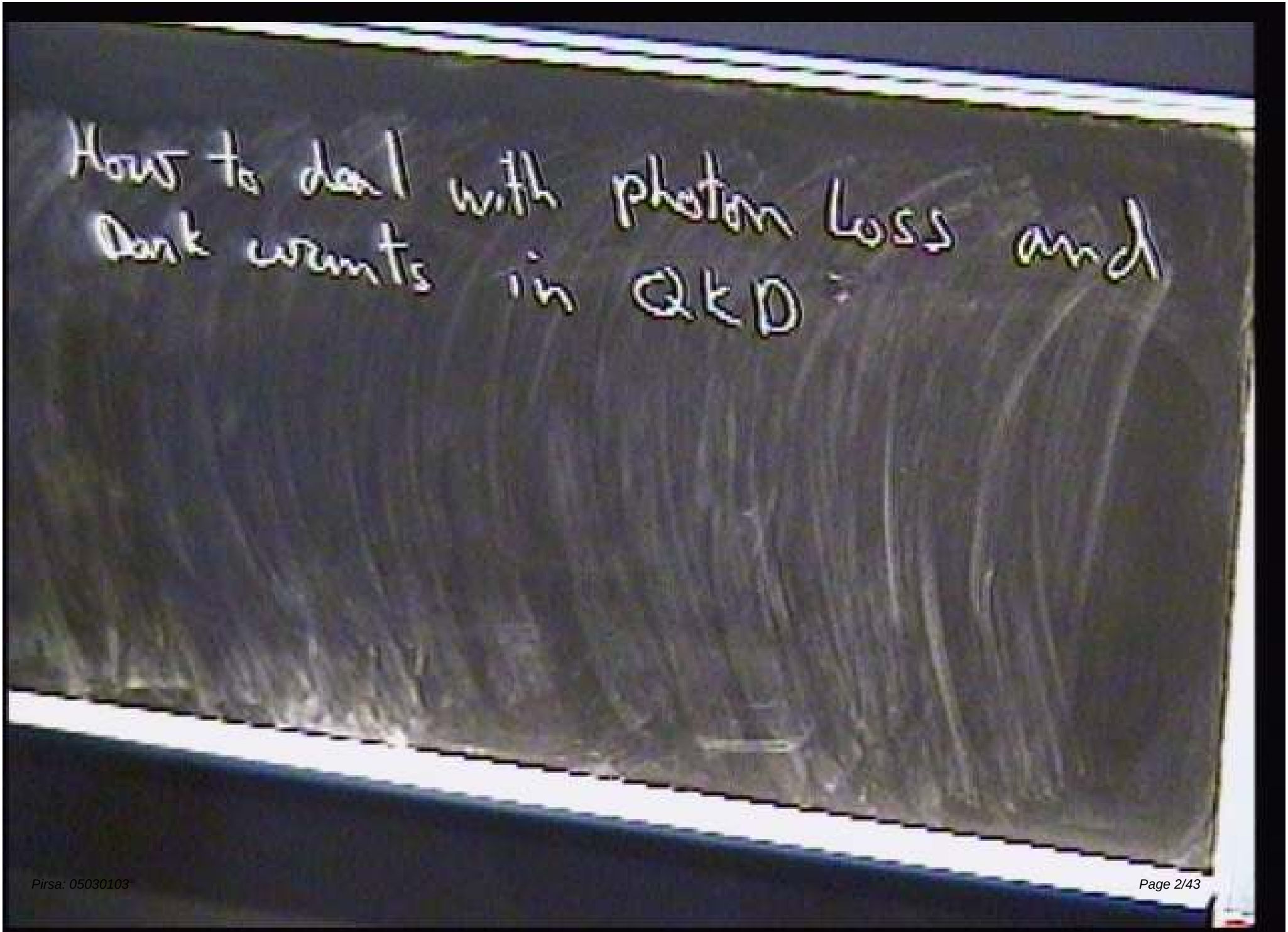
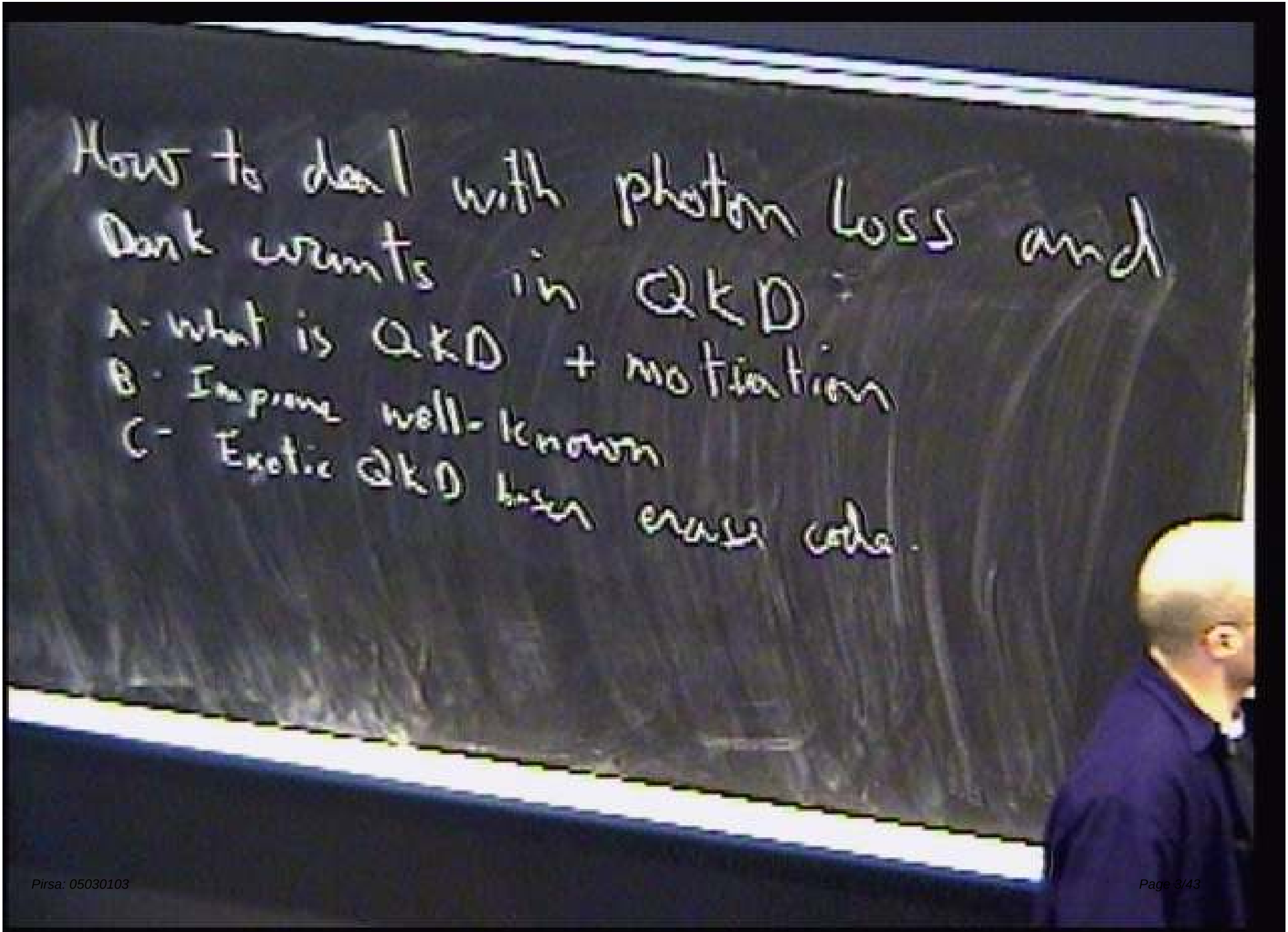
Title: Dealing with Photon Loss and Dark Counts in Quantum Key Distribution

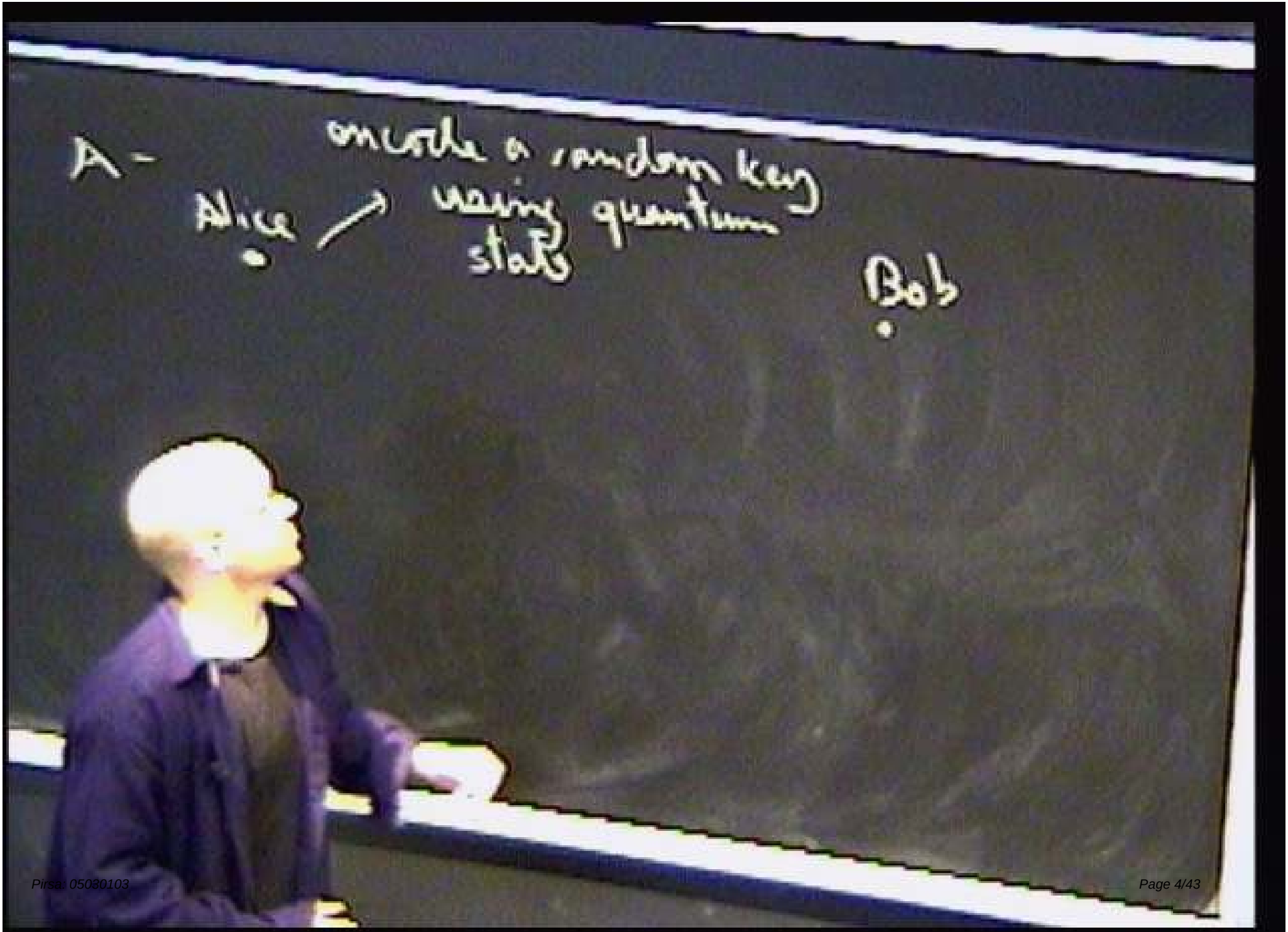
Date: Mar 09, 2005 04:05 PM

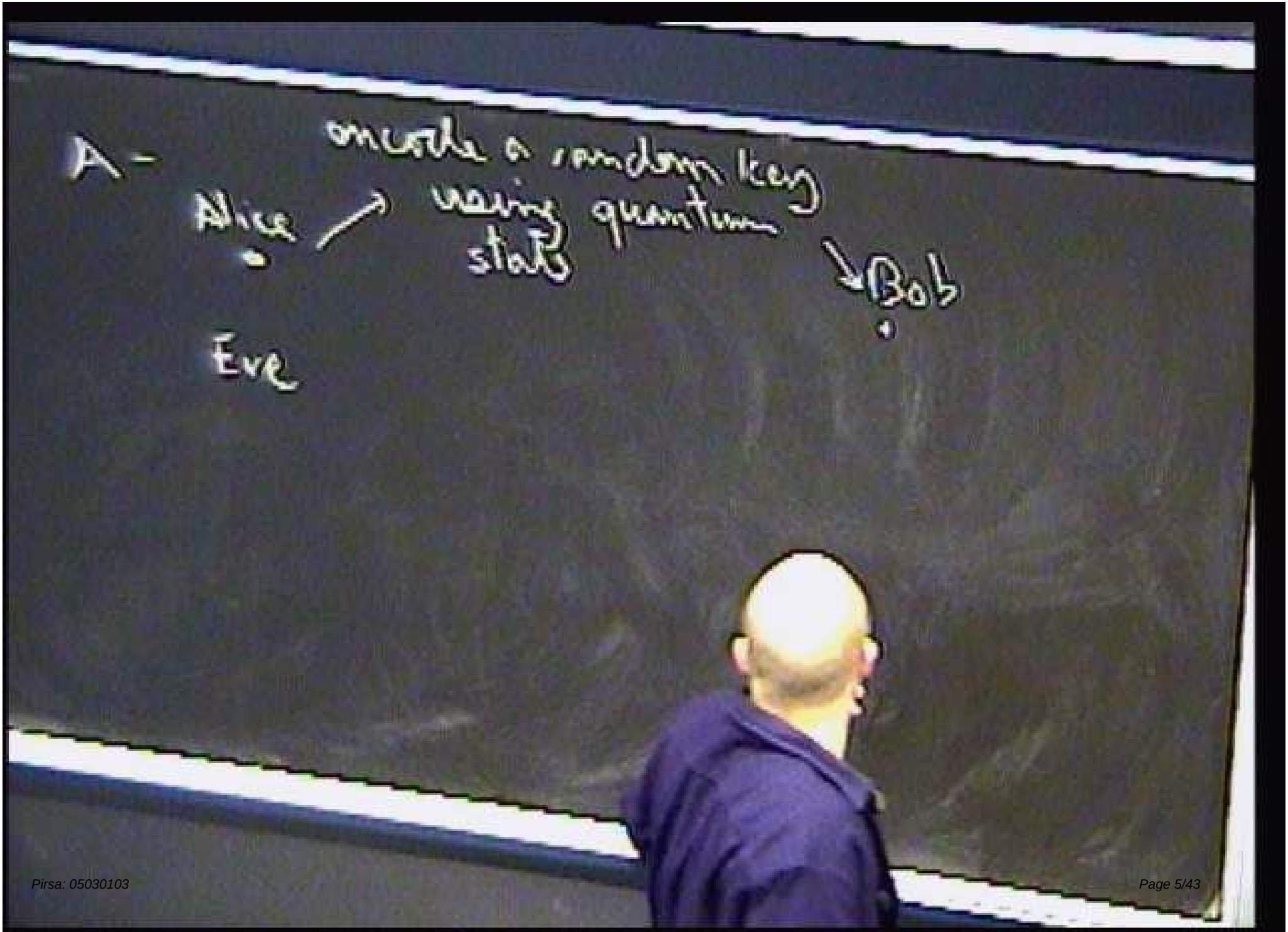
URL: http://pirsa.org/05030103

Abstract:


How to deal with photon loss and
Dark counts in QKD


How to deal with photon loss and
Dark counts in QKD:
A- what is QKD + motivation
B- Improve well-known
C- Exotic QKD has enough code.


