Title: Introduction to Quantum Information and Computation from a Foundational Standpoint

Date: Nov 30, 2006 10:30 AM

URL: http://pirsa.org/06110042

Abstract: Quantum Computation

Pre and Post-Selection

(i) Alice prepares a system in a certain state $|\mathrm{pre}\rangle$ at time t_1,

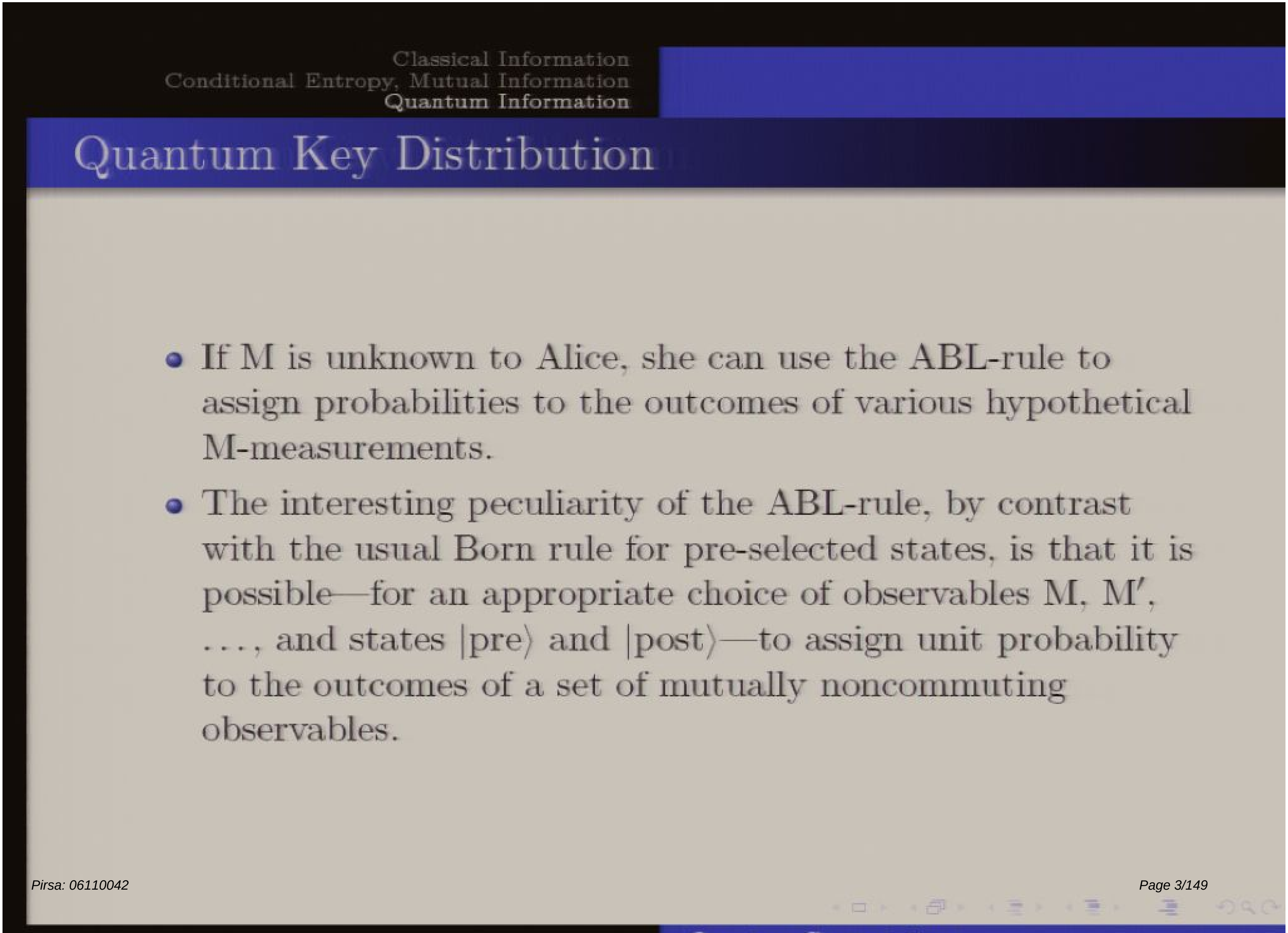
(ii) Bob measures some observable M on the system at time t_2,

(iii) Alice measures an observable of which $|\mathrm{post}\rangle$ is an eigenstate at time t_3, and post-selects for $|\mathrm{post}\rangle$,

then Alice can assign probabilities to the outcomes of Bob's M-measurement at t_2, conditional on the states $|\mathrm{pre}\rangle$ and $|\mathrm{post}\rangle$ at times t_1 and t_3, respectively, as follows:

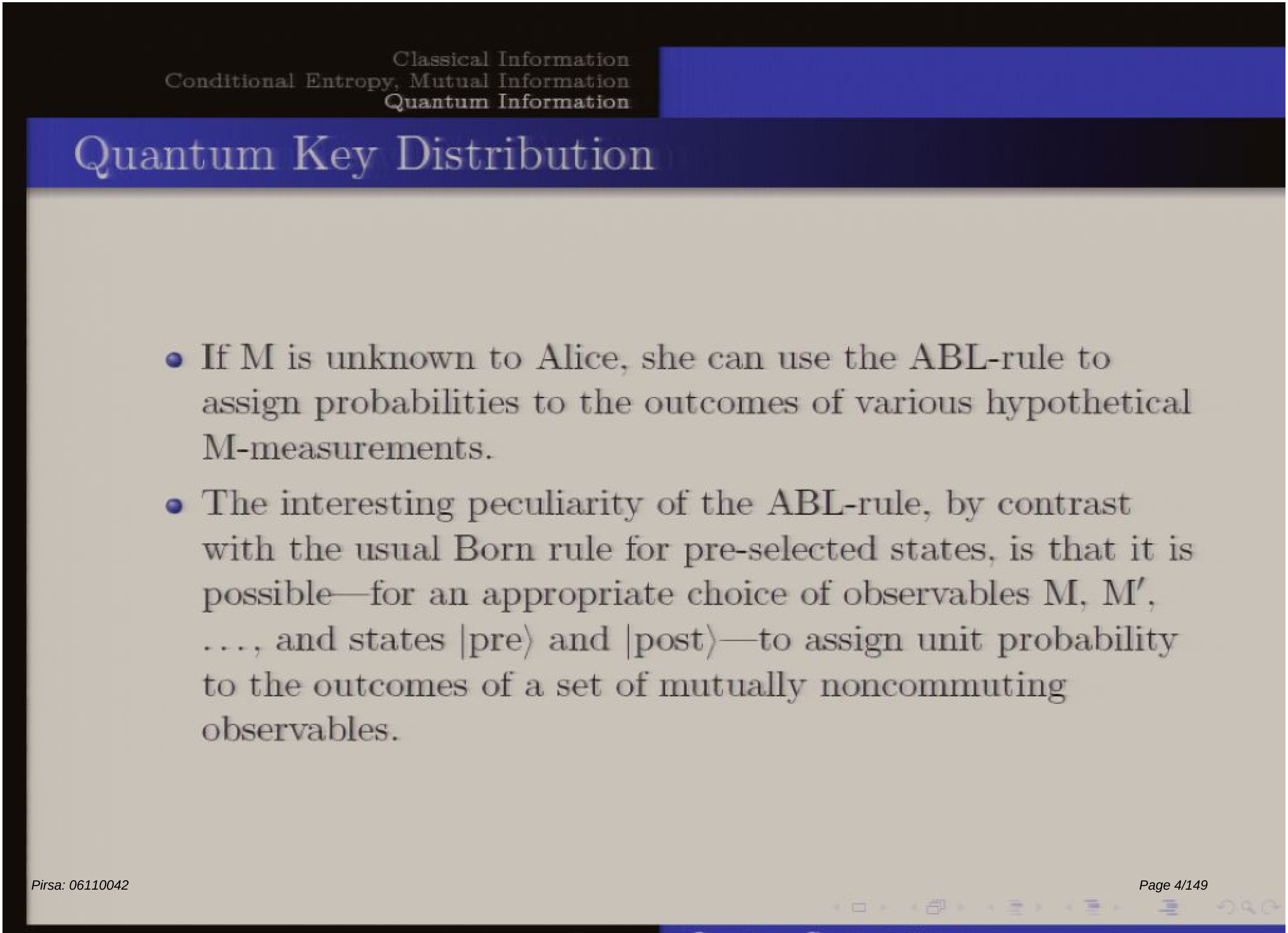
$$\mathrm{prob}(q_k) = \frac{|\langle \mathrm{pre}|P_k|\mathrm{post}\rangle|^2}{\sum_i |\langle \mathrm{pre}|P_i|\mathrm{post}\rangle|^2} \qquad (0)$$

where P_i is the projection operator onto the i'th eigenspace of M.



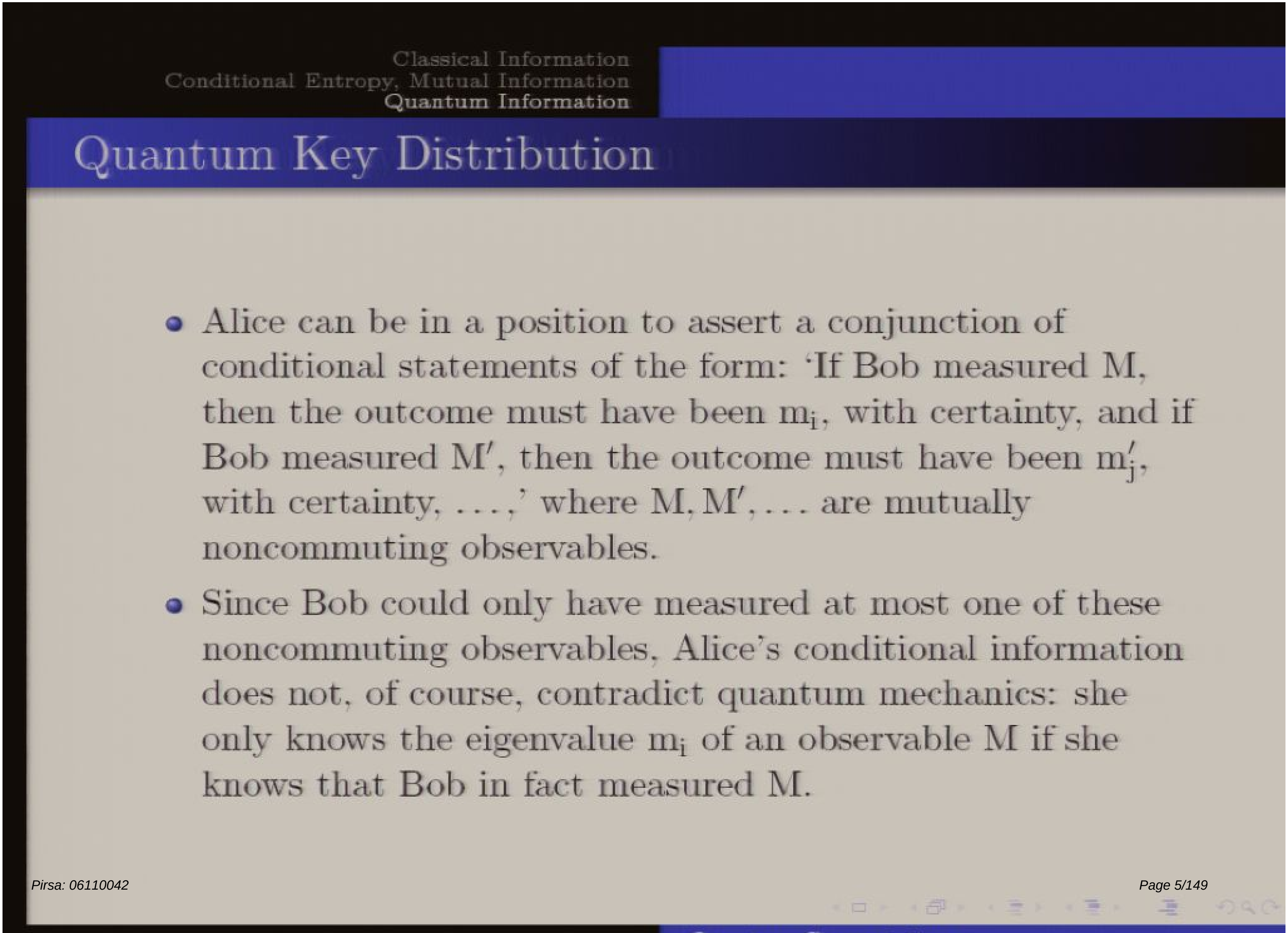
Quantum Key Distribution

- If M is unknown to Alice, she can use the ABL-rule to assign probabilities to the outcomes of various hypothetical M-measurements.
- The interesting peculiarity of the ABL-rule, by contrast with the usual Born rule for pre-selected states, is that it is possible—for an appropriate choice of observables M, M′, . . . , and states $|\text{pre}\rangle$ and $|\text{post}\rangle$—to assign unit probability to the outcomes of a set of mutually noncommuting observables.



Quantum Key Distribution

- If M is unknown to Alice, she can use the ABL-rule to assign probabilities to the outcomes of various hypothetical M-measurements.
- The interesting peculiarity of the ABL-rule, by contrast with the usual Born rule for pre-selected states, is that it is possible—for an appropriate choice of observables M, M′, …, and states $|\text{pre}\rangle$ and $|\text{post}\rangle$—to assign unit probability to the outcomes of a set of mutually noncommuting observables.



Quantum Key Distribution

- Alice can be in a position to assert a conjunction of conditional statements of the form: ‘If Bob measured M, then the outcome must have been $\mathrm{m_i}$, with certainty, and if Bob measured M$'$, then the outcome must have been $\mathrm{m'_j}$, with certainty, . . . ,’ where $\mathrm{M}, \mathrm{M}', \ldots$ are mutually noncommuting observables.
- Since Bob could only have measured at most one of these noncommuting observables, Alice’s conditional information does not, of course, contradict quantum mechanics: she only knows the eigenvalue $\mathrm{m_i}$ of an observable M if she knows that Bob in fact measured M.

Quantum Key Distribution

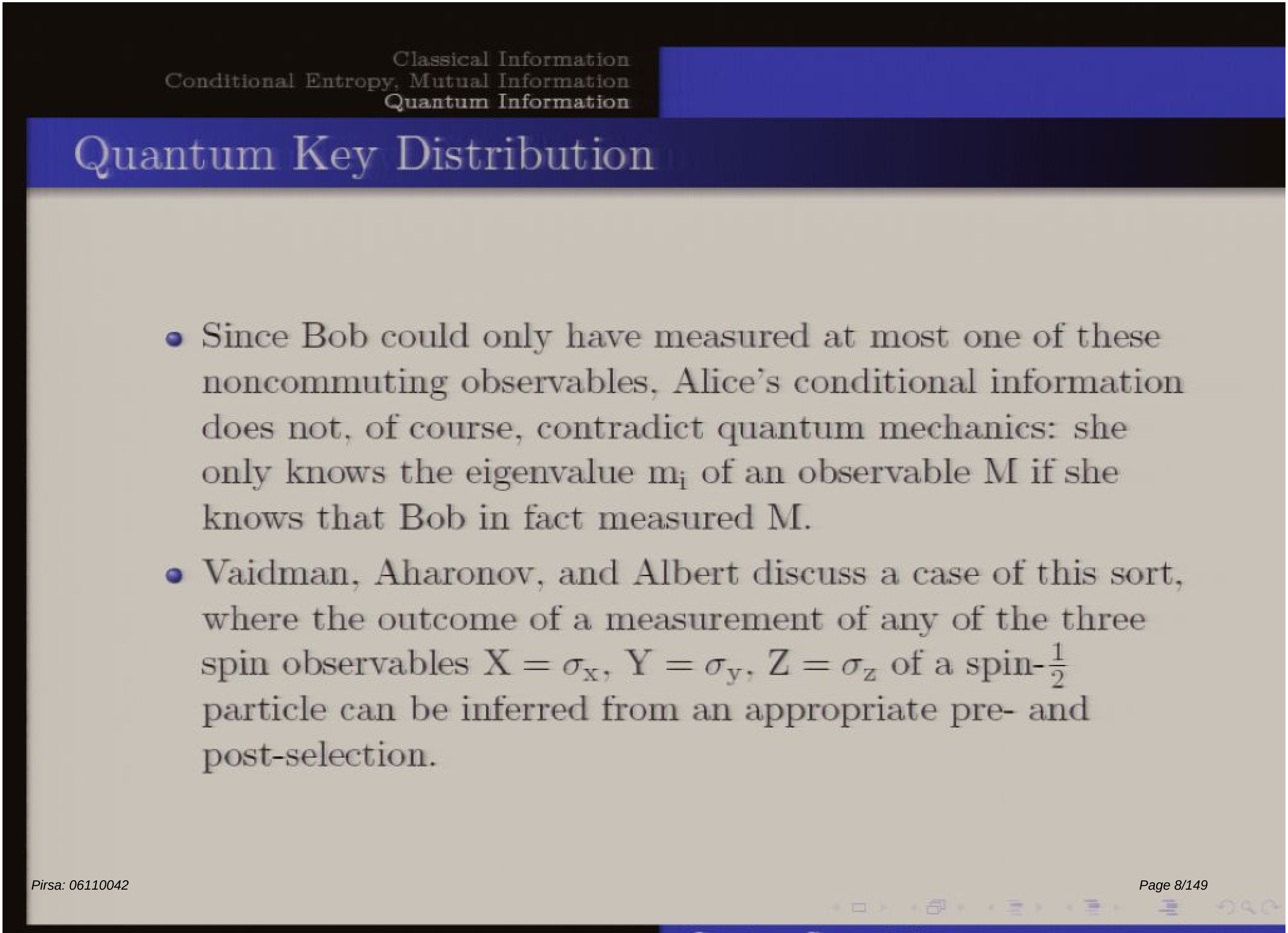
- Vaidman, Aharonov, and Albert discuss a case of this sort, where the outcome of a measurement of any of the three spin observables $\mathrm{X} = \sigma_{\mathrm{x}}$, $\mathrm{Y} = \sigma_{\mathrm{y}}$, $\mathrm{Z} = \sigma_{\mathrm{z}}$ of a spin-$\frac{1}{2}$ particle can be inferred from an appropriate pre- and post-selection.
- Alice prepares the Bell state

$$|\mathrm{pre}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{z}}\rangle_{\mathrm{A}}|\uparrow_{\mathrm{z}}\rangle_{\mathrm{C}} + |\downarrow_{\mathrm{z}}\rangle_{\mathrm{A}}|\downarrow_{\mathrm{z}}\rangle_{\mathrm{C}}$$

where $|\uparrow_{\mathrm{z}}\rangle$ and $|\downarrow_{\mathrm{z}}\rangle$ denote the σ_{z}-eigenstates.

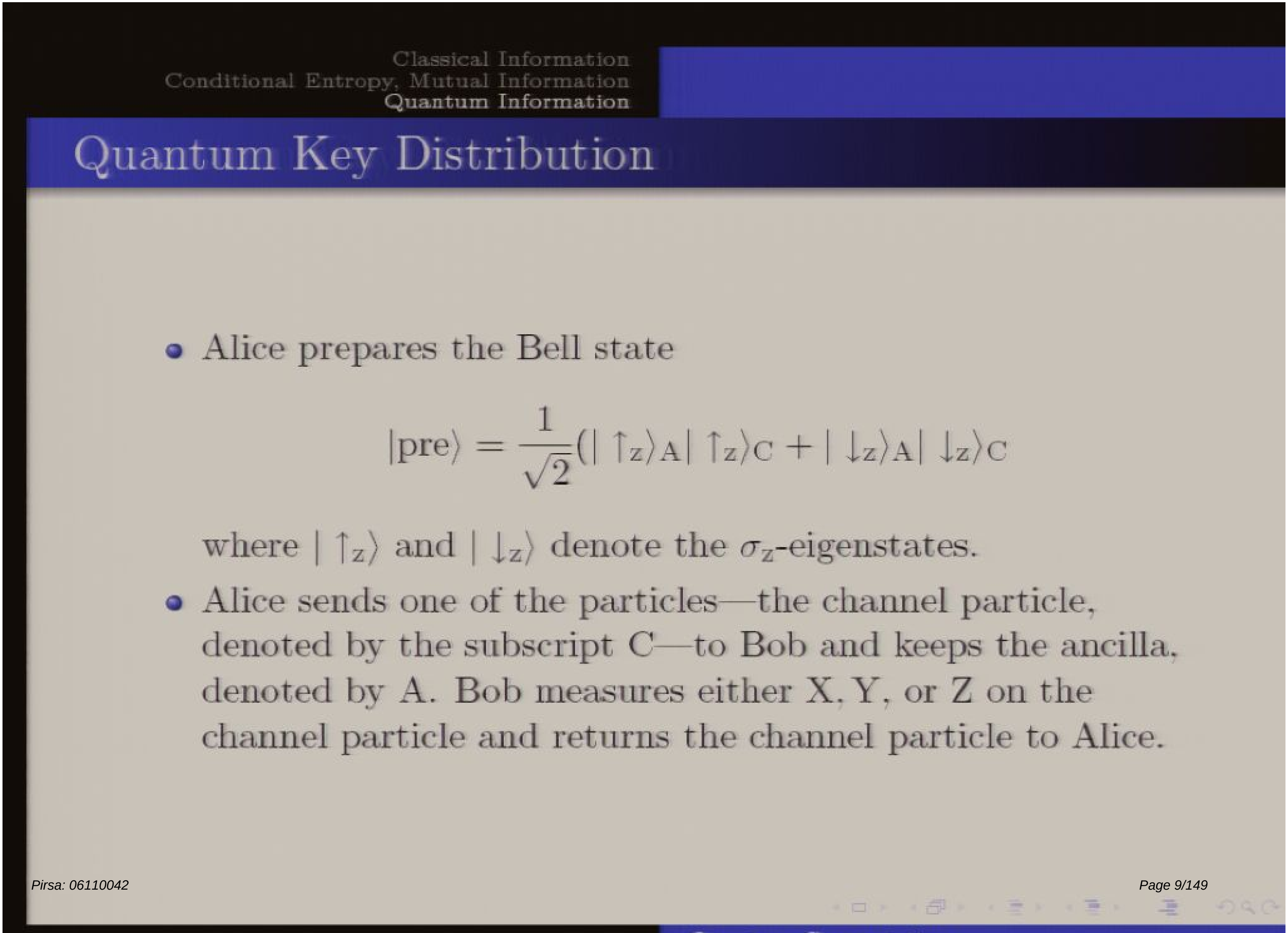
Quantum Key Distribution

- Alice sends one of the particles—the channel particle, denoted by the subscript C—to Bob and keeps the ancilla, denoted by A. Bob measures either X, Y, or Z on the channel particle and returns the channel particle to Alice.
- Alice can be in a position to assert a conjunction of conditional statements of the form: 'If Bob measured M, then the outcome must have been $\mathrm{m_i}$, with certainty, and if Bob measured $\mathrm{M'}$, then the outcome must have been $\mathrm{m'_j}$, with certainty, $\ldots$,' where $\mathrm{M}, \mathrm{M'}, \ldots$ are mutually noncommuting observables.



Quantum Key Distribution

- Since Bob could only have measured at most one of these noncommuting observables, Alice's conditional information does not, of course, contradict quantum mechanics: she only knows the eigenvalue $\mathrm{m_i}$ of an observable M if she knows that Bob in fact measured M.
- Vaidman, Aharonov, and Albert discuss a case of this sort, where the outcome of a measurement of any of the three spin observables $\mathrm{X} = \sigma_{\mathrm{x}}$, $\mathrm{Y} = \sigma_{\mathrm{y}}$, $\mathrm{Z} = \sigma_{\mathrm{z}}$ of a spin-$\frac{1}{2}$ particle can be inferred from an appropriate pre- and post-selection.



Quantum Key Distribution

- Alice prepares the Bell state

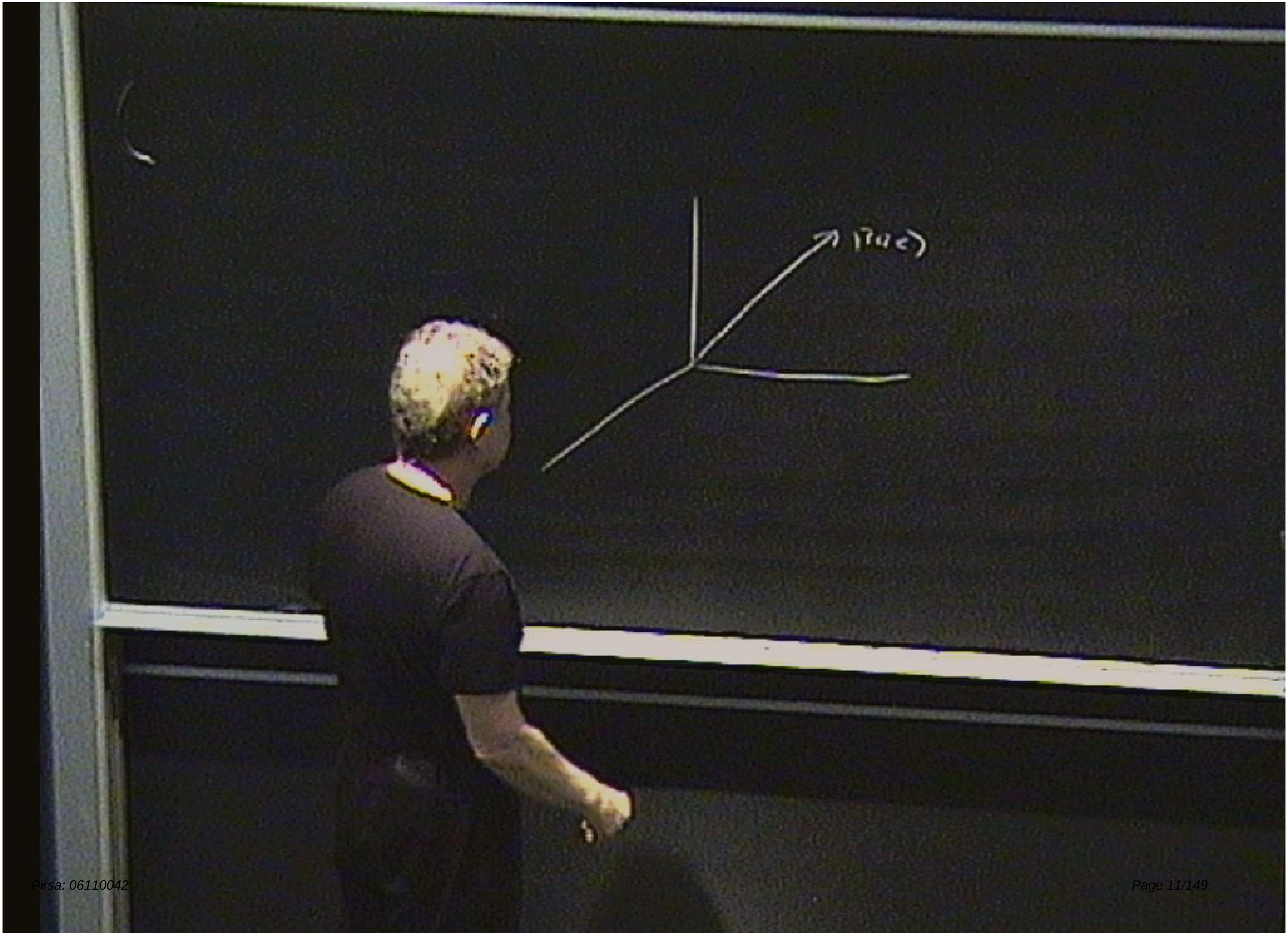
$$|\mathrm{pre}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{z}}\rangle_{\mathrm{A}}|\uparrow_{\mathrm{z}}\rangle_{\mathrm{C}} + |\downarrow_{\mathrm{z}}\rangle_{\mathrm{A}}|\downarrow_{\mathrm{z}}\rangle_{\mathrm{C}}$$

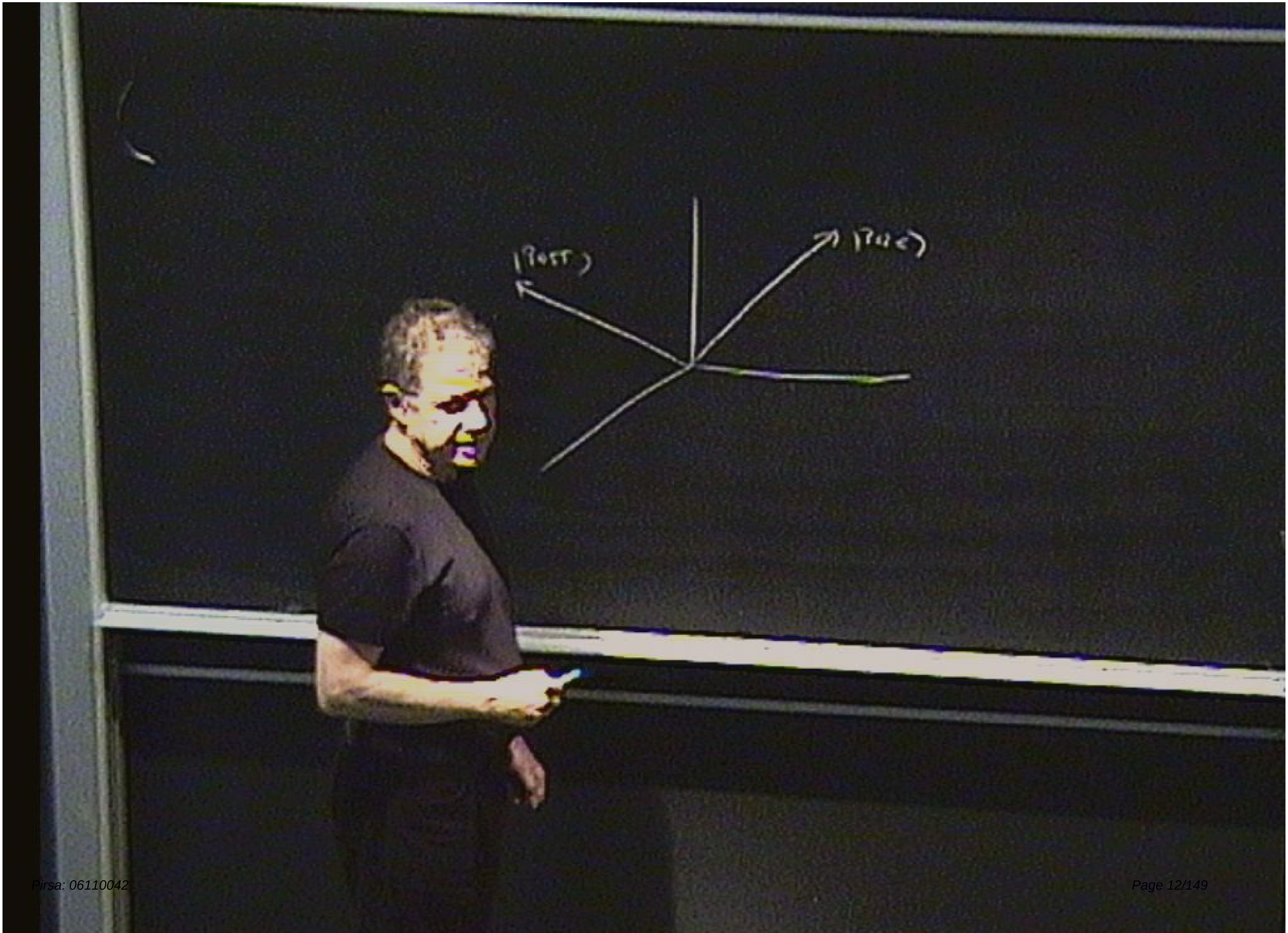
  where $|\uparrow_{\mathrm{z}}\rangle$ and $|\downarrow_{\mathrm{z}}\rangle$ denote the σ_{z}-eigenstates.
- Alice sends one of the particles—the channel particle, denoted by the subscript C—to Bob and keeps the ancilla, denoted by A. Bob measures either X, Y, or Z on the channel particle and returns the channel particle to Alice.

