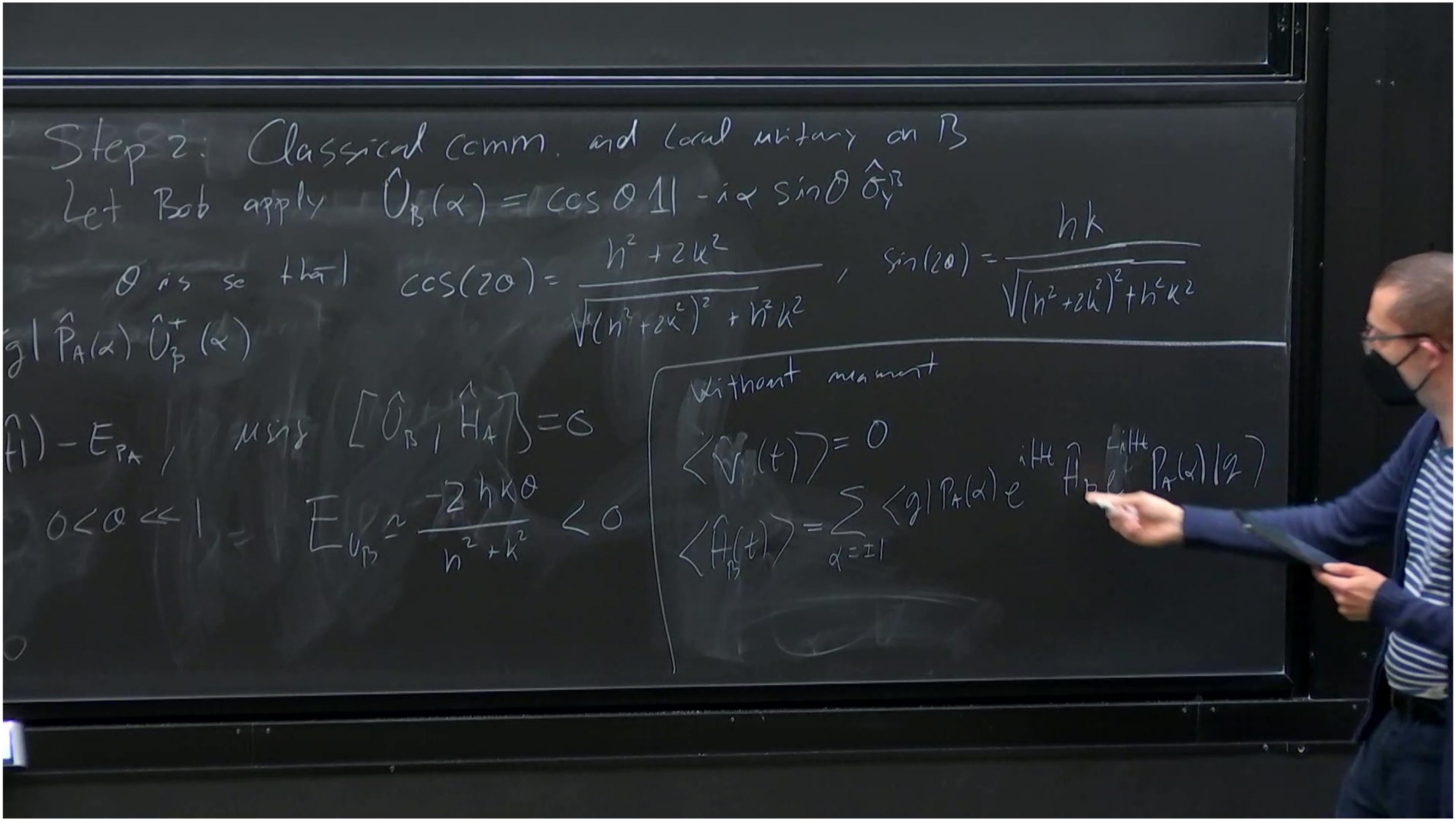
θ is so that $\cos(2\theta) = \dfrac{h^2 + 2k^2}{\sqrt{(h^2+2k^2)^2 + h^2k^2}}$, $\sin(2\theta) = \dfrac{hk}{\sqrt{(h^2+2k^2)^2 + h^2k^2}}$