A -
Alice
Bob


A -
Alice
Eve
Bob

A - Create a random key

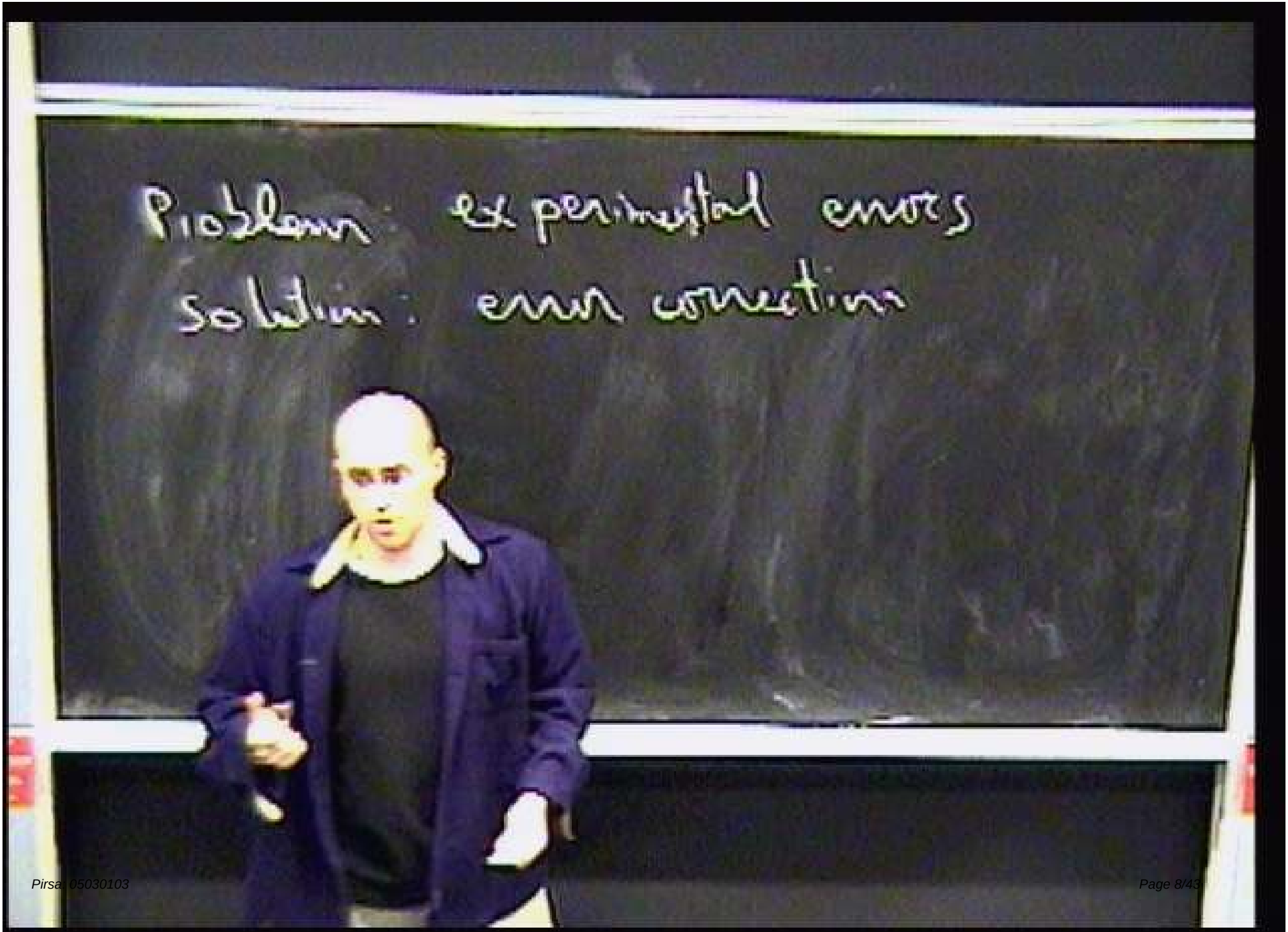
Alice → using quantum states → Bob

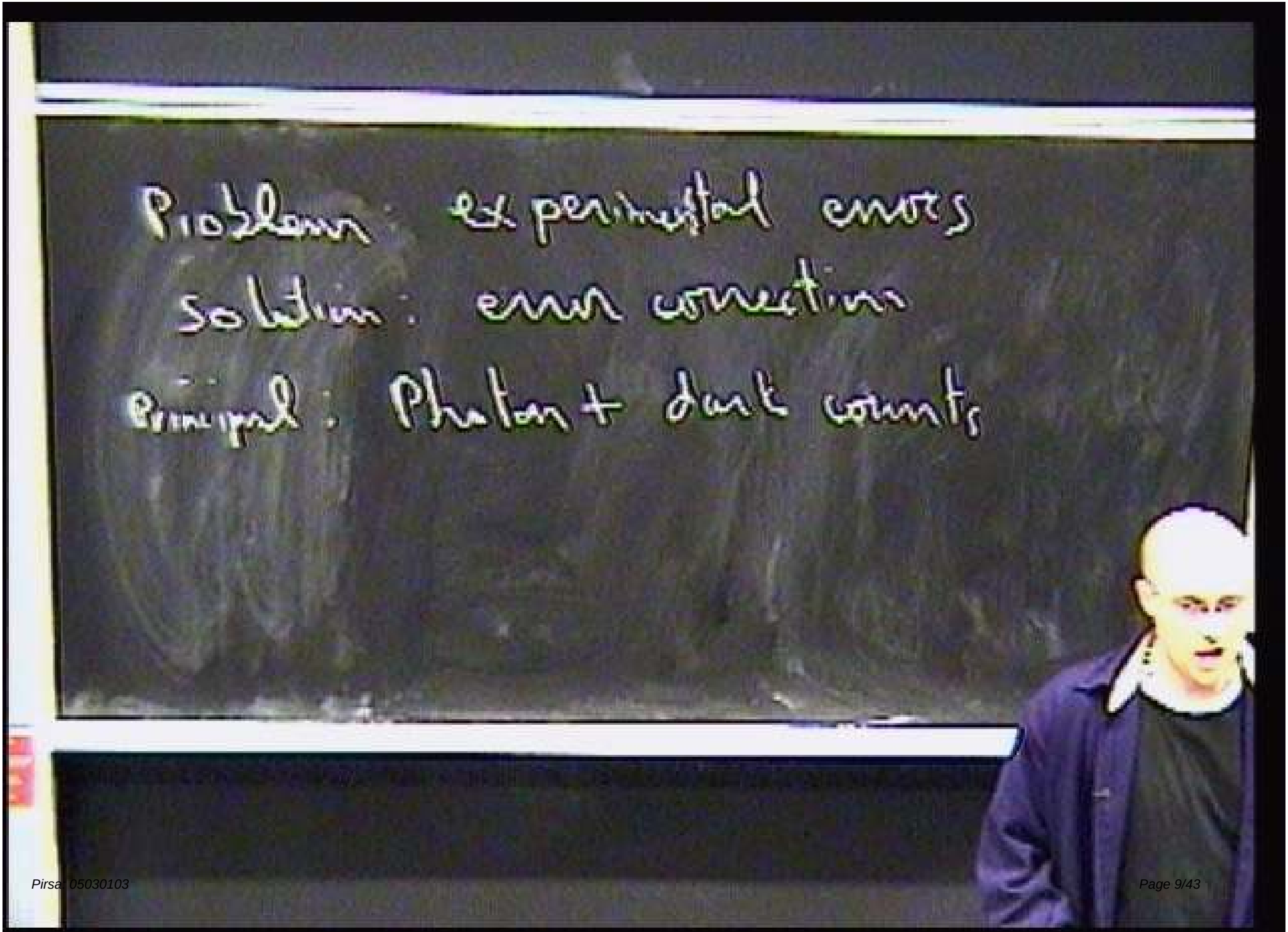
Eve induces errors => detectable

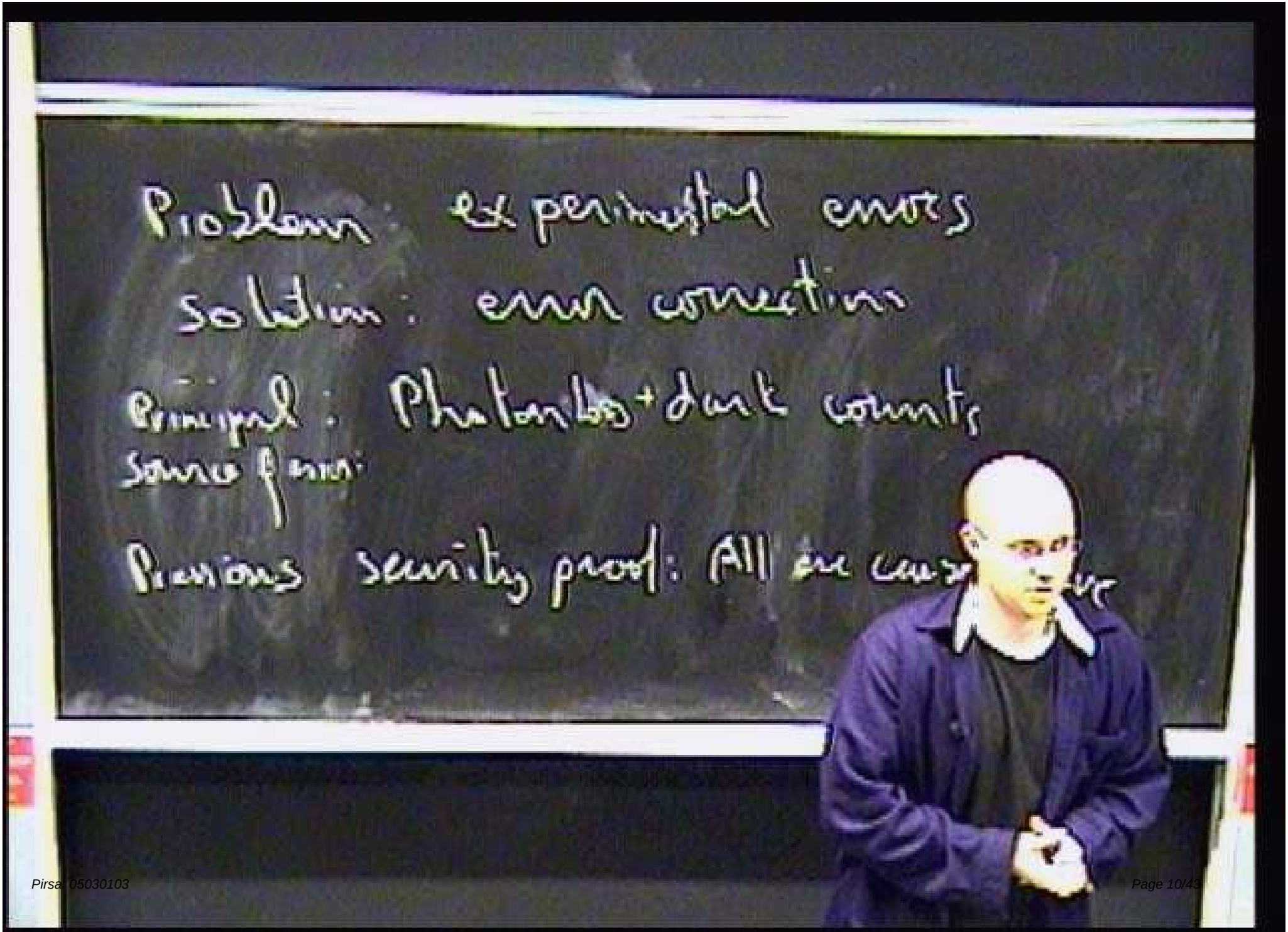
A - Alice → sends a random key using quantum states → Bob

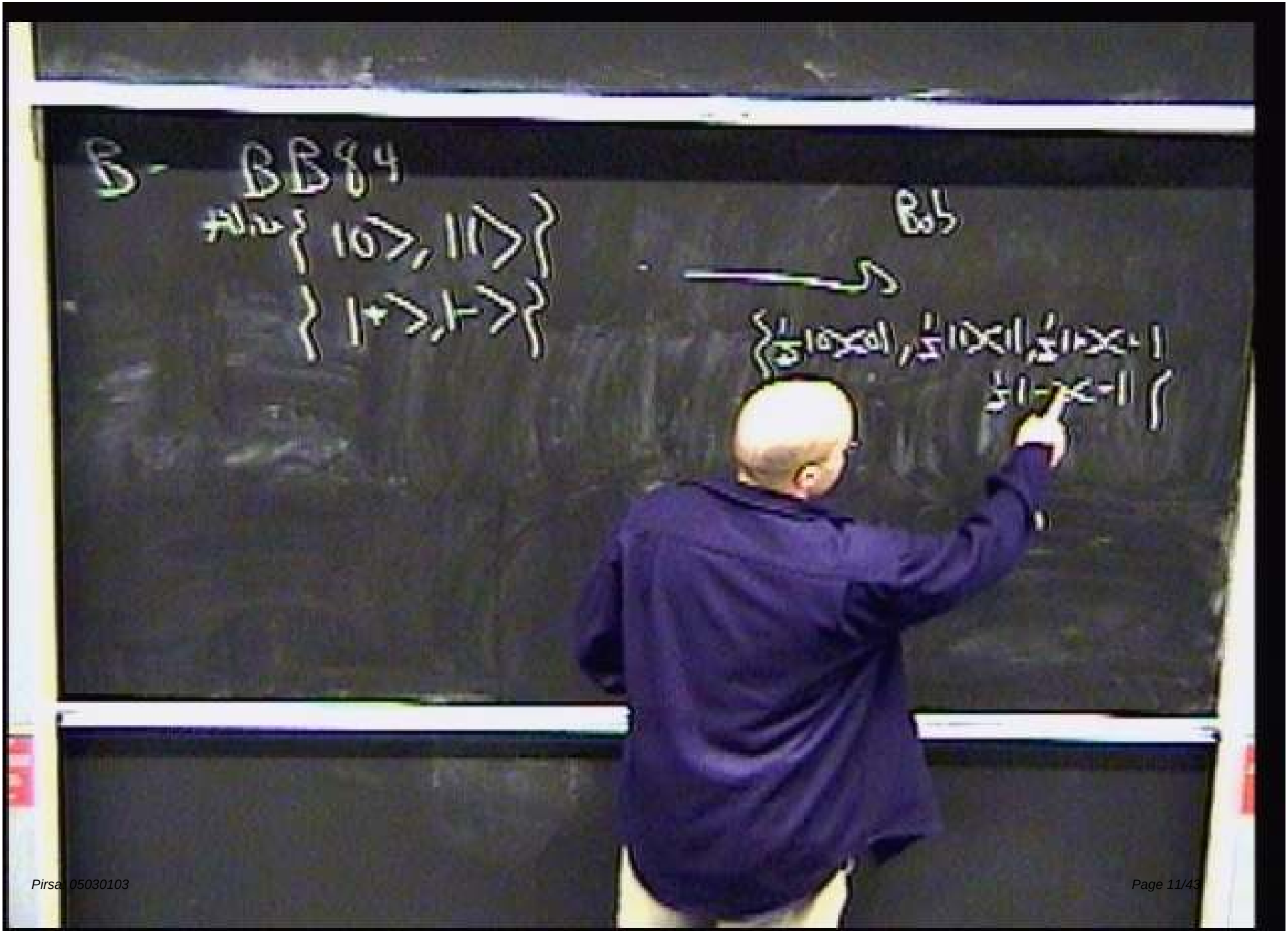
Eve induces errors => detectable

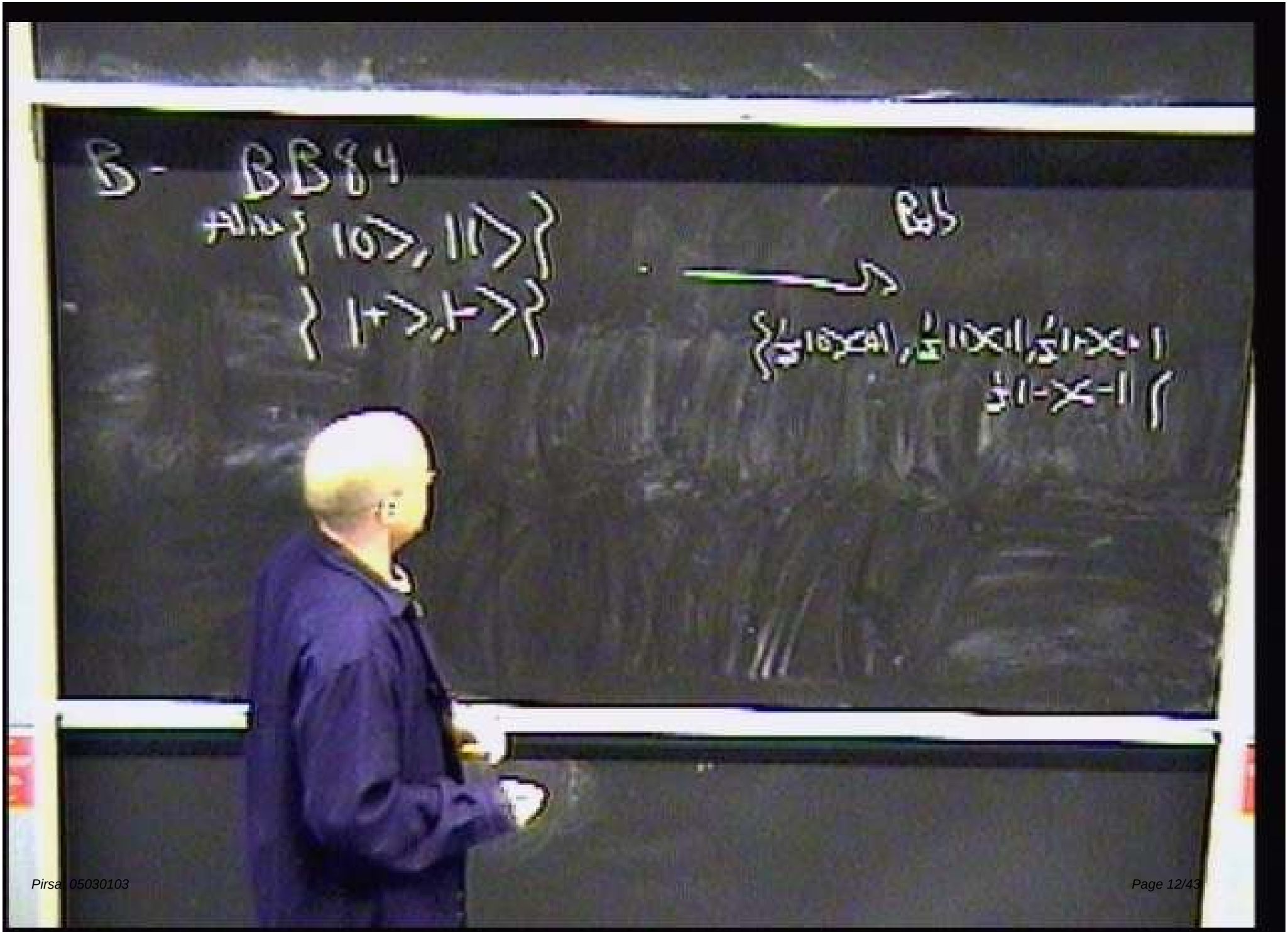
Security is based on laws of quantum mechanics !!