Quantum Key Distribution

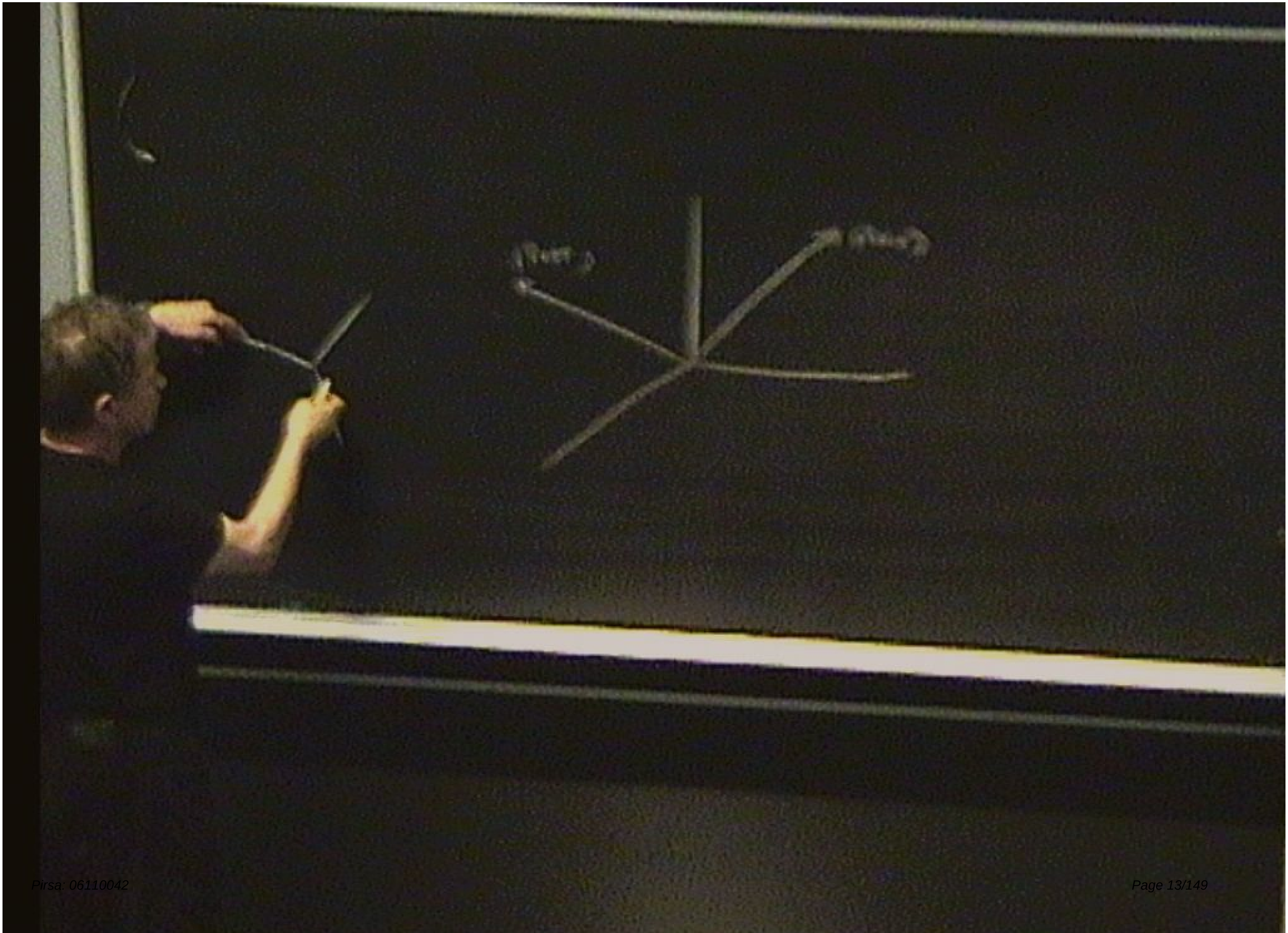
Alice then measures an observable R on the pair of particles, where R has the eigenstates (the subscripts A and C are suppressed):

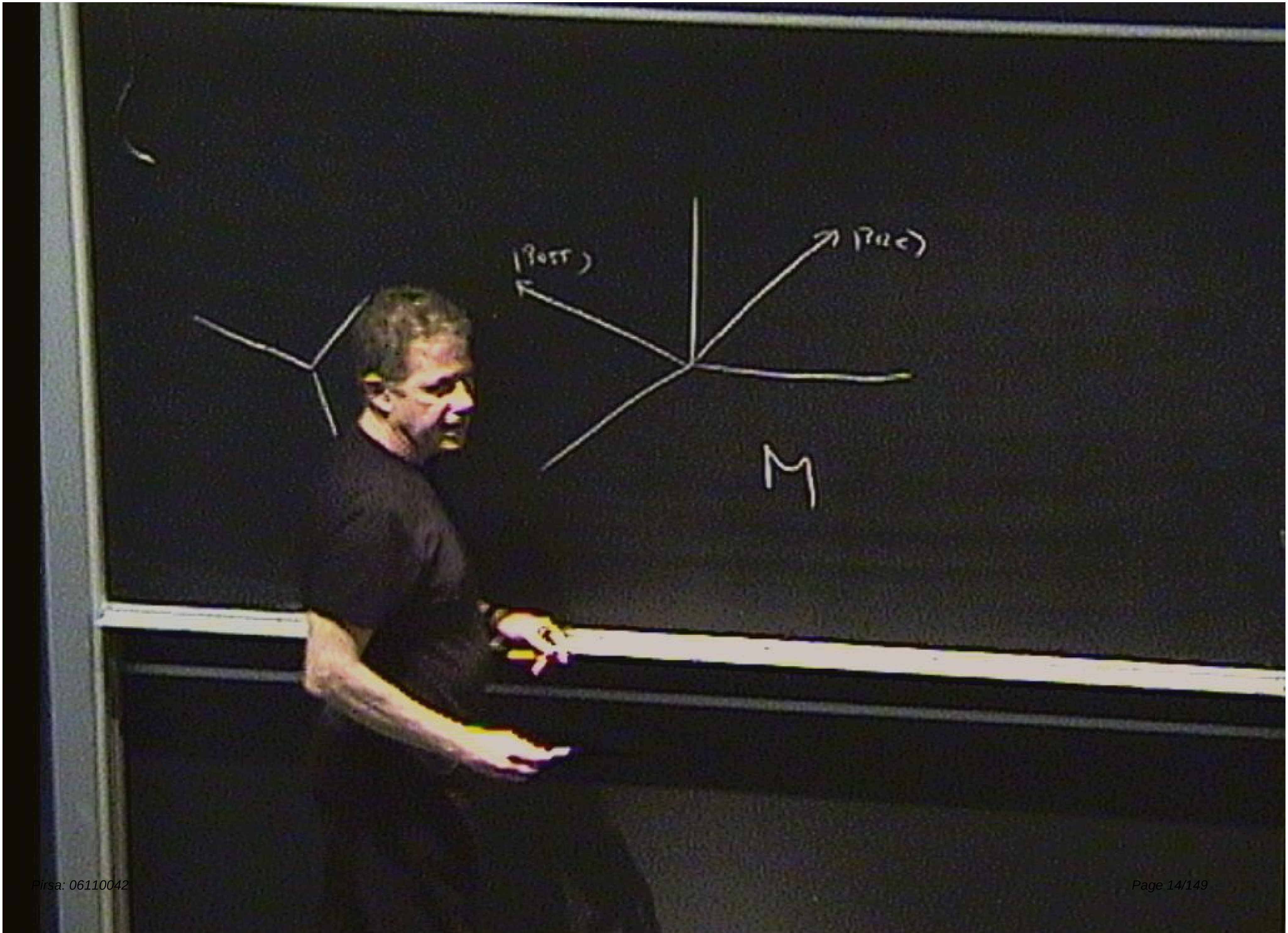
$$\begin{aligned}
|\mathrm{r}_1\rangle &= \frac{1}{\sqrt{2}}|\uparrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle + \frac{1}{2}(|\uparrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle \mathrm{e}^{\mathrm{i}\pi/4} + |\downarrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle \mathrm{e}^{-\mathrm{i}\pi/4}) \\
|\mathrm{r}_2\rangle &= \frac{1}{\sqrt{2}}|\uparrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle - \frac{1}{2}(|\uparrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle \mathrm{e}^{\mathrm{i}\pi/4} + |\downarrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle \mathrm{e}^{-\mathrm{i}\pi/4}) \\
|\mathrm{r}_3\rangle &= \frac{1}{\sqrt{2}}|\downarrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle + \frac{1}{2}(|\uparrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle \mathrm{e}^{-\mathrm{i}\pi/4} + |\downarrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle \mathrm{e}^{\mathrm{i}\pi/4}) \\
|\mathrm{r}_4\rangle &= \frac{1}{\sqrt{2}}|\downarrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle - \frac{1}{2}(|\uparrow_\mathrm{z}\rangle|\downarrow_\mathrm{z}\rangle \mathrm{e}^{-\mathrm{i}\pi/4} + |\downarrow_\mathrm{z}\rangle|\uparrow_\mathrm{z}\rangle \mathrm{e}^{\mathrm{i}\pi/4})
\end{aligned}$$

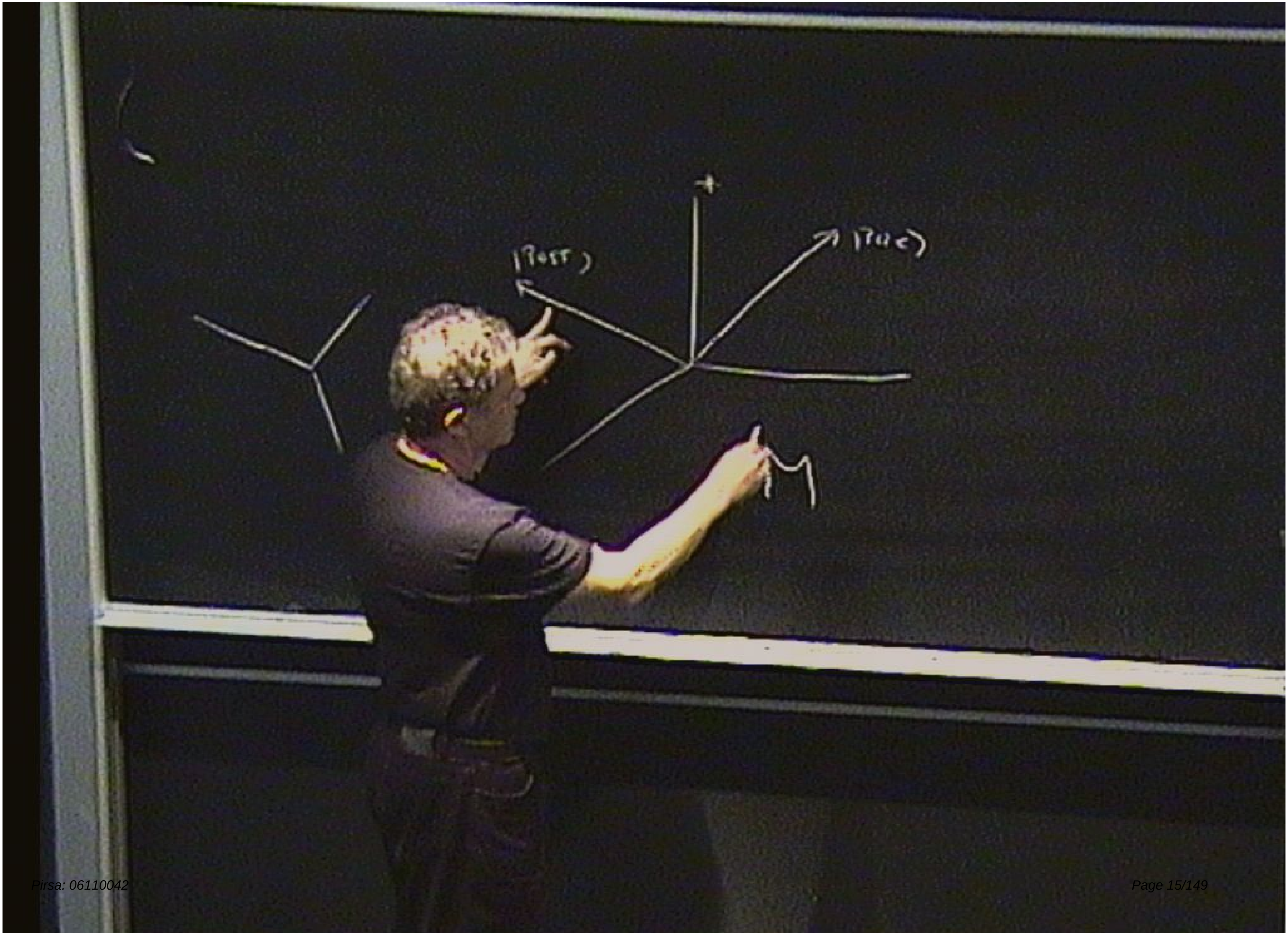

|Tue⟩

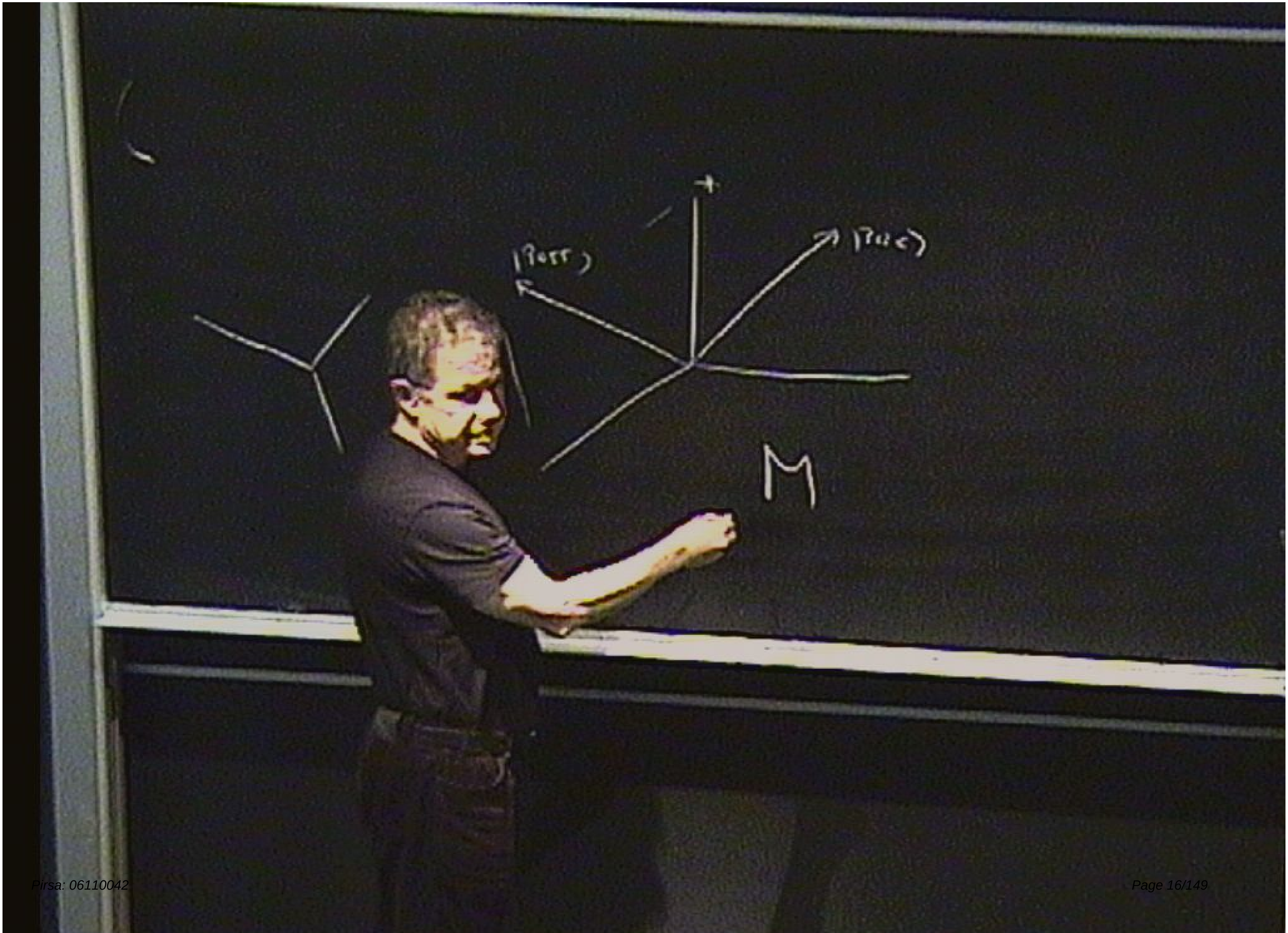


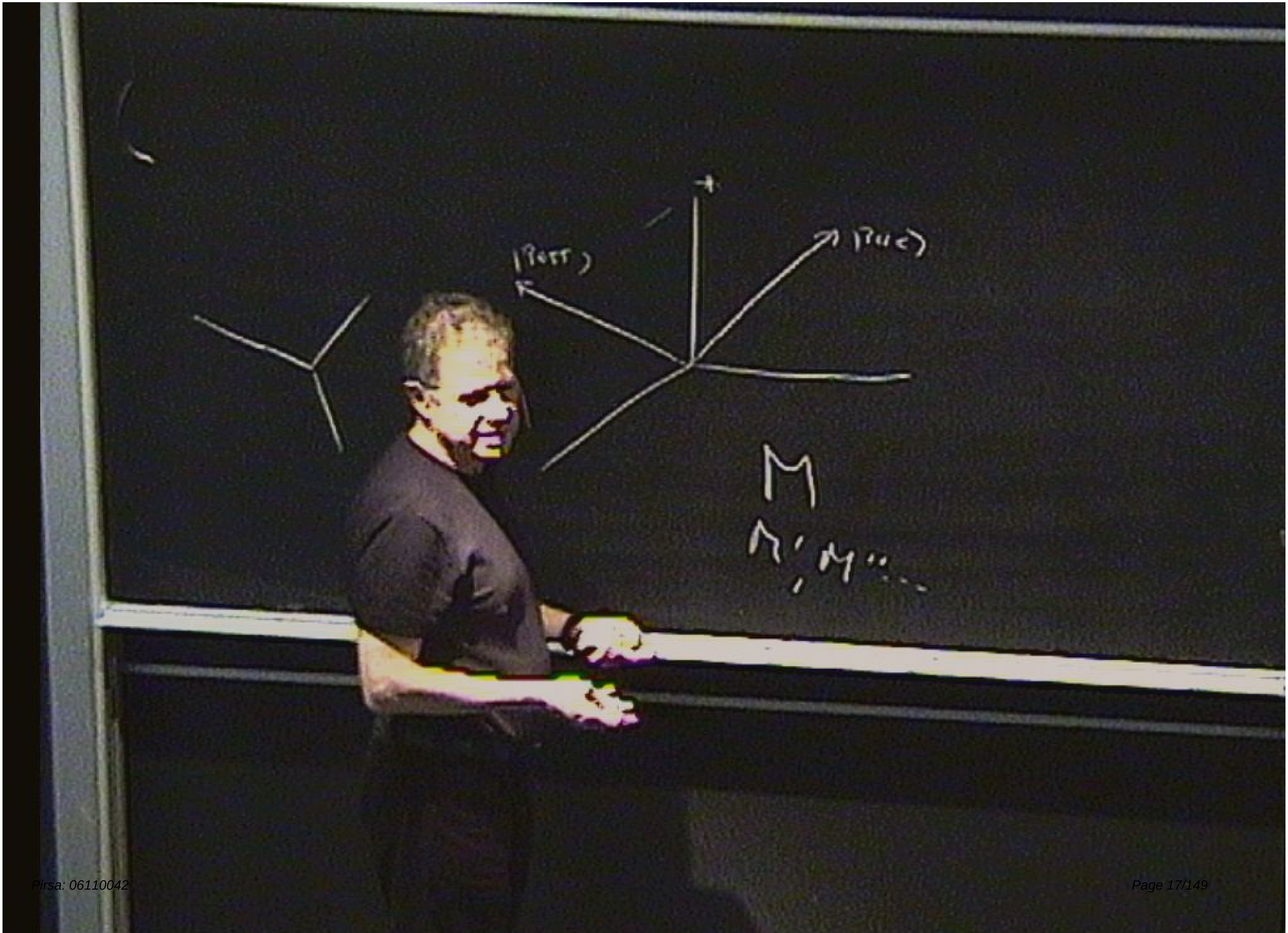
|Post⟩
|Pre⟩

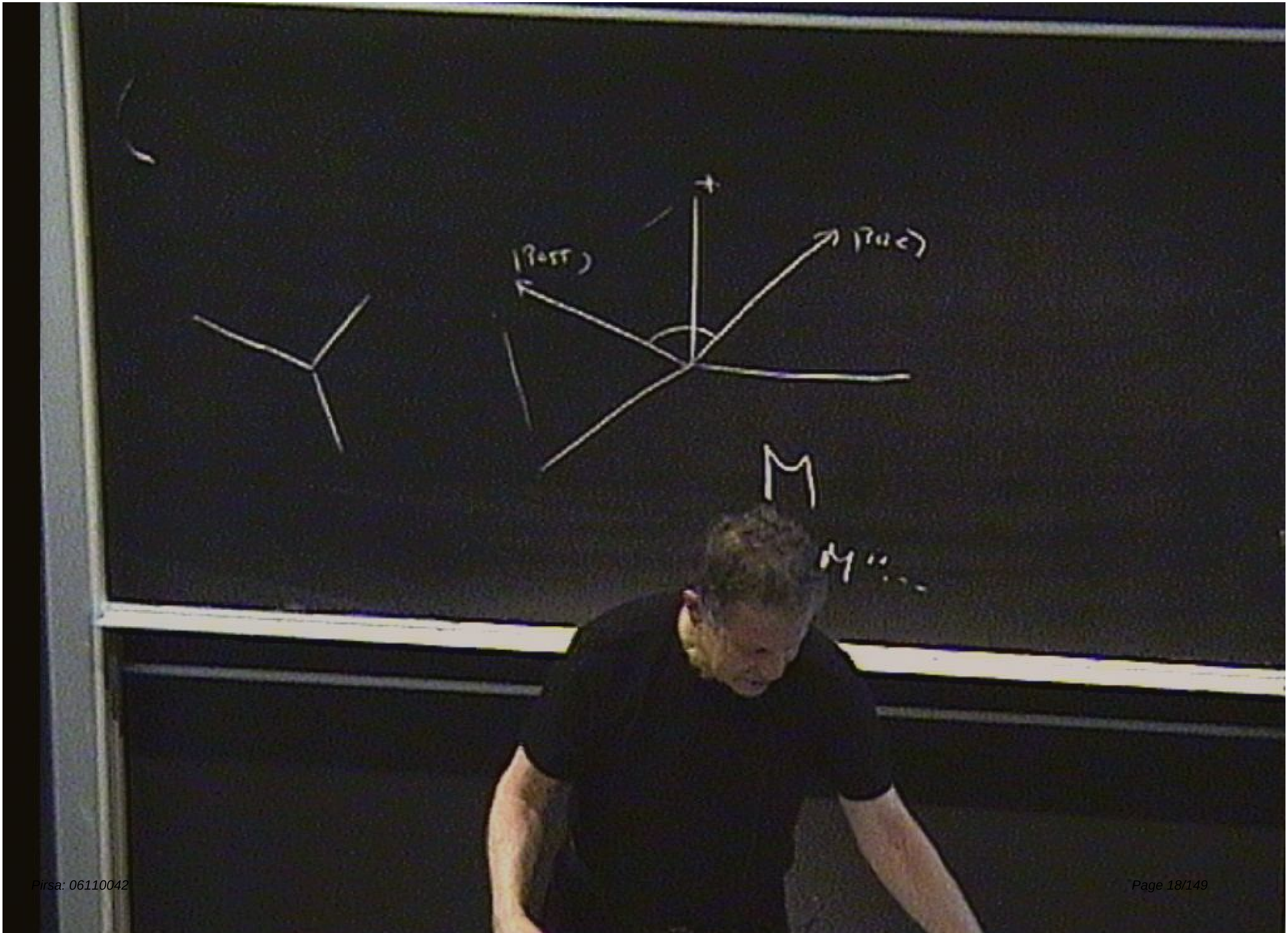


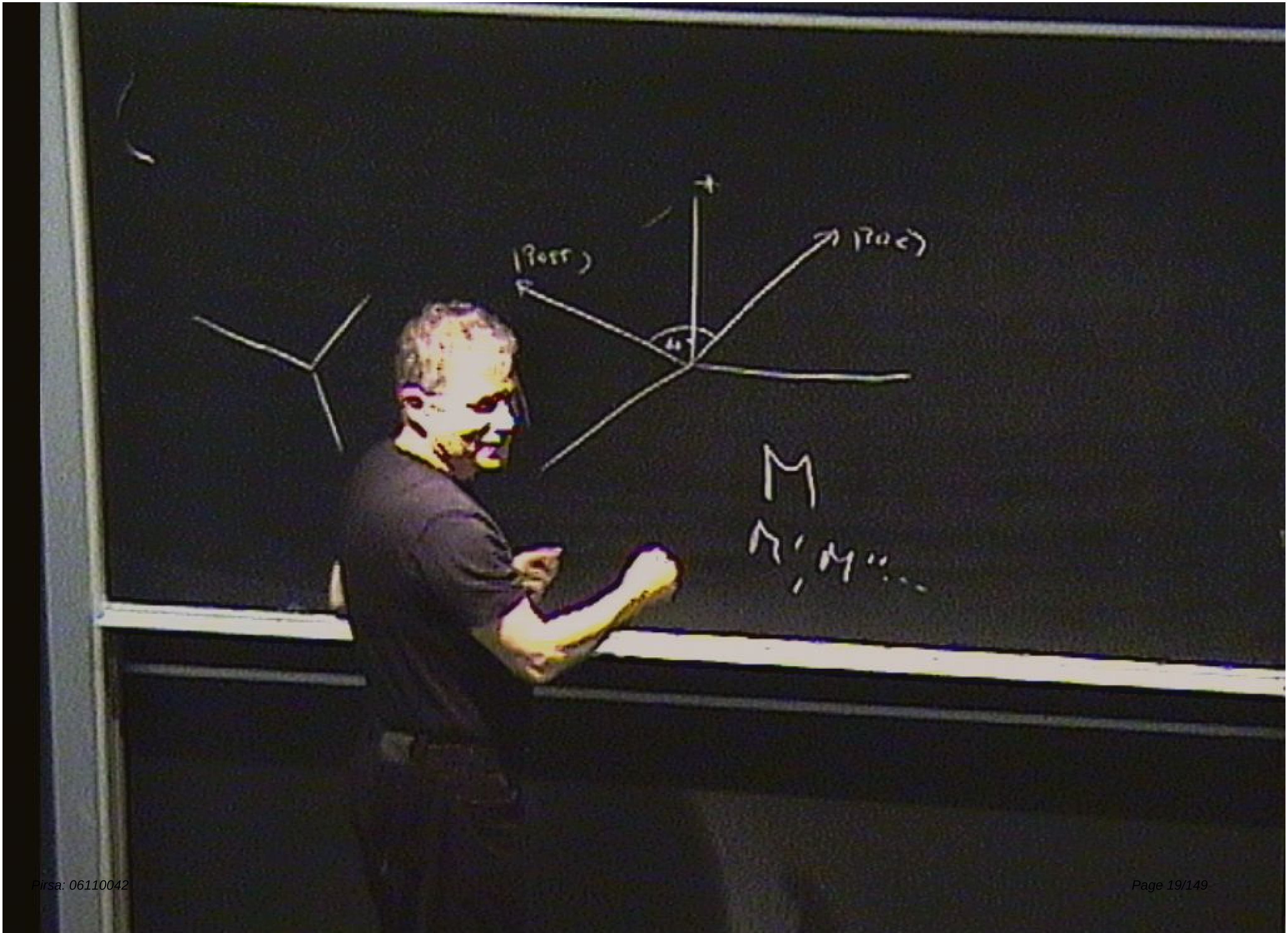

|Post⟩
|Pre⟩
M

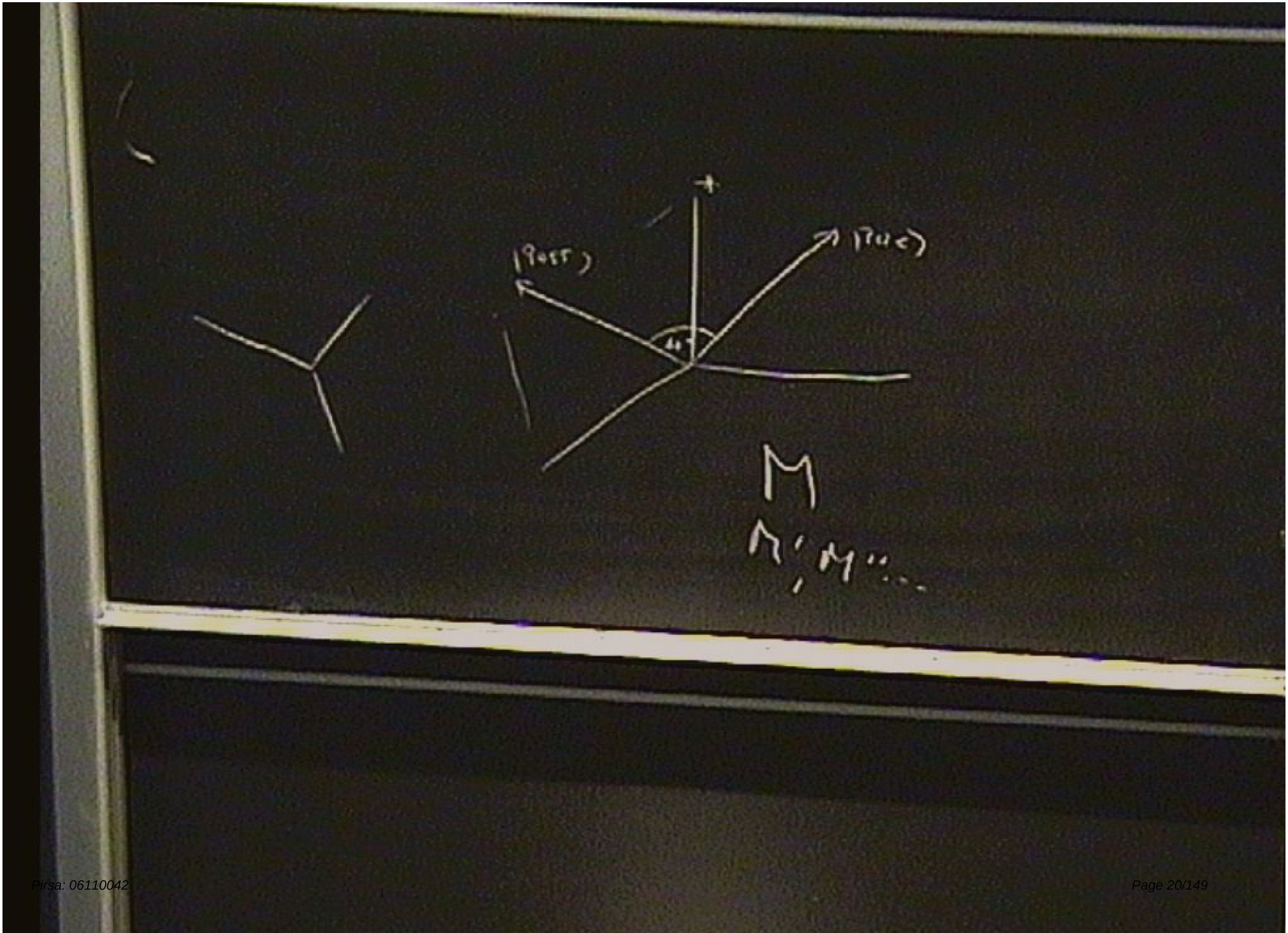

t
|Past⟩
|Pure⟩
M

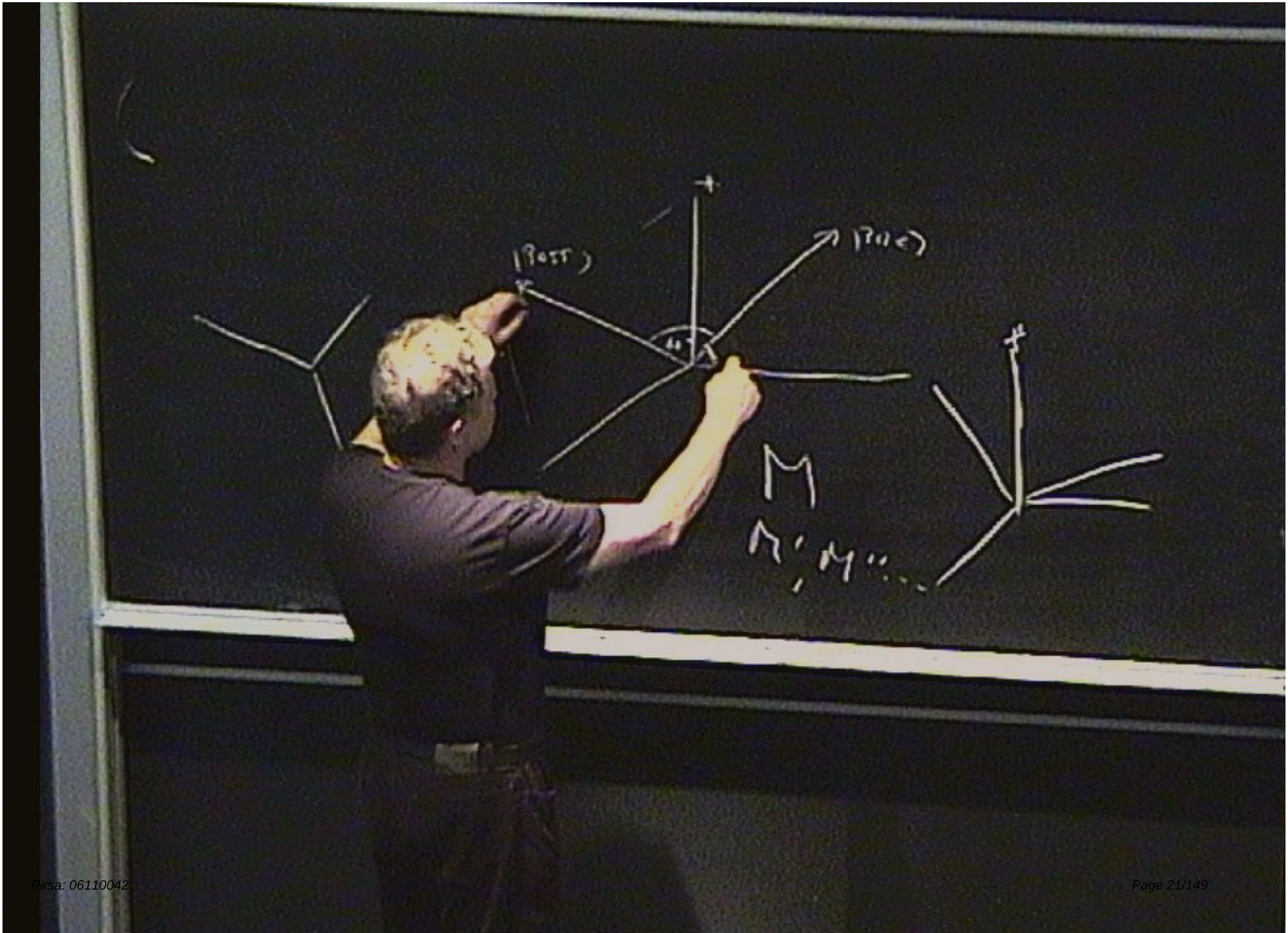

$|\Psi_{off}\rangle$
$|\Psi_{acc}\rangle$
M

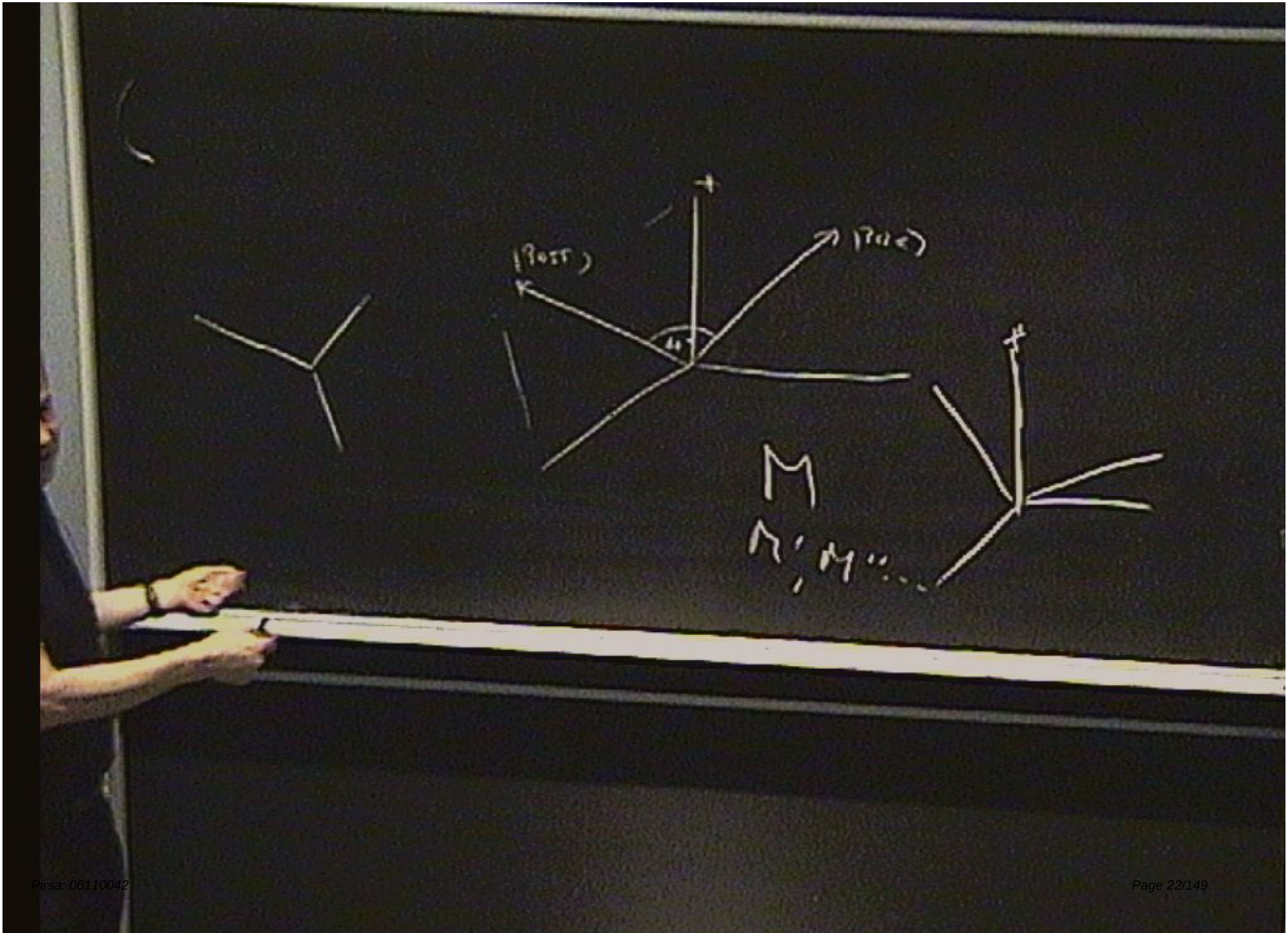

|Poff⟩
|Puc⟩
M
M', M''...