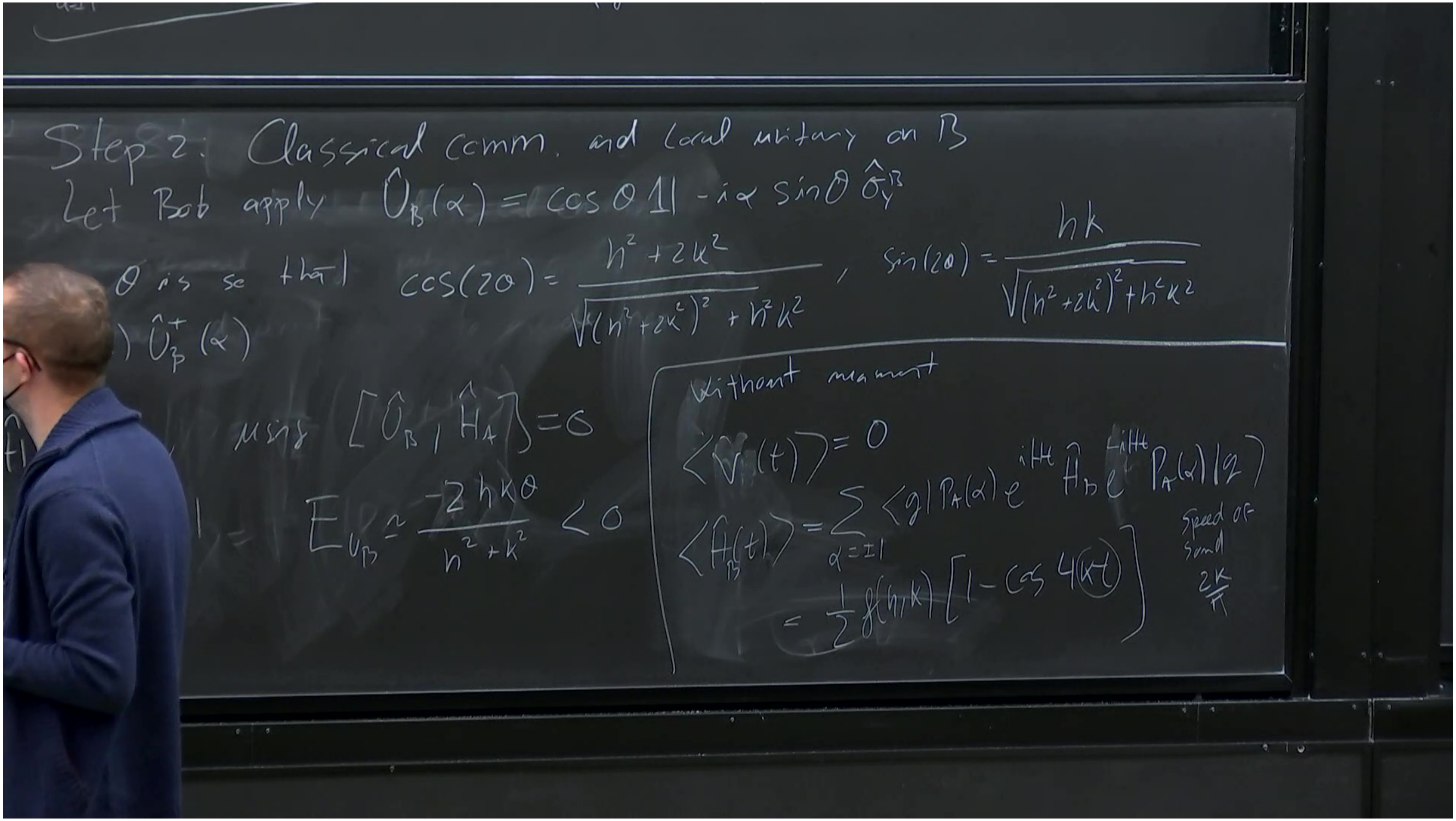


E_PA = tr ρ̂1 Ĥ − tr(|g⟩⟨g|H) = Σ_{α=±1} ⟨g|P_A(α) Ĥ_A P̂_A(α)|g⟩ = f(h,k) > 0
shot experiment: Û(α)|Ψ_PM⟩ = 1/√P_A(α) Û_B(α) P̂_A(α)|g⟩
For of many PVM + Unitary operations ρ̂_2 = Σ_{α=±1} Û_B(α) P̂_A(α)|g⟩