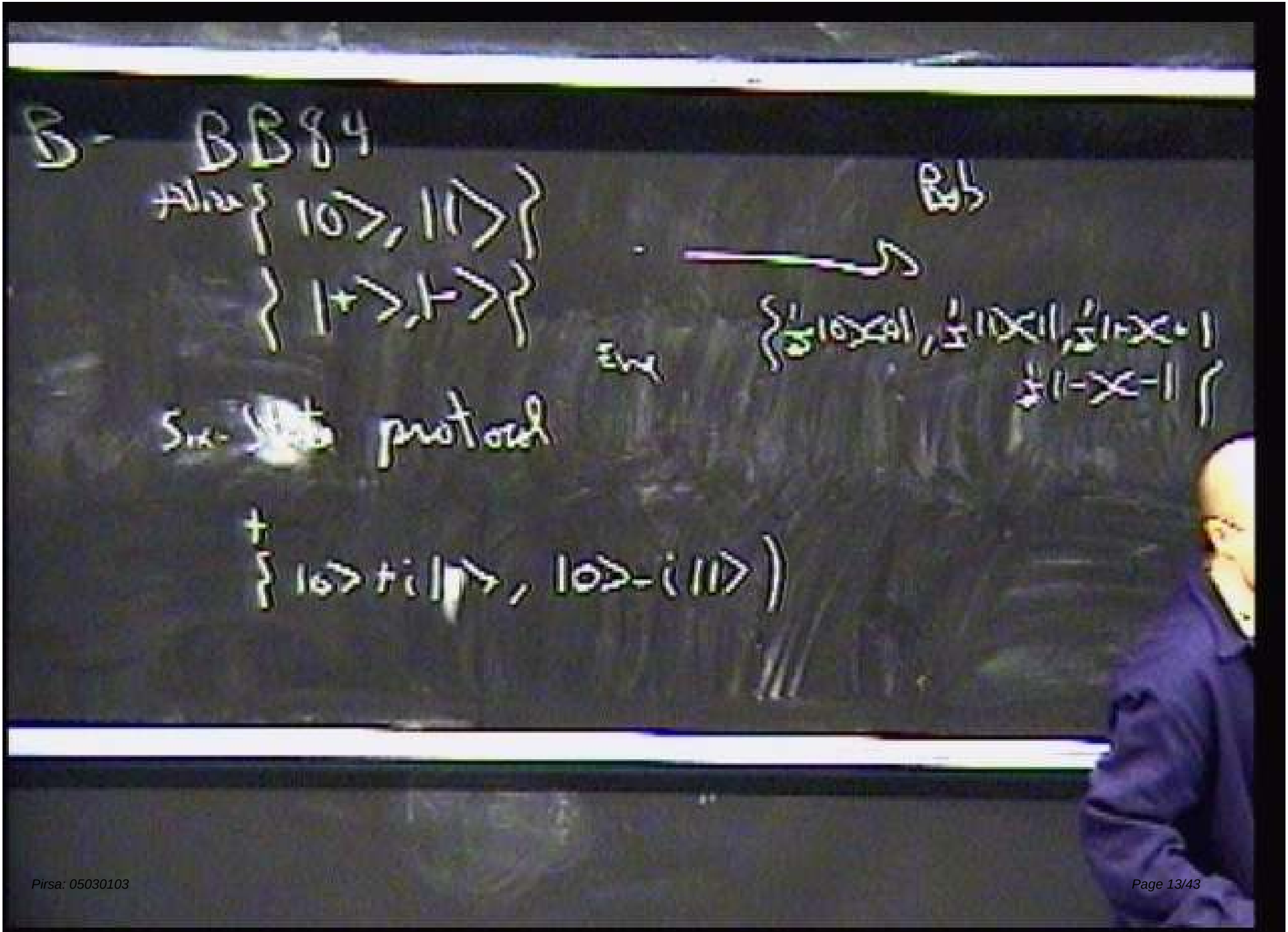

Problem: ex perimental errors
Solution: error correction

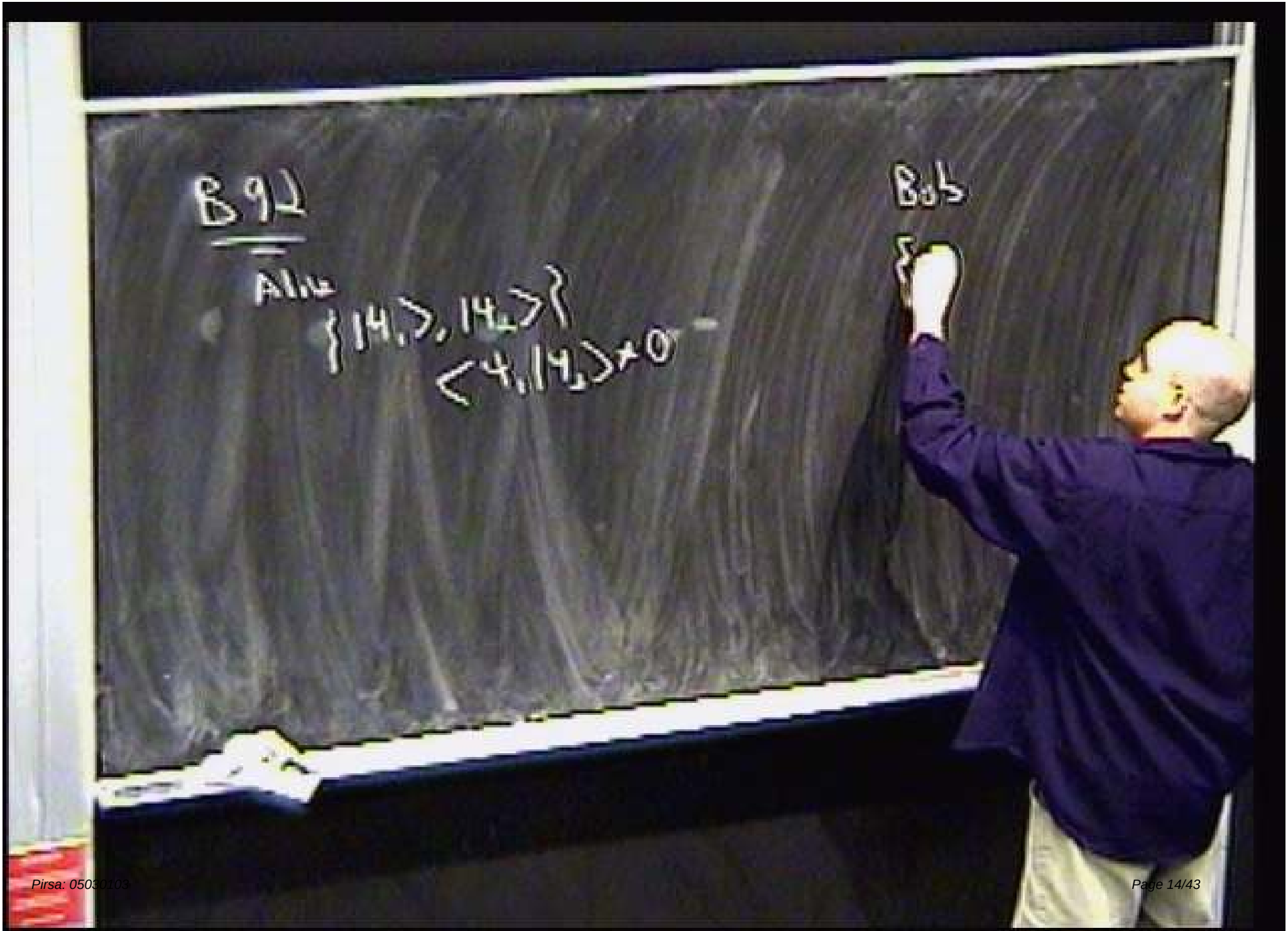

Problem: ex perturbative corrs
Solution: exact correlations
Principle: Photon + dark counts

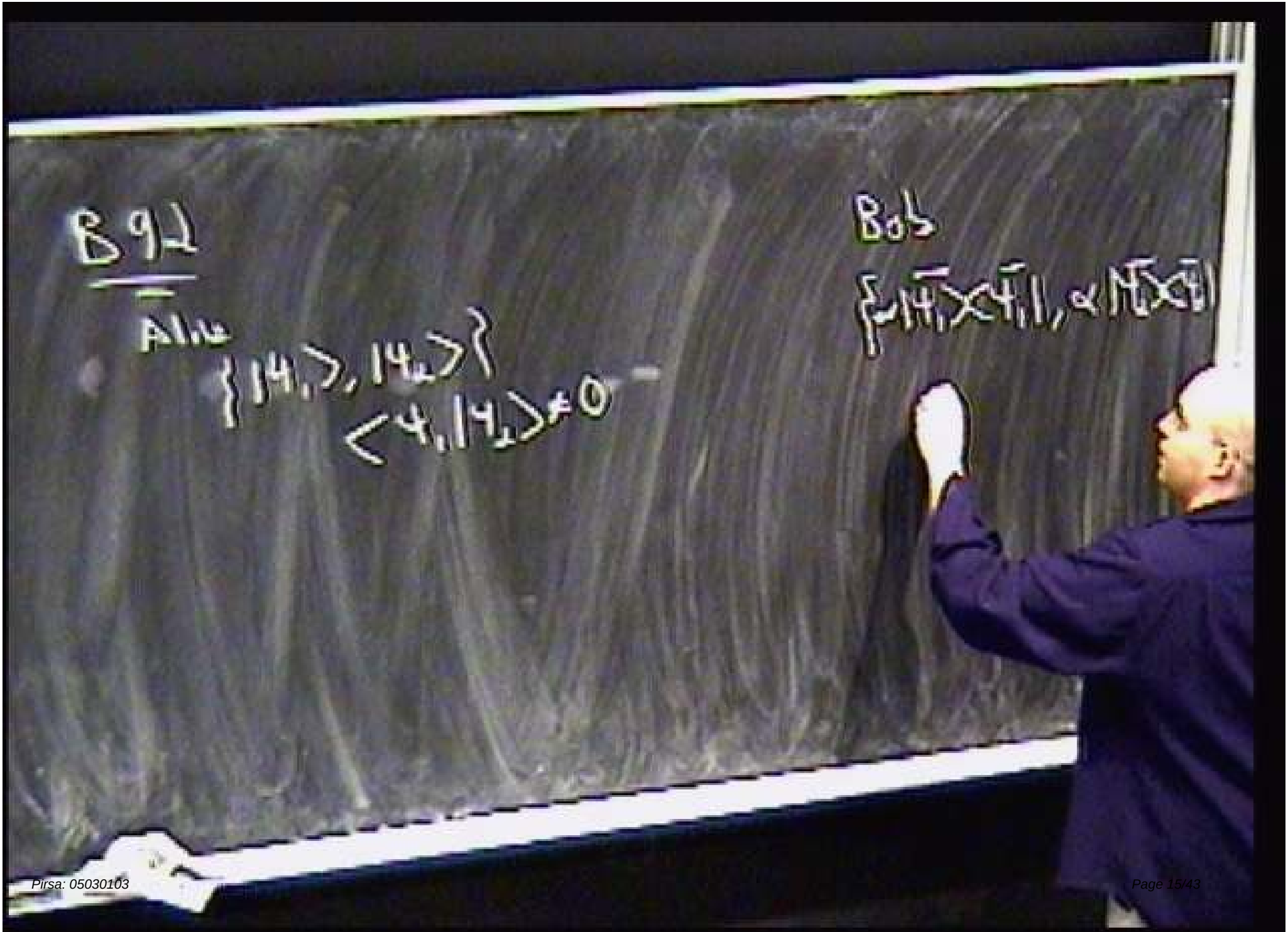

Problem: experimental errors
Solution: error corrections
Principal: Photon loss + dark counts
Source flaw:
Previous security proof: All the