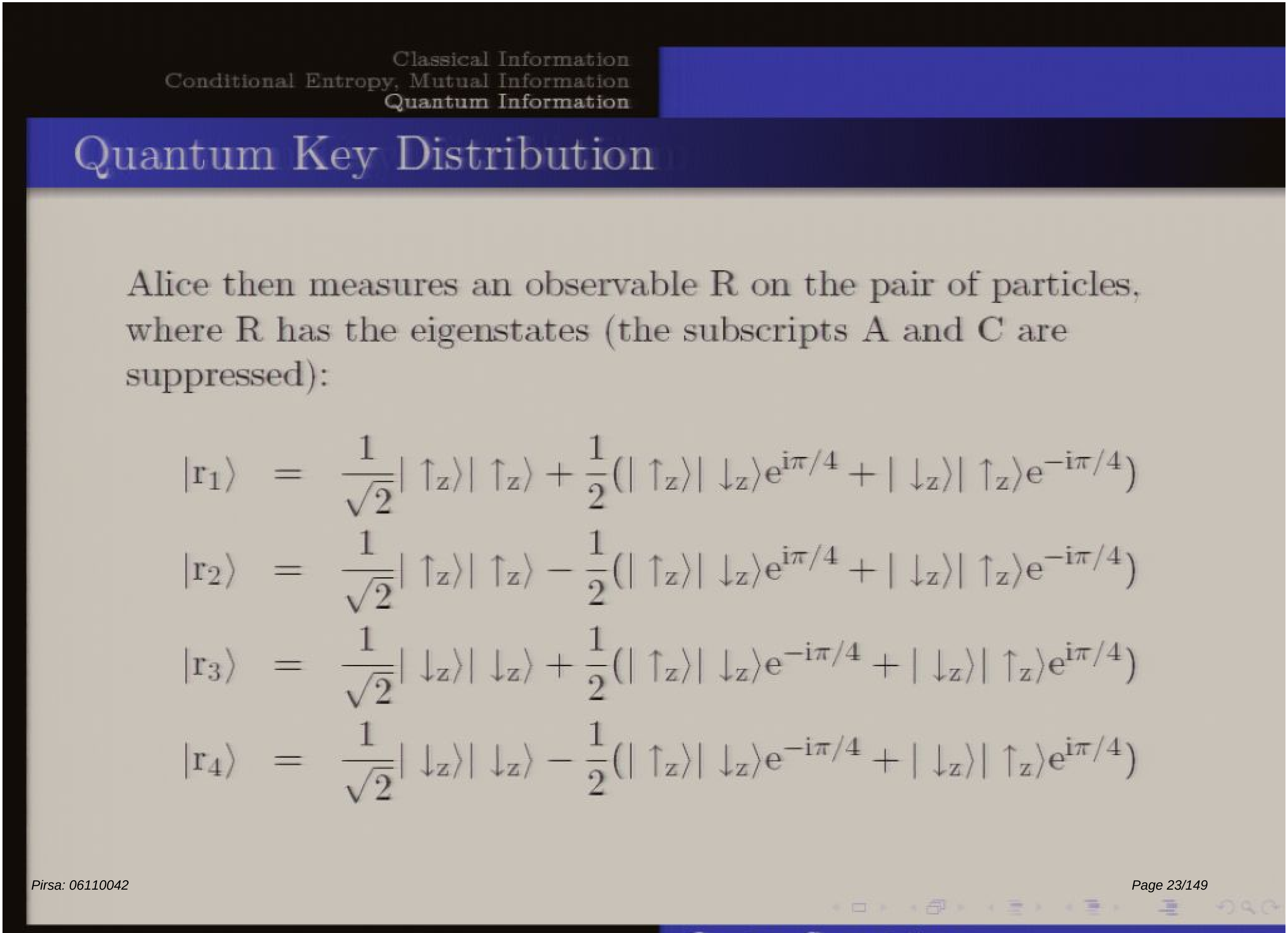

|Pass⟩
|Rec⟩
M
M'...


|Pass⟩
|Rec⟩
45
M
M′, M″...


|false⟩
|true⟩
45°
M
M', M''...


t
|Ψout⟩
|Ψin⟩
t
M
M', M''...


t
|Post⟩
|Pre⟩
45
t
M
M', M''...



Quantum Key Distribution

Alice then measures an observable R on the pair of particles, where R has the eigenstates (the subscripts A and C are suppressed):

$$\begin{aligned}
|\mathrm{r}_1\rangle &= \frac{1}{\sqrt{2}}|\uparrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle + \frac{1}{2}(|\uparrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle \mathrm{e}^{\mathrm{i}\pi/4} + |\downarrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle \mathrm{e}^{-\mathrm{i}\pi/4}) \\
|\mathrm{r}_2\rangle &= \frac{1}{\sqrt{2}}|\uparrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle - \frac{1}{2}(|\uparrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle \mathrm{e}^{\mathrm{i}\pi/4} + |\downarrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle \mathrm{e}^{-\mathrm{i}\pi/4}) \\
|\mathrm{r}_3\rangle &= \frac{1}{\sqrt{2}}|\downarrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle + \frac{1}{2}(|\uparrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle \mathrm{e}^{-\mathrm{i}\pi/4} + |\downarrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle \mathrm{e}^{\mathrm{i}\pi/4}) \\
|\mathrm{r}_4\rangle &= \frac{1}{\sqrt{2}}|\downarrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle - \frac{1}{2}(|\uparrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle \mathrm{e}^{-\mathrm{i}\pi/4} + |\downarrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle \mathrm{e}^{\mathrm{i}\pi/4})
\end{aligned}$$

Quantum Key Distribution

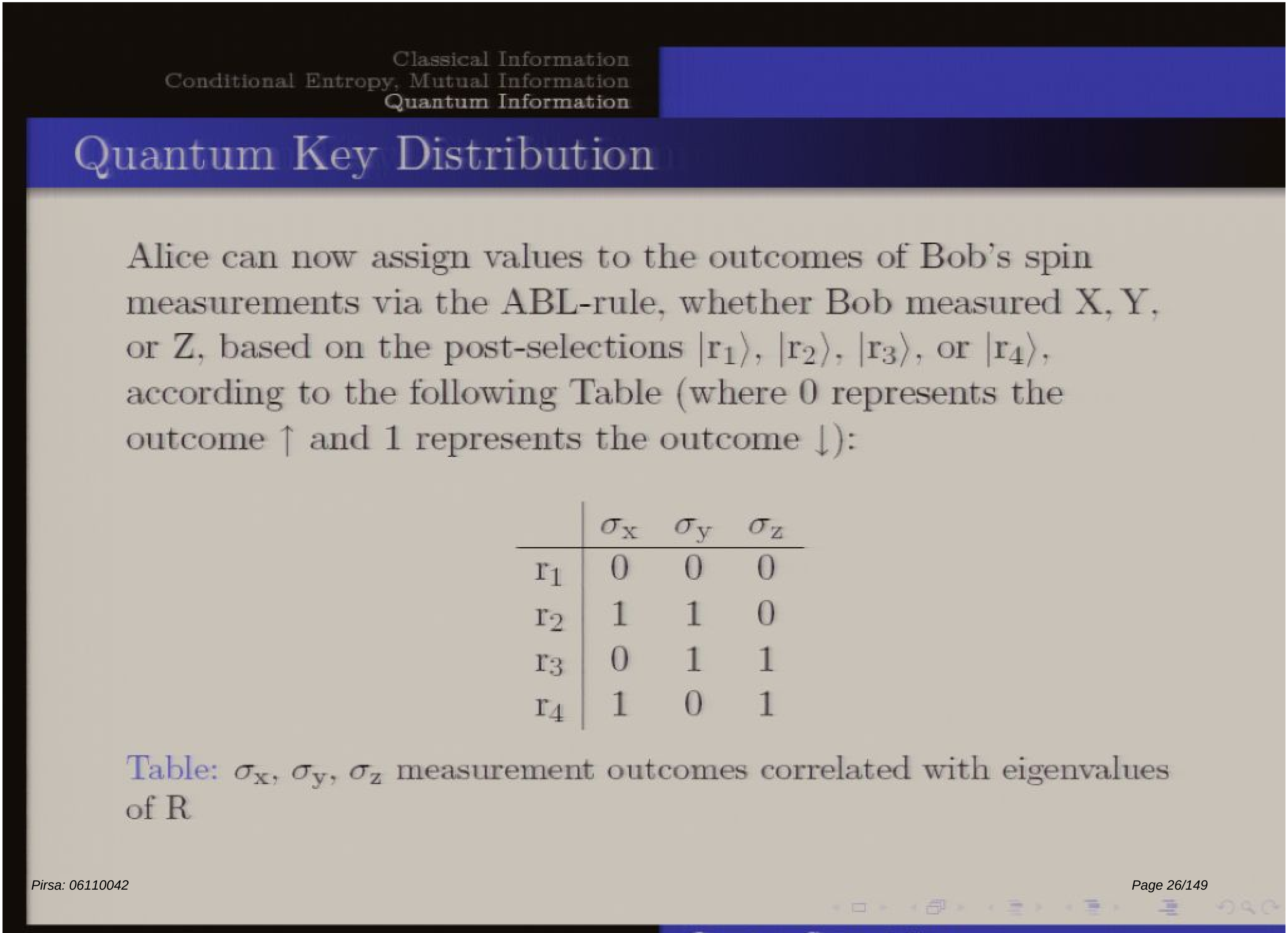
Note that:

$$
\begin{aligned}
|\mathrm{pre}\rangle &= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle + |\downarrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle) && (1)\\
&= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{x}}\rangle|\uparrow_{\mathrm{x}}\rangle + |\downarrow_{\mathrm{x}}\rangle|\downarrow_{\mathrm{x}}\rangle) && (2)\\
&= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{y}}\rangle|\downarrow_{\mathrm{y}}\rangle + |\downarrow_{\mathrm{y}}\rangle|\uparrow_{\mathrm{y}}\rangle) && (3)\\
&= \frac{1}{2}(|\mathrm{r}_1\rangle + |\mathrm{r}_2\rangle + |\mathrm{r}_3\rangle + |\mathrm{r}_4\rangle) && (4)
\end{aligned}
$$

Quantum Key Distribution

Note that:

$$
\begin{aligned}
|\mathrm{pre}\rangle &= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{z}}\rangle|\uparrow_{\mathrm{z}}\rangle + |\downarrow_{\mathrm{z}}\rangle|\downarrow_{\mathrm{z}}\rangle \qquad (1)\\
&= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{x}}\rangle|\uparrow_{\mathrm{x}}\rangle + |\downarrow_{\mathrm{x}}\rangle|\downarrow_{\mathrm{x}}\rangle \qquad (2)\\
&= \frac{1}{\sqrt{2}}(|\uparrow_{\mathrm{y}}\rangle|\downarrow_{\mathrm{y}}\rangle + |\downarrow_{\mathrm{y}}\rangle|\uparrow_{\mathrm{y}}\rangle \qquad (3)\\
&= \frac{1}{2}(|\mathrm{r}_1\rangle + |\mathrm{r}_2\rangle + |\mathrm{r}_3\rangle + |\mathrm{r}_4\rangle) \qquad (4)
\end{aligned}
$$

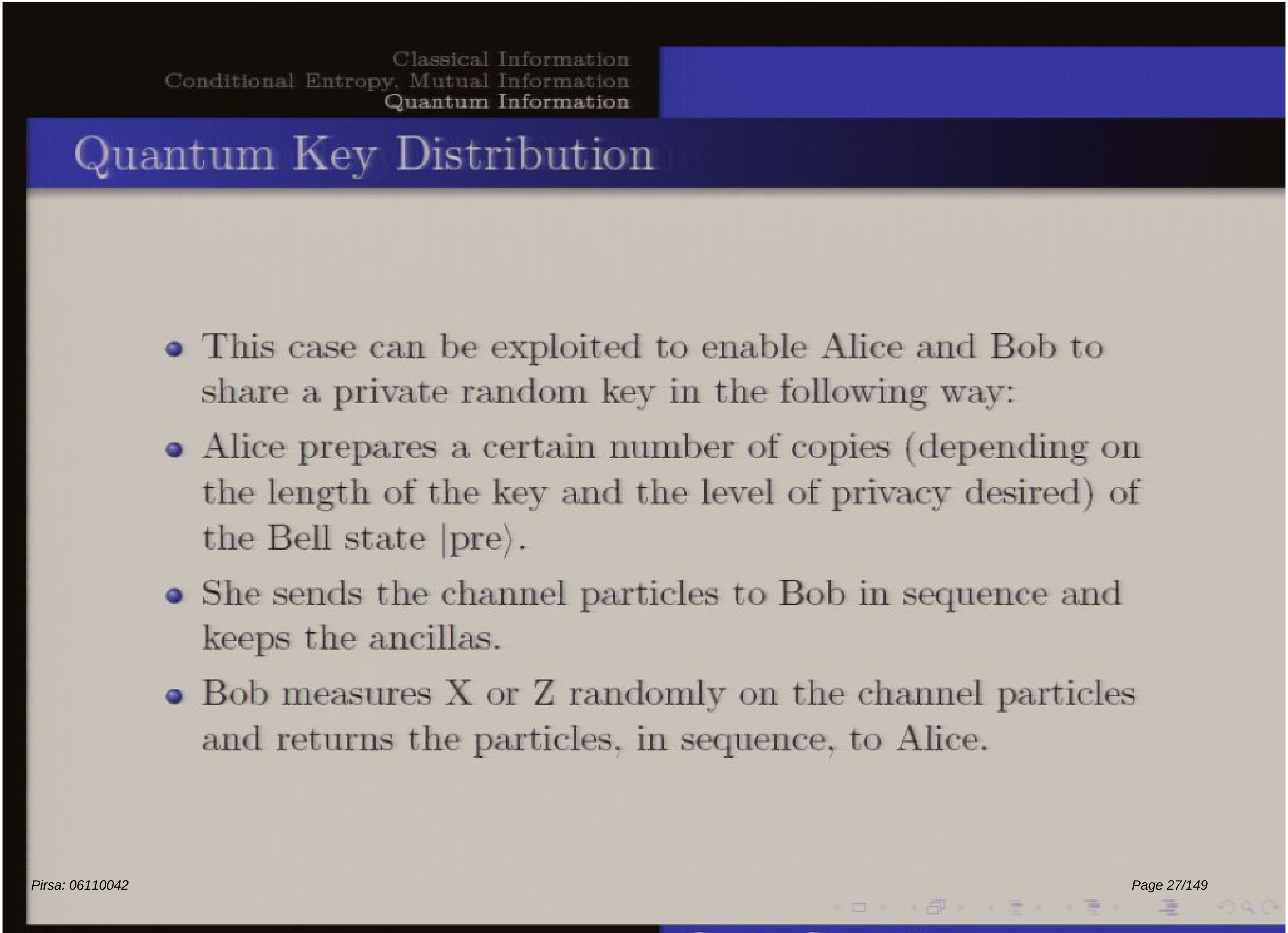


Quantum Key Distribution

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL-rule, whether Bob measured X, Y, or Z, based on the post-selections $|r_1\rangle$, $|r_2\rangle$, $|r_3\rangle$, or $|r_4\rangle$, according to the following Table (where 0 represents the outcome ↑ and 1 represents the outcome ↓):

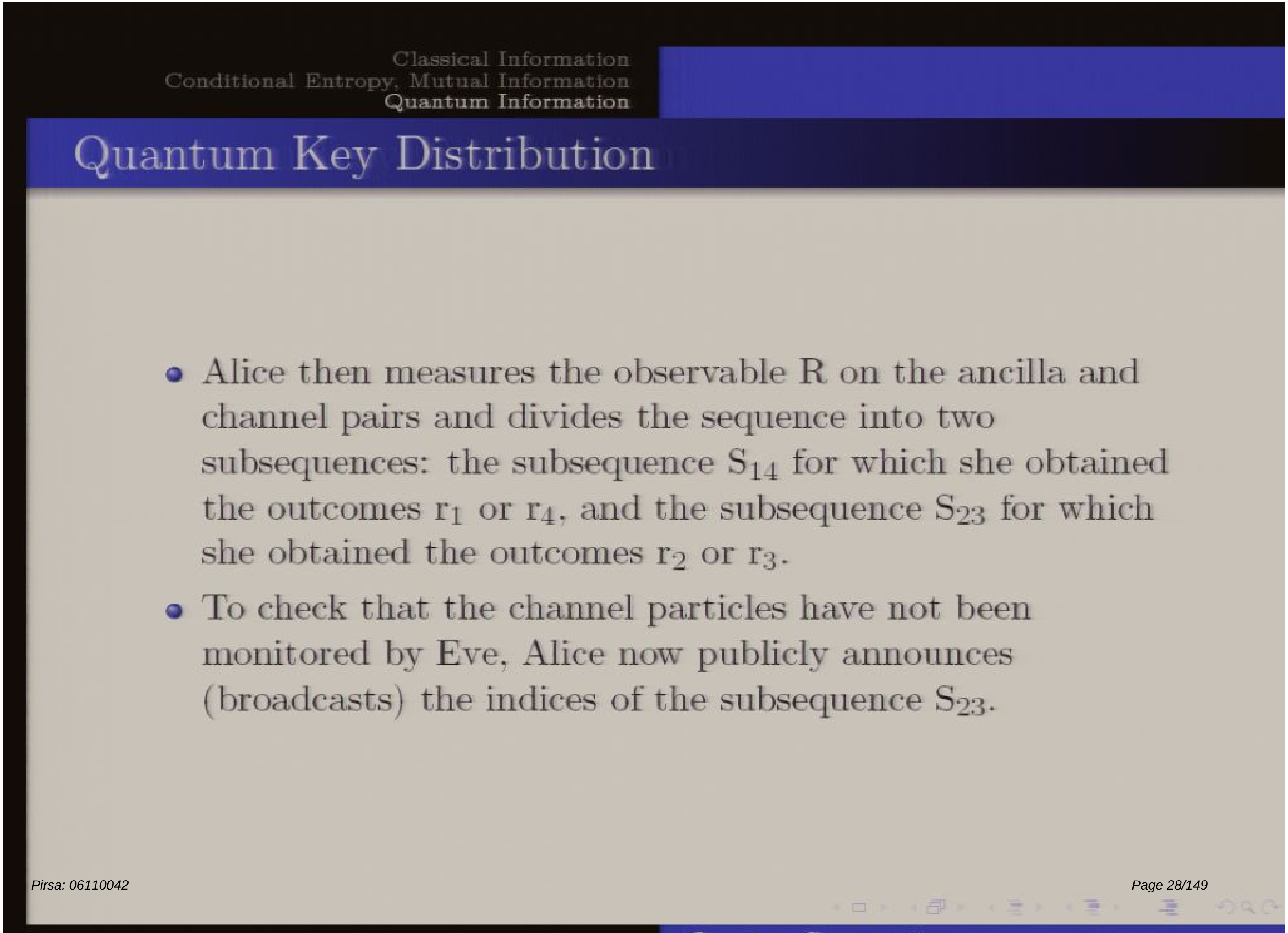
	σ_x	σ_y	σ_z
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

Table: σ_x, σ_y, σ_z measurement outcomes correlated with eigenvalues of R



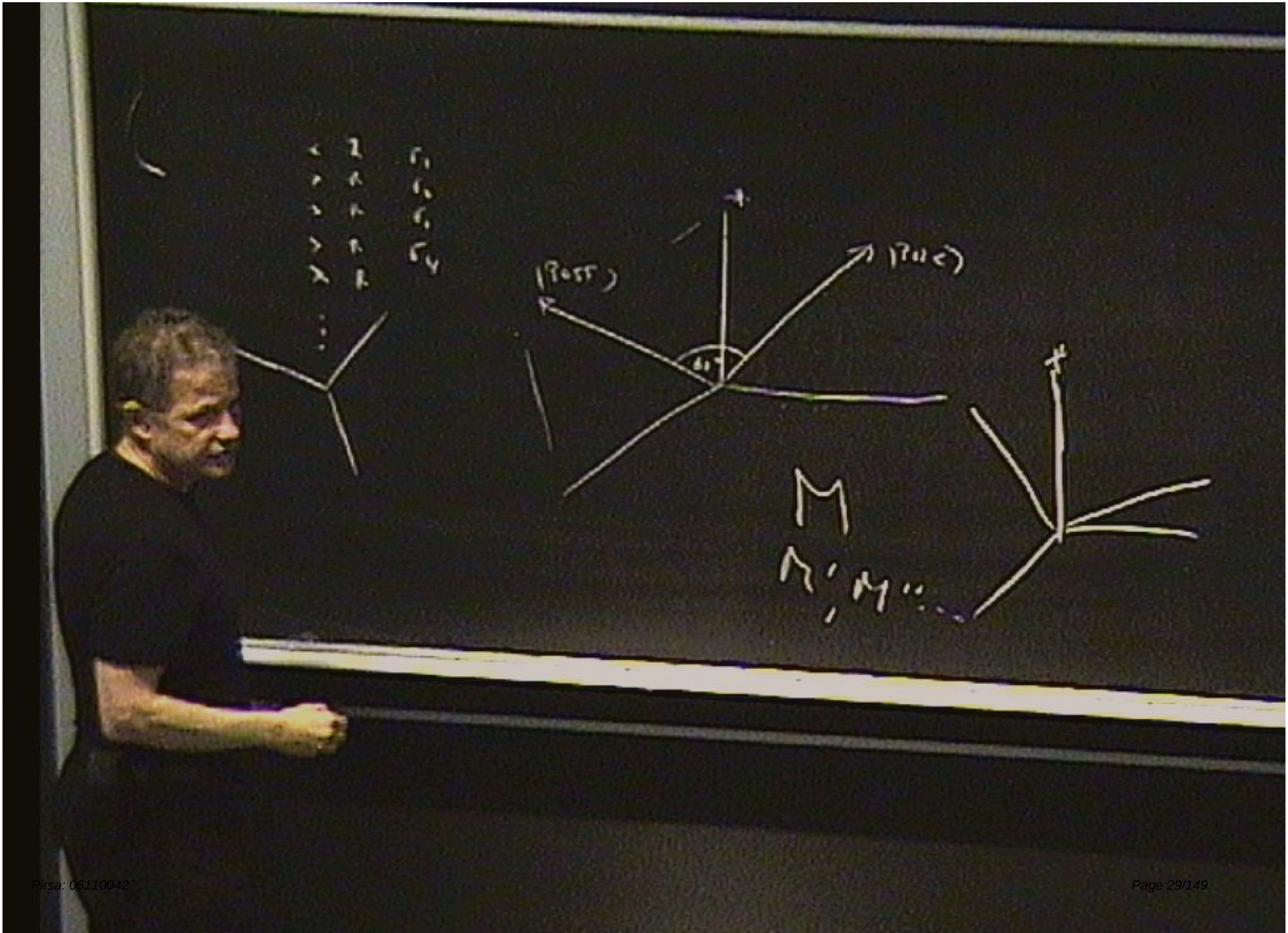
Quantum Key Distribution

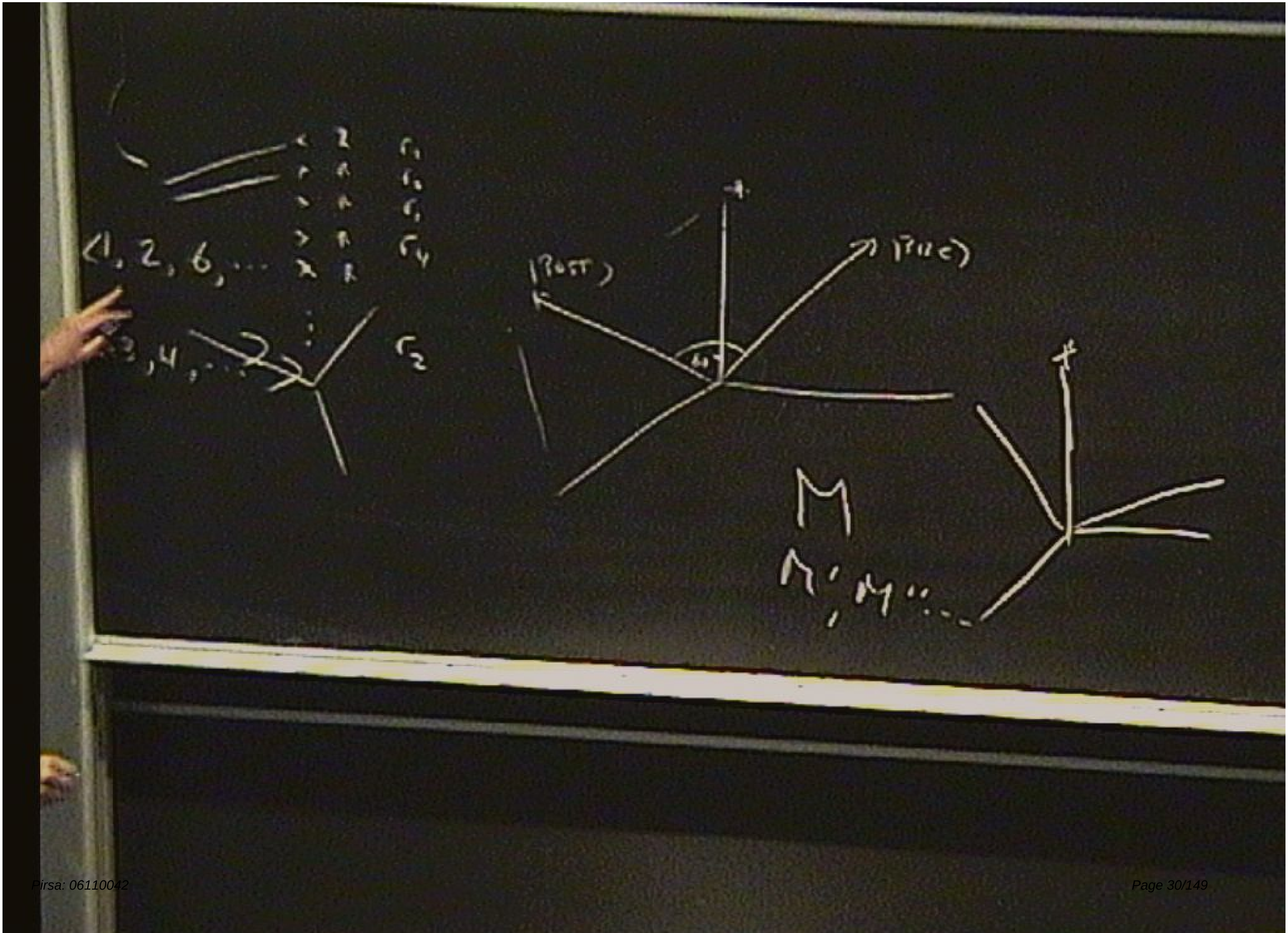
- This case can be exploited to enable Alice and Bob to share a private random key in the following way:
- Alice prepares a certain number of copies (depending on the length of the key and the level of privacy desired) of the Bell state $|\mathrm{pre}\rangle$.
- She sends the channel particles to Bob in sequence and keeps the ancillas.
- Bob measures X or Z randomly on the channel particles and returns the particles, in sequence, to Alice.



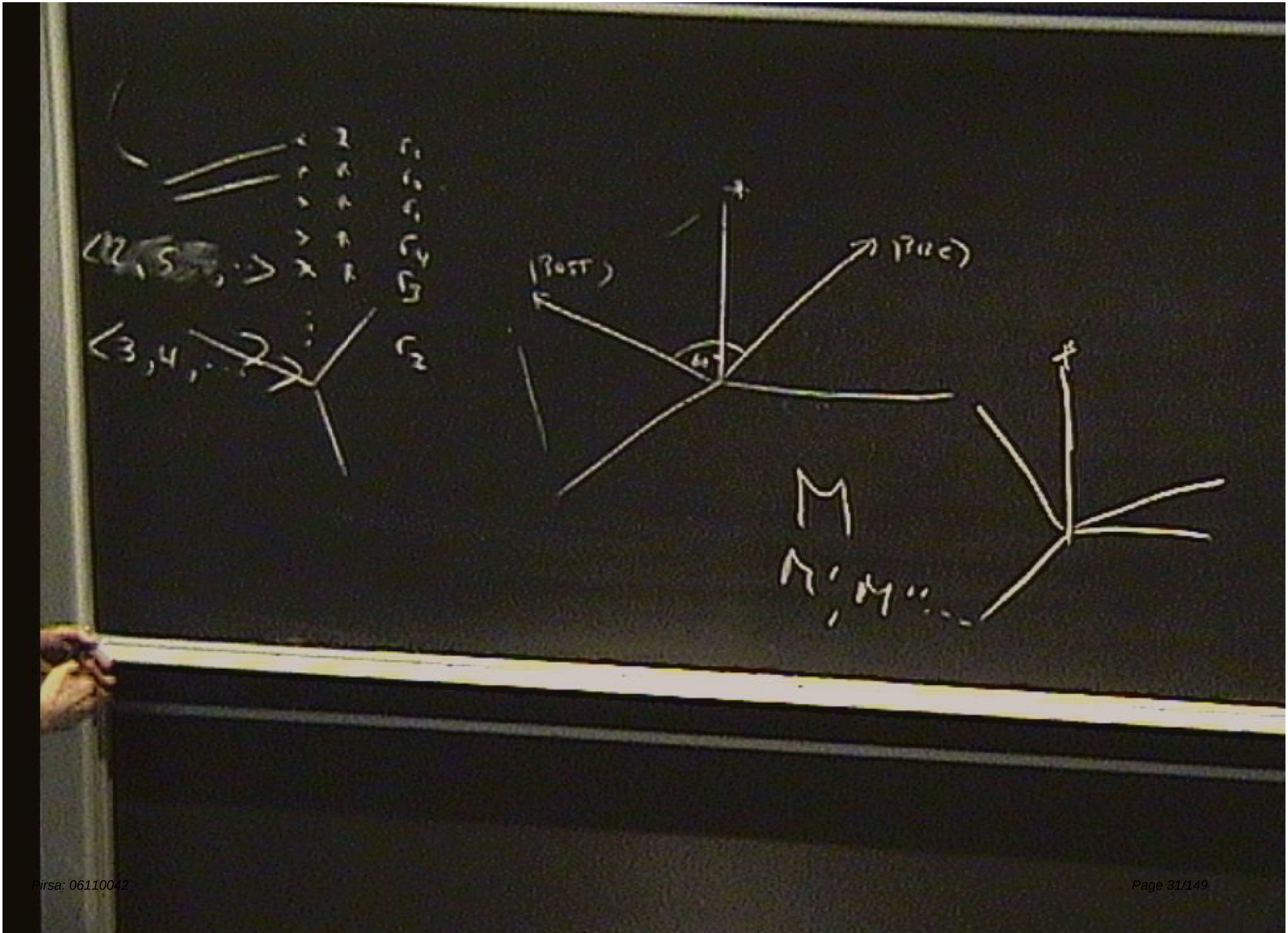
Quantum Key Distribution

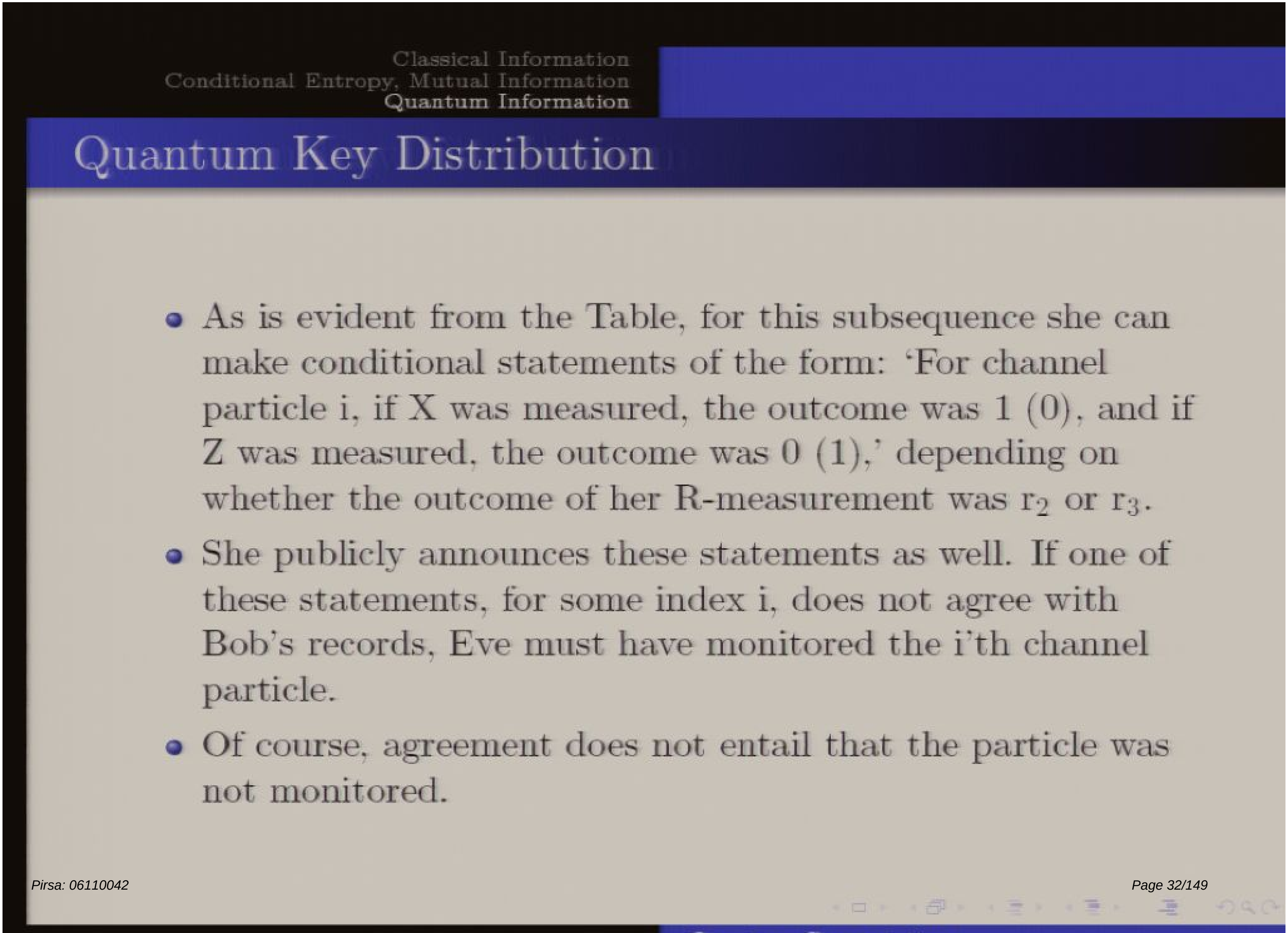
- Alice then measures the observable R on the ancilla and channel pairs and divides the sequence into two subsequences: the subsequence S_{14} for which she obtained the outcomes r_1 or r_4, and the subsequence S_{23} for which she obtained the outcomes r_2 or r_3.
- To check that the channel particles have not been monitored by Eve, Alice now publicly announces (broadcasts) the indices of the subsequence S_{23}.


M



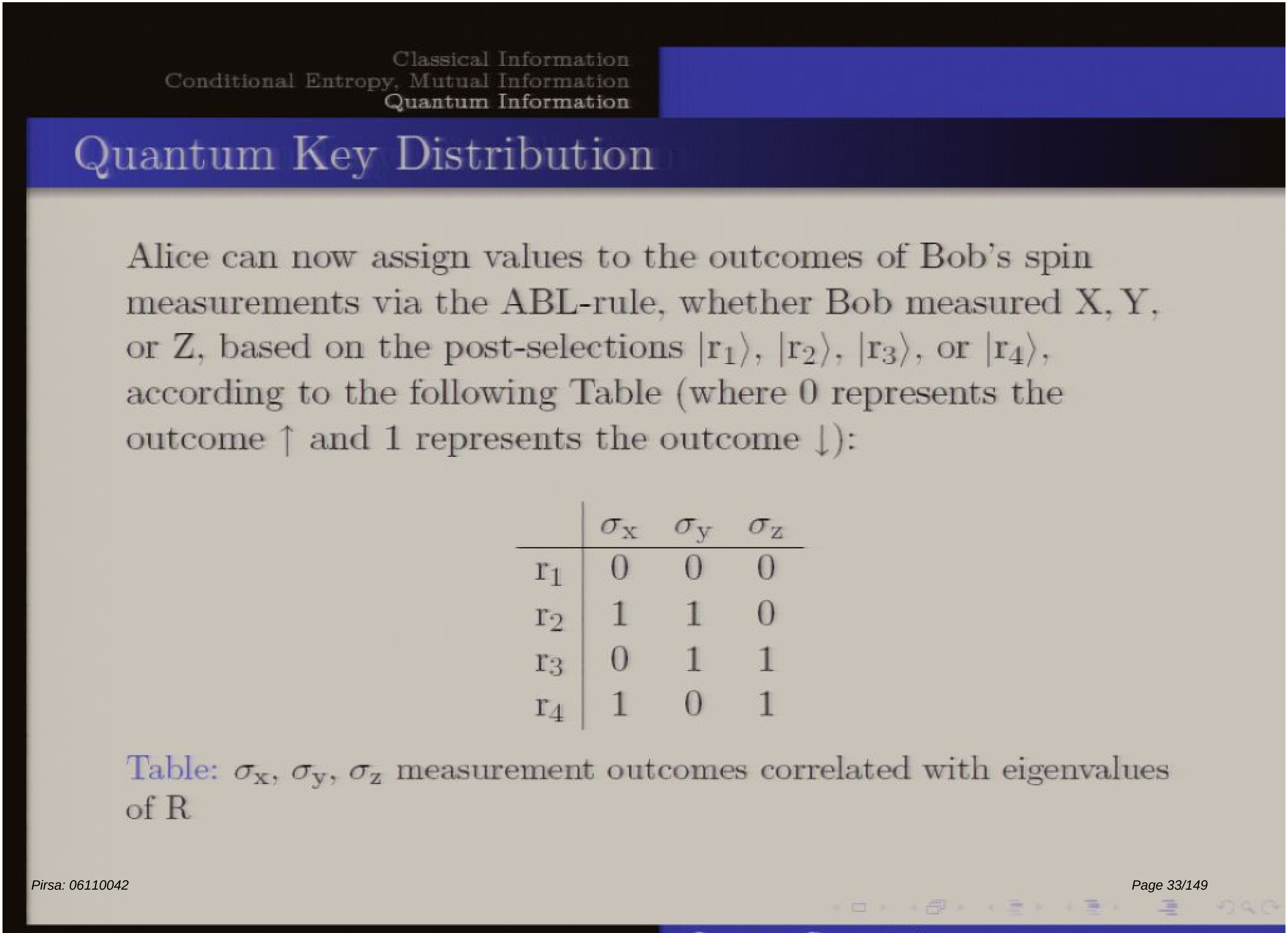
<1, 2, 6, ...
3, 4, ...
r_1
r_0
r_3
r_4
r_2
|POST⟩
|RICE⟩
M
M', M'', ...