$E_{P_A} = tr\, \hat{\rho}_1 \hat{H} - tr(|g\rangle\langle g| H) = \sum_{\alpha=\pm 1} \langle g| P_A(\alpha) \hat{H}_A \hat{P}_A(\alpha) |g\rangle = f(h,k) > 0$
In a single shot experiment: $\hat{U}(\alpha)\, |\Psi_{PM}\rangle = \frac{1}{\sqrt{P_A(\alpha)}} \hat{U}_B(\alpha) \hat{P}_A(\alpha) |g\rangle$
For an ensemble of many PVM + Unitary operations
Average energy cost of going from $\hat{\rho}_1 \to \hat{\rho}_2$
$E_{U_B} = tr\left(\hat{\rho}_2 (\hat{H}_B + \hat{V})\right) = \frac{-1}{h^2+k^2}\left[hk \sin(\ \ \cos(2\alpha))\right]$


Step 2: Classical comm. and local unitary
Let Bob apply $\hat{U}_B(\alpha) = \cos\theta\, 1\!\!1 - i\alpha \sin\theta$
θ is so that $\cos(2\theta) = \frac{h^2+2k^2}{\sqrt{(h^2+2k^2)^2 + h^2k^2}}$,
$\hat{\rho}_2 = \sum_{\alpha=\pm1} \hat{U}_B(\alpha)\hat{P}_A(\alpha)|g\rangle\langle g|\hat{P}_A(\alpha)\hat{U}_B^\dagger(\alpha)$
$E_{U_B} = tr(\hat{\rho}_2\hat{H}) - tr(\hat{\rho}_1\hat{H}) = tr(\hat{\rho}_2\hat{H}) - E_{P_A}$, using $[\hat{U}_B, \hat{H}_A] = 0$
$0<\theta\ll1 \Rightarrow E_{U_B} \simeq \frac{-2hk\theta}{h^2+k^2} < 0$


Step 2: Classical comm. and local unitary on B
Let Bob apply
θ is so that
without measurement