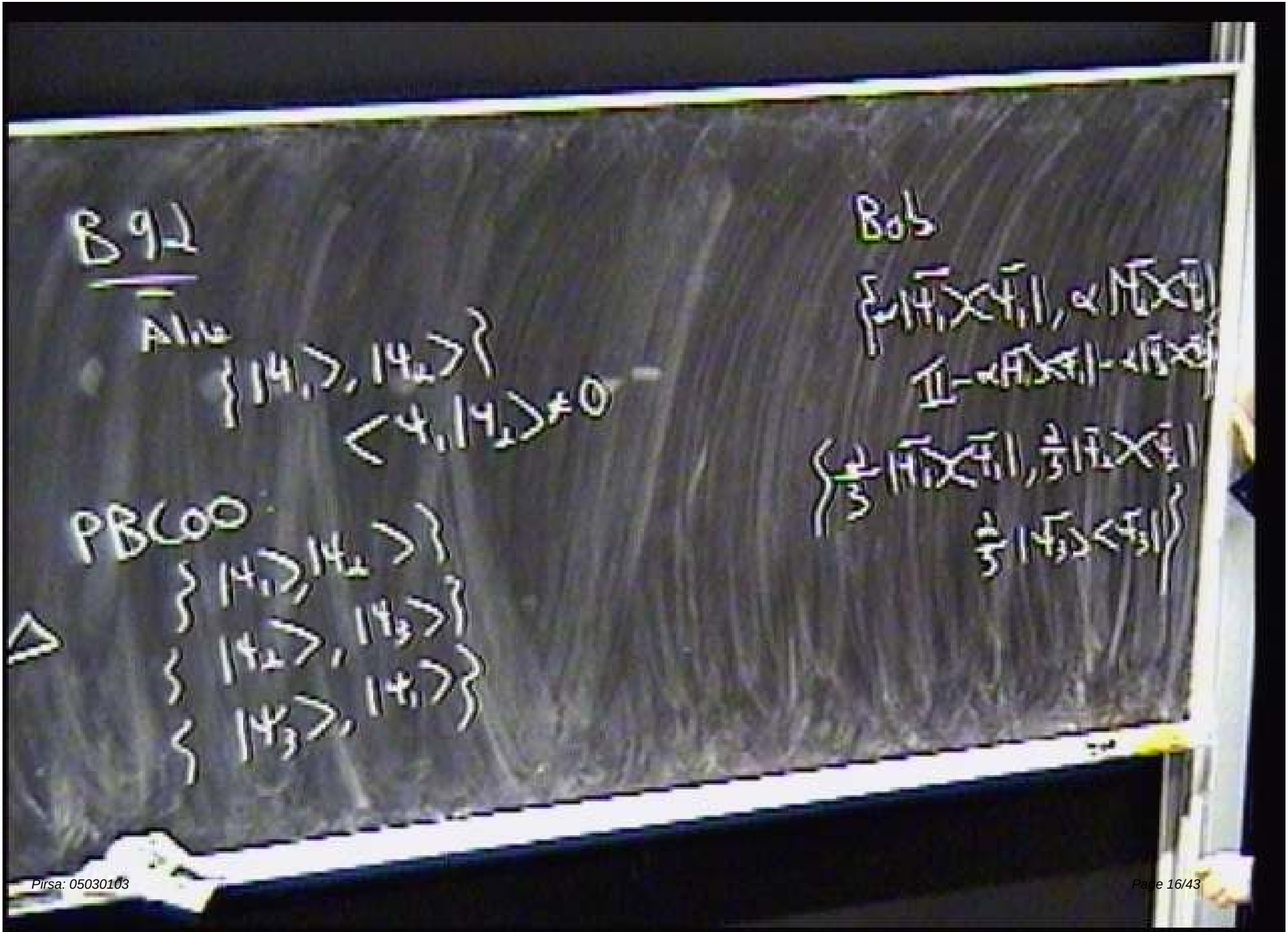


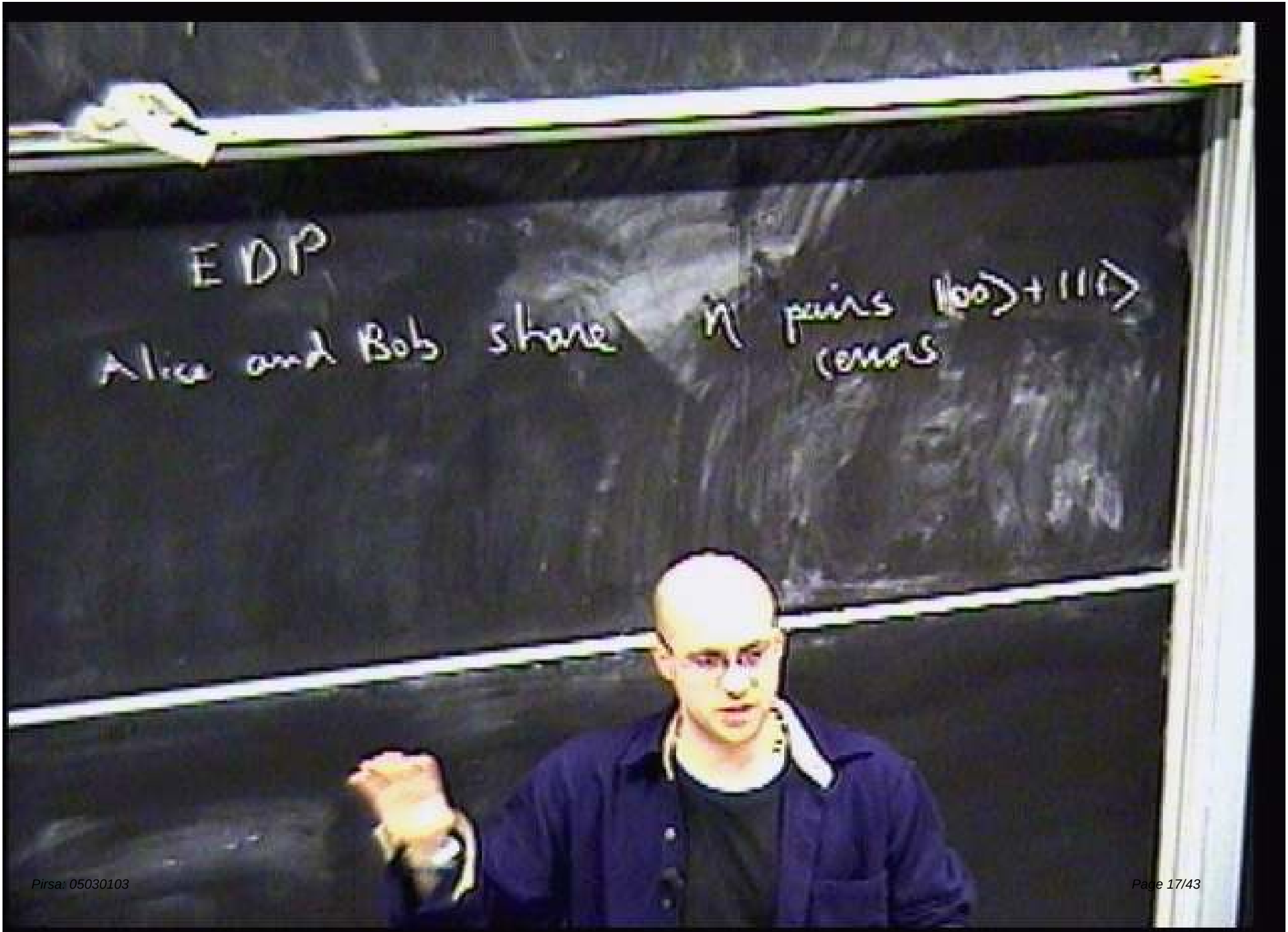


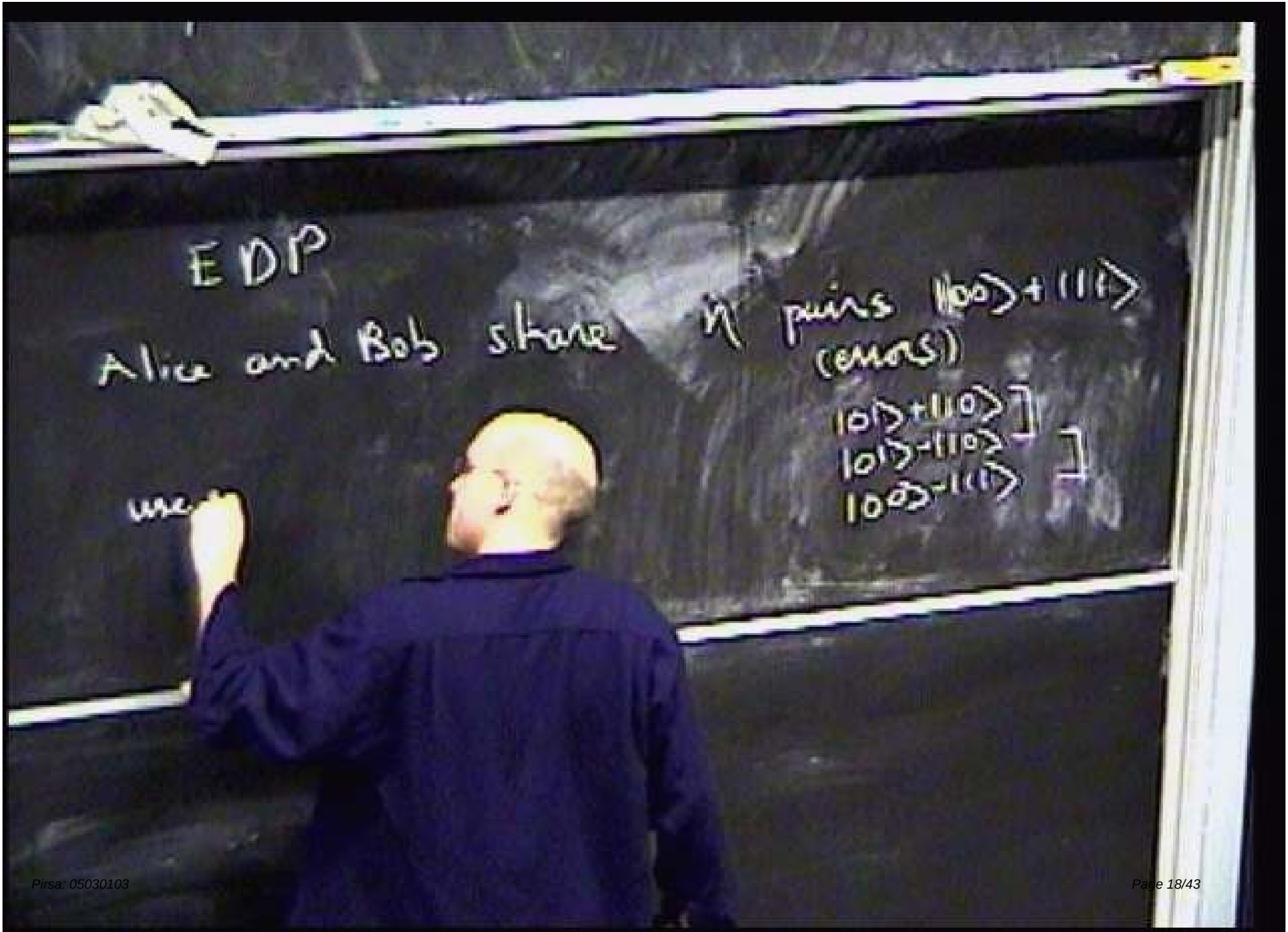

B - BB84
Alice
|0>, |1>
|+>, |->
Bob
Eve
Sift - Public
|0> + i|1>, |0> - i|1>

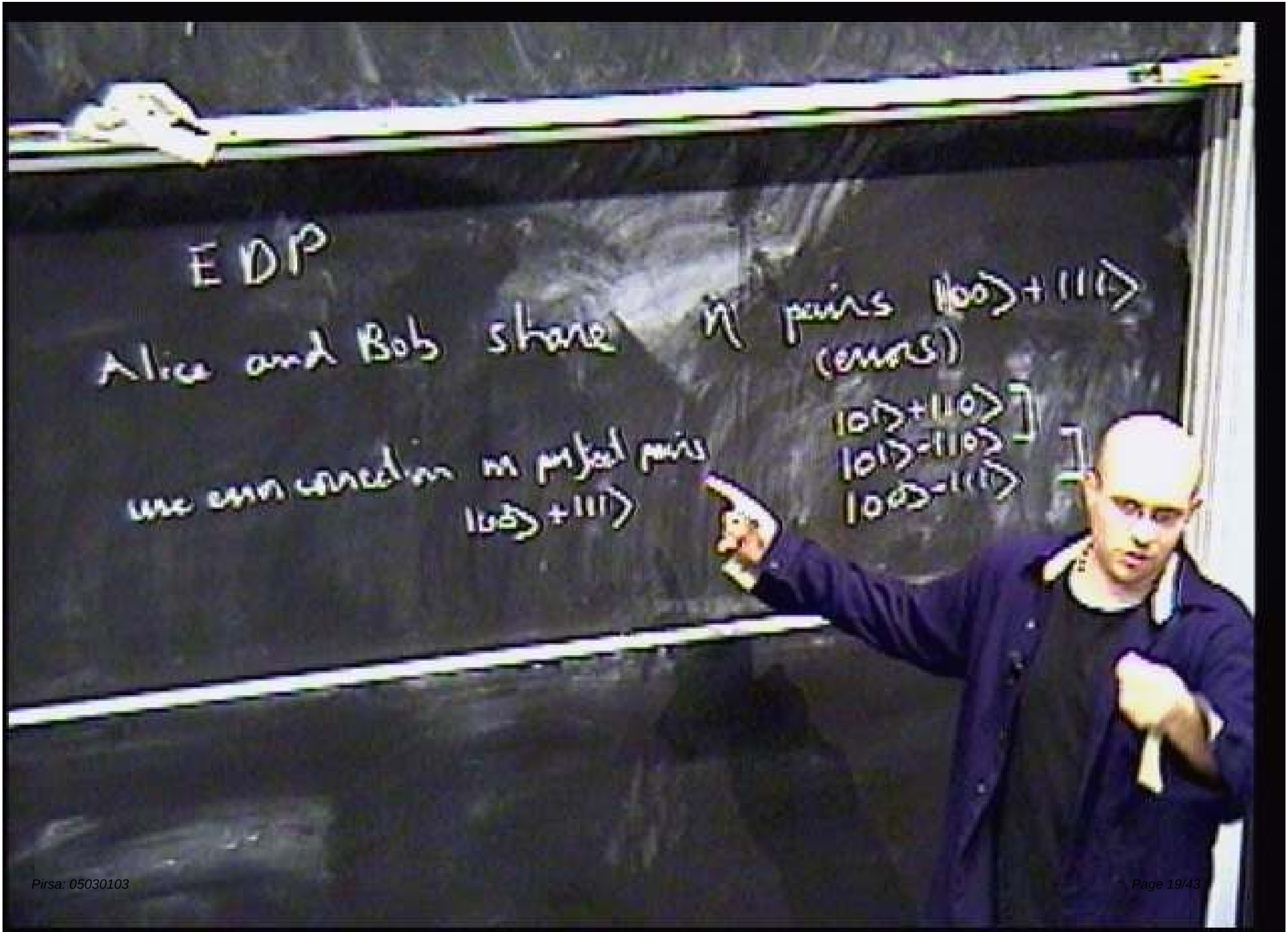

B9L
Alice
{|4,>, |4,>}
<4,|4,>=0
Bob

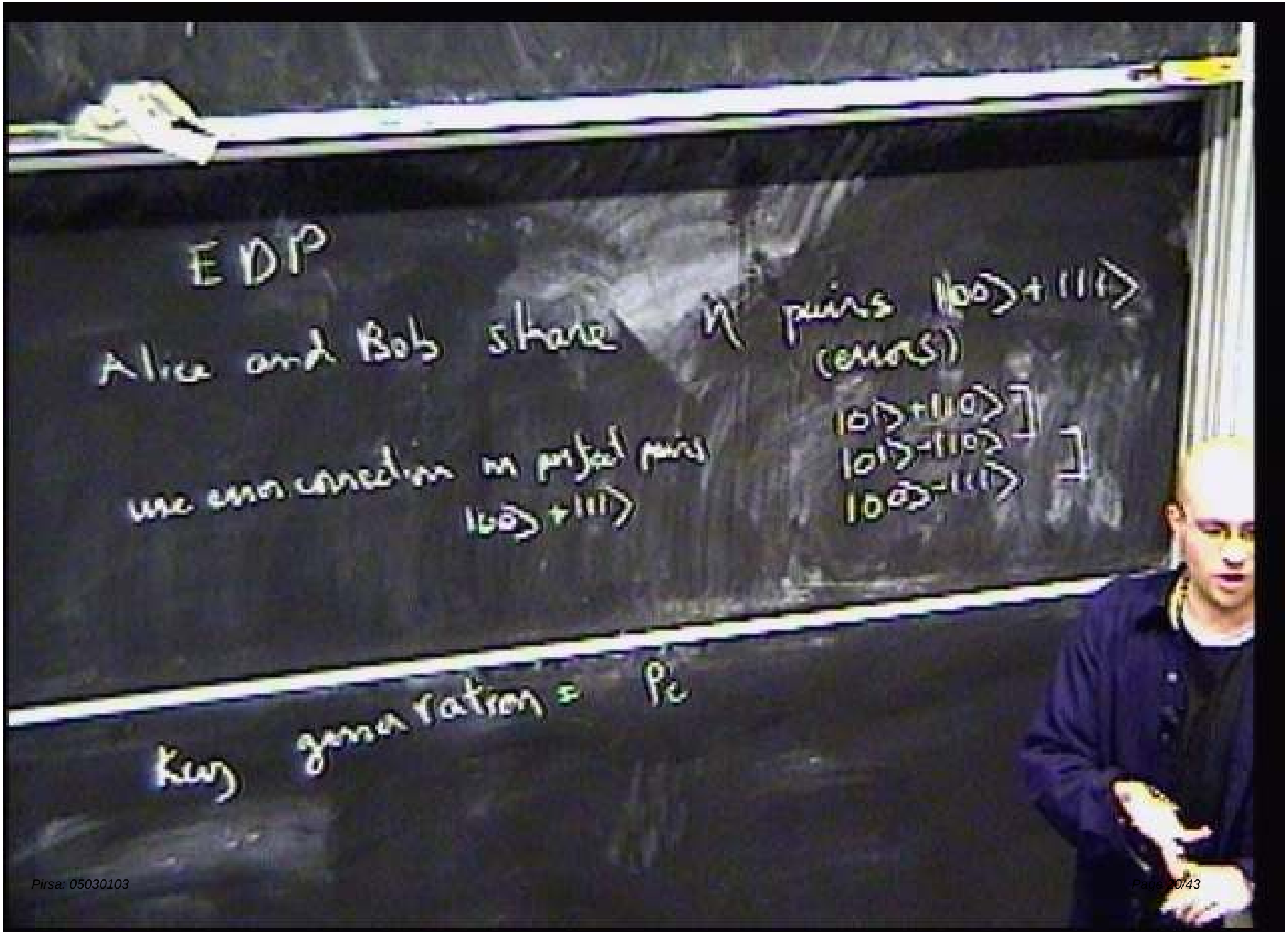

B 92
Alice
{|ψ1⟩, |ψ2⟩}
⟨ψ1|ψ2⟩≠0
Bob
{|ψ1⟩⟨ψ1|, |ψ2⟩⟨ψ2|}

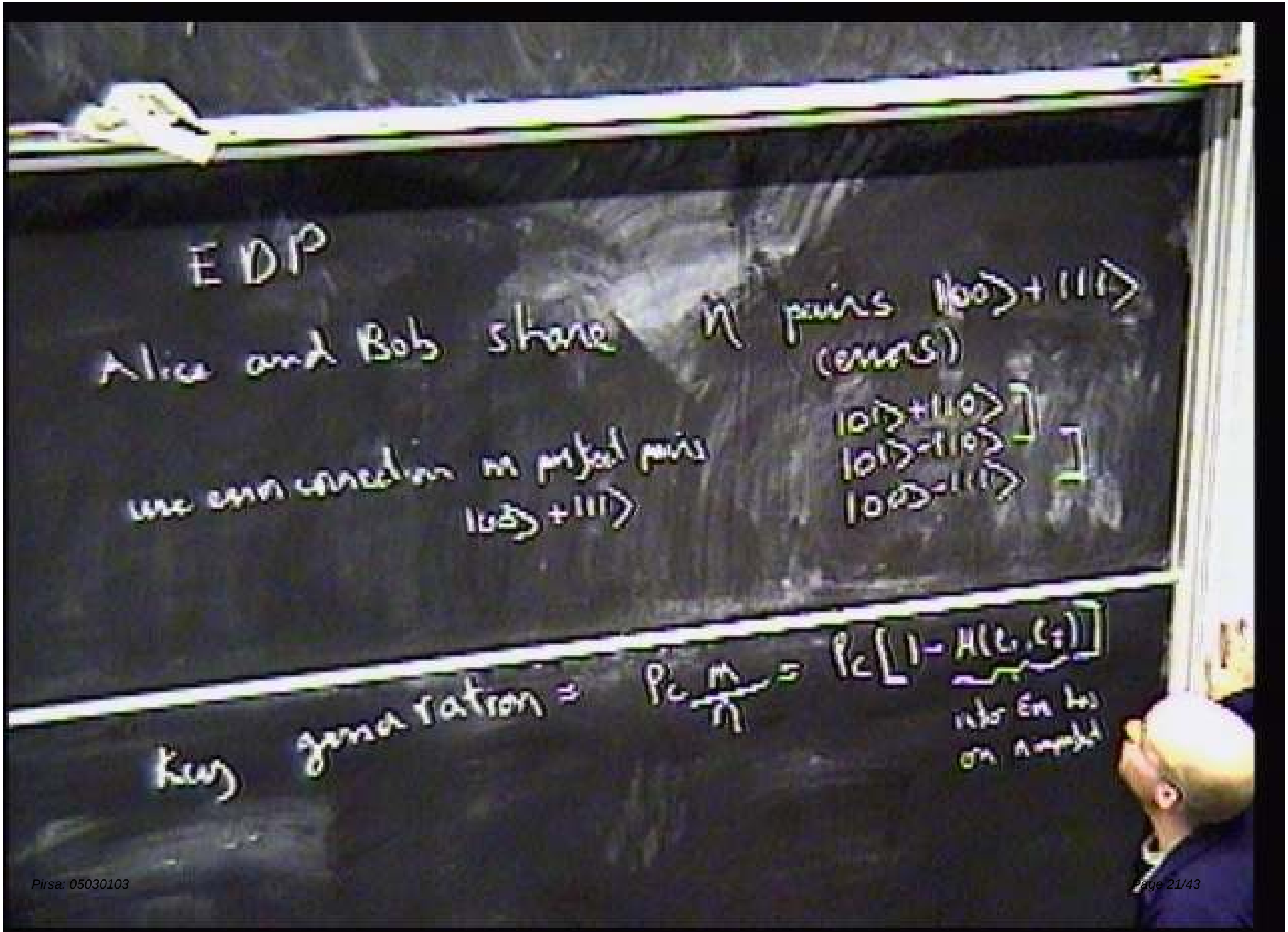

B92
Alice
$\{|\psi_1\rangle, |\psi_2\rangle\}$
$\langle\psi_1|\psi_2\rangle \neq 0$
PBC00
$\{|\psi_1\rangle, |\psi_2\rangle\}$
$\{|\psi_2\rangle, |\psi_3\rangle\}$
$\{|\psi_3\rangle, |\psi_1\rangle\}$
Bob
$\{\alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|$
$\mathbb{I} - \alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1| - \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|\}$
$\{\frac{2}{3}|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \frac{2}{3}|\bar{\psi}_2\rangle\langle\bar{\psi}_2|$
$\frac{2}{3}|\bar{\psi}_3\rangle\langle\bar{\psi}_3|\}$