<12, 5, ..>
<3, 4, ...>
r1
r2
r3
r4
r5
|Bost>
|Rue>
M
M; M'...



Quantum Key Distribution

- As is evident from the Table, for this subsequence she can make conditional statements of the form: ‘For channel particle i, if X was measured, the outcome was 1 (0), and if Z was measured, the outcome was 0 (1),’ depending on whether the outcome of her R-measurement was r_2 or r_3.
- She publicly announces these statements as well. If one of these statements, for some index i, does not agree with Bob’s records, Eve must have monitored the i’th channel particle.
- Of course, agreement does not entail that the particle was not monitored.



Quantum Key Distribution

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL-rule, whether Bob measured X, Y, or Z, based on the post-selections $|\mathrm{r}_1\rangle$, $|\mathrm{r}_2\rangle$, $|\mathrm{r}_3\rangle$, or $|\mathrm{r}_4\rangle$, according to the following Table (where 0 represents the outcome ↑ and 1 represents the outcome ↓):

	σ_{x}	σ_{y}	σ_{z}
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

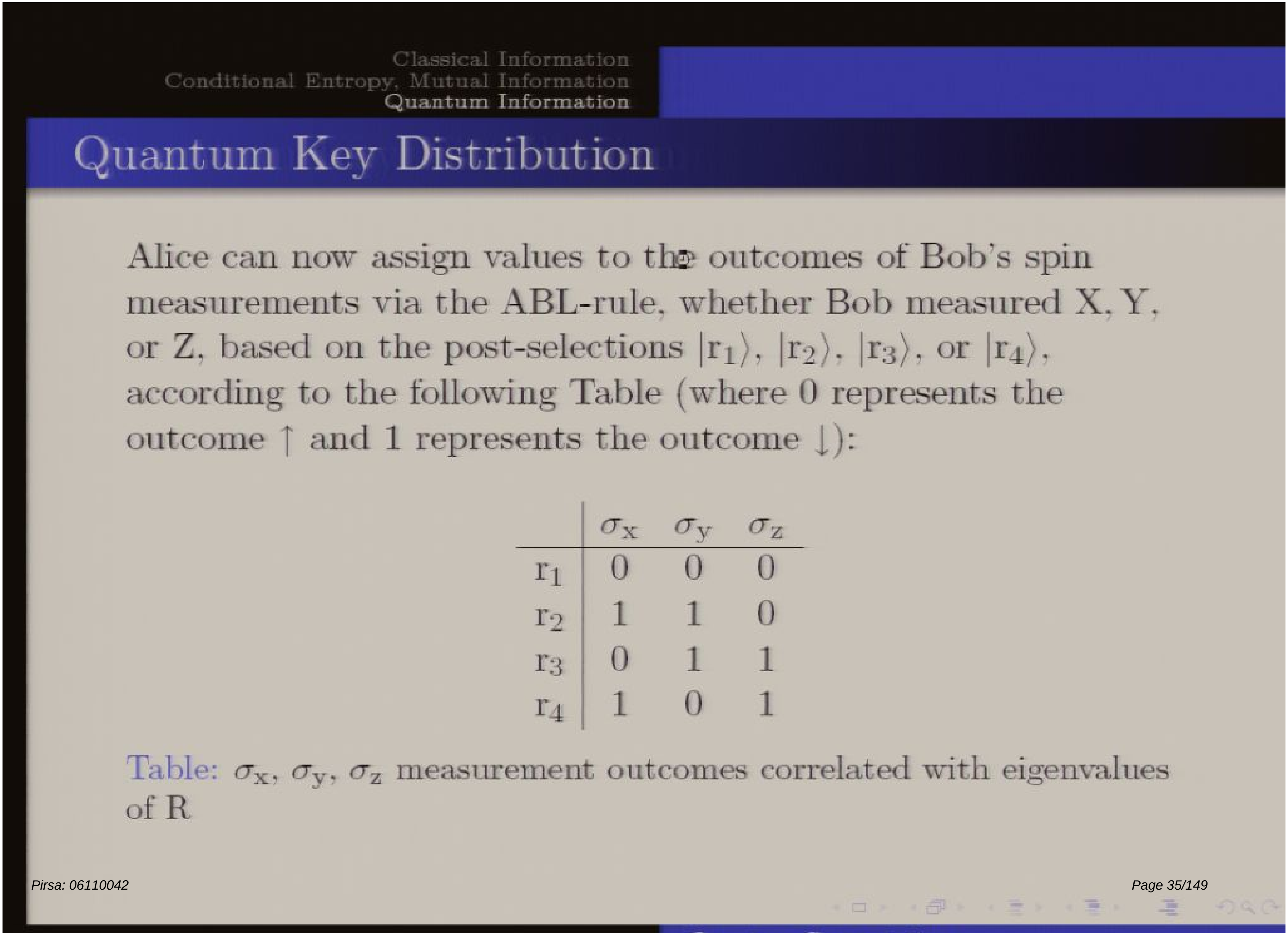
Table: σ_{x}, σ_{y}, σ_{z} measurement outcomes correlated with eigenvalues of R

Quantum Key Distribution

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL-rule, whether Bob measured X, Y, or Z, based on the post-selections $|\mathrm{r}_1\rangle$, $|\mathrm{r}_2\rangle$, $|\mathrm{r}_3\rangle$, or $|\mathrm{r}_4\rangle$, according to the following Table (where 0 represents the outcome ↑ and 1 represents the outcome ↓):

	σ_x	σ_y	σ_z
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

Table: σ_x, σ_y, σ_z measurement outcomes correlated with eigenvalues of R

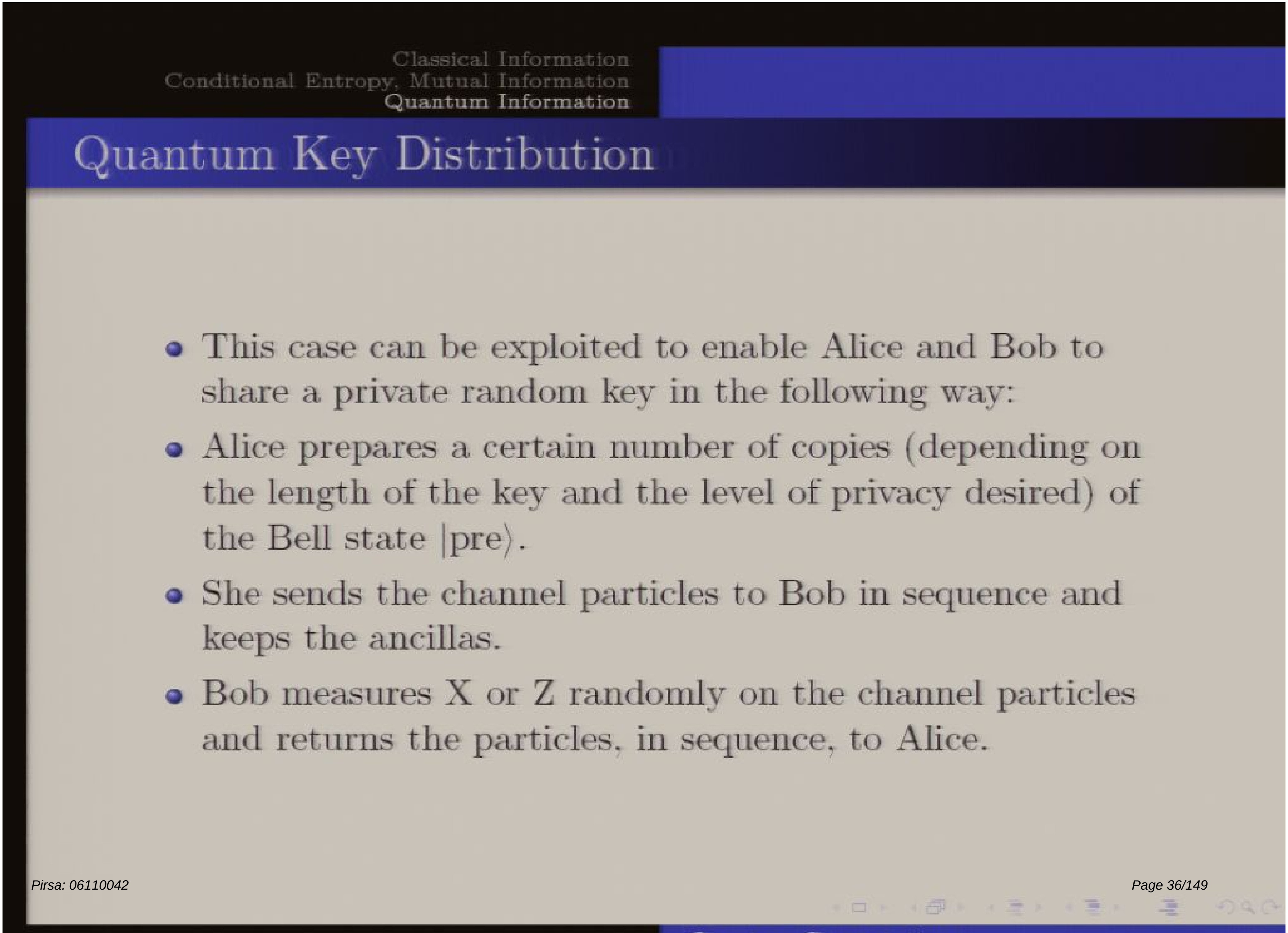


Quantum Key Distribution

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL-rule, whether Bob measured X, Y, or Z, based on the post-selections $|r_1\rangle$, $|r_2\rangle$, $|r_3\rangle$, or $|r_4\rangle$, according to the following Table (where 0 represents the outcome $\uparrow$ and 1 represents the outcome $\downarrow$):

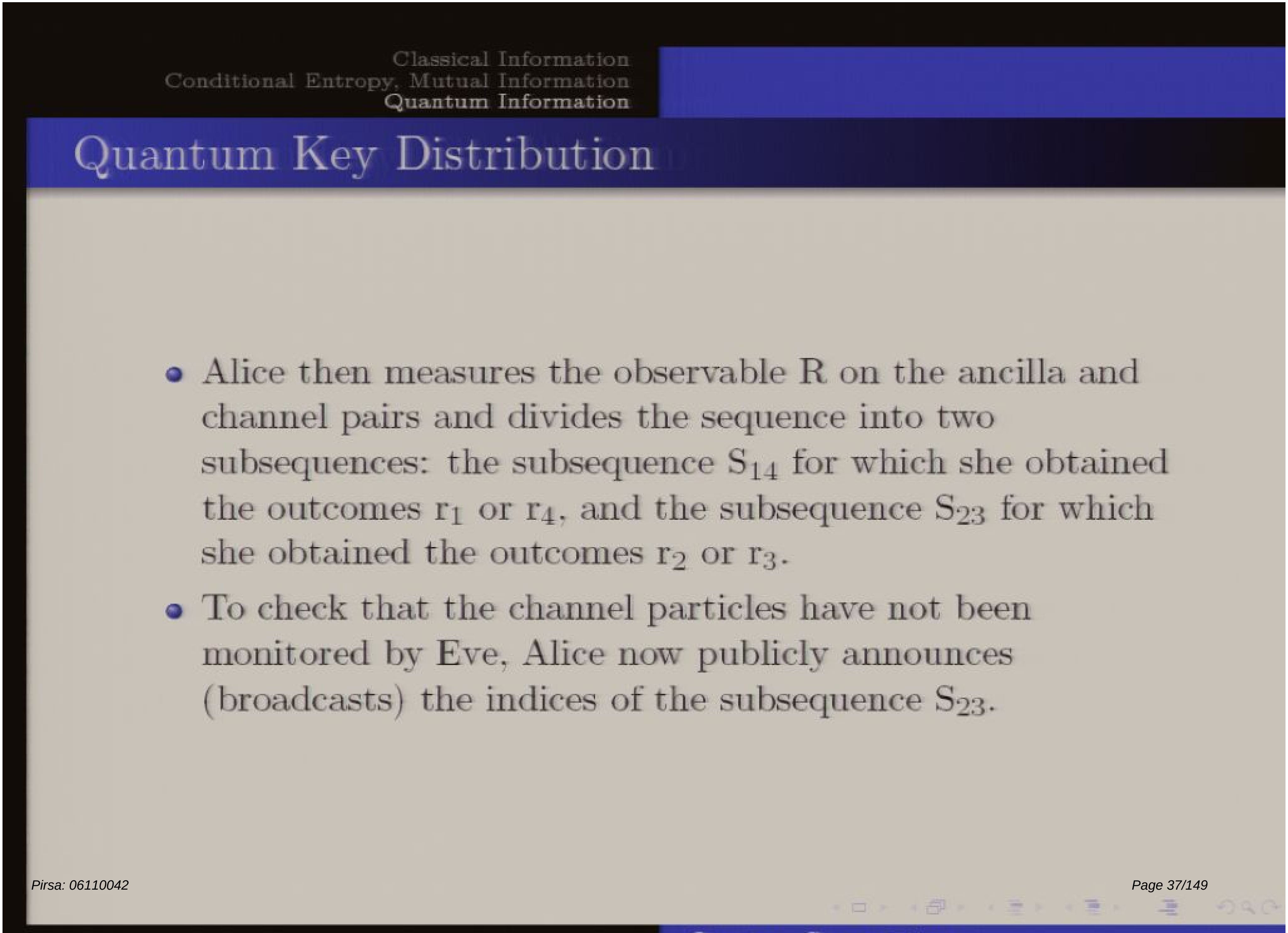
	σ_x	σ_y	σ_z
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

Table: σ_x, σ_y, σ_z measurement outcomes correlated with eigenvalues of R



Quantum Key Distribution

- This case can be exploited to enable Alice and Bob to share a private random key in the following way:
- Alice prepares a certain number of copies (depending on the length of the key and the level of privacy desired) of the Bell state $|\text{pre}\rangle$.
- She sends the channel particles to Bob in sequence and keeps the ancillas.
- Bob measures X or Z randomly on the channel particles and returns the particles, in sequence, to Alice.



Quantum Key Distribution

- Alice then measures the observable R on the ancilla and channel pairs and divides the sequence into two subsequences: the subsequence S_{14} for which she obtained the outcomes r_1 or r_4, and the subsequence S_{23} for which she obtained the outcomes r_2 or r_3.
- To check that the channel particles have not been monitored by Eve, Alice now publicly announces (broadcasts) the indices of the subsequence S_{23}.

Quantum Key Distribution

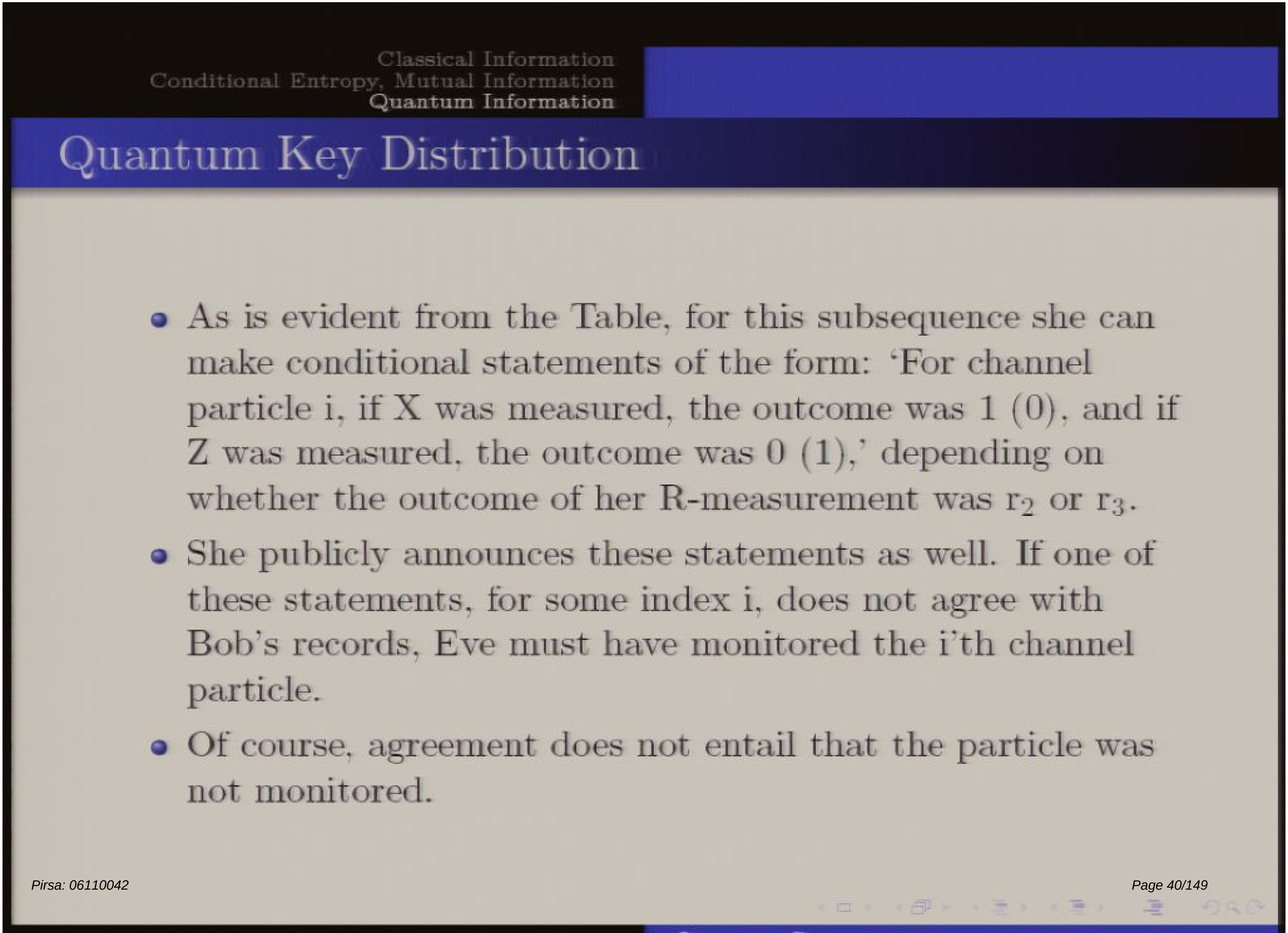
- As is evident from the Table, for this subsequence she can make conditional statements of the form: 'For channel particle i, if X was measured, the outcome was 1 (0), and if Z was measured, the outcome was 0 (1),' depending on whether the outcome of her R-measurement was r_2 or r_3.
- She publicly announces these statements as well. If one of these statements, for some index i, does not agree with Bob's records, Eve must have monitored the i'th channel particle.
- Of course, agreement does not entail that the particle was not monitored.

Quantum Key Distribution

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL-rule, whether Bob measured X, Y, or Z, based on the post-selections $|r_1\rangle$, $|r_2\rangle$, $|r_3\rangle$, or $|r_4\rangle$, according to the following Table (where 0 represents the outcome ↑ and 1 represents the outcome ↓):

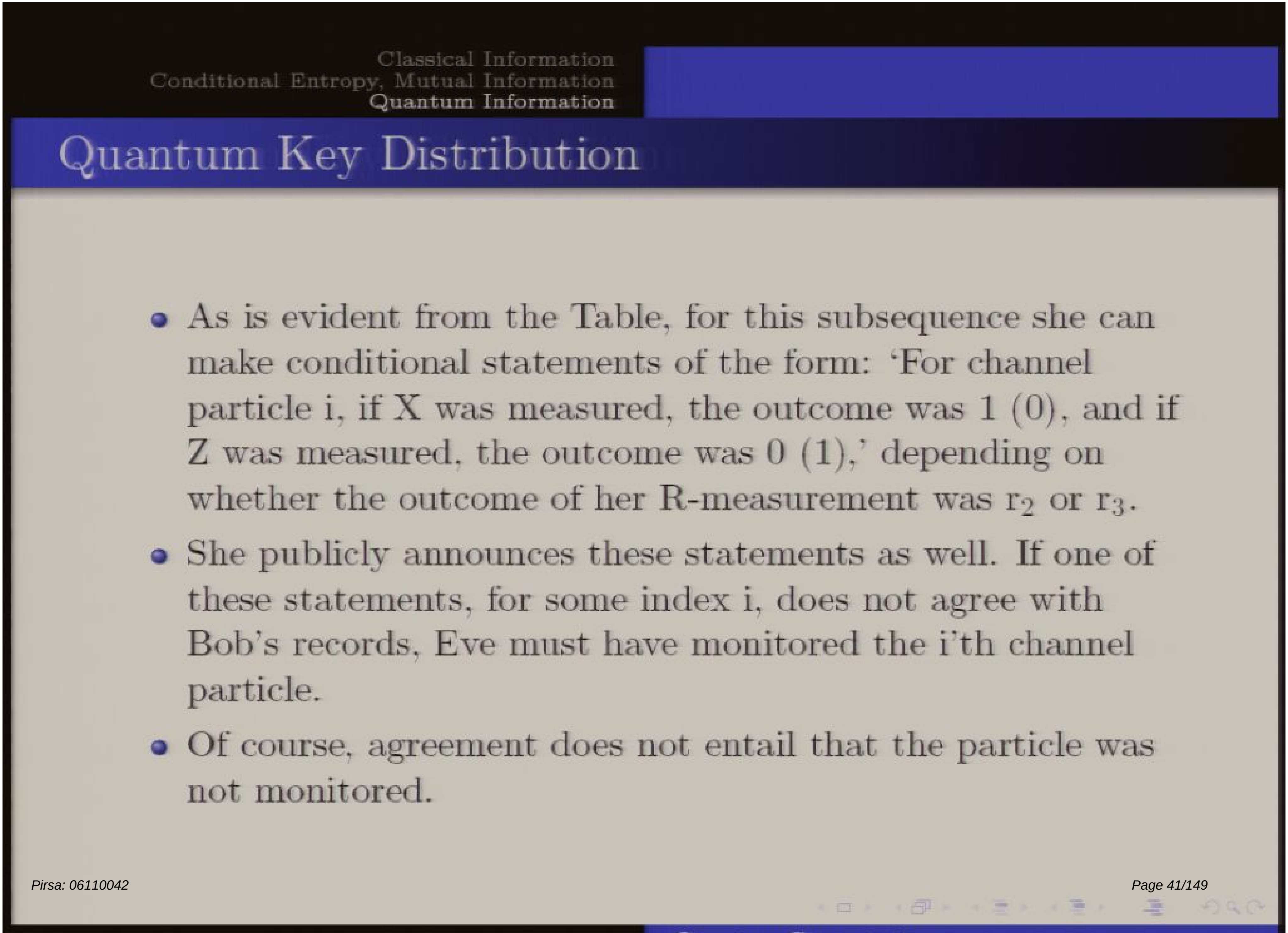
	σ_x	σ_y	σ_z
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

Table: σ_x, σ_y, σ_z measurement outcomes correlated with eigenvalues of R



Quantum Key Distribution

- As is evident from the Table, for this subsequence she can make conditional statements of the form: ‘For channel particle i, if X was measured, the outcome was 1 (0), and if Z was measured, the outcome was 0 (1),’ depending on whether the outcome of her R-measurement was r_2 or r_3.
- She publicly announces these statements as well. If one of these statements, for some index i, does not agree with Bob’s records, Eve must have monitored the i’th channel particle.
- Of course, agreement does not entail that the particle was not monitored.

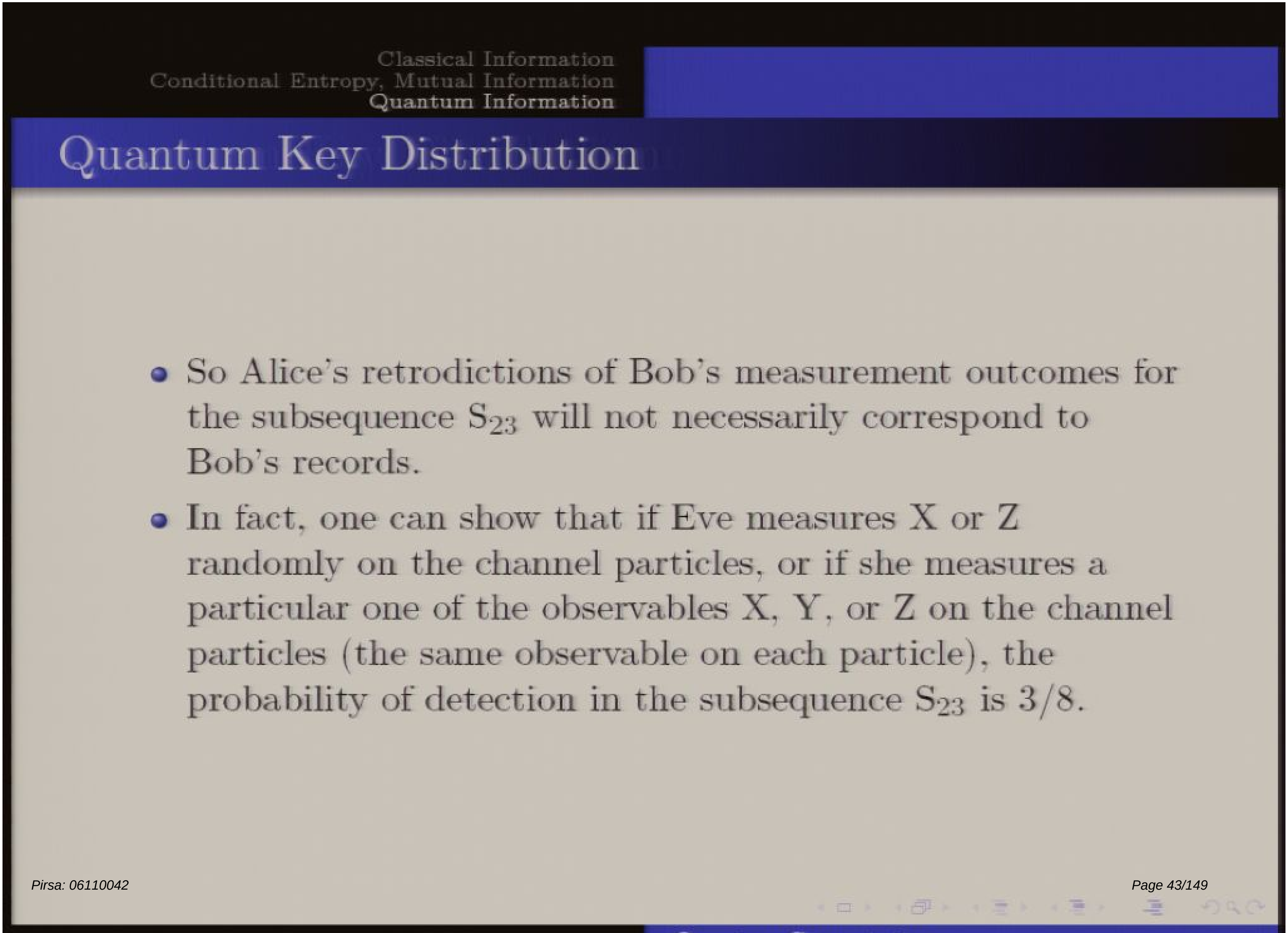


Quantum Key Distribution

- As is evident from the Table, for this subsequence she can make conditional statements of the form: ‘For channel particle i, if X was measured, the outcome was 1 (0), and if Z was measured, the outcome was 0 (1),’ depending on whether the outcome of her R-measurement was r_2 or r_3.
- She publicly announces these statements as well. If one of these statements, for some index i, does not agree with Bob’s records, Eve must have monitored the i’th channel particle.
- Of course, agreement does not entail that the particle was not monitored.

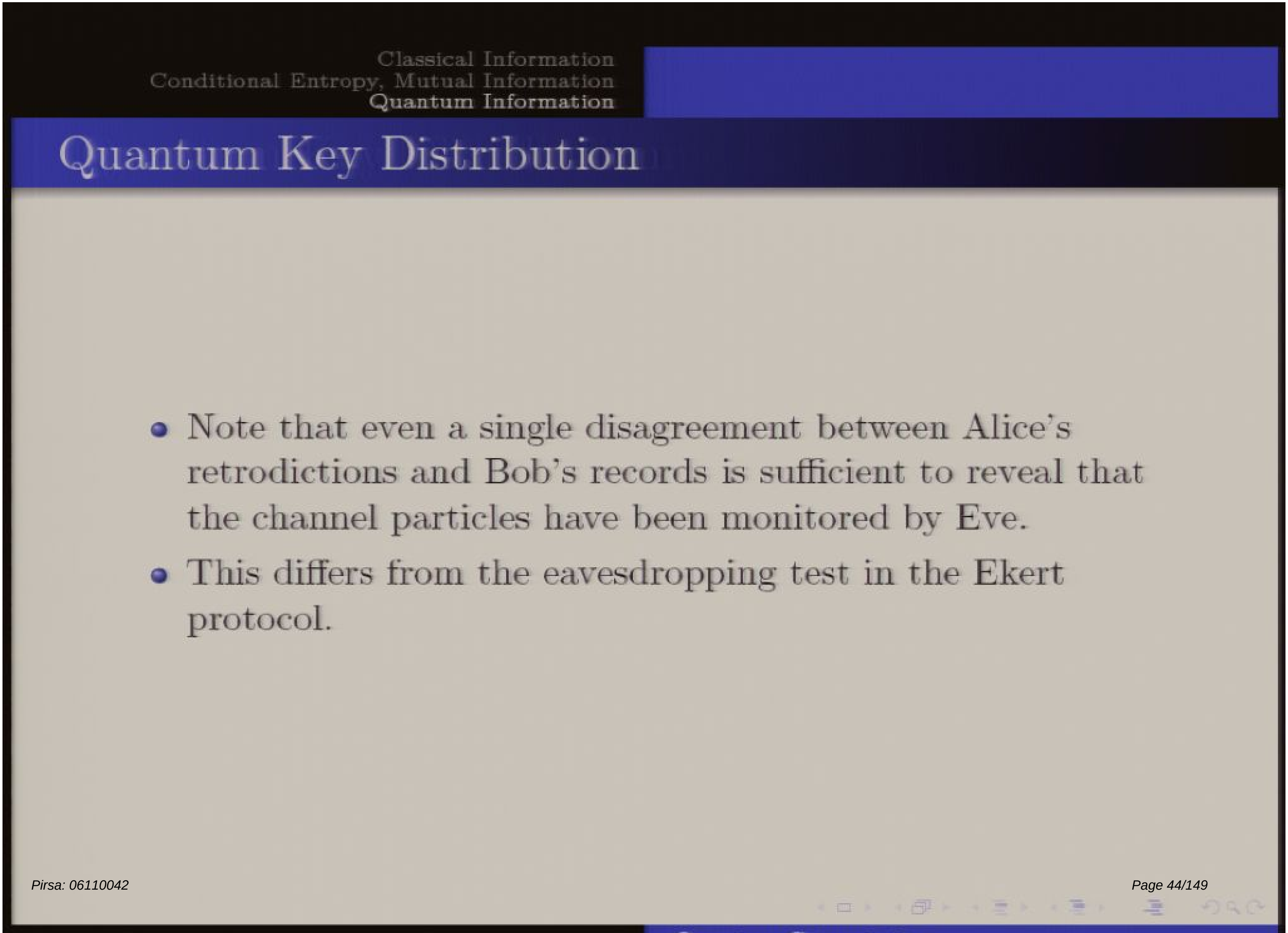
Quantum Key Distribution

- For suppose Eve measures a different spin component observable than Bob on a channel particle and Alice subsequently obtains one of the eigenvalues r_2 or r_3 when she measures R.
- Bob's measurement outcome, either 0 or 1, will be compatible with just one of these eigenvalues, assuming no intervention by Eve.
- But after Eve's measurement, both of these eigenvalues will be possible outcomes of Alice's measurement.



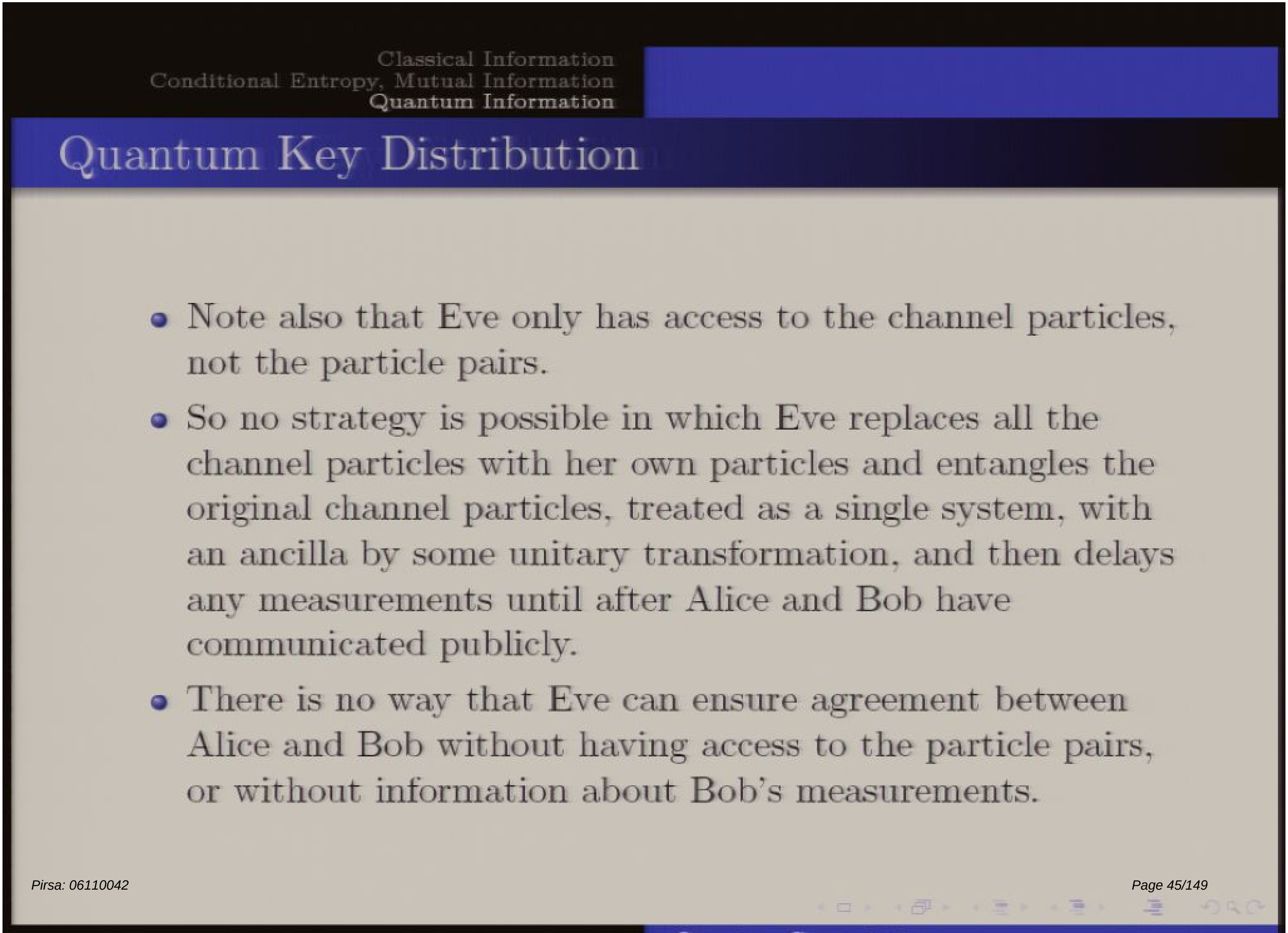
Quantum Key Distribution

- So Alice's retrodictions of Bob's measurement outcomes for the subsequence S_{23} will not necessarily correspond to Bob's records.
- In fact, one can show that if Eve measures X or Z randomly on the channel particles, or if she measures a particular one of the observables X, Y, or Z on the channel particles (the same observable on each particle), the probability of detection in the subsequence S_{23} is $3/8$.