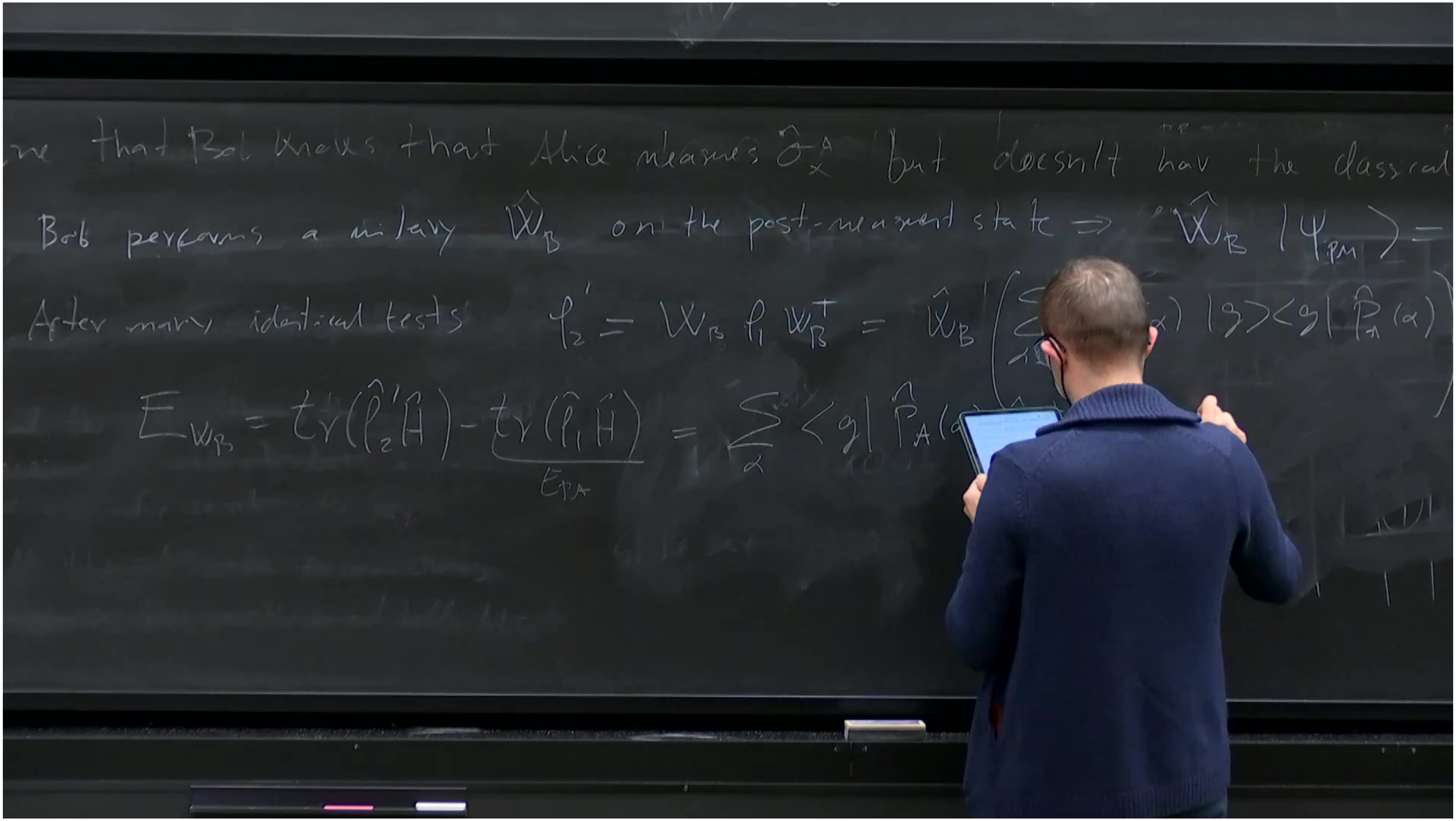

Step 2: Classical comm. and local unitary on B
Let Bob apply $\hat{U}_B(\alpha) = \cos\theta \, \mathbb{1} - i\alpha \sin\theta \, \hat{\sigma}_y^B$
θ is so that $\cos(2\theta) = \frac{h^2+2k^2}{\sqrt{(h^2+2k^2)^2+h^2k^2}}$, $\sin(2\theta) = \frac{hk}{\sqrt{(h^2+2k^2)^2+h^2k^2}}$
$\hat{U}_B^\dagger(\alpha)$
using $[\hat{U}_B, \hat{H}_A] = 0$
$E_{U_B} \simeq \frac{-2hk\theta}{h^2+k^2} < 0$
Without measurement
$\langle \hat{V}(t) \rangle = 0$
$\langle \hat{H}_B(t) \rangle = \sum_{\alpha=\pm1} \langle g | P_A(\alpha) e^{i\hat{H}t} \hat{H}_B e^{-i\hat{H}t} P_A(\alpha) | g \rangle$
$= \frac{1}{2} f(h,k) [1 - \cos 4(kt)]$
Speed of sound
$2k$

eavesdropper

...ice measures $\hat{\sigma}_x^A$ but doesn't have the classical bit α

on the post-measured state $\Rightarrow$ $\hat{W}_B |\Psi_{PM}\rangle = \frac{1}{\sqrt{p_A(\alpha)}} \hat{W}_B \hat{P}_A(\alpha)|g\rangle$

$$\rho'_2 = W_B \rho_1 W_B^\dagger = \hat{W}_B \left(\sum_{\alpha=\pm 1} \hat{P}_A(\alpha)\, |g\rangle\langle g|\, \hat{P}_A(\alpha) \right) \hat{W}_B^\dagger$$


that Bob knows that Alice measures σ̂ₓᴬ but doesn't hav the classical
Bob performs a unitary Ŵ_B on the post-measurement state ⇒ Ŵ_B |ψ_PM⟩ =
After many identical tests ρ₂' = W_B ρ₁ W_B† = Ŵ_B
E_{W_B} = tr(ρ̂₂'Â) - tr(ρ̂₁Â) = Σ_α <g| P̂_A(
E_PA