EDP
Alice and Bob share N pairs

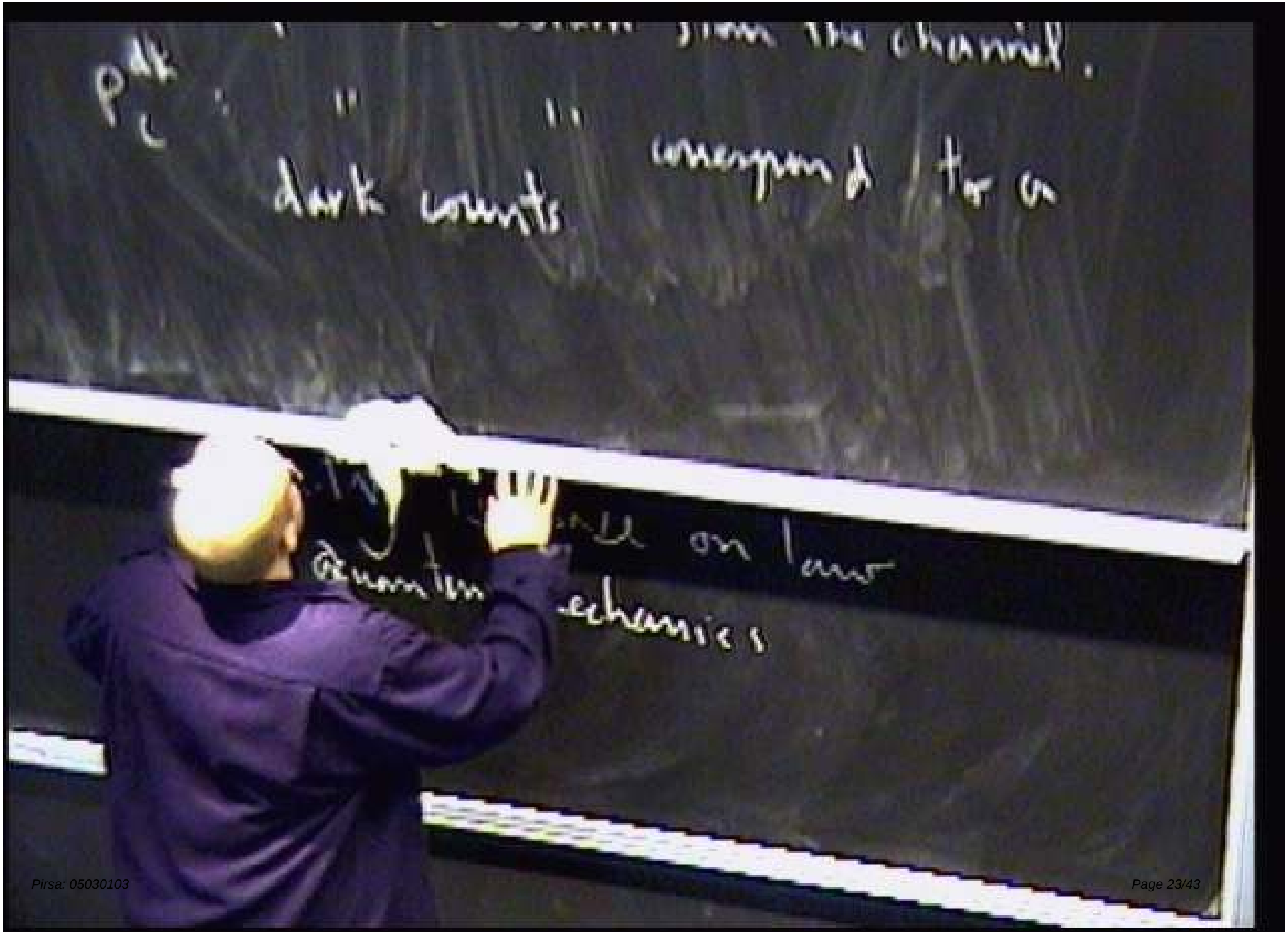

EDP
Alice and Bob share
(errors)

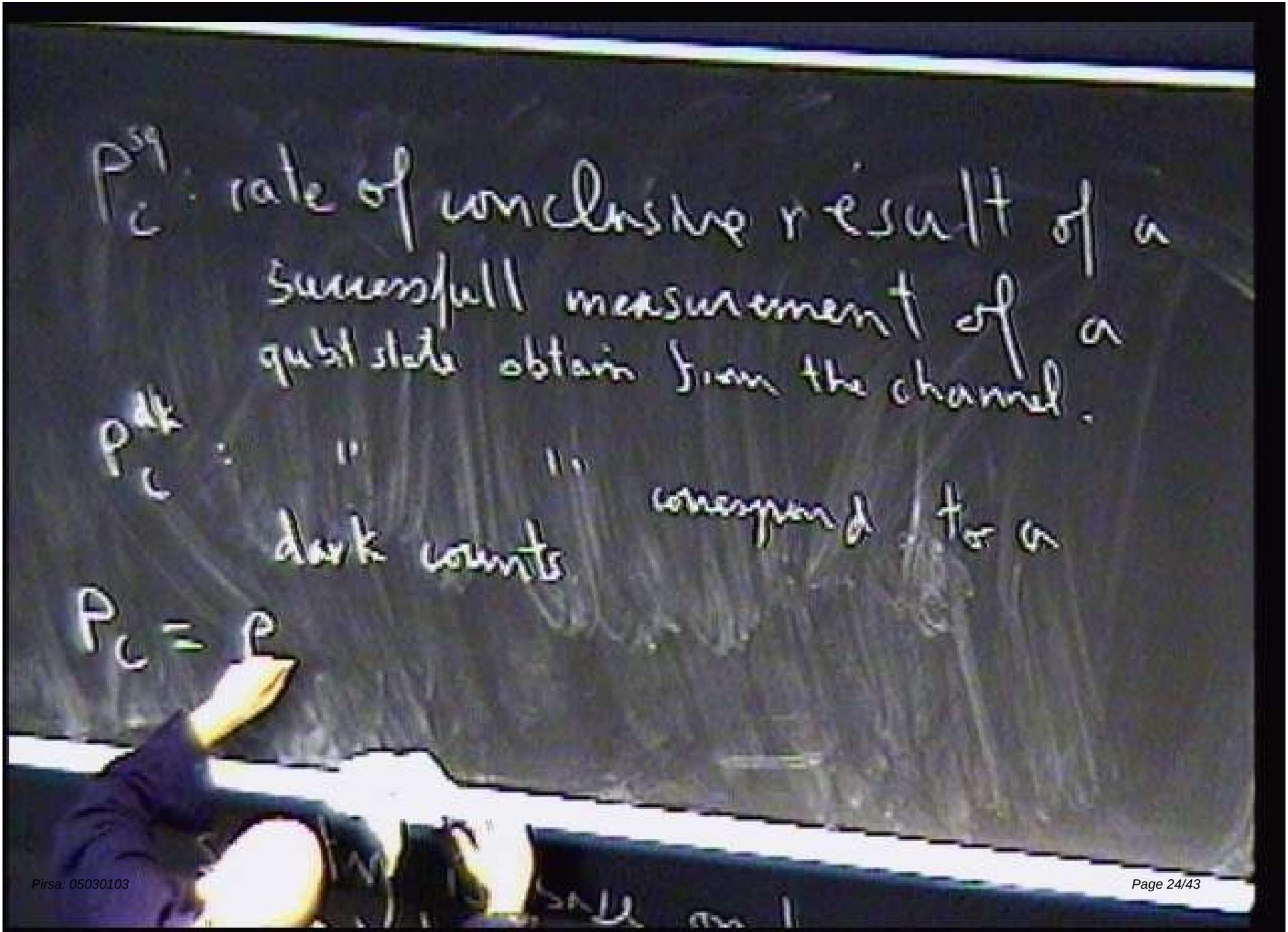

EDP
Alice and Bob share N pairs |00⟩+|11⟩
(ebits)
|01⟩+|10⟩
|01⟩-|10⟩
|00⟩-|11⟩
one can create N qubit pairs
|00⟩+|11⟩


EDP
Alice and Bob share N pairs |00⟩+|11⟩
(ebits)
one error correction on initial pairs
|00⟩+|11⟩
|01⟩+|10⟩
|01⟩-|10⟩
|00⟩-|11⟩
key generation = P_E


EDP
Alice and Bob share N pairs |00⟩+|11⟩
(ebits)
one can consider as initial pairs
|00⟩+|11⟩
|01⟩+|10⟩
|01⟩-|10⟩
|00⟩-|11⟩
key generation =
1-H(
ebit in his
or her

P_2^{succ}: rate of conclusive result of a successful measurement of a qubit state obtain from the channel.


dark counts


P_c^{sig}: rate of conclusive result of a successful measurement of a qubit state obtain from the channel.
P_c^{dk}: " " " corresponded to a dark counts
$P_c = P$

quantities obtain from the channel.