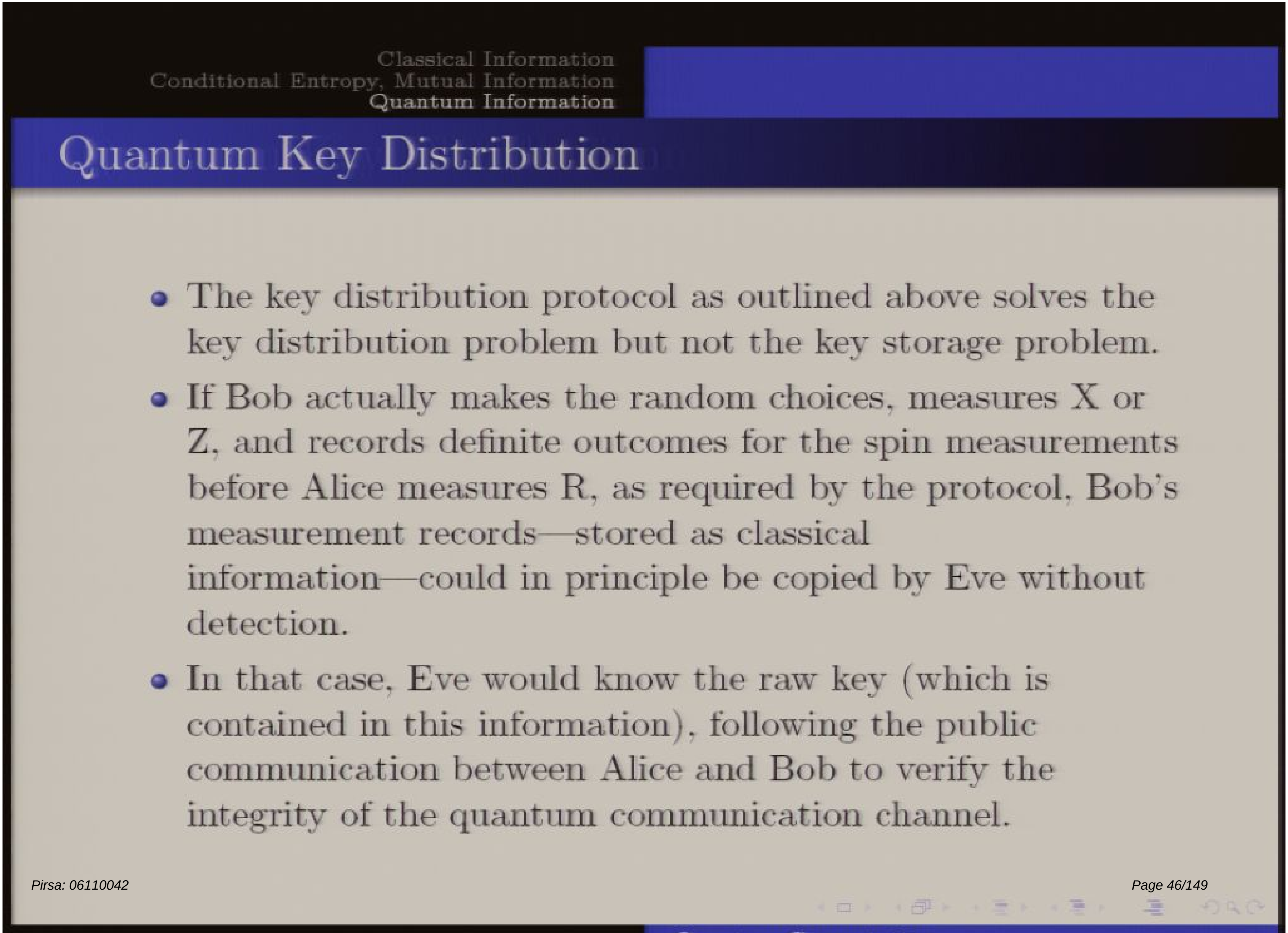
Quantum Key Distribution

- Note that even a single disagreement between Alice's retrodictions and Bob's records is sufficient to reveal that the channel particles have been monitored by Eve.
- This differs from the eavesdropping test in the Ekert protocol.



Quantum Key Distribution

- Note also that Eve only has access to the channel particles, not the particle pairs.
- So no strategy is possible in which Eve replaces all the channel particles with her own particles and entangles the original channel particles, treated as a single system, with an ancilla by some unitary transformation, and then delays any measurements until after Alice and Bob have communicated publicly.
- There is no way that Eve can ensure agreement between Alice and Bob without having access to the particle pairs, or without information about Bob's measurements.

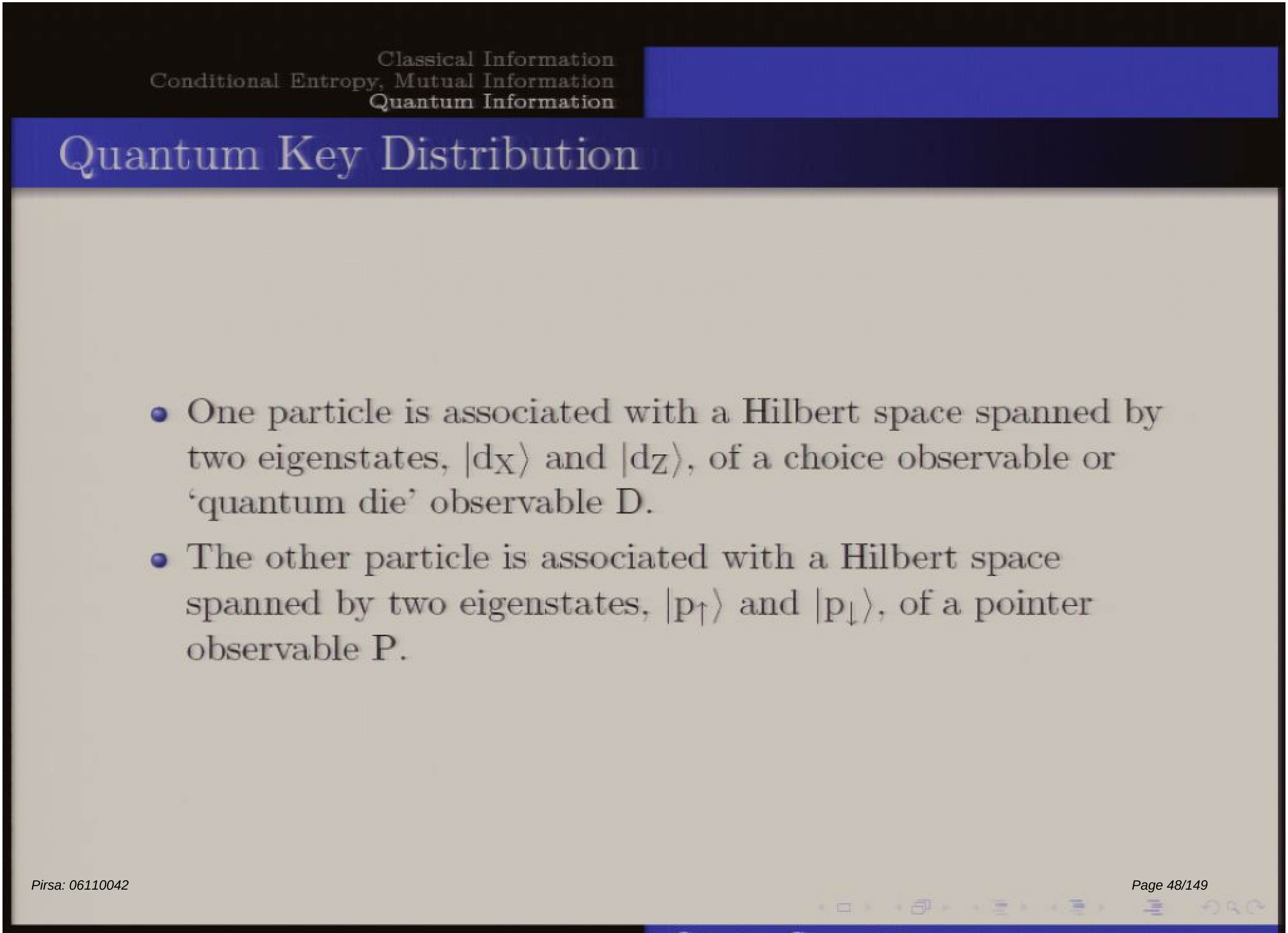


Quantum Key Distribution

- The key distribution protocol as outlined above solves the key distribution problem but not the key storage problem.
- If Bob actually makes the random choices, measures X or Z, and records definite outcomes for the spin measurements before Alice measures R, as required by the protocol, Bob's measurement records—stored as classical information—could in principle be copied by Eve without detection.
- In that case, Eve would know the raw key (which is contained in this information), following the public communication between Alice and Bob to verify the integrity of the quantum communication channel.

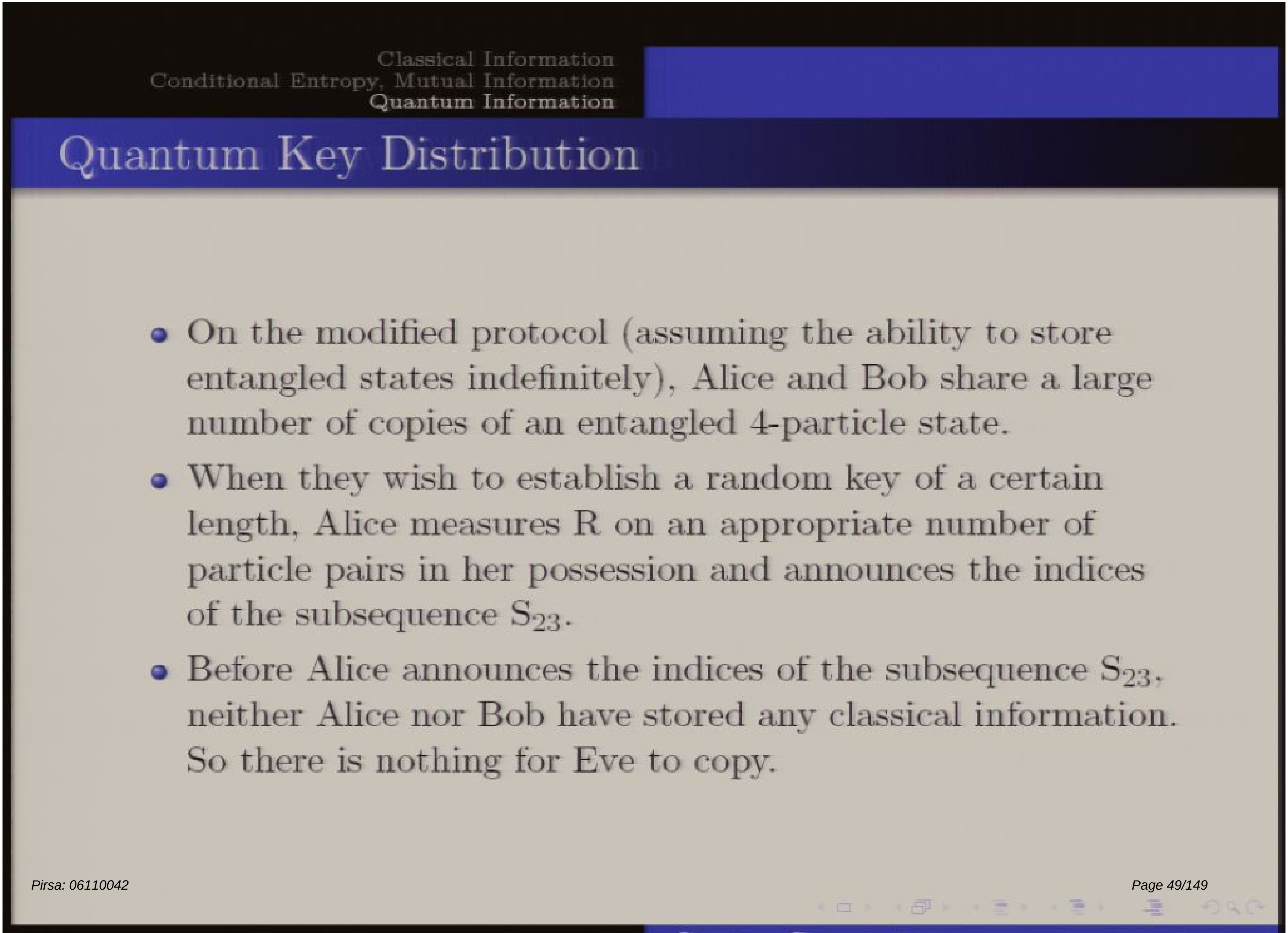
Quantum Key Distribution

- To solve the key storage problem, the protocol is modified in the following way: Instead of actually making the random choice for each channel particle, measuring one of the spin observables, and recording the outcome of the measurement, Bob keeps the random choices and the spin measurements ‘at the quantum level’ until after Alice announces the indices of the subsequence S_{23} of her R measurements.
- To do this, Bob enlarges the Hilbert space by entangling the quantum state of the channel particle via a unitary transformation with the states of two ancilla particles that he introduces.



Quantum Key Distribution

- One particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Z}\rangle$, of a choice observable or ‘quantum die’ observable D.
- The other particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{p}_\uparrow\rangle$ and $|\mathrm{p}_\downarrow\rangle$, of a pointer observable P.

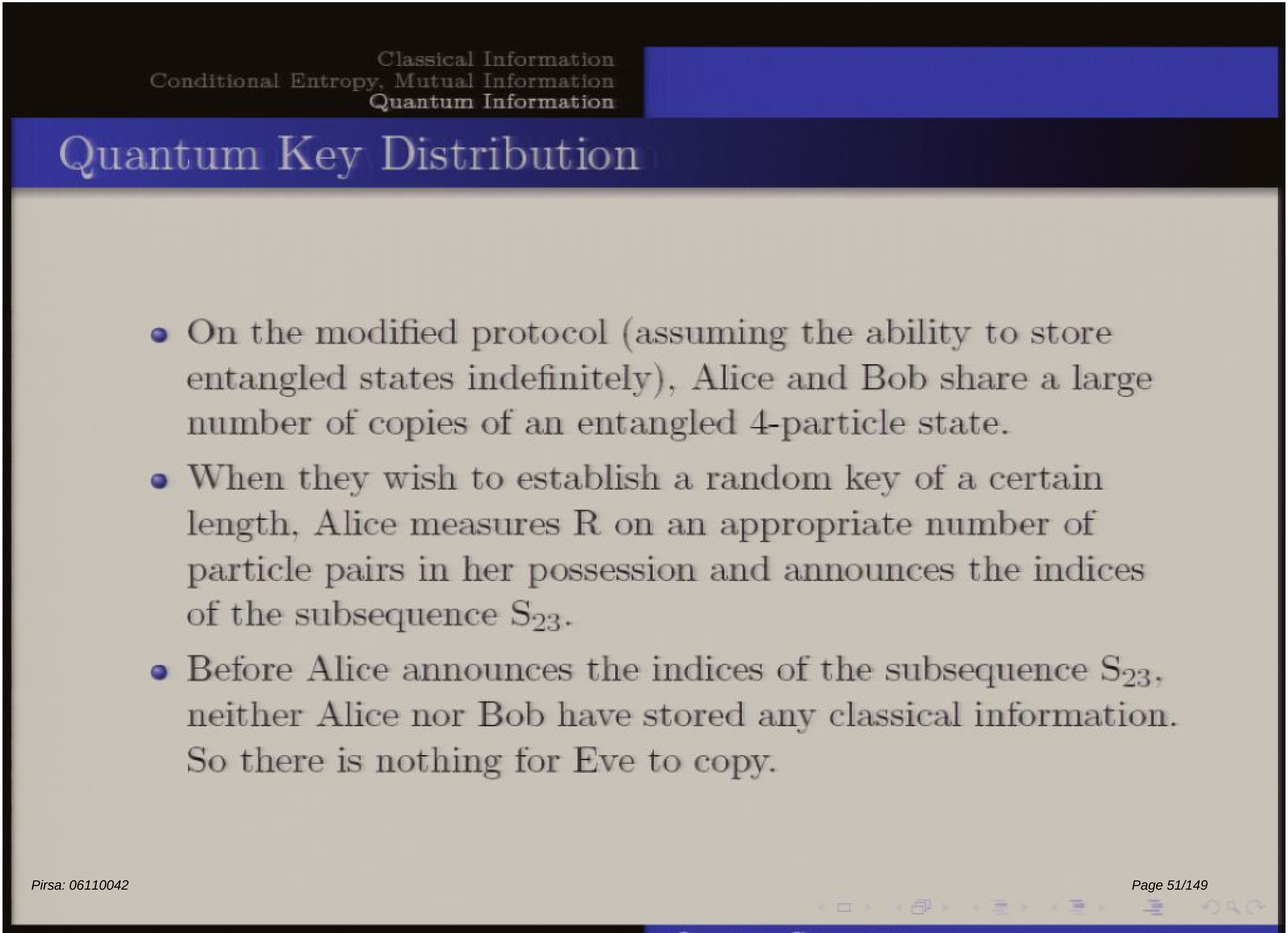


Quantum Key Distribution

- On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled 4-particle state.
- When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}.
- Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy.

Quantum Key Distribution

- After Alice announces the indices of the subsequence S_{23}, Bob measures the observables D and P on his ancillas with these indices and announces the eigenvalue $|p_{\uparrow}\rangle$ or $|p_{\downarrow}\rangle$ as the outcome of his X or Z measurement, depending on the eigenvalue of D.
- If Alice and Bob decide that there has been no eavesdropping by Eve, Bob measures C and P on his ancillas in the subsequence S_{14}.



Quantum Key Distribution

- On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled 4-particle state.
- When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}.
- Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy.

Quantum Key Distribution

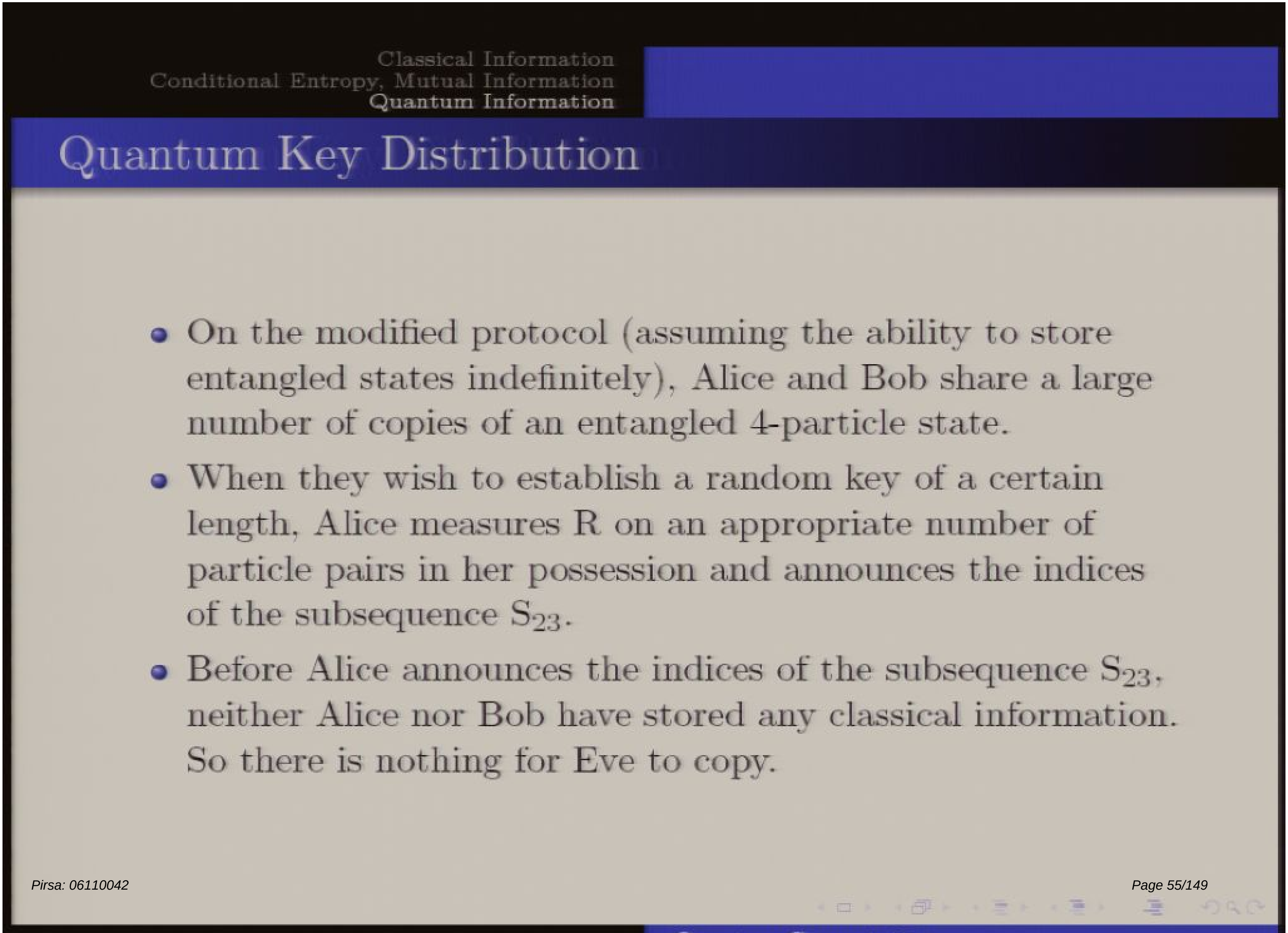
- One particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{d}_X\rangle$ and $|\mathrm{d}_Z\rangle$, of a choice observable or ‘quantum die’ observable D.
- The other particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{p}_\uparrow\rangle$ and $|\mathrm{p}_\downarrow\rangle$, of a pointer observable P.

Quantum Key Distribution

- To solve the key storage problem, the protocol is modified in the following way: Instead of actually making the random choice for each channel particle, measuring one of the spin observables, and recording the outcome of the measurement, Bob keeps the random choices and the spin measurements 'at the quantum level' until after Alice announces the indices of the subsequence S_{23} of her R measurements.
- To do this, Bob enlarges the Hilbert space by entangling the quantum state of the channel particle via a unitary transformation with the states of two ancilla particles that he introduces.

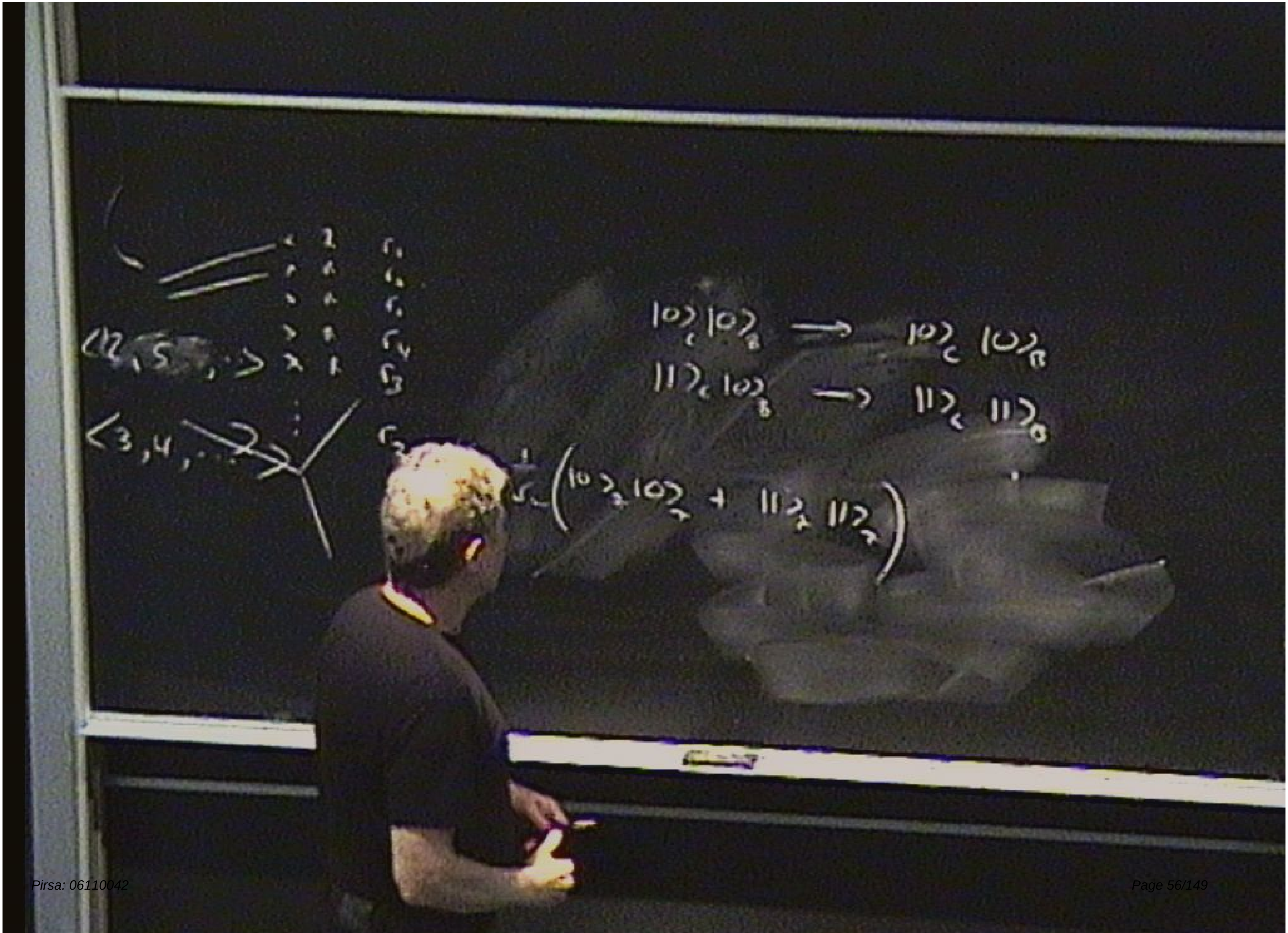
Quantum Key Distribution

- One particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{d}_{\mathrm{X}}\rangle$ and $|\mathrm{d}_{\mathrm{Z}}\rangle$, of a choice observable or 'quantum die' observable D.
- The other particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{p}_{\uparrow}\rangle$ and $|\mathrm{p}_{\downarrow}\rangle$, of a pointer observable P.



Quantum Key Distribution

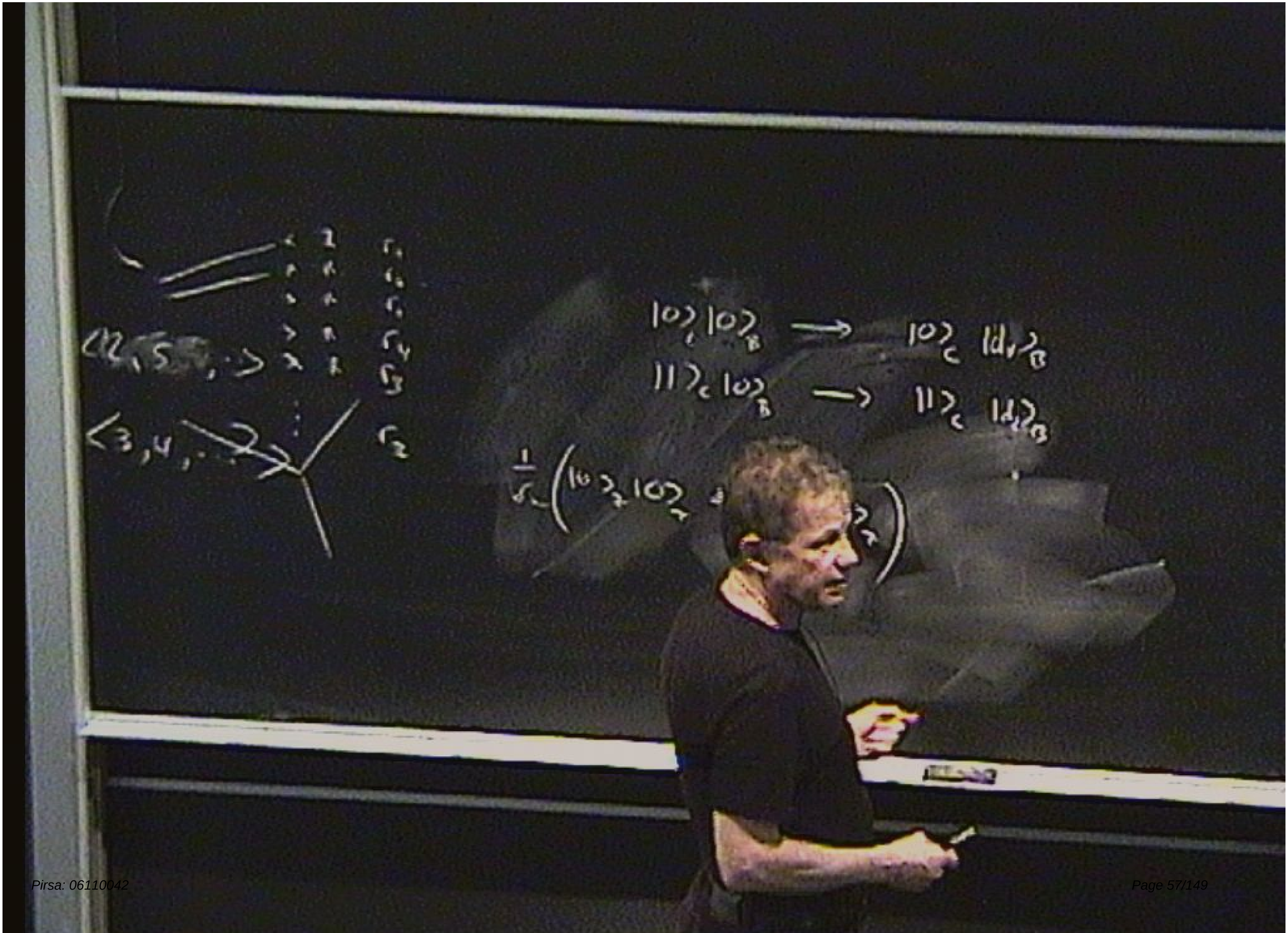
- On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled 4-particle state.
- When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}.
- Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy.



$$|0\rangle_C|0\rangle_B \longrightarrow |0\rangle_C|0\rangle_B$$

$$|1\rangle_C|0\rangle_B \longrightarrow |1\rangle_C|1\rangle_B$$

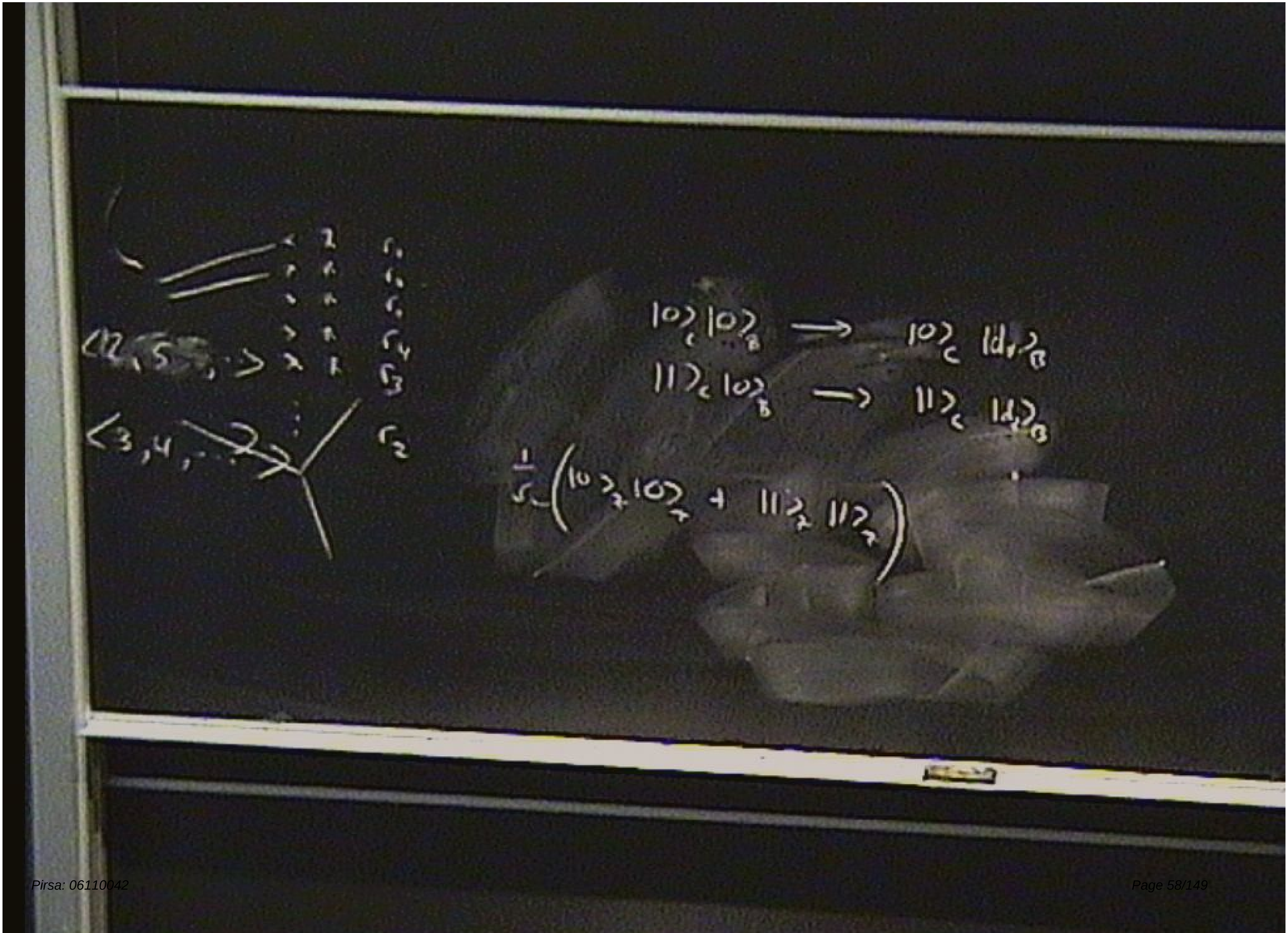
$$\frac{1}{\sqrt{2}}\left(|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B\right)$$


$\langle 2, 5, \ldots \rangle$
$\langle 3, 4, \ldots \rangle$
r_1
r_4
r_3
r_2

$$|0\rangle_C |0\rangle_B \longrightarrow |0\rangle_C |d_1\rangle_B$$

$$|1\rangle_C |0\rangle_B \longrightarrow |1\rangle_C |d_2\rangle_B$$

$$\frac{1}{\sqrt{2}}\Big(|0\rangle_1 |0\rangle_2 \quad \rangle_2\Big)$$



$$|0\rangle_c |0\rangle_B \longrightarrow |0\rangle_c \, |d_1\rangle_B$$

$$|1\rangle_c |0\rangle_B \longrightarrow |1\rangle_c \, |d_2\rangle_B$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle_2 |0\rangle_2 + |1\rangle_2 |1\rangle_2\right)$$

Bit Commitment

The entanglement is implemented by a unitary transformation. Define two unitary transformations, $\mathrm{U_X}$ and $\mathrm{U_Y}$, that implement the X and Y measurements 'at the quantum level' on the tensor product of the Hilbert space of the channel particle, $\mathcal{H}_\mathrm{C}$, and the Hilbert space of Bob's pointer ancilla, $\mathcal{H}_{\mathrm{B_P}}$:

$$|\mathrm{x}_1\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_X}} |\mathrm{x}_1\rangle_\mathrm{C}|\mathrm{p}_1\rangle_\mathrm{B}$$

$$|\mathrm{x}_2\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_X}} |\mathrm{x}_2\rangle_\mathrm{C}|\mathrm{p}_2\rangle_\mathrm{B}$$

and

$$|\mathrm{y}_1\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_Y}} |\mathrm{y}_1\rangle_\mathrm{C}|\mathrm{p}_1\rangle_\mathrm{B}$$

$$|\mathrm{y}_2\rangle_\mathrm{C}||\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_Y}} |\mathrm{y}_2\rangle_\mathrm{C}|\mathrm{p}_2\rangle_\mathrm{B}$$

Bit Commitment

The entanglement is implemented by a unitary transformation. Define two unitary transformations, $\mathrm{U_X}$ and $\mathrm{U_Y}$, that implement the X and Y measurements 'at the quantum level' on the tensor product of the Hilbert space of the channel particle, $\mathcal{H}_\mathrm{C}$, and the Hilbert space of Bob's pointer ancilla, $\mathcal{H}_{\mathrm{B_P}}$:

$$|\mathrm{x}_1\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_X}} |\mathrm{x}_1\rangle_\mathrm{C}|\mathrm{p}_1\rangle_\mathrm{B}$$
$$|\mathrm{x}_2\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_X}} |\mathrm{x}_2\rangle_\mathrm{C}|\mathrm{p}_2\rangle_\mathrm{B}$$

and

$$|\mathrm{y}_1\rangle_\mathrm{C}|\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_Y}} |\mathrm{y}_1\rangle_\mathrm{C}|\mathrm{p}_1\rangle_\mathrm{B}$$
$$|\mathrm{y}_2\rangle_\mathrm{C}||\mathrm{p}_0\rangle_\mathrm{B} \xrightarrow{\mathrm{U_Y}} |\mathrm{y}_2\rangle_\mathrm{C}|\mathrm{p}_2\rangle_\mathrm{B}$$

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.