p_c^{dk} : " " " corresponding to / for a

dark counts

$$p_c = p_c^{sig} + p_c^{dk}$$

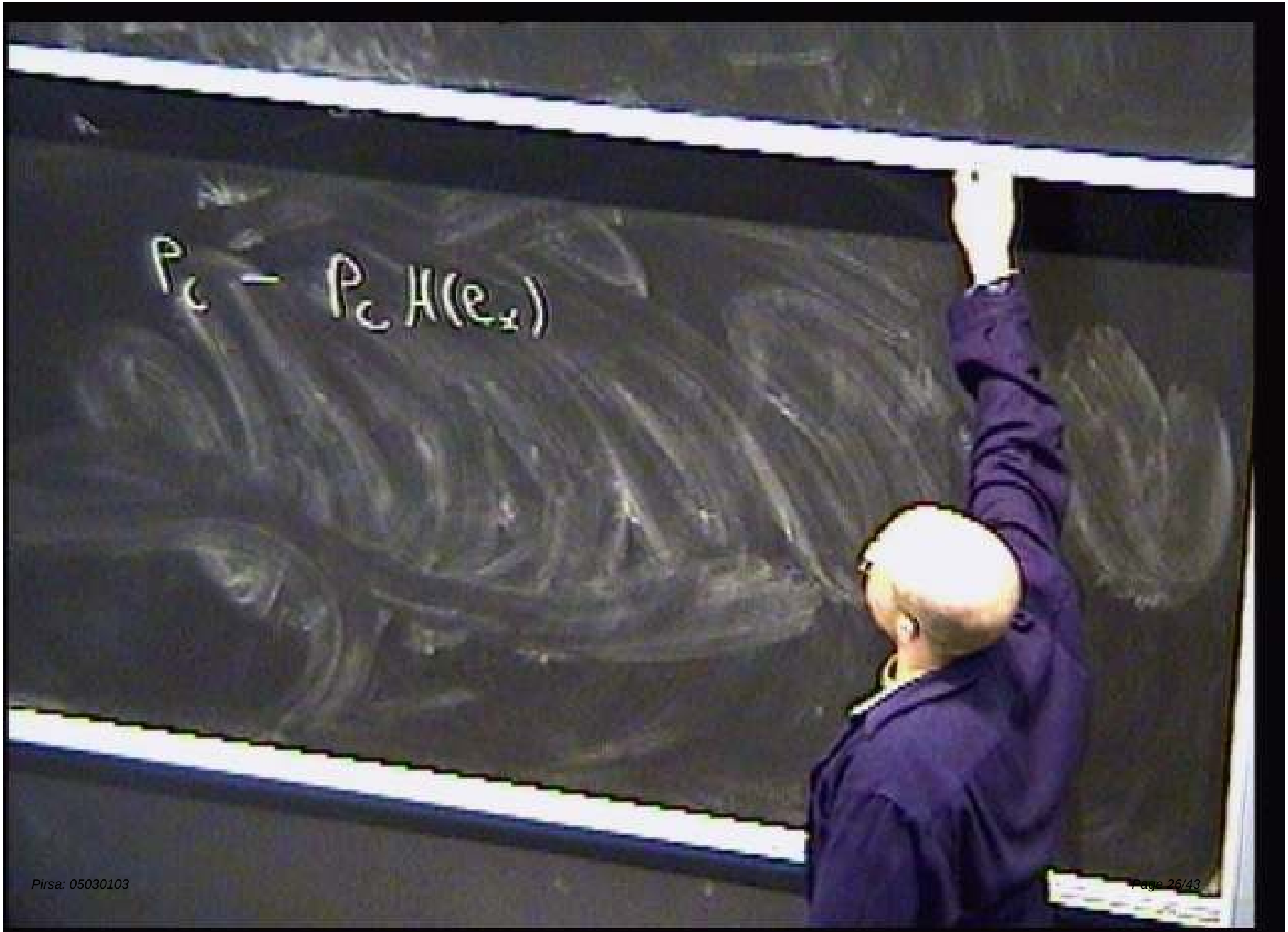
A -

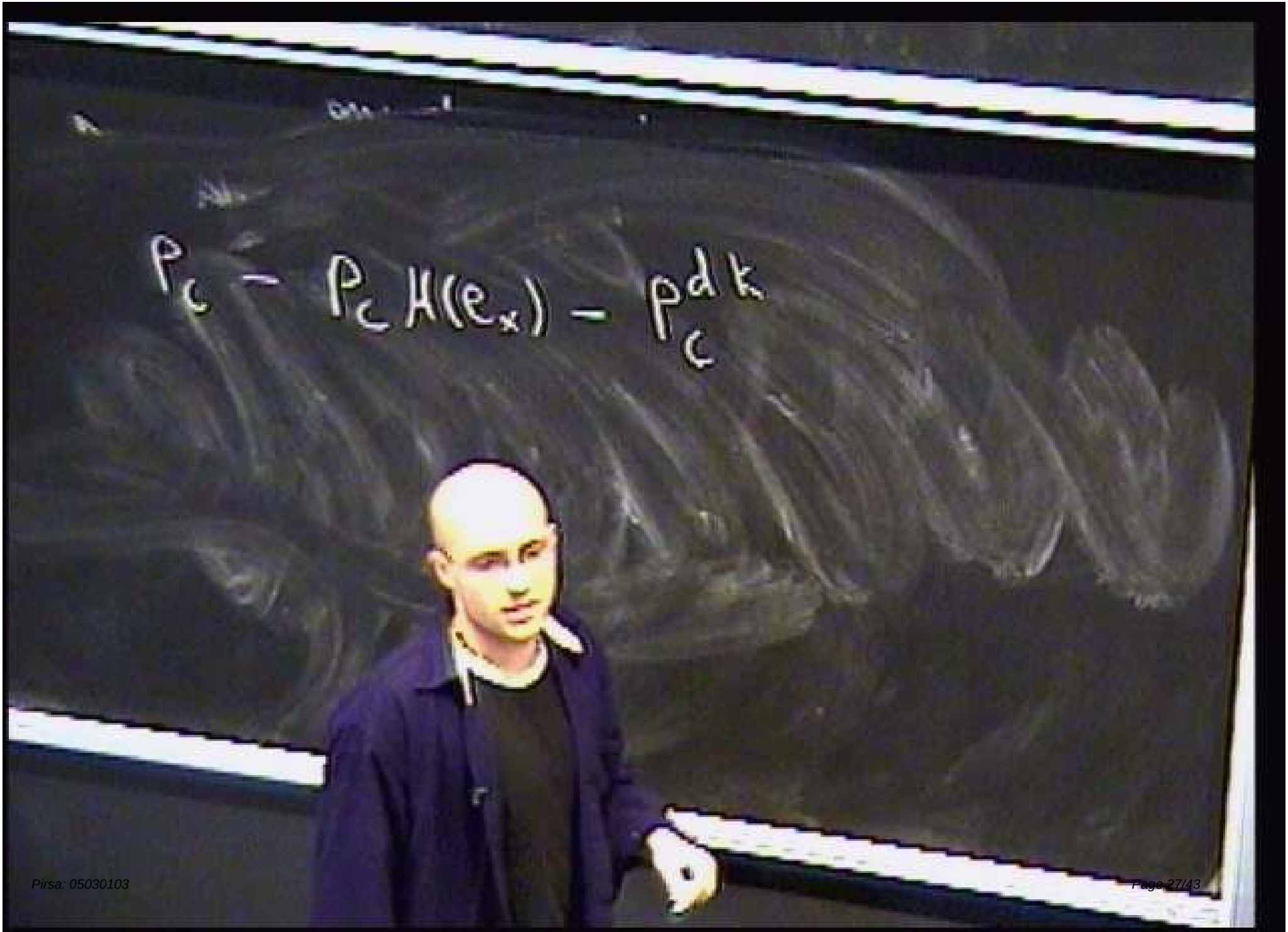
Alice → using quantum → Bob

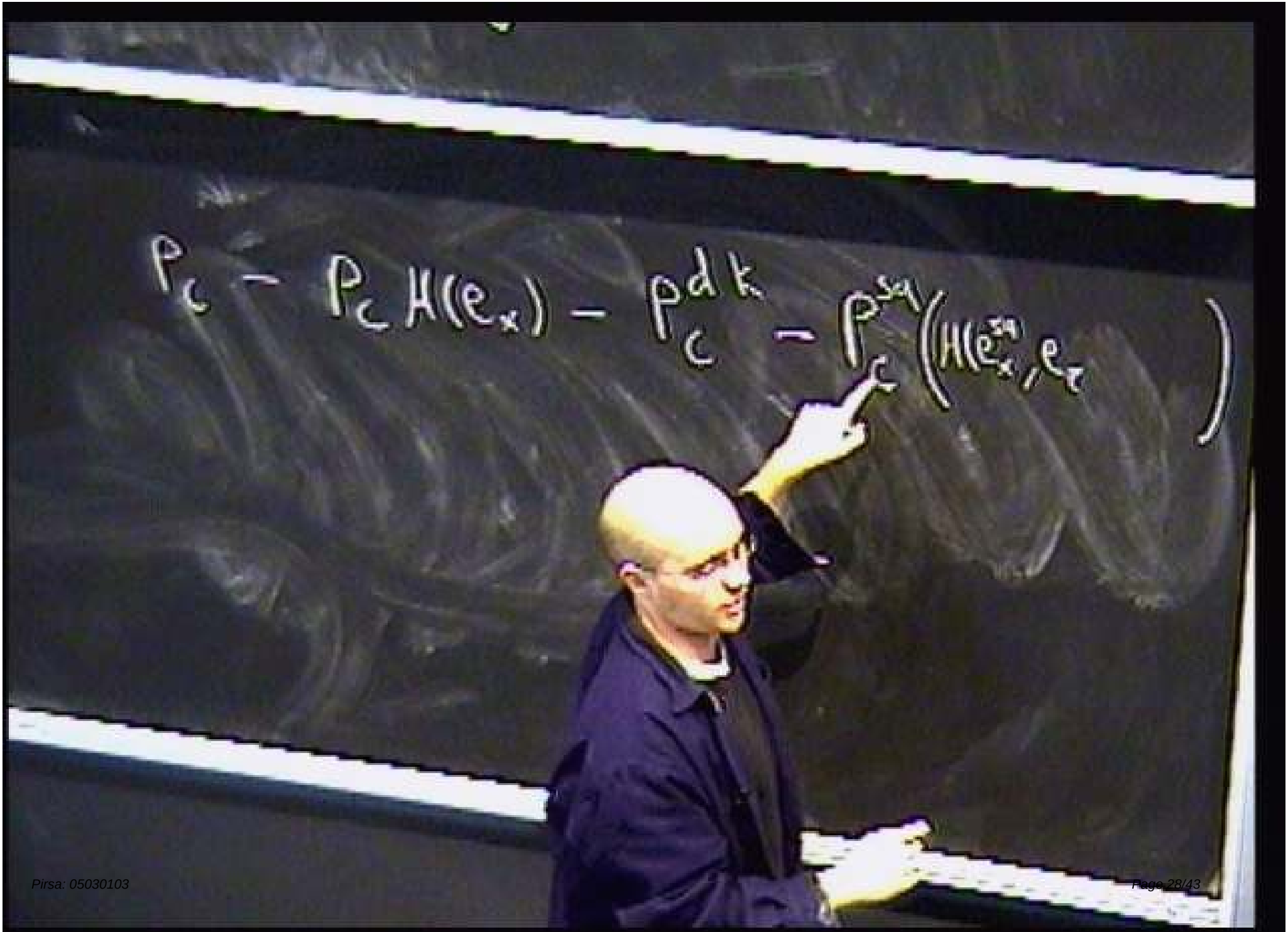
stat

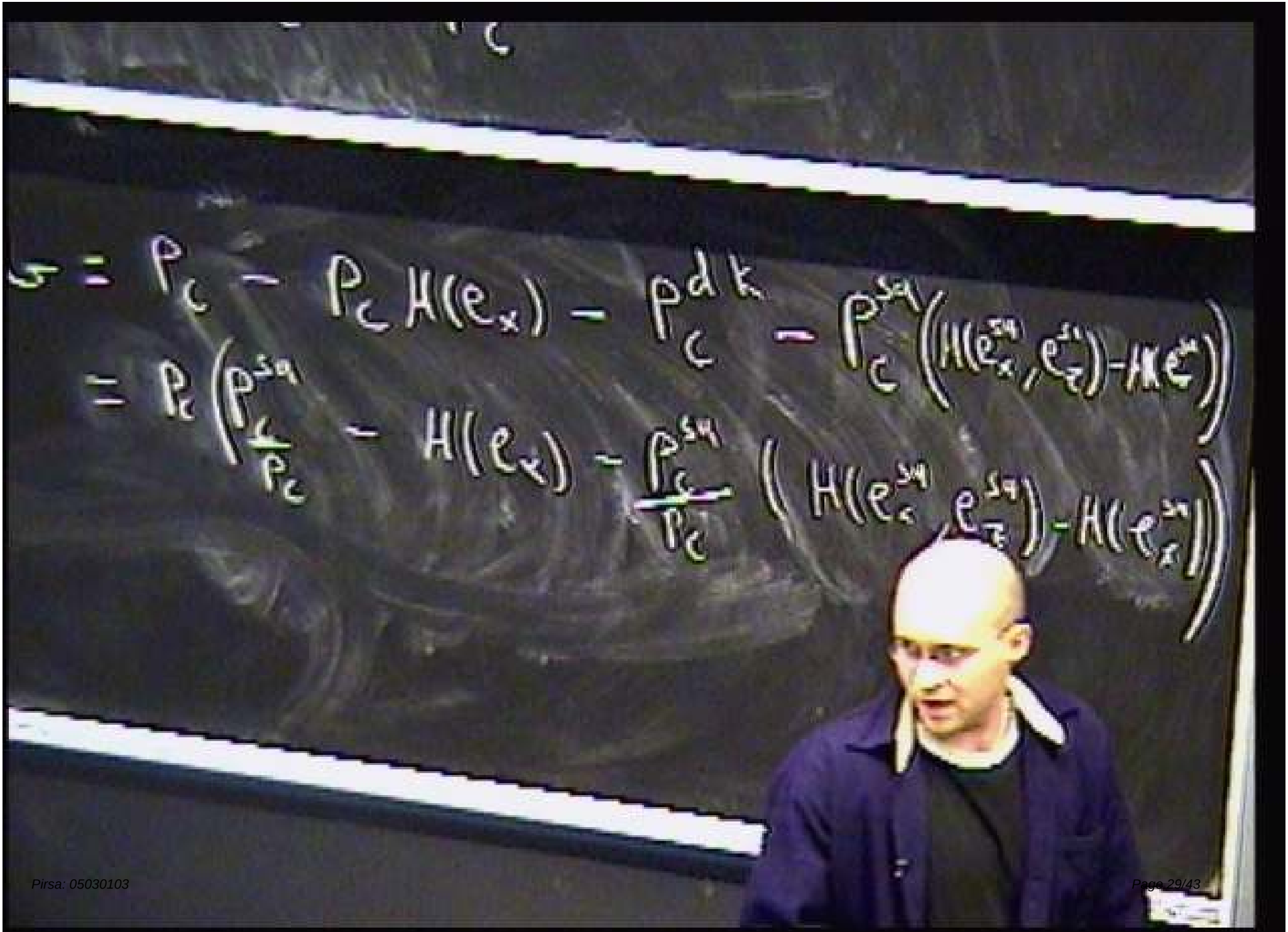
Eve induces error => detectable

security is based on


$\rho_c - \rho_c H(e_x)$


$P_c - P_c H(e_x) - P_c^{dk}$





Pirsa: 05030103

$$= P_c - P_c H(e_x) - P_c^{dk} - P_c^{jq}\left(\left(H(e_x^{jq}, e_x^{jl})\right) - H(e_x^{jq})\right)$$

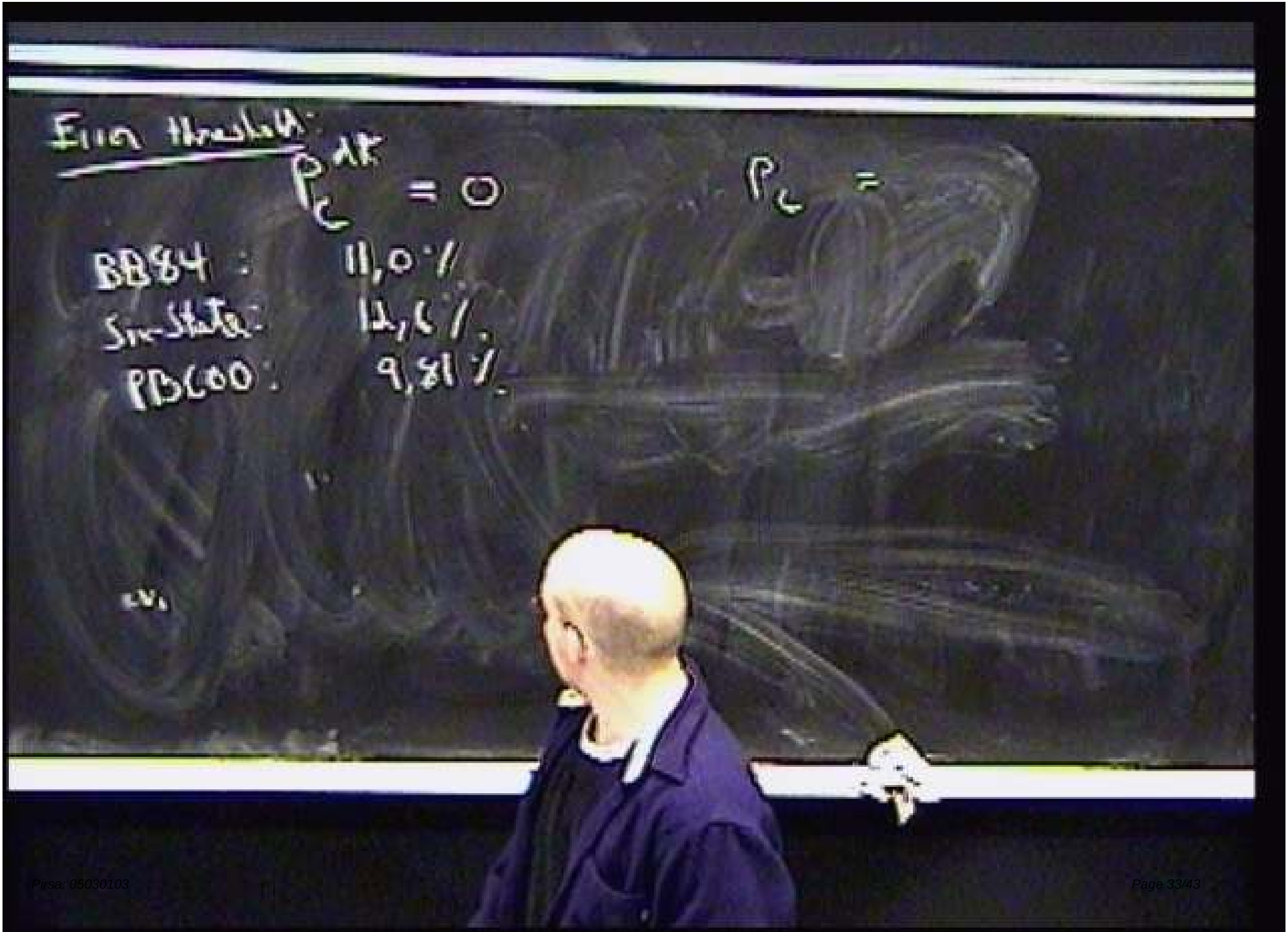
$$= P_x\left(\frac{P_c^{jq}}{P_c} - H(e_x) - \frac{P_c^{jq}}{P_c}\left(\left(H(e_x^{jq}, e_x^{jq})\right) - H(e_x^{jq})\right)\right)$$

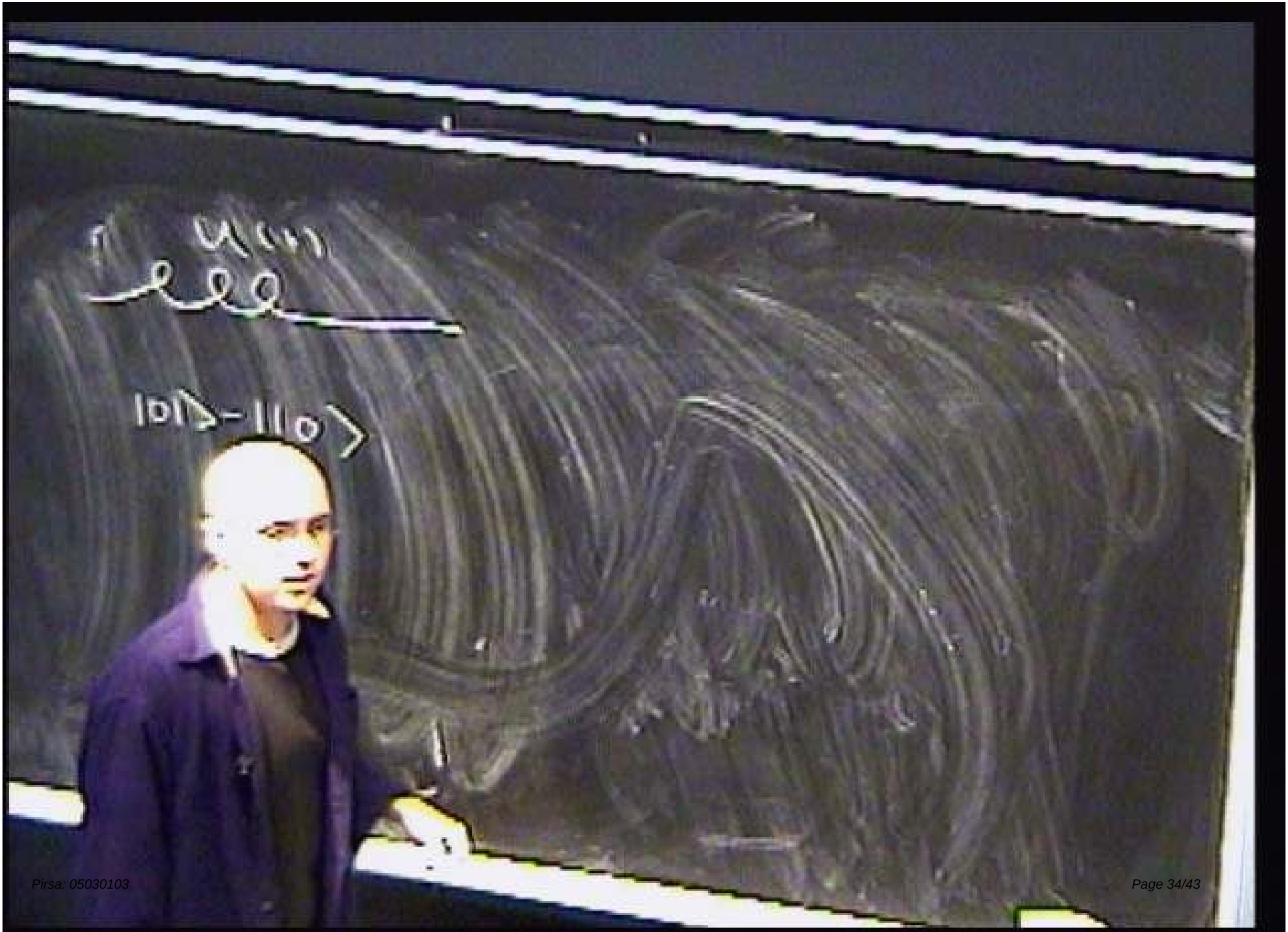
$$= \rho_c - \rho_c H(e_x) - \rho_c^{dk} - \rho_c^{sq}\left(\left(H(e_x^{sq}, e_x^{sq}) - H(e_x^{sq})\right)\right)$$

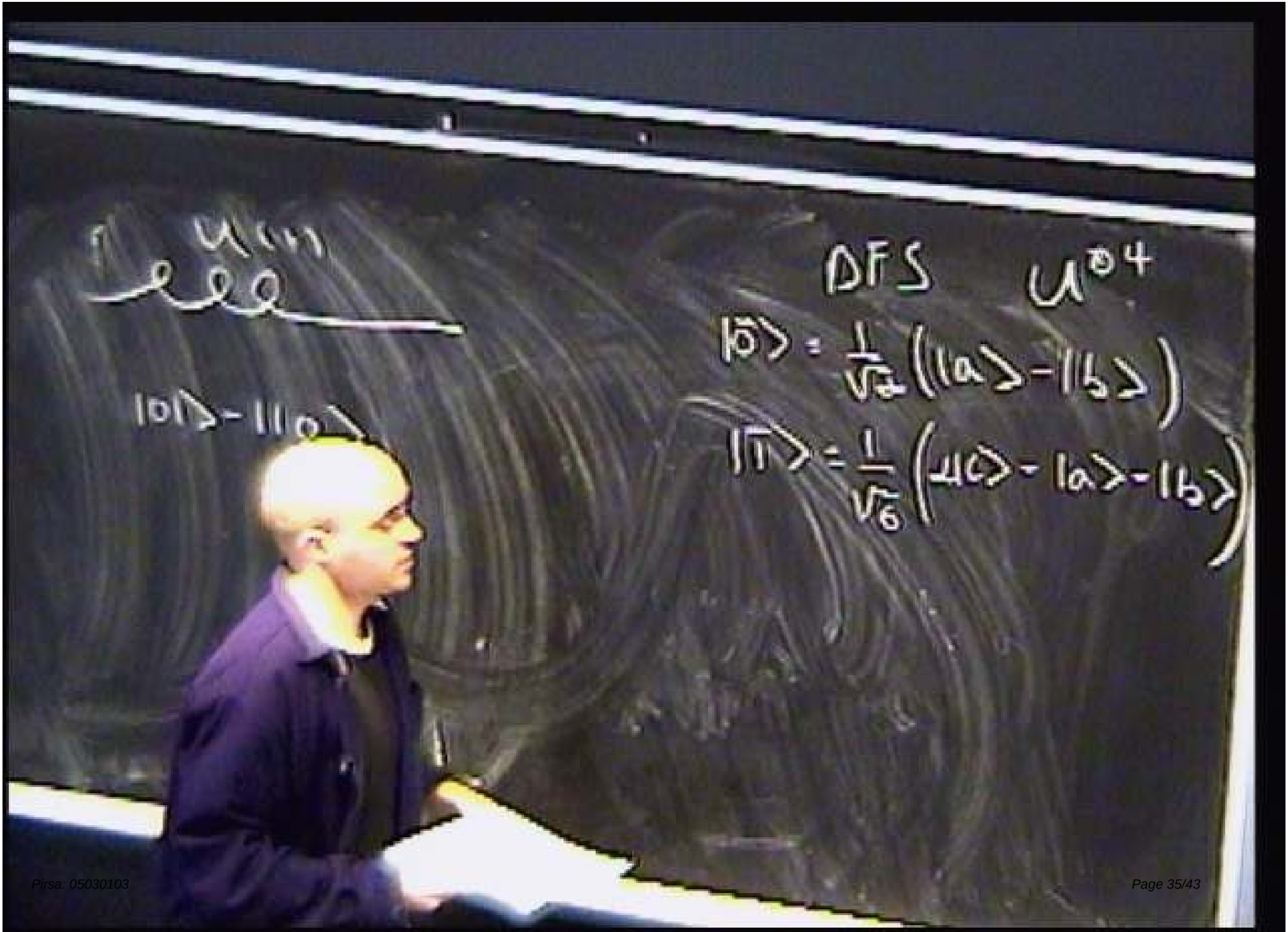
$$= \rho_x\left(\frac{\rho_c^{sq}}{\rho_c} - H(e_x) - \frac{\rho_c^{sq}}{\rho_c}\left(\left(H(e_x^{sq}, e_x^{sq}) - H(e_x^{sq})\right)\right)\right)$$

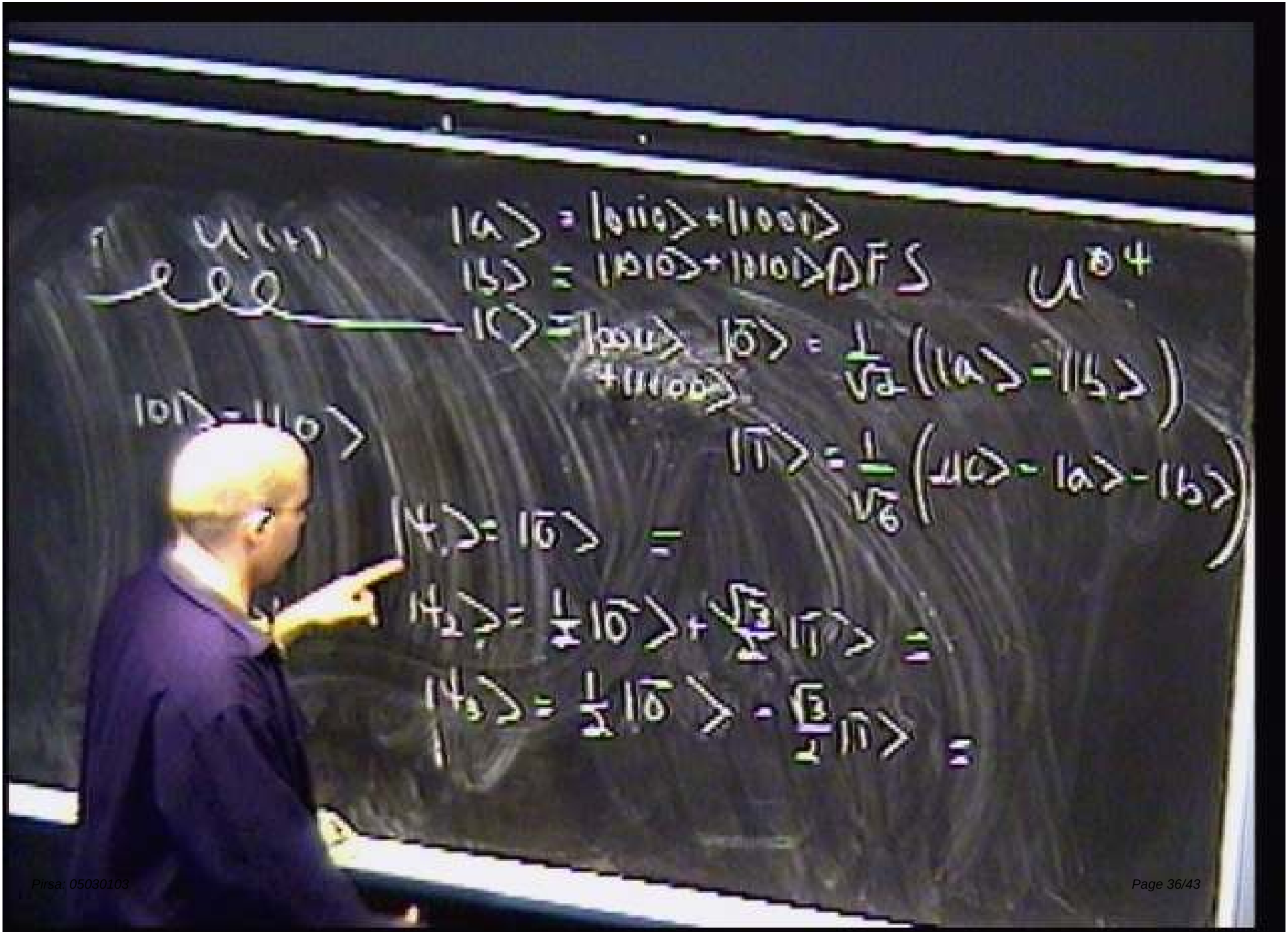
$$e_x = \frac{\rho_c^{sq}\, e_y^{sq} + \rho_c^{dk}\, e_x^{dk}}{\rho_c}$$

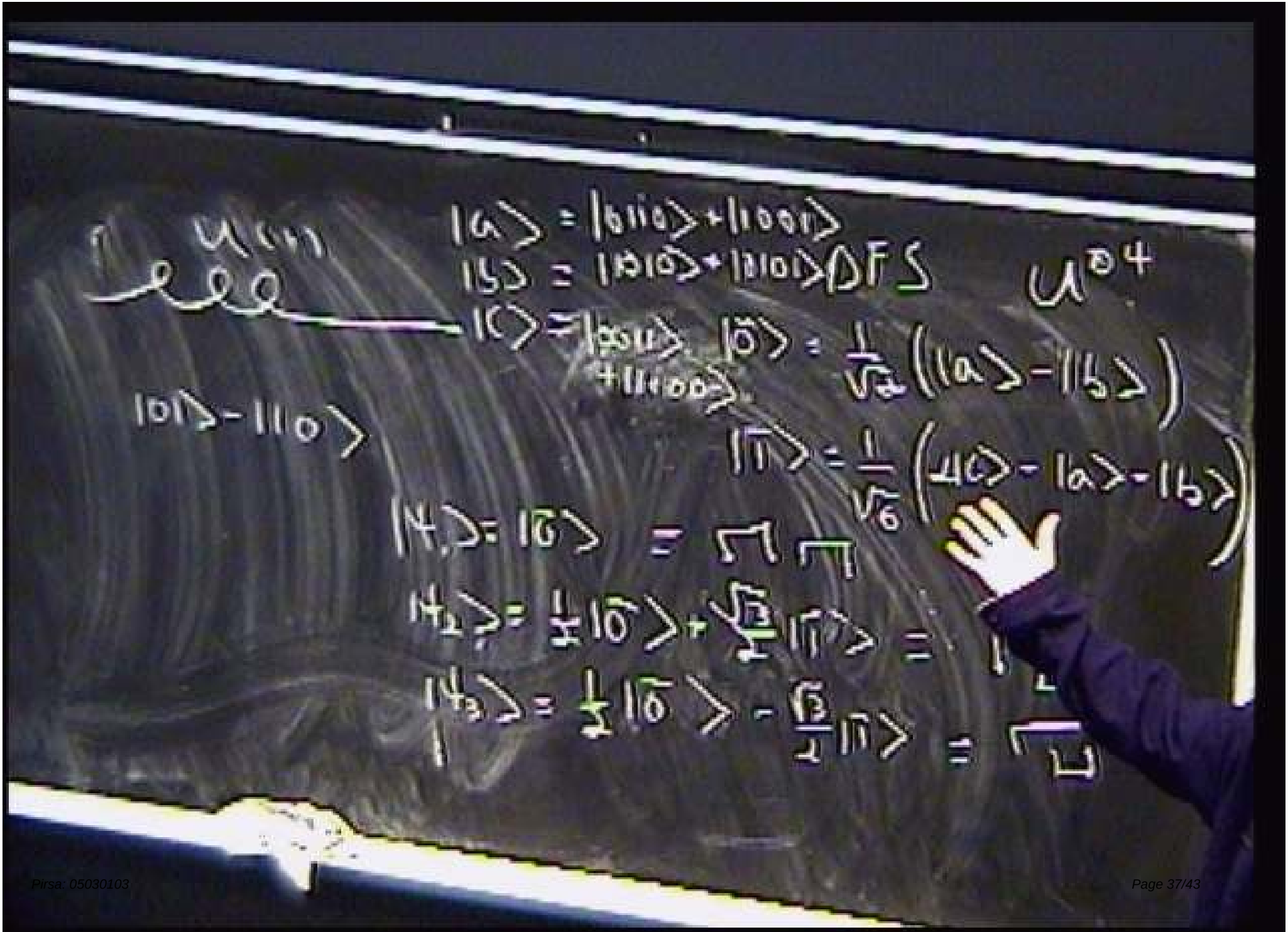
$P_c^{Air} = 0$

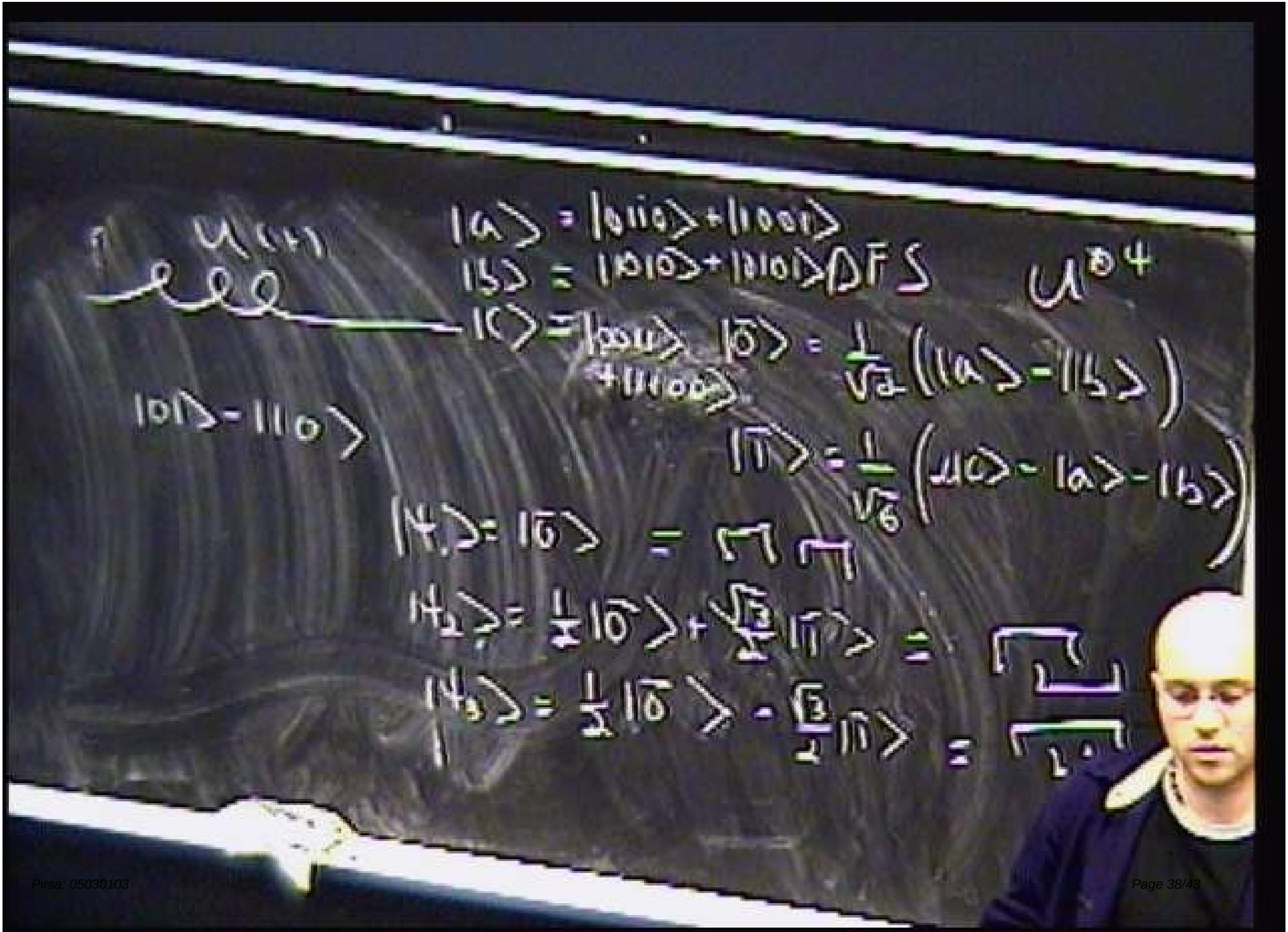

Ein Problem:
$P_c^{AF} = 0$
$P_c =$
BB84 : 11,0 %
Six-State: 12,6 %
PBC00 : 9,81 %

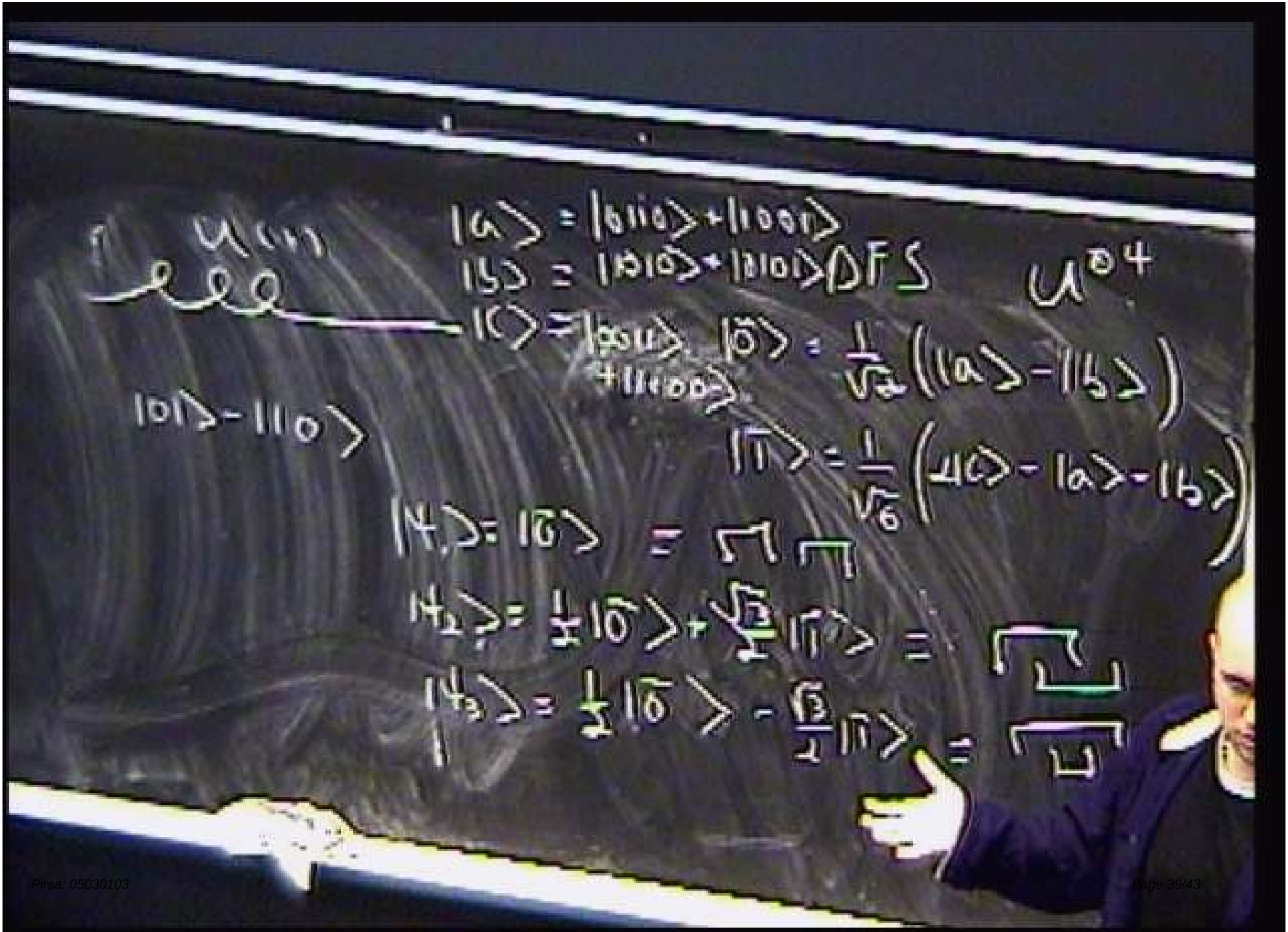

|0⟩ - |1|0⟩

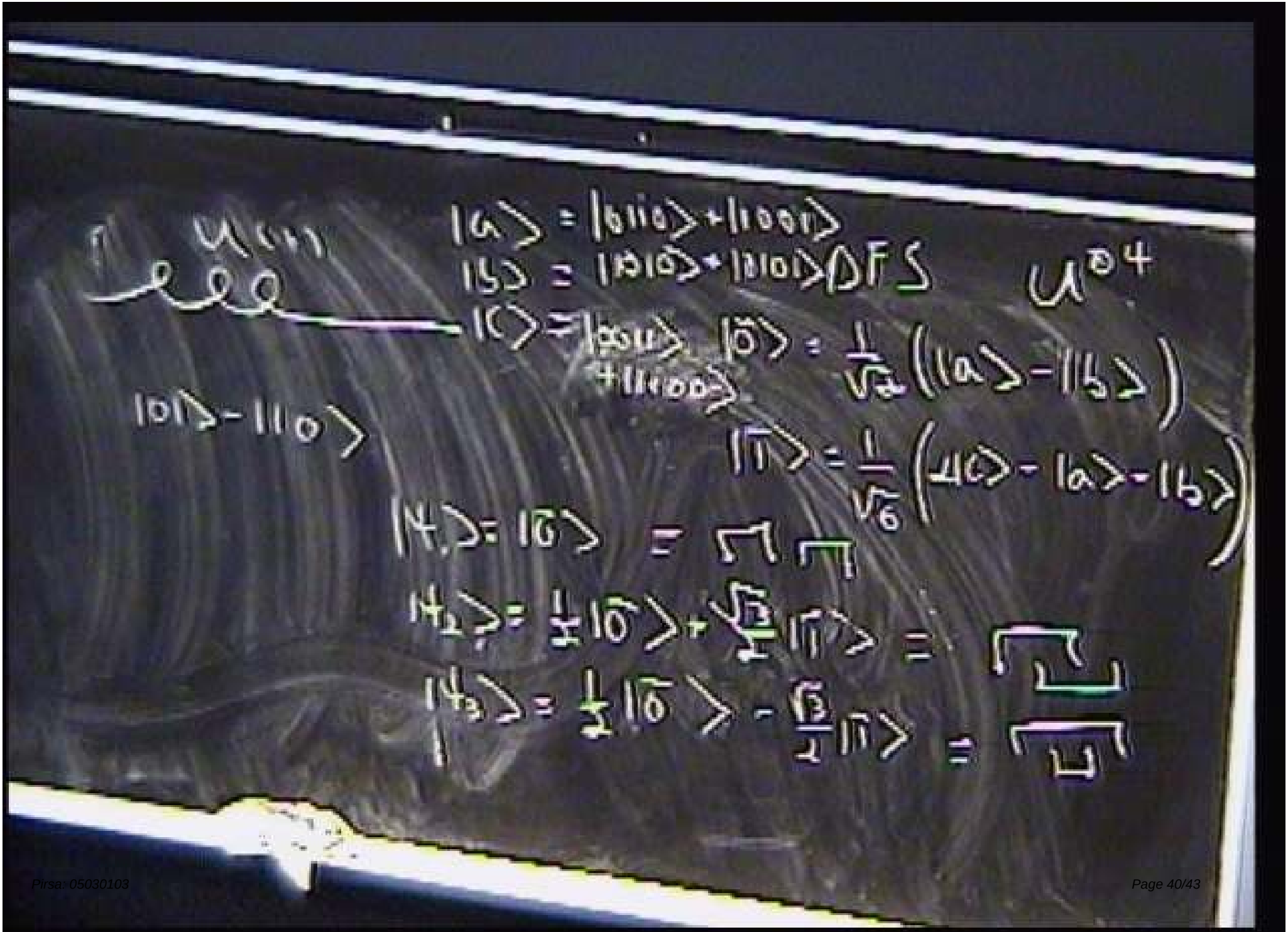

DFS
$|5\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$
$|\pi\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$