Bit Commitment

Then (suppressing the obvious subscripts) V is defined by:

$$\begin{aligned} |\mathrm{d_X}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle \\ |\mathrm{d_Y}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \end{aligned} \tag{5}$$

so that

$$\begin{aligned} &|\mathrm{d_0}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle \xrightarrow{\mathrm{V}} \\ &\quad \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \end{aligned} \tag{6}$$

where the tensor product symbol has been introduced selectively to indicate that $\mathrm{U_x}$ and $\mathrm{U_y}$ are defined on $\mathcal{H}_\mathrm{C} \otimes \mathcal{H}_{\mathrm{B_P}}$.

Bit Commitment

- If Bob were to actually choose the observable X or Y randomly, and actually perform the measurement and obtain a particular eigenvalue, Alice's density operator for the channel particle would be:

$$\frac{1}{2}(|\langle \mathrm{x}_1|\psi\rangle|^2\,|\mathrm{x}_1\rangle\langle \mathrm{x}_1| + |\langle \mathrm{x}_2|\psi\rangle|^2\,|\mathrm{x}_2\rangle\langle \mathrm{x}_2|)$$
$$+\frac{1}{2}(|\langle \mathrm{y}_1|\psi\rangle|^2\,|\mathrm{y}_1\rangle\langle \mathrm{y}_1| + |\langle \mathrm{y}_2|\psi\rangle|^2\,|\mathrm{y}_2\rangle\langle \mathrm{y}_2|)$$

  assuming that Alice does not know what observable Bob chose to measure, nor what outcome he obtained.

- But this is precisely the same density operator generated by tracing over Bob's ancilla particles in the state $\frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle$.

Bit Commitment

Then (suppressing the obvious subscripts) V is defined by:

$$\begin{aligned} |\mathrm{d_X}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle \\ |\mathrm{d_Y}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (5) \end{aligned}$$

so that

$$\begin{aligned} &|\mathrm{d_0}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle \xrightarrow{\mathrm{V}} \\ &\qquad \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (6) \end{aligned}$$

where the tensor product symbol has been introduced selectively to indicate that $\mathrm{U_x}$ and $\mathrm{U_y}$ are defined on $\mathcal{H}_\mathrm{C} \otimes \mathcal{H}_{\mathrm{B_P}}$.

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.

Bit Commitment

It follows that:

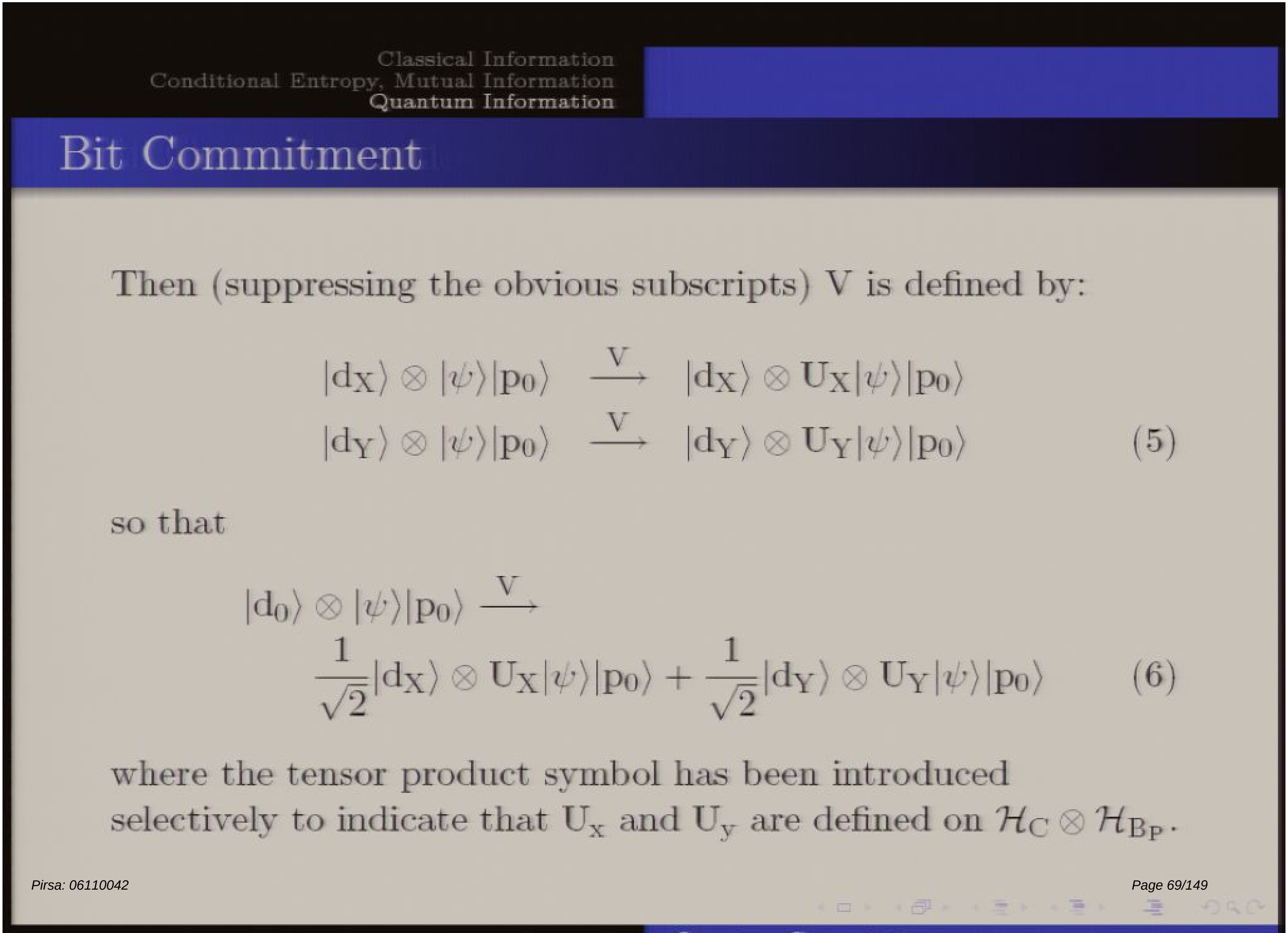
$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_X}} \langle \mathrm{x}_1|\psi\rangle|\mathrm{x}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{x}_2|\psi\rangle|\mathrm{x}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

and

$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_Y}} \langle \mathrm{y}_1|\psi\rangle|\mathrm{y}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{y}_2|\psi\rangle|\mathrm{y}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.



Bit Commitment

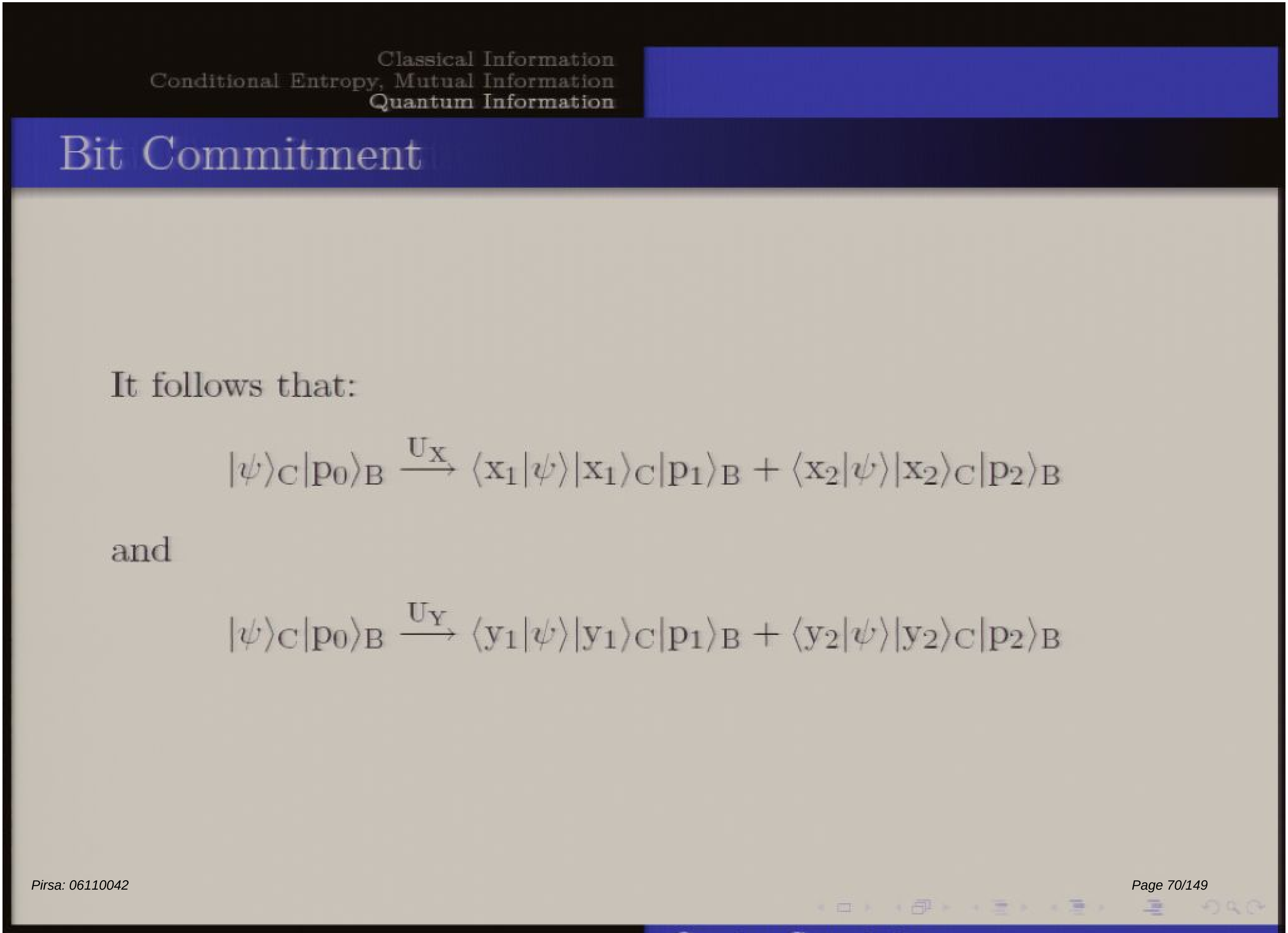
Then (suppressing the obvious subscripts) V is defined by:

$$\begin{aligned} |\mathrm{d_X}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle \\ |\mathrm{d_Y}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (5) \end{aligned}$$

so that

$$|\mathrm{d_0}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle \xrightarrow{\mathrm{V}}$$
$$\frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (6)$$

where the tensor product symbol has been introduced selectively to indicate that $\mathrm{U_x}$ and $\mathrm{U_y}$ are defined on $\mathcal{H}_\mathrm{C} \otimes \mathcal{H}_{\mathrm{B_P}}$.



Bit Commitment

It follows that:

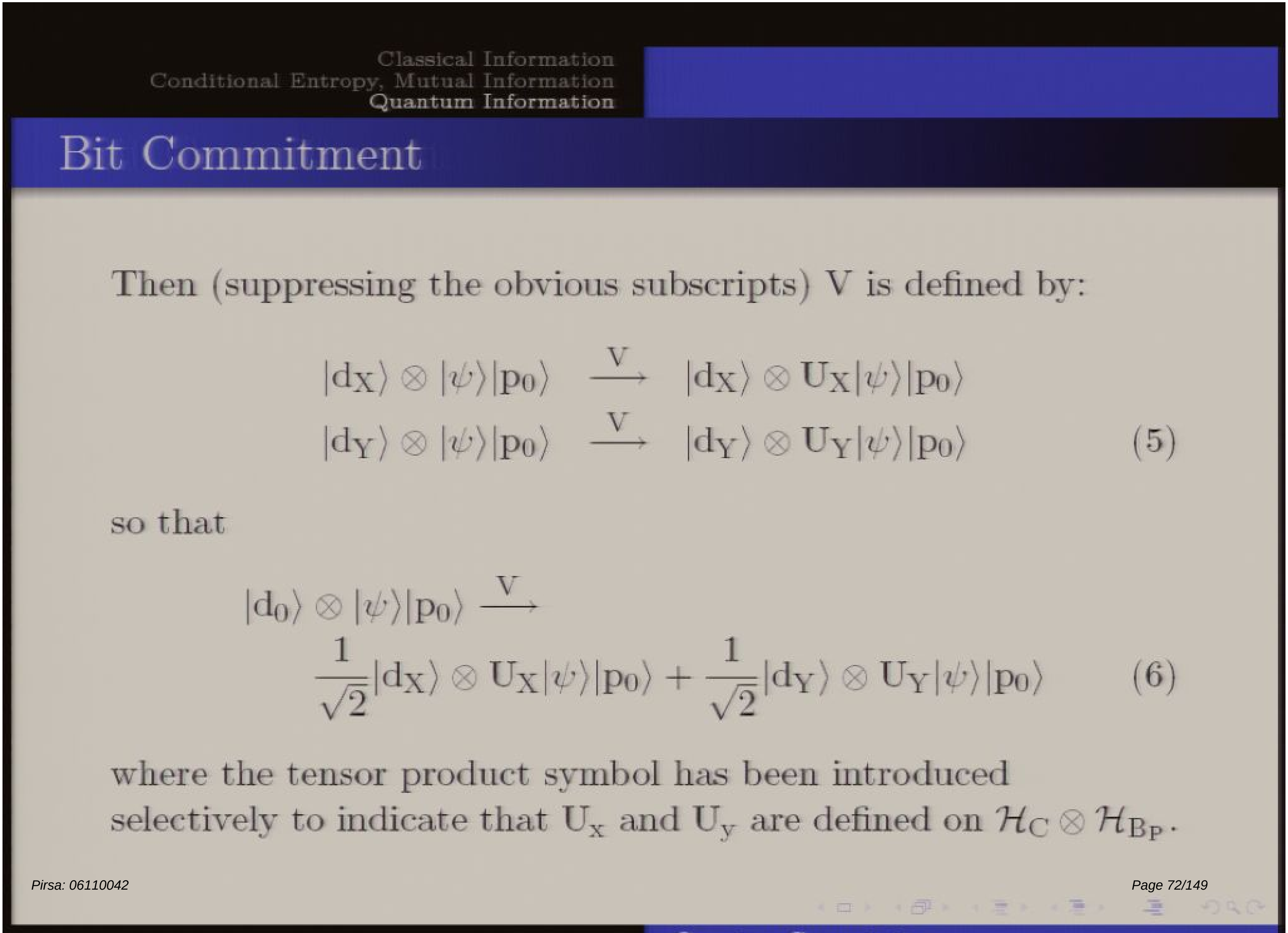
$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_X}} \langle \mathrm{x}_1|\psi\rangle|\mathrm{x}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{x}_2|\psi\rangle|\mathrm{x}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

and

$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_Y}} \langle \mathrm{y}_1|\psi\rangle|\mathrm{y}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{y}_2|\psi\rangle|\mathrm{y}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.



Bit Commitment

Then (suppressing the obvious subscripts) V is defined by:

$$\begin{aligned} |\mathrm{d_X}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle \\ |\mathrm{d_Y}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (5) \end{aligned}$$

so that

$$\begin{aligned} &|\mathrm{d_0}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle \xrightarrow{\mathrm{V}} \\ &\qquad \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \qquad (6) \end{aligned}$$

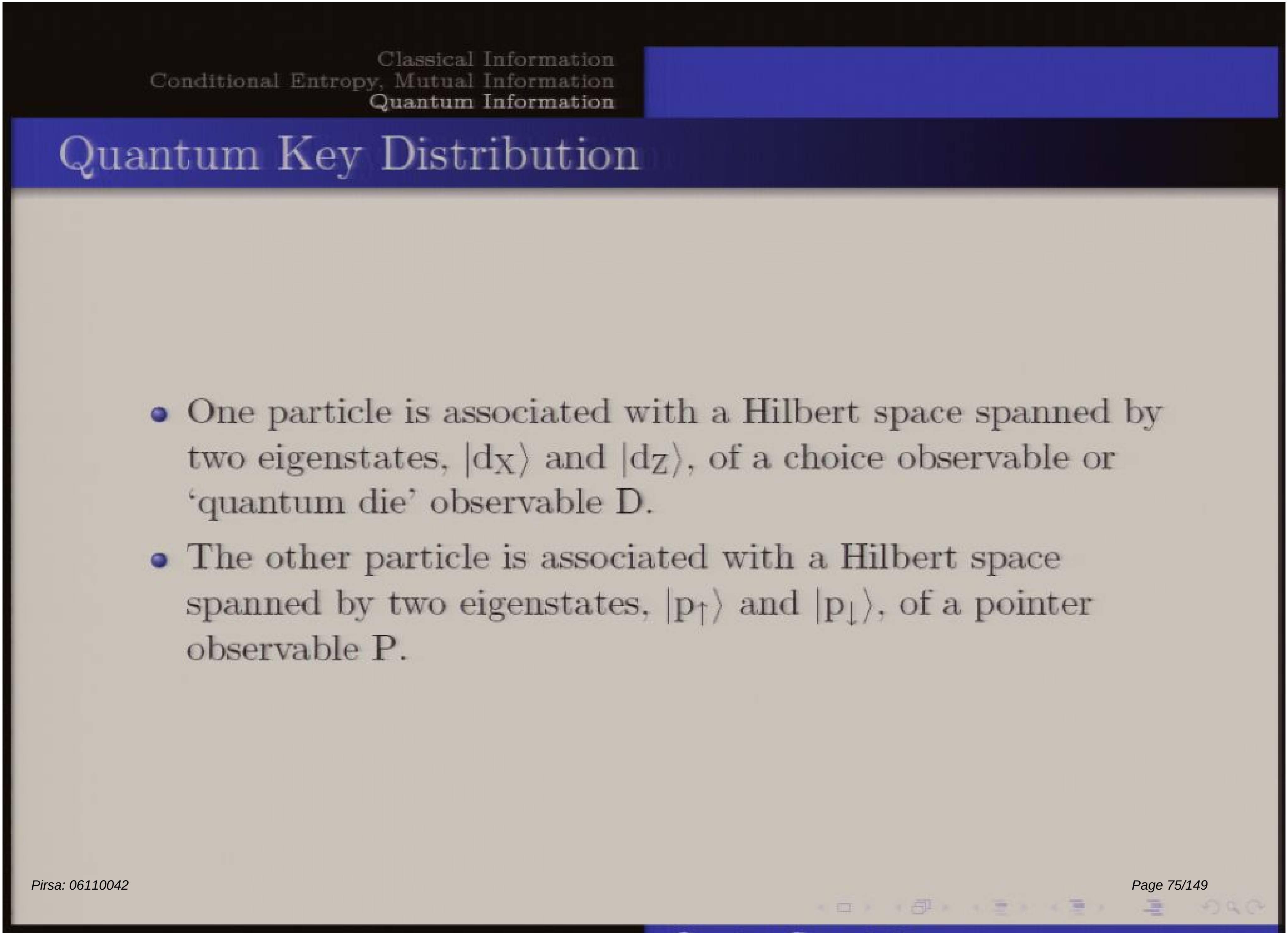
where the tensor product symbol has been introduced selectively to indicate that $\mathrm{U_x}$ and $\mathrm{U_y}$ are defined on $\mathcal{H}_\mathrm{C} \otimes \mathcal{H}_{\mathrm{B_P}}$.

Bit Commitment

- In a bit commitment protocol, one party, Alice, supplies an encrypted bit to a second party, Bob.
- The information available in the encrypted bit should be insufficient for Bob to ascertain the value of the bit, but sufficient, together with further information supplied by Alice at a subsequent stage when she is supposed to reveal the value of the bit, for Bob to be convinced that the protocol does not allow Alice to cheat by encrypting the bit in a way that leaves her free to reveal either 0 or 1 at will.

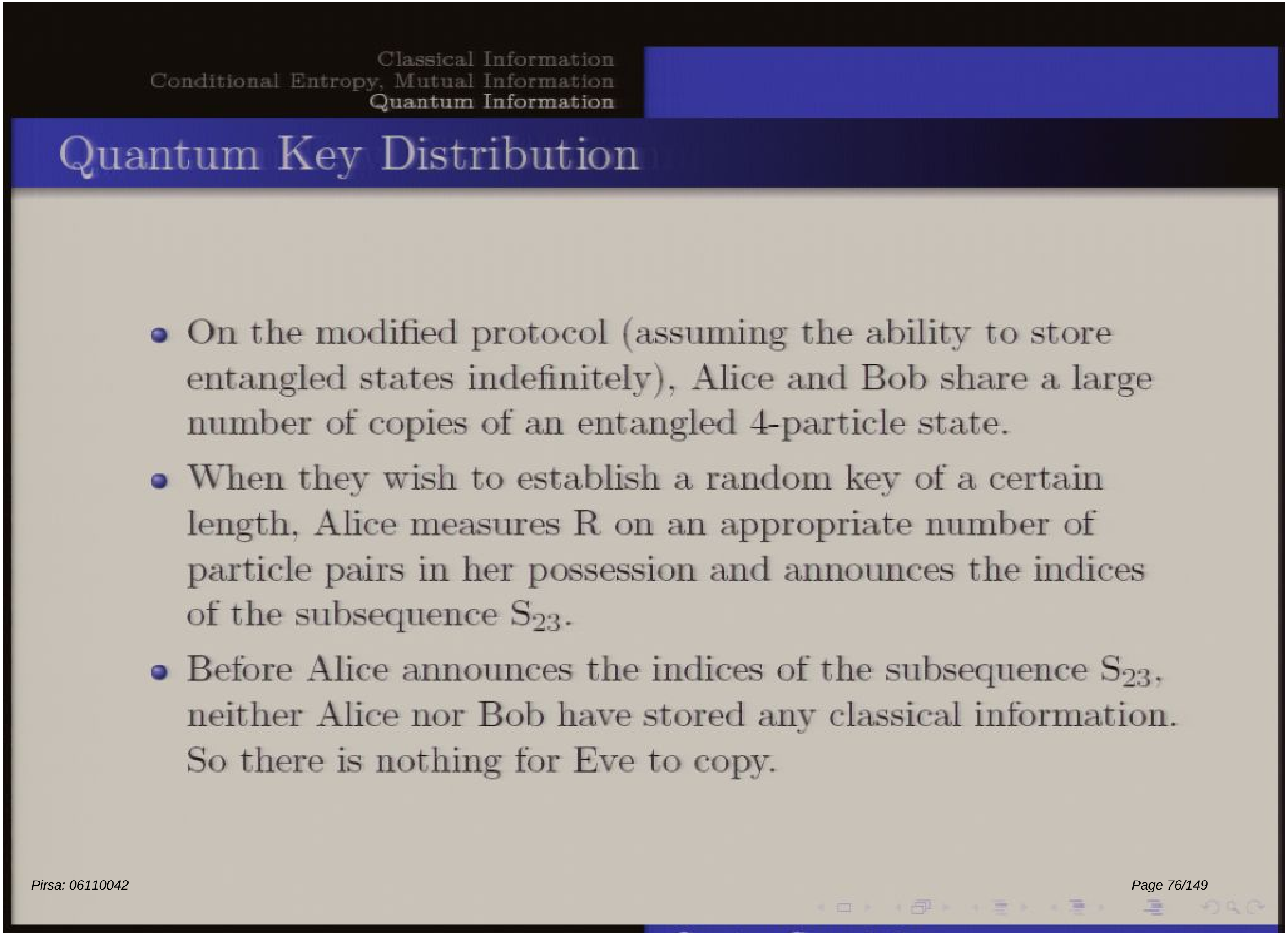
Quantum Key Distribution

- On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled 4-particle state.
- When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}.
- Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy.



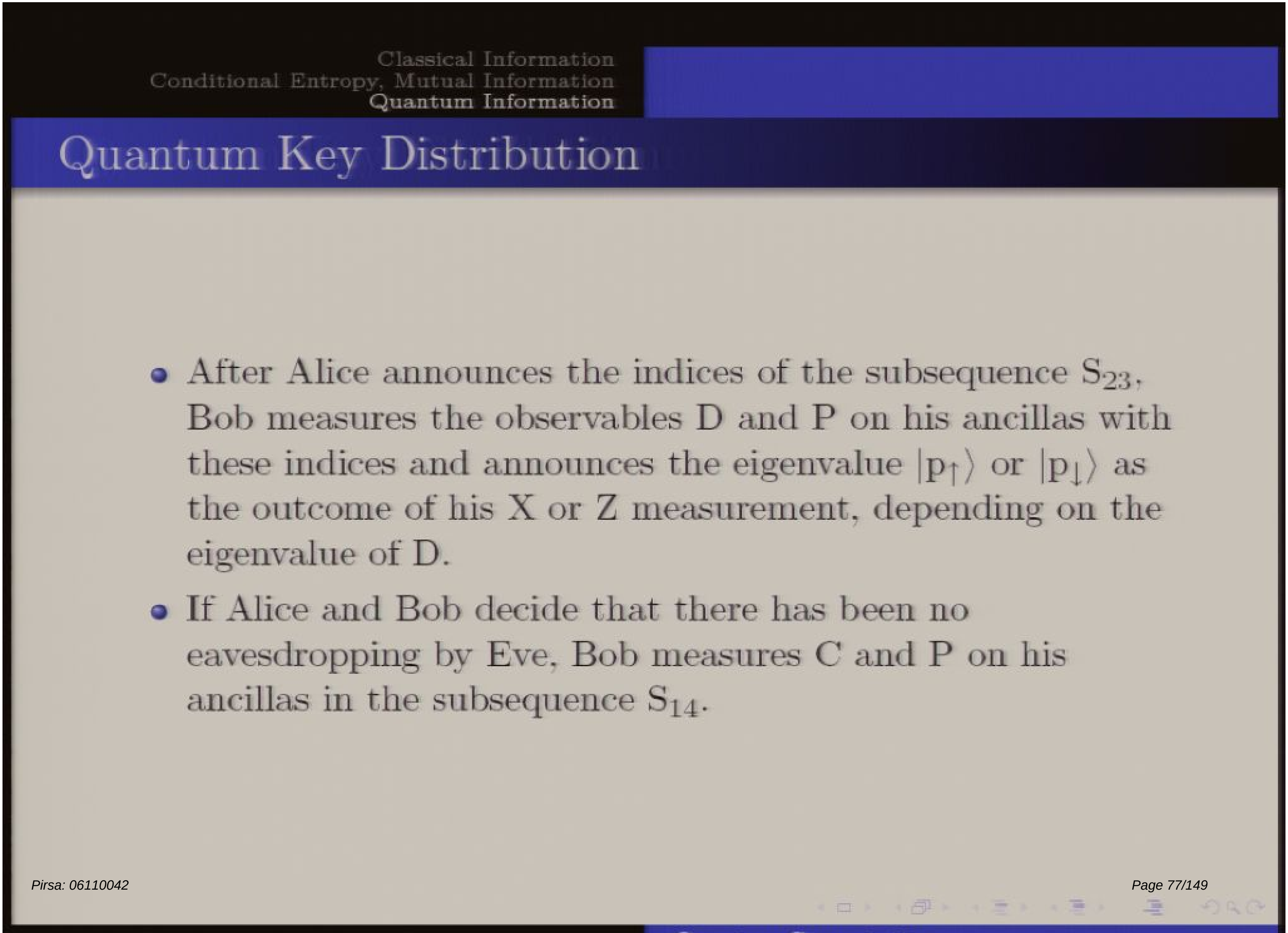
Quantum Key Distribution

- One particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{d}_X\rangle$ and $|\mathrm{d}_Z\rangle$, of a choice observable or 'quantum die' observable D.
- The other particle is associated with a Hilbert space spanned by two eigenstates, $|\mathrm{p}_\uparrow\rangle$ and $|\mathrm{p}_\downarrow\rangle$, of a pointer observable P.



Quantum Key Distribution

- On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled 4-particle state.
- When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}.
- Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy.



Quantum Key Distribution

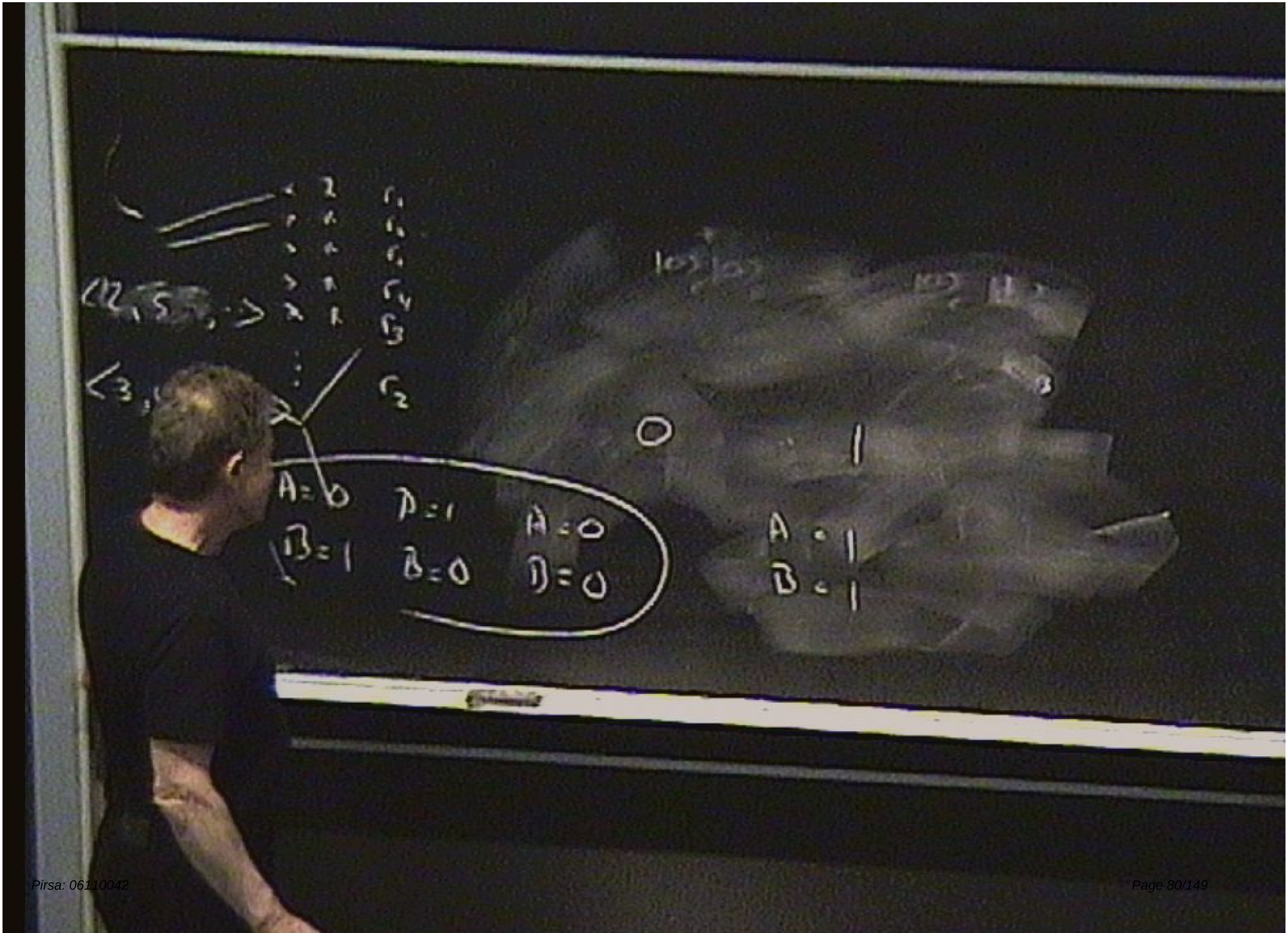
- After Alice announces the indices of the subsequence S_{23}, Bob measures the observables D and P on his ancillas with these indices and announces the eigenvalue $|p_{\uparrow}\rangle$ or $|p_{\downarrow}\rangle$ as the outcome of his X or Z measurement, depending on the eigenvalue of D.
- If Alice and Bob decide that there has been no eavesdropping by Eve, Bob measures C and P on his ancillas in the subsequence S_{14}.

Quantum Key Distribution

- It is easy to see that the ABL-rule applies in this case, just as it applies in the case where Bob actually makes the random choice and actually records definite outcomes of his X or Z measurements before Alice measures R.
- In fact, if the two cases were not equivalent for Alice—if Alice could tell from her R-measurements whether Bob had actually made the random choice and actually performed the spin measurements, or had merely implemented these actions 'at the quantum level'—the difference could be exploited to signal superluminally.

Bit Commitment

- In a bit commitment protocol, one party, Alice, supplies an encrypted bit to a second party, Bob.
- The information available in the encrypted bit should be insufficient for Bob to ascertain the value of the bit, but sufficient, together with further information supplied by Alice at a subsequent stage when she is supposed to reveal the value of the bit, for Bob to be convinced that the protocol does not allow Alice to cheat by encrypting the bit in a way that leaves her free to reveal either 0 or 1 at will.



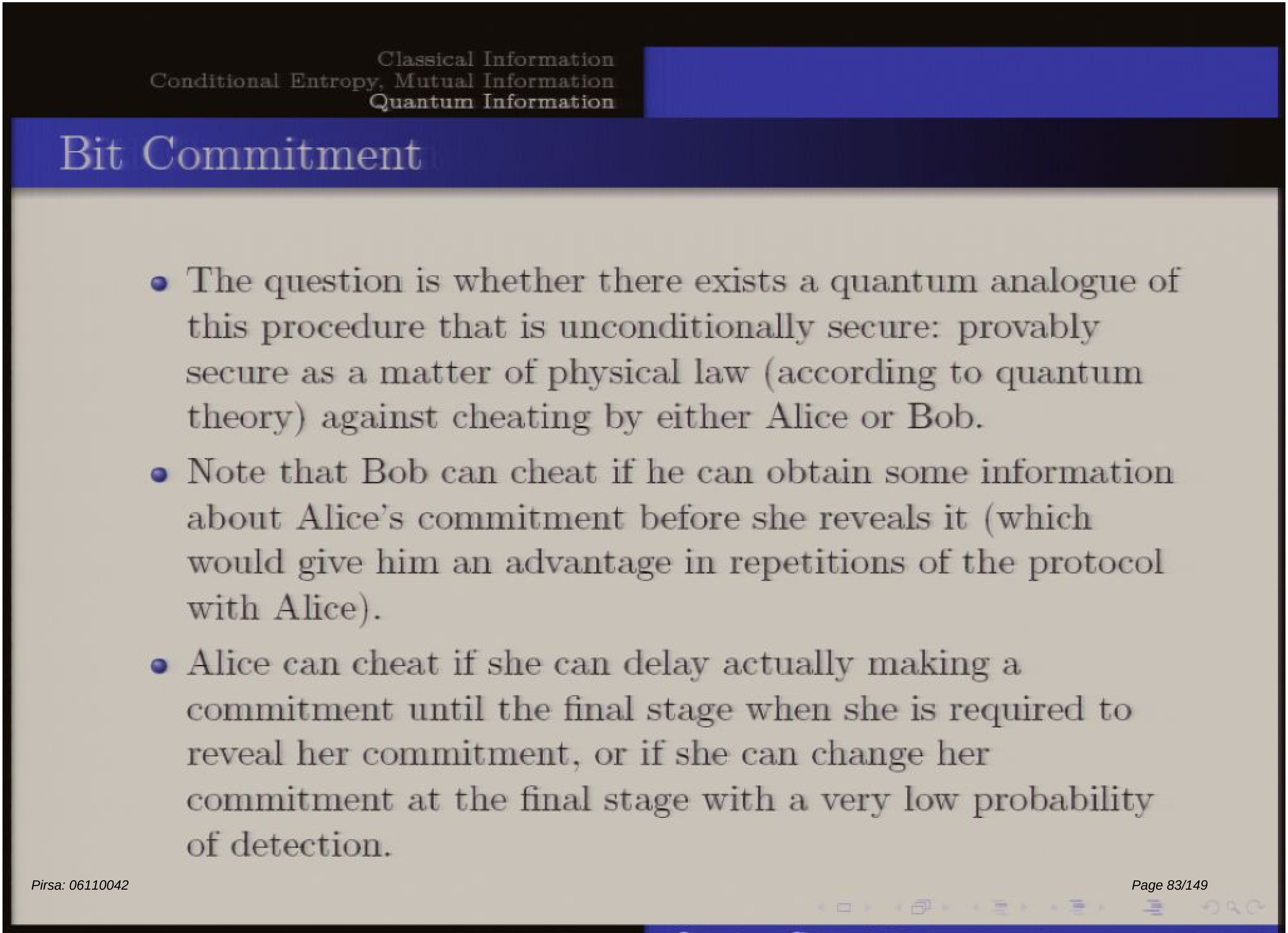
r_1
r_2
r_3
r_4
r_5
r_2
0
1
A=0
B=1
A=1
B=0
A=0
B=0
A=1
B=1

Bit Commitment

- Alice can send (encrypted) information to Bob that guarantees the truth of an exclusive classical disjunction (equivalent to her commitment to a 0 or a 1) only if the information is biased towards one of the alternative disjuncts (because a classical exclusive disjunction is true if and only if one of the disjuncts is true and the other false).
- No principle of classical mechanics precludes Bob from extracting this information, so the security of a classical bit commitment protocol can only be a matter of computational complexity.

Bit Commitment

- The question is whether there exists a quantum analogue of this procedure that is unconditionally secure: provably secure as a matter of physical law (according to quantum theory) against cheating by either Alice or Bob.
- Note that Bob can cheat if he can obtain some information about Alice's commitment before she reveals it (which would give him an advantage in repetitions of the protocol with Alice).
- Alice can cheat if she can delay actually making a commitment until the final stage when she is required to reveal her commitment, or if she can change her commitment at the final stage with a very low probability of detection.

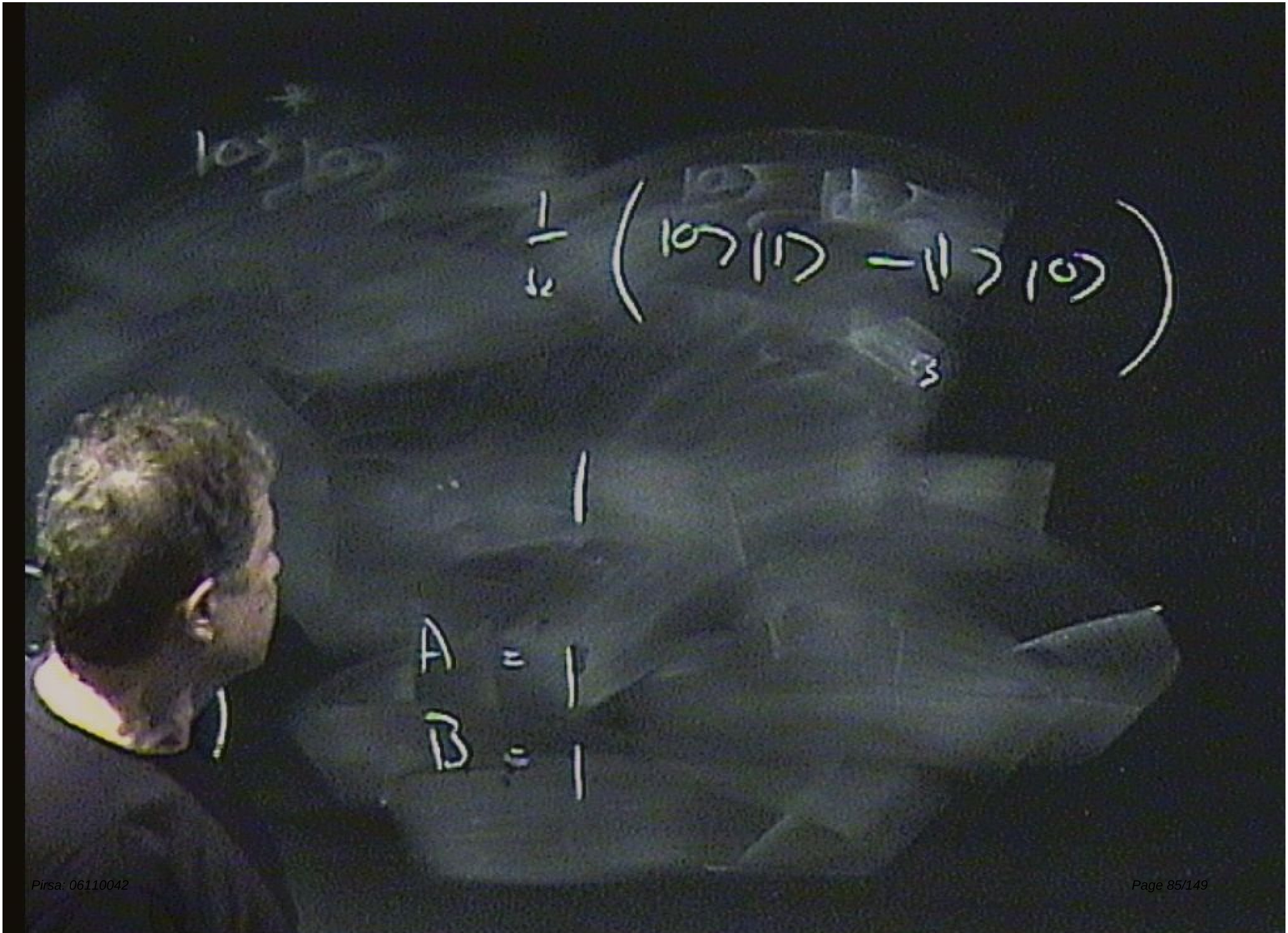


Bit Commitment

- The question is whether there exists a quantum analogue of this procedure that is unconditionally secure: provably secure as a matter of physical law (according to quantum theory) against cheating by either Alice or Bob.
- Note that Bob can cheat if he can obtain some information about Alice's commitment before she reveals it (which would give him an advantage in repetitions of the protocol with Alice).
- Alice can cheat if she can delay actually making a commitment until the final stage when she is required to reveal her commitment, or if she can change her commitment at the final stage with a very low probability of detection.

Bit Commitment

- Bennett and Brassard originally proposed a quantum bit commitment protocol in 1984. The basic idea was to associate the 0 and 1 commitments with two different mixtures represented by the same density operator.
- As they showed in the same paper, Alice can cheat by adopting an ‘EPR attack’ or cheating strategy: she prepares entangled pairs of qubits, keeps one of each pair (the ancilla) and sends the second qubit (the channel particle) to Bob.
- In this way she can fake sending one of two equivalent mixtures to Bob and reveal either bit at will at the opening stage by effectively steering Bob’s particle into the desired mixture by an appropriate measurement. Bob cannot detect this cheating strategy.

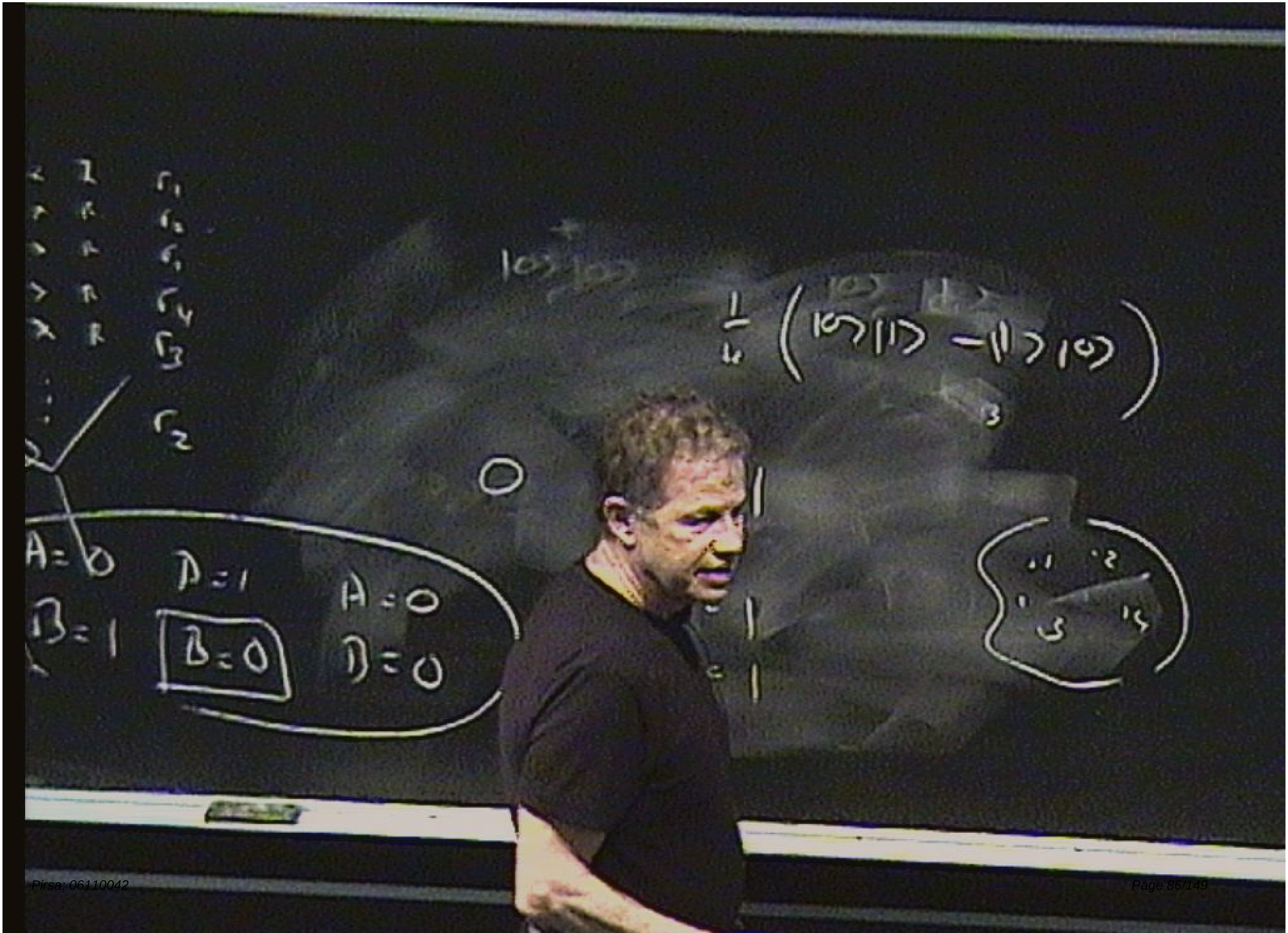


$|0\rangle|0\rangle$

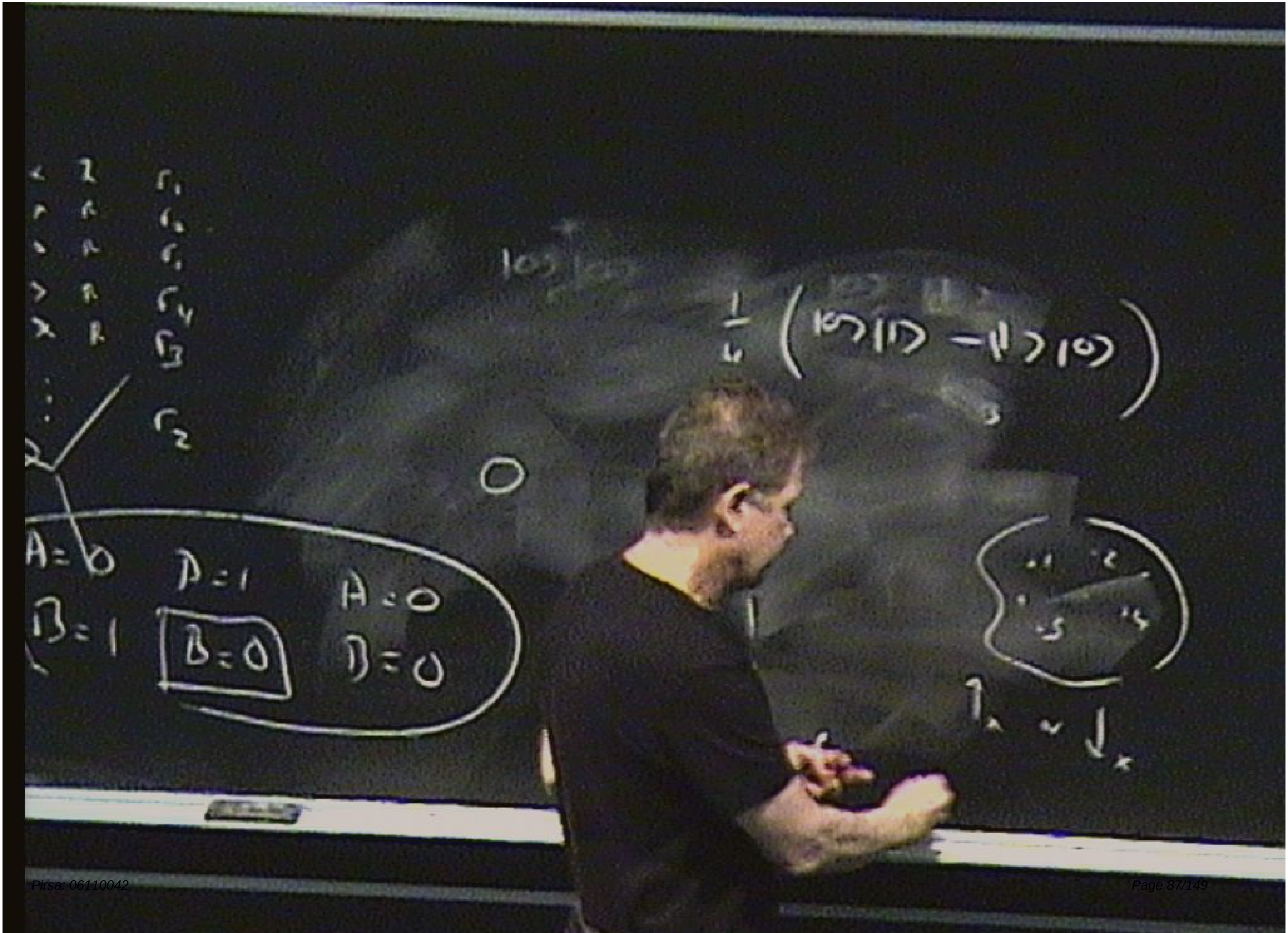
$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

$A = 1$

$B = 1$



r_1
r_2
r_3
r_4
r_5
r_2
$\frac{1}{4}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$
0
A=0
B=1
D=1
B=0
A=0
D=0
1 2 3 4



r_1

r_2

r_3

r_4

r_5

r_2

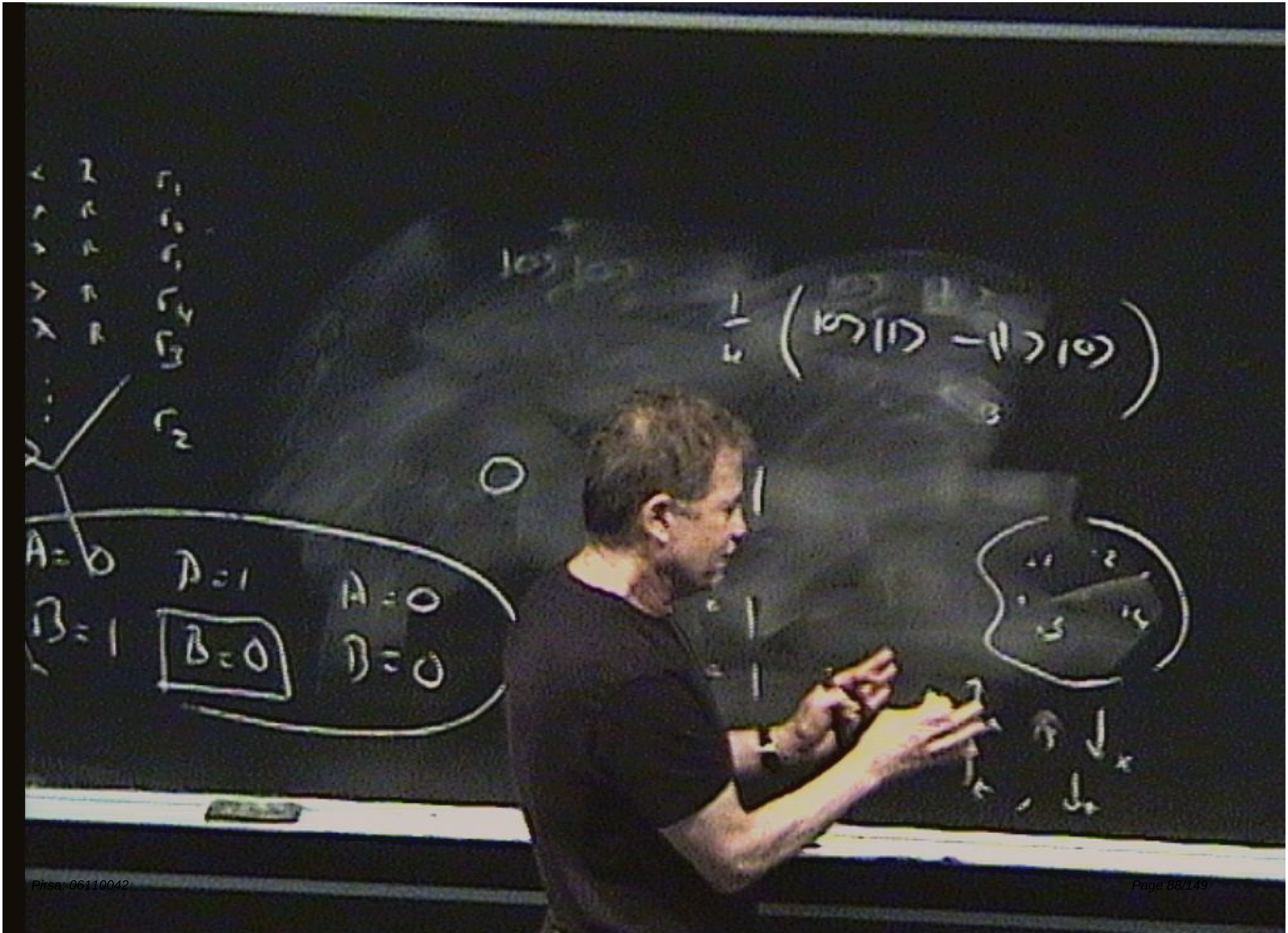
$$\frac{1}{4}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

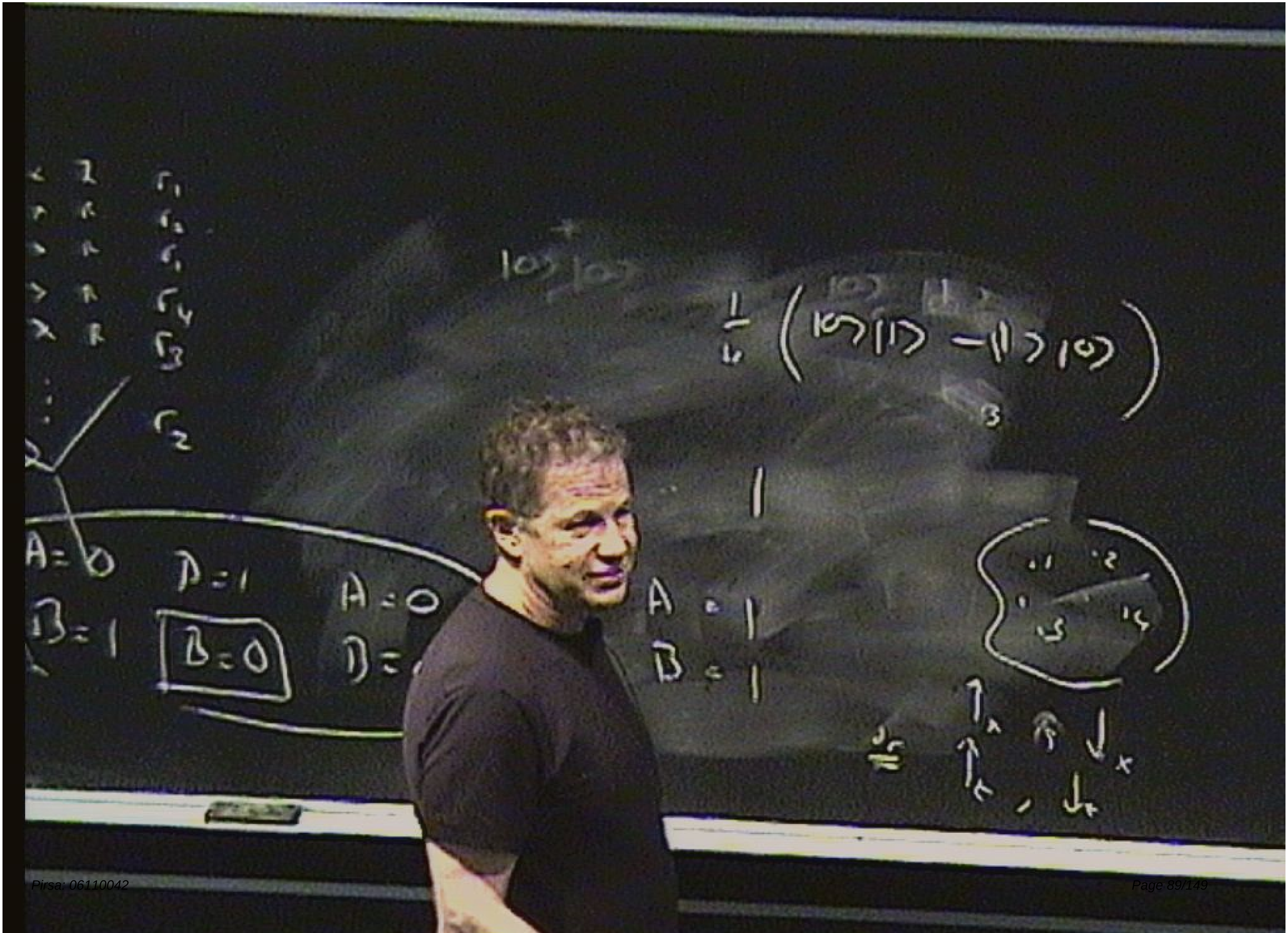
0

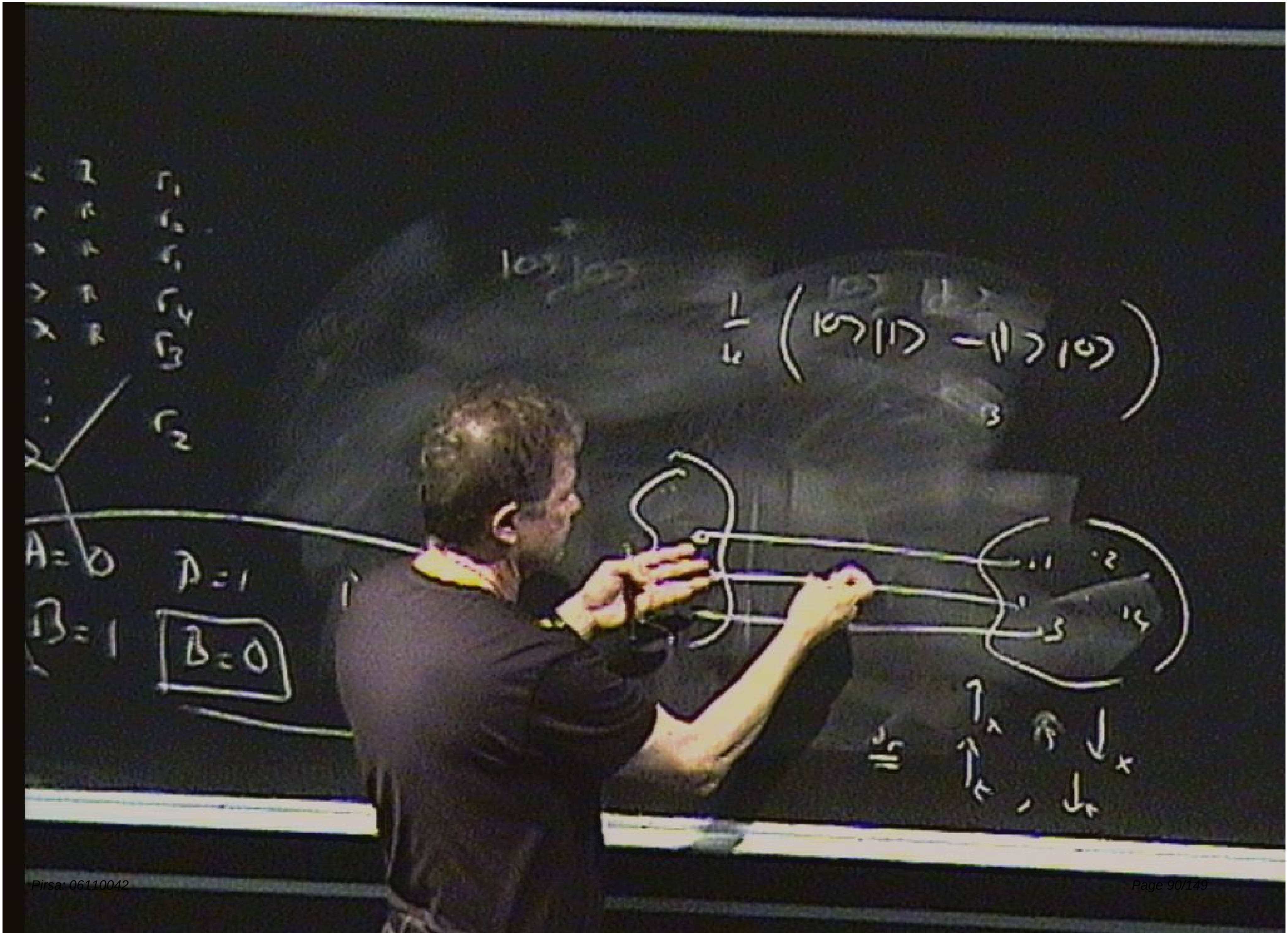
$A=0$ $B=1$ $A=0$

$B=1$ $\boxed{B=0}$ $B=0$

$1_x \sim J_x$


$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$
A=0
B=1
B=1
B=0
A=0
B=0
J_x
J_z , J_y


|0⟩|0⟩
1/√2 (|0⟩|1⟩ − |1⟩|0⟩)
A=0
B=1
B=1
B=0
A=0
B=
A=1
B=1
r1
r2
r3
r4
r5
r2



$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

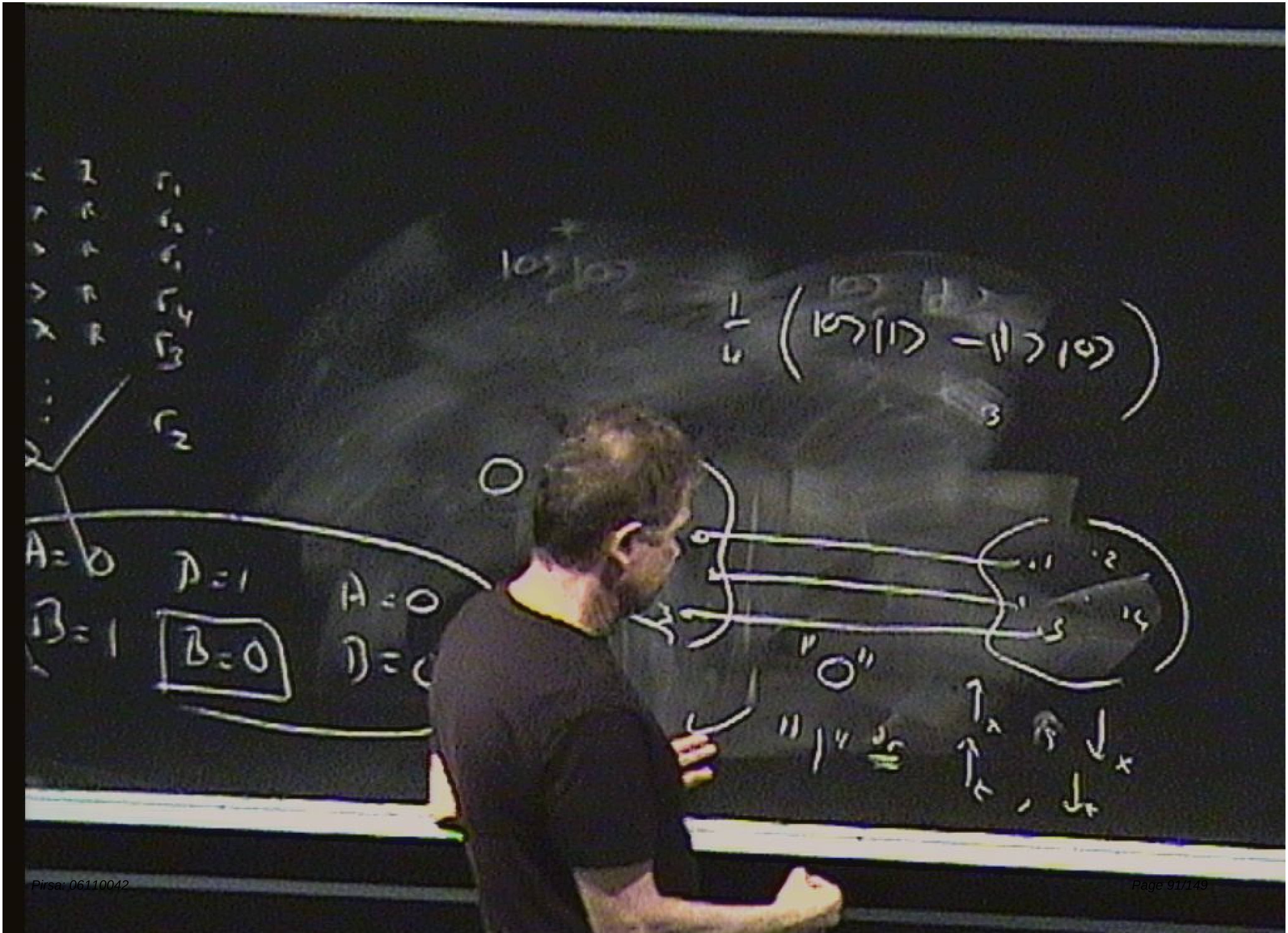
$A=0$ $\quad D=1$

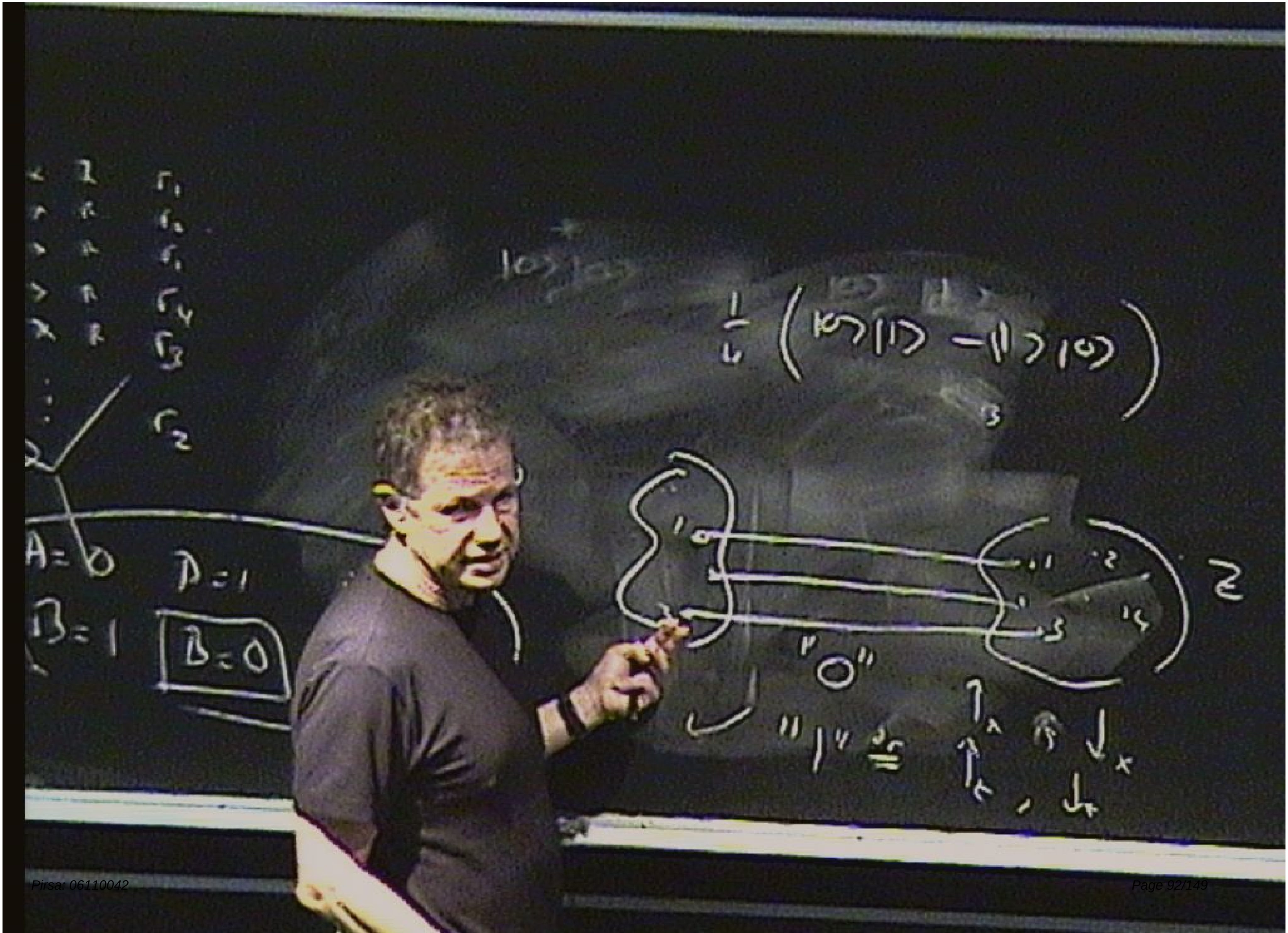
$B=1$ $\quad \boxed{B=0}$

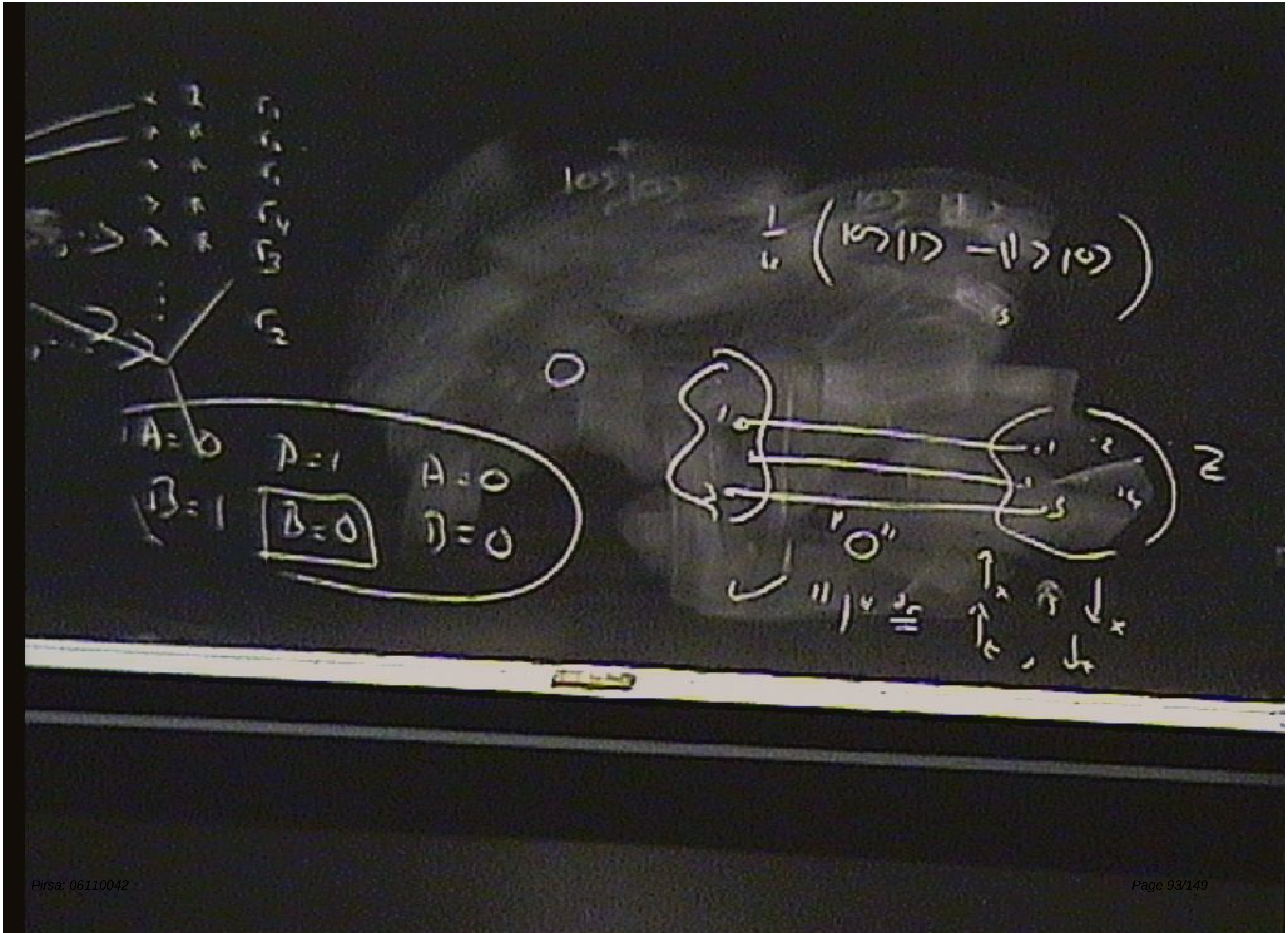
r_1, r_2, r_3, r_4, r_5, r_2

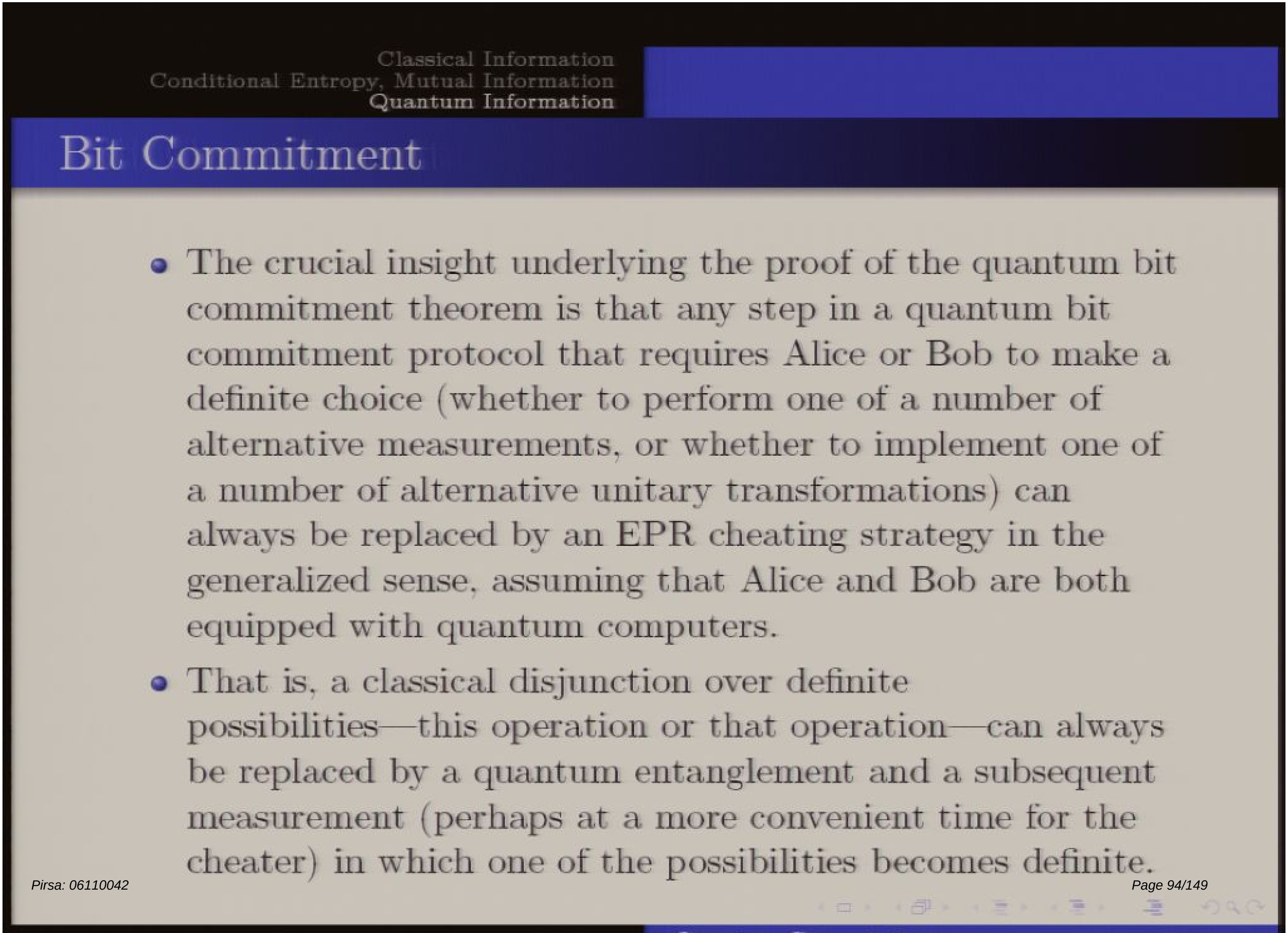
$\uparrow_x \; \Uparrow \; \downarrow_x$

$\overset{?}{=} \; \uparrow_z \, , \; \downarrow_z$


A = 0
B = 1
B = 0
A = 0
B = 0
1/√2 (|0⟩|1⟩ − |1⟩|0⟩)
"0"
"1"

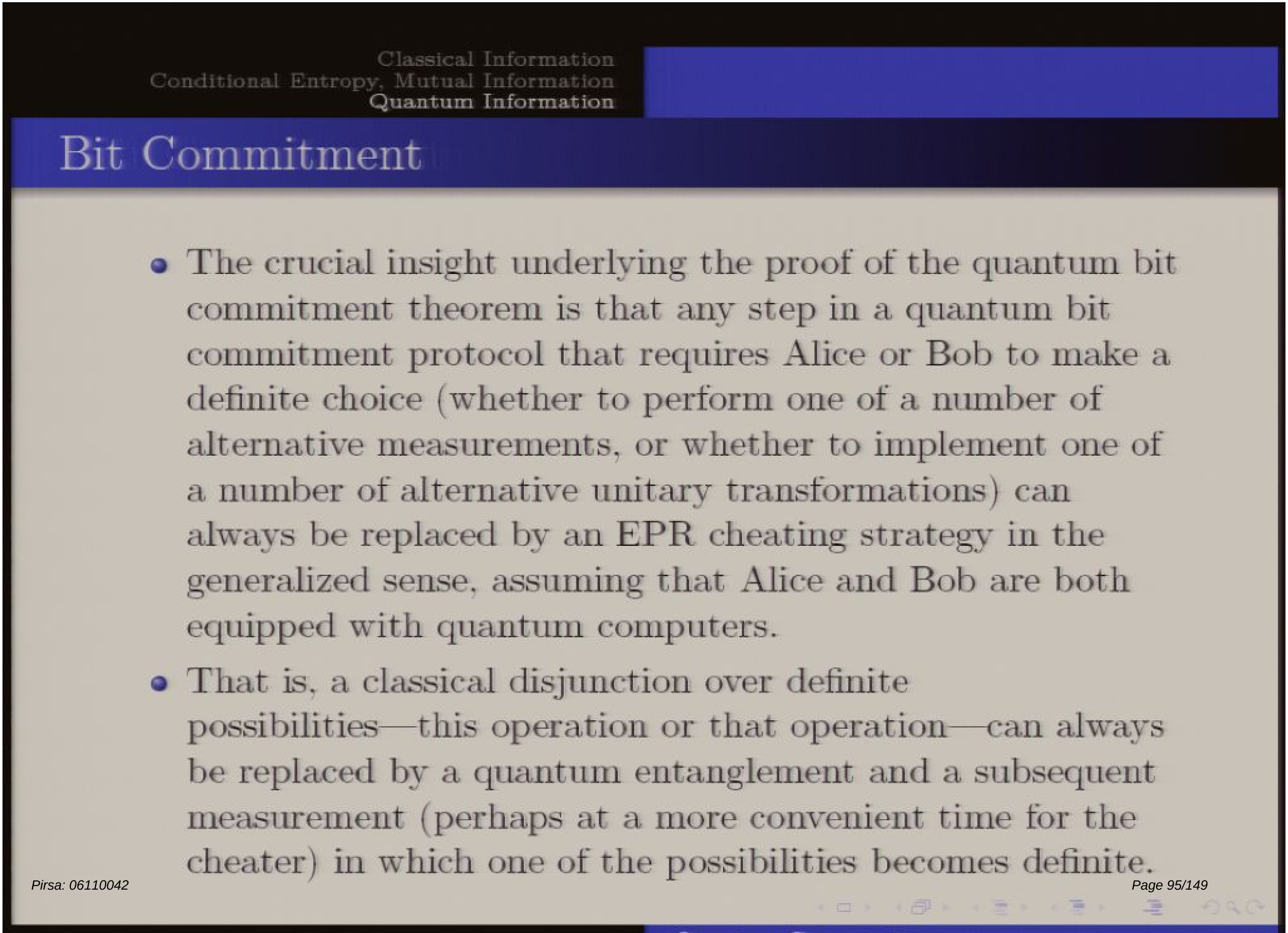
r1
r2
r3
r4
r5
r2
A=0
B=1
D=1
B=0
1/√2 (|0⟩|1⟩ − |1⟩|0⟩)
1
3
"0"
"1"
Σ
1
2
3
4


r_1
r_2
r_3
r_4
r_5
r_2
$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$
0
A=0
B=1
A=1
B=0
A=0
B=0
1
2
3
4
5
Z
"0"
"1"
$\uparrow_x$
$\downarrow_x$
$\uparrow_z$, $\downarrow_z$



Bit Commitment

- The crucial insight underlying the proof of the quantum bit commitment theorem is that any step in a quantum bit commitment protocol that requires Alice or Bob to make a definite choice (whether to perform one of a number of alternative measurements, or whether to implement one of a number of alternative unitary transformations) can always be replaced by an EPR cheating strategy in the generalized sense, assuming that Alice and Bob are both equipped with quantum computers.
- That is, a classical disjunction over definite possibilities—this operation or that operation—can always be replaced by a quantum entanglement and a subsequent measurement (perhaps at a more convenient time for the cheater) in which one of the possibilities becomes definite.



Bit Commitment

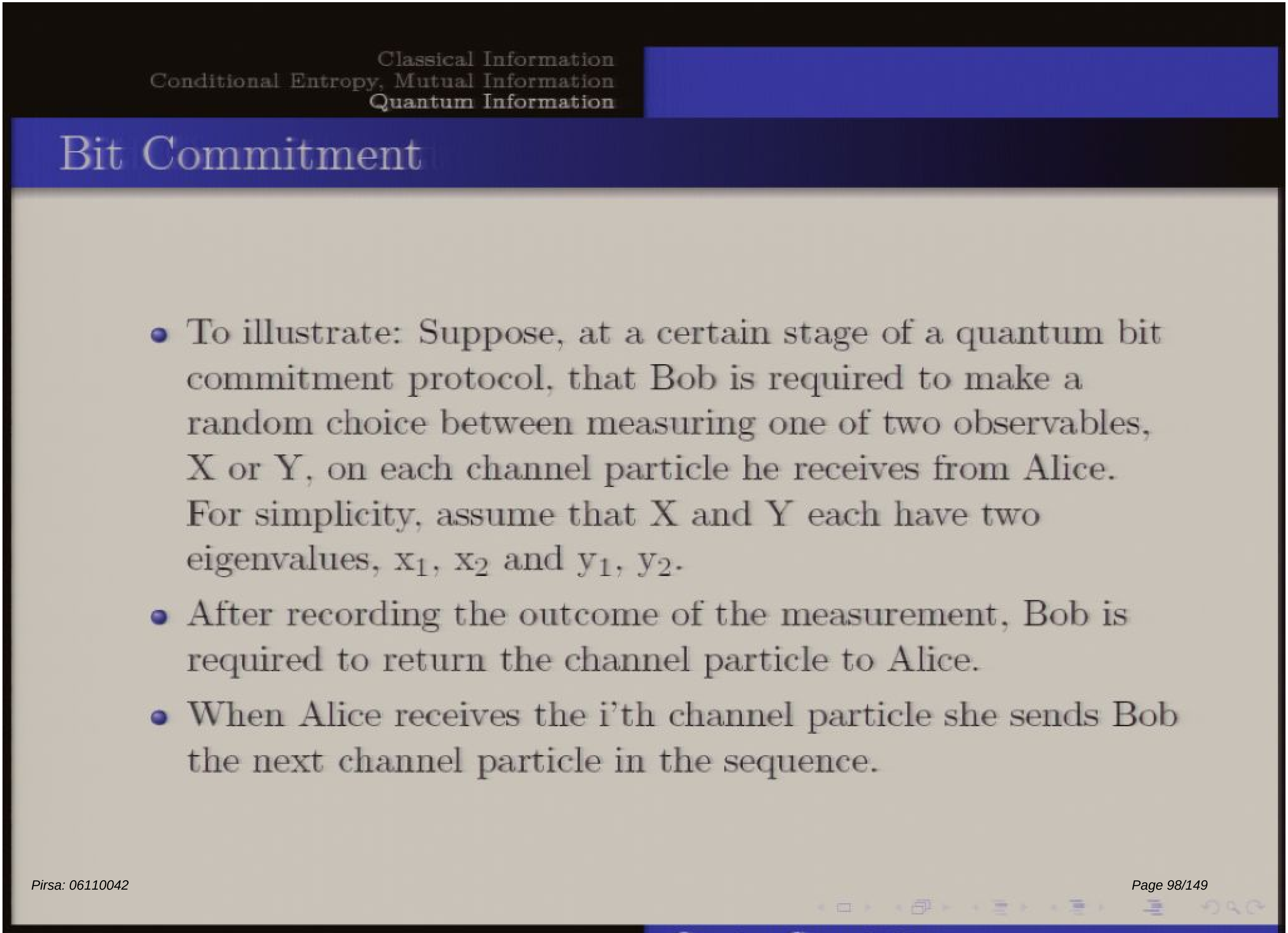
- The crucial insight underlying the proof of the quantum bit commitment theorem is that any step in a quantum bit commitment protocol that requires Alice or Bob to make a definite choice (whether to perform one of a number of alternative measurements, or whether to implement one of a number of alternative unitary transformations) can always be replaced by an EPR cheating strategy in the generalized sense, assuming that Alice and Bob are both equipped with quantum computers.
- That is, a classical disjunction over definite possibilities—this operation or that operation—can always be replaced by a quantum entanglement and a subsequent measurement (perhaps at a more convenient time for the cheater) in which one of the possibilities becomes definite.

Bit Commitment

- Similarly, a measurement can be 'held at the quantum level' without detection: instead of performing the measurement and obtaining a definite outcome as one of a number of possible outcomes, a suitable unitary transformation can be performed on an enlarged Hilbert space, in which the system is entangled with a 'pointer' ancilla in an appropriate way, and the procedure of obtaining a definite outcome can be delayed.
- The key point is the possibility of keeping the series of transactions between Alice and Bob at the quantum level by enlarging the Hilbert space, until the final exchange of classical information when Alice reveals her commitment.

Bit Commitment

- Any quantum bit commitment scheme will involve a series of transactions between Alice and Bob, where a certain number, n, of quantum systems—the ‘channel particles’—are passed between them and subjected to various quantum operations (unitary transformations, measurements, etc.), possibly chosen randomly.
- These operations can always be replaced, without detection, by entangling a channel particle with one or more ancilla particles that function as ‘pointer’ particles for measurements or ‘die’ particles for random choices.
- In effect, this is the (generalized) EPR cheating strategy.



Bit Commitment

- To illustrate: Suppose, at a certain stage of a quantum bit commitment protocol, that Bob is required to make a random choice between measuring one of two observables, X or Y, on each channel particle he receives from Alice. For simplicity, assume that X and Y each have two eigenvalues, x_1, x_2 and y_1, y_2.
- After recording the outcome of the measurement, Bob is required to return the channel particle to Alice.
- When Alice receives the i'th channel particle she sends Bob the next channel particle in the sequence.

Bit Commitment

- Instead of following the protocol, Bob can construct a device that entangles the input state $|\psi\rangle_C$ of a channel particle with the initial states, $|d_0\rangle_B$ and $|p_0\rangle_B$, of two ancilla particles that he introduces, the first of which functions as a 'quantum die' for the random choice and the second as a 'quantum pointer' for the measurement.
- It is assumed that Bob's ability to construct such a device—in effect, a special purpose quantum computer—is restricted only by the laws of quantum mechanics.

Bit Commitment

The entanglement is implemented by a unitary transformation. Define two unitary transformations, U_X and U_Y, that implement the X and Y measurements ‘at the quantum level’ on the tensor product of the Hilbert space of the channel particle, $\mathcal{H}_C$, and the Hilbert space of Bob’s pointer ancilla, $\mathcal{H}_{B_P}$:

$$|x_1\rangle_C|p_0\rangle_B \xrightarrow{U_X} |x_1\rangle_C|p_1\rangle_B$$
$$|x_2\rangle_C|p_0\rangle_B \xrightarrow{U_X} |x_2\rangle_C|p_2\rangle_B$$

and

$$|y_1\rangle_C|p_0\rangle_B \xrightarrow{U_Y} |y_1\rangle_C|p_1\rangle_B$$
$$|y_2\rangle_C||p_0\rangle_B \xrightarrow{U_Y} |y_2\rangle_C|p_2\rangle_B$$

Bit Commitment

It follows that:

$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_X}} \langle \mathrm{x}_1|\psi\rangle|\mathrm{x}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{x}_2|\psi\rangle|\mathrm{x}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

and

$$|\psi\rangle_{\mathrm{C}}|\mathrm{p}_0\rangle_{\mathrm{B}} \xrightarrow{\mathrm{U_Y}} \langle \mathrm{y}_1|\psi\rangle|\mathrm{y}_1\rangle_{\mathrm{C}}|\mathrm{p}_1\rangle_{\mathrm{B}} + \langle \mathrm{y}_2|\psi\rangle|\mathrm{y}_2\rangle_{\mathrm{C}}|\mathrm{p}_2\rangle_{\mathrm{B}}$$

Bit Commitment

- The random choice is defined similarly by a unitary transformation V on the tensor product of the Hilbert space of Bob's die ancilla, $\mathcal{H}_{\mathrm{B_D}}$, and the Hilbert space $\mathcal{H}_{\mathrm{C}} \otimes \mathcal{H}_{\mathrm{B_P}}$.
- Suppose $|\mathrm{d_X}\rangle$ and $|\mathrm{d_Y}\rangle$ are two orthogonal states in $\mathcal{H}_{\mathrm{B_D}}$ and that $|\mathrm{d_0}\rangle = \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle$.

Bit Commitment

Then (suppressing the obvious subscripts) V is defined by:

$$\begin{aligned} |\mathrm{d_X}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle \\ |\mathrm{d_Y}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle &\xrightarrow{\mathrm{V}} |\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \end{aligned} \tag{5}$$

so that

$$\begin{aligned} &|\mathrm{d_0}\rangle \otimes |\psi\rangle|\mathrm{p_0}\rangle \xrightarrow{\mathrm{V}} \\ &\quad \frac{1}{\sqrt{2}}|\mathrm{d_X}\rangle \otimes \mathrm{U_X}|\psi\rangle|\mathrm{p_0}\rangle + \frac{1}{\sqrt{2}}|\mathrm{d_Y}\rangle \otimes \mathrm{U_Y}|\psi\rangle|\mathrm{p_0}\rangle \end{aligned} \tag{6}$$

where the tensor product symbol has been introduced selectively to indicate that $\mathrm{U_x}$ and $\mathrm{U_y}$ are defined on $\mathcal{H}_\mathrm{C} \otimes \mathcal{H}_{\mathrm{B_P}}$.

Bit Commitment

- If Bob were to actually choose the observable X or Y randomly, and actually perform the measurement and obtain a particular eigenvalue, Alice's density operator for the channel particle would be:

$$\frac{1}{2}(|\langle x_1|\psi\rangle|^2 |x_1\rangle\langle x_1| + |\langle x_2|\psi\rangle|^2 |x_2\rangle\langle x_2|)$$
$$+\frac{1}{2}(|\langle y_1|\psi\rangle|^2 |y_1\rangle\langle y_1| + |\langle y_2|\psi\rangle|^2 |y_2\rangle\langle y_2|)$$

  assuming that Alice does not know what observable Bob chose to measure, nor what outcome he obtained.

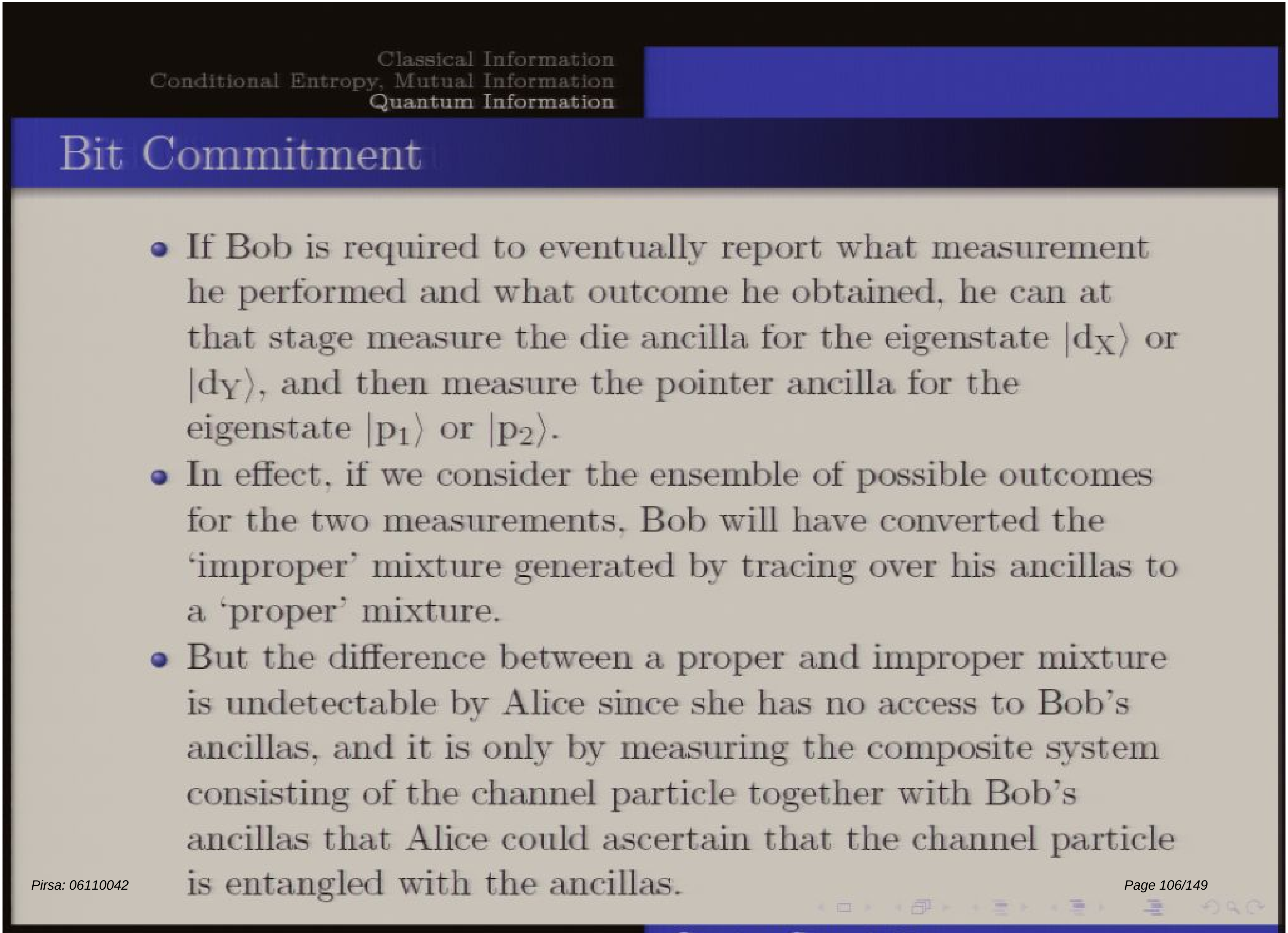
- But this is precisely the same density operator generated by tracing over Bob's ancilla particles in the state $\frac{1}{\sqrt{2}}|d_X\rangle \otimes U_X|\psi\rangle|p_0\rangle + \frac{1}{\sqrt{2}}|d_Y\rangle \otimes U_Y|\psi\rangle|p_0\rangle$.

Bit Commitment

In other words, the density operator for the channel particle is the same for Alice, whether Bob randomly chooses which observable to measure and actually performs the measurement, or whether he implements an EPR cheating strategy with his two ancillas that produces the transition:

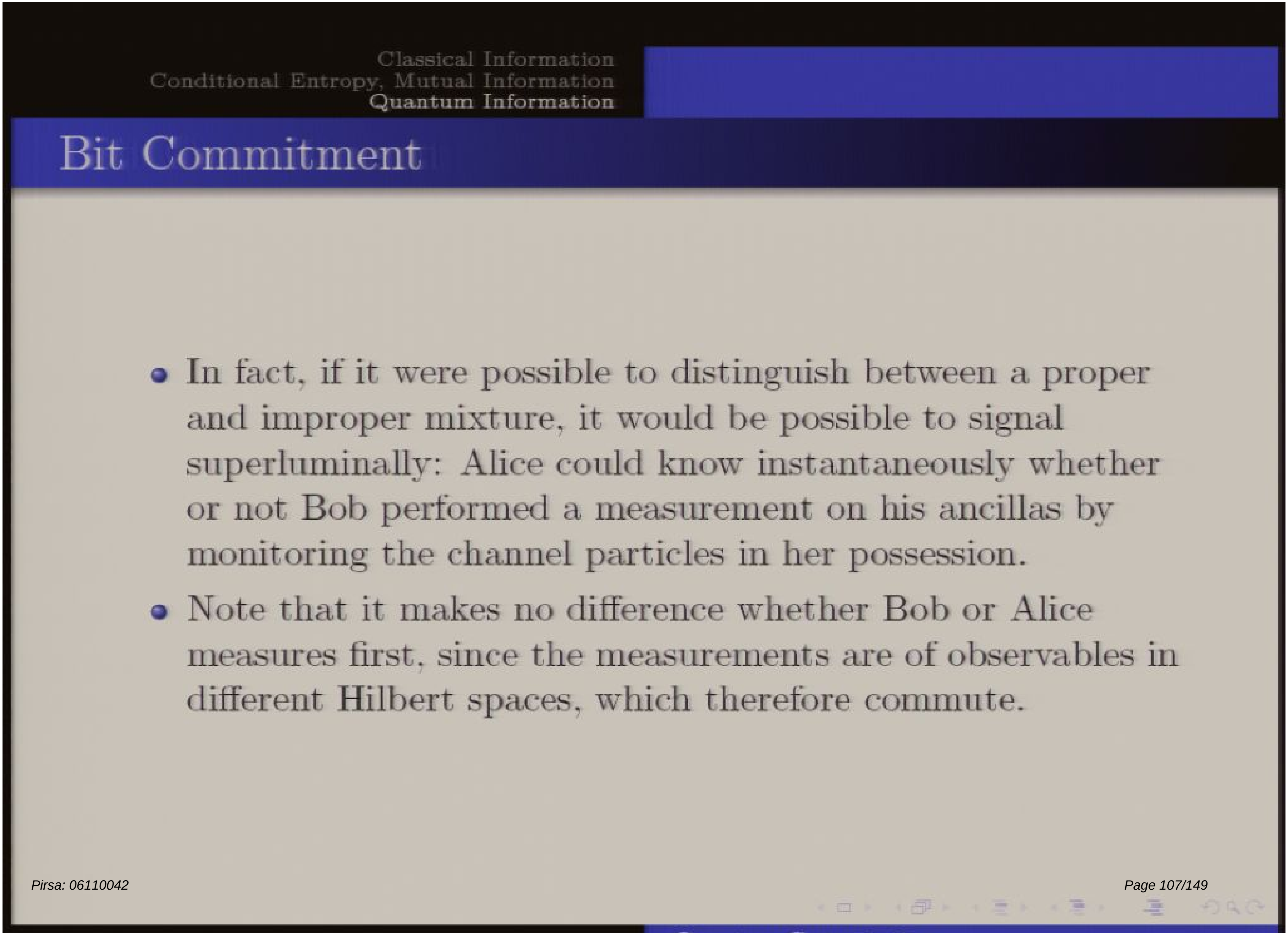
$$|\mathrm{d}_0\rangle \otimes |\psi\rangle|\mathrm{p}_0\rangle \xrightarrow{\mathrm{V}}$$
$$\frac{1}{\sqrt{2}}|\mathrm{d}_\mathrm{X}\rangle \otimes \mathrm{U}_\mathrm{X}|\psi\rangle|\mathrm{p}_0\rangle + \frac{1}{\sqrt{2}}|\mathrm{d}_\mathrm{Y}\rangle \otimes \mathrm{U}_\mathrm{Y}|\psi\rangle|\mathrm{p}_0\rangle$$

on the enlarged Hilbert space.



Bit Commitment

- If Bob is required to eventually report what measurement he performed and what outcome he obtained, he can at that stage measure the die ancilla for the eigenstate $|d_X\rangle$ or $|d_Y\rangle$, and then measure the pointer ancilla for the eigenstate $|p_1\rangle$ or $|p_2\rangle$.
- In effect, if we consider the ensemble of possible outcomes for the two measurements, Bob will have converted the 'improper' mixture generated by tracing over his ancillas to a 'proper' mixture.
- But the difference between a proper and improper mixture is undetectable by Alice since she has no access to Bob's ancillas, and it is only by measuring the composite system consisting of the channel particle together with Bob's ancillas that Alice could ascertain that the channel particle is entangled with the ancillas.

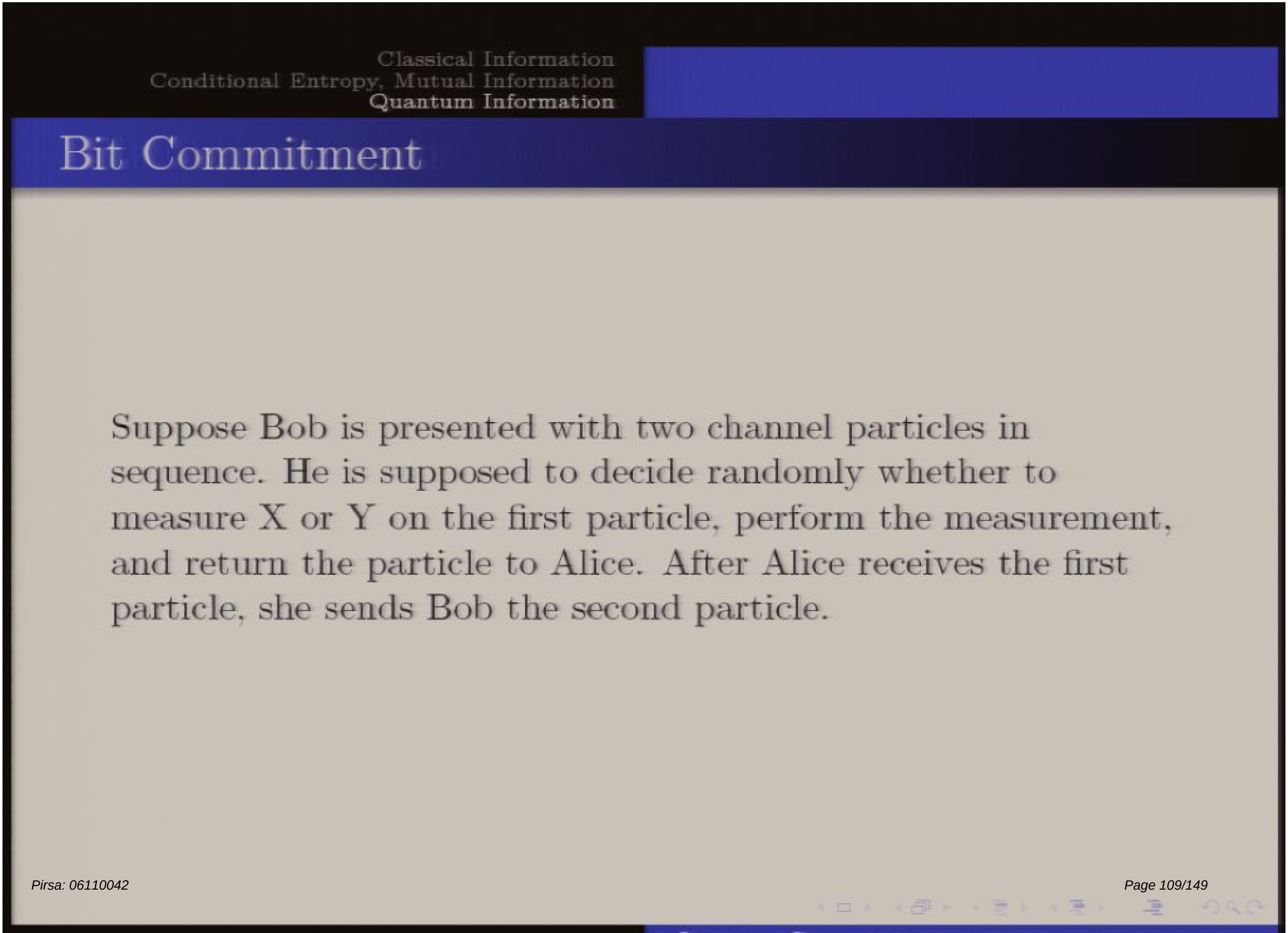


Bit Commitment

- In fact, if it were possible to distinguish between a proper and improper mixture, it would be possible to signal superluminally: Alice could know instantaneously whether or not Bob performed a measurement on his ancillas by monitoring the channel particles in her possession.
- Note that it makes no difference whether Bob or Alice measures first, since the measurements are of observables in different Hilbert spaces, which therefore commute.

Bit Commitment

- An EPR cheating strategy is also possible if Bob is required to perform a measurement on channel particle $i + 1$, conditional on the outcome of a prior measurement on channel particle i, or conditional on a prior choice of some operation from among a set of alternative operations.
- If Bob is in possession of all the channel particles at the same time, he can perform an entanglement with ancillas on the entire sequence, considered as a single composite system.
- If Bob only has access to one channel particle at a time (which he is required to return to Alice after performing a measurement before she sends him the next channel particle), he can always entangle channel particle $i + 1$ with the ancillas he used to entangle channel particle i.



Bit Commitment

Suppose Bob is presented with two channel particles in sequence. He is supposed to decide randomly whether to measure X or Y on the first particle, perform the measurement, and return the particle to Alice. After Alice receives the first particle, she sends Bob the second particle.

Bit Commitment

- If Bob measured X