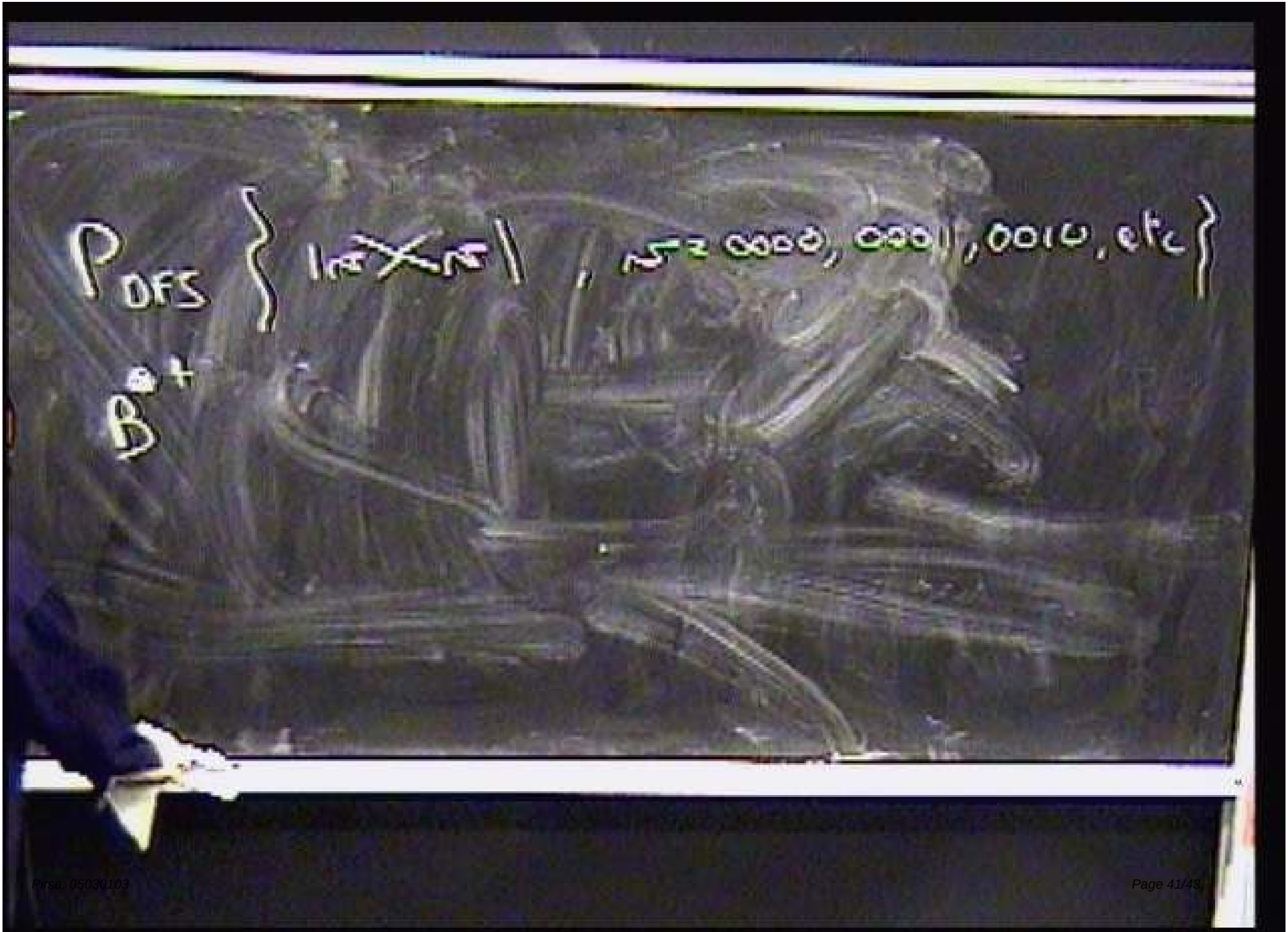

$|A\rangle = |0110\rangle + |1001\rangle$
$|S\rangle = |0110\rangle + |1001\rangle$
$|0\rangle = |00\rangle \quad |\bar{0}\rangle = \frac{1}{\sqrt{2}}(|A\rangle - |S\rangle)$
$+|11\rangle$
$|01\rangle - |10\rangle$
$|1\rangle = |\bar{0}\rangle =$
$|\Psi_1\rangle = \frac{1}{\sqrt{3}}|\bar{0}\rangle + \sqrt{\frac{2}{3}}|\bar{1}\rangle =$
$|\Psi_2\rangle = \frac{1}{\sqrt{3}}|\bar{0}\rangle - \sqrt{\frac{2}{3}}|\bar{1}\rangle =$

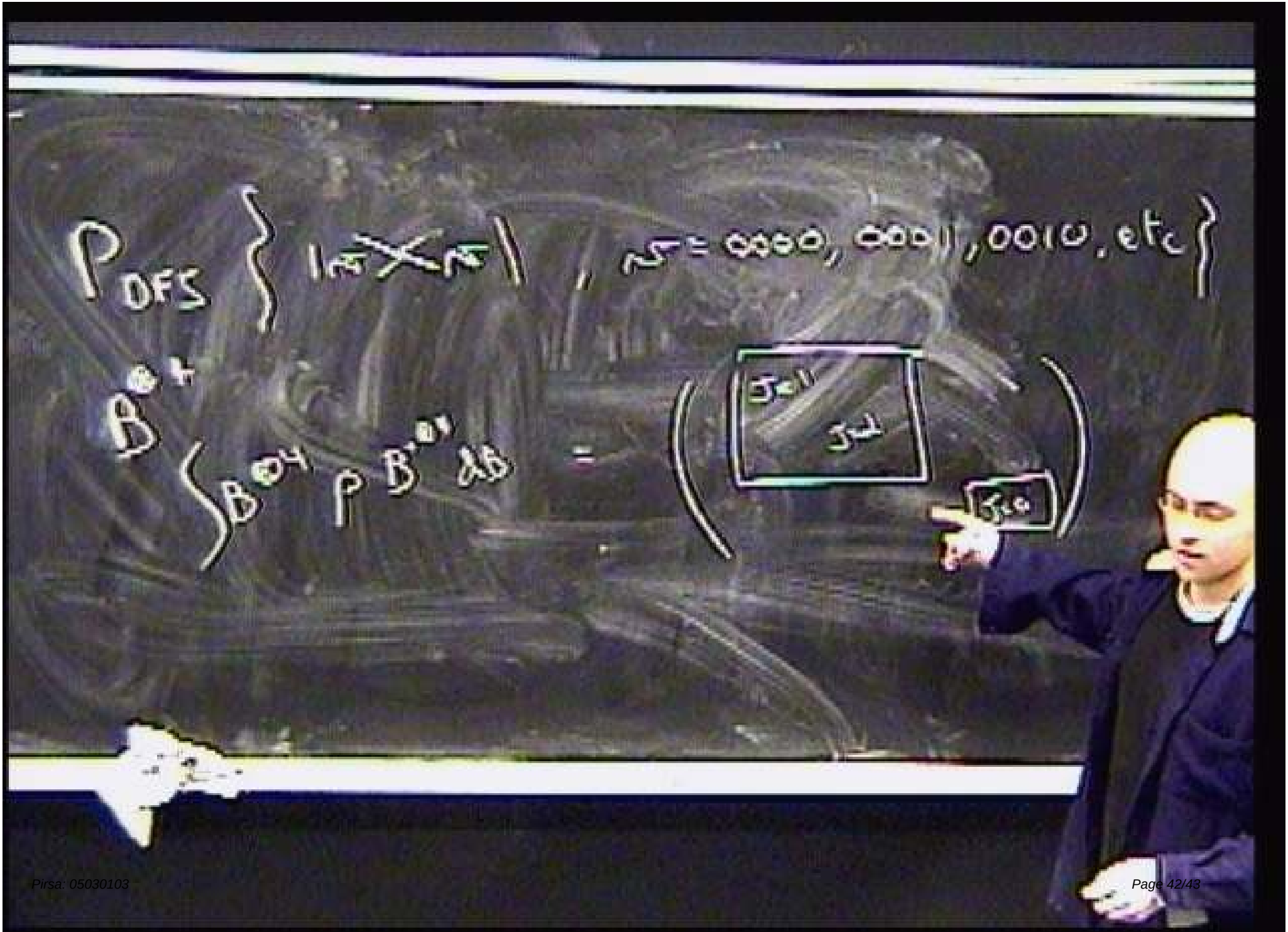

$|a\rangle = |01\rangle + |00\rangle$
$|b\rangle = |10\rangle + |01\rangle$
$|c\rangle = |00\rangle + |11\rangle$
$|01\rangle - |10\rangle$
$|\bar{b}\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$
$|\bar{T}\rangle = \frac{1}{\sqrt{6}}(|c\rangle - |a\rangle - |b\rangle)$
$|\psi_1\rangle = |\bar{a}\rangle$
$|\psi_2\rangle = \frac{1}{\sqrt{2}}|\bar{b}\rangle + \sqrt{\frac{2}{3}}|\bar{T}\rangle$
$|\psi_3\rangle = \frac{1}{\sqrt{2}}|\bar{b}\rangle - \sqrt{\frac{2}{3}}|\bar{T}\rangle$

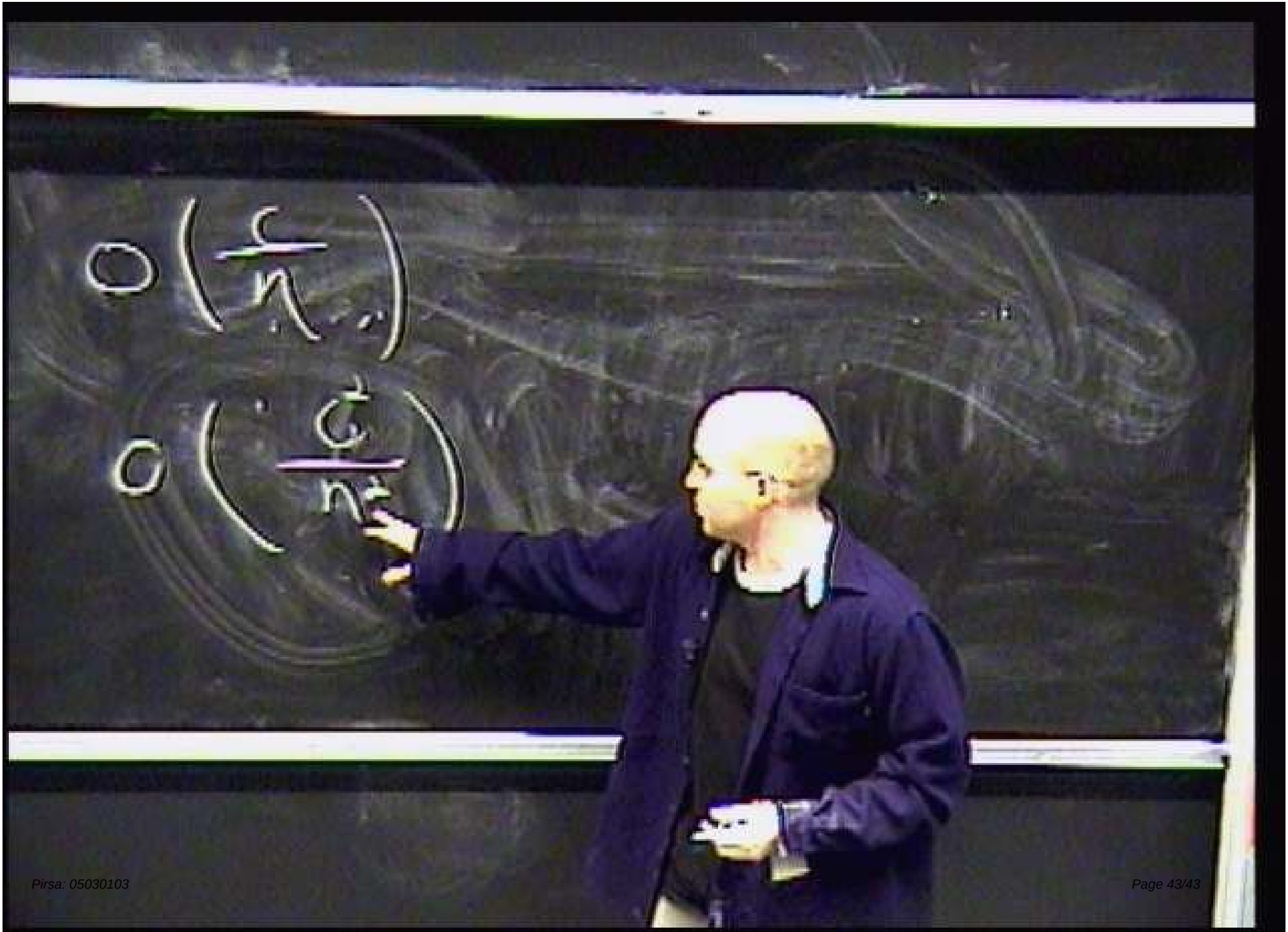

$|A\rangle = |0110\rangle + |1001\rangle$
$|B\rangle = |0101\rangle + |1010\rangle$
$|C\rangle = |0011\rangle + |1100\rangle$
$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|A\rangle - |B\rangle)$
$|\bar{1}\rangle = \frac{1}{\sqrt{6}}(|C\rangle - |A\rangle - |B\rangle)$
$|\psi_1\rangle = |\bar{0}\rangle$
$|\psi_2\rangle = \frac{1}{\sqrt{2}}|\bar{0}\rangle + \frac{\sqrt{3}}{2}|\bar{1}\rangle$
$|\psi_3\rangle = \frac{1}{\sqrt{2}}|\bar{0}\rangle - \frac{\sqrt{3}}{2}|\bar{1}\rangle$


$|A\rangle = |01\rangle + |10\rangle$
$|S\rangle = |01\rangle + |10\rangle$
$|0\rangle = |00\rangle + |11\rangle$
$|01\rangle - |10\rangle$
$|4\rangle = |6\rangle$
$|4_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{\sqrt{3}}{\sqrt{2}}|1\rangle$
$|4_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{\sqrt{3}}{\sqrt{2}}|1\rangle$
$|5\rangle = \frac{1}{\sqrt{2}}(|A\rangle - |S\rangle)$
$|1\rangle = \frac{1}{\sqrt{6}}(|4\rangle - |A\rangle - |S\rangle)$


$|a\rangle = |01\rangle + |10\rangle$
$|b\rangle = |01\rangle - |10\rangle$
$|c\rangle = |00\rangle$
$|d\rangle = |11\rangle$
$|\bar{b}\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$
$|\bar{a}\rangle = \frac{1}{\sqrt{6}}(|d\rangle - |a\rangle - |b\rangle)$
$|4\rangle = |\bar{c}\rangle$
$|4_1\rangle = \frac{1}{\sqrt{3}}|\bar{c}\rangle + \sqrt{\frac{2}{3}}|\bar{a}\rangle$
$|4_2\rangle = \frac{1}{\sqrt{2}}|\bar{c}\rangle - \frac{1}{\sqrt{2}}|\bar{b}\rangle$


P_{DFS}
B^0




$O\left(\frac{f}{n}\right)$
$O\left(\frac{G}{n^2}\right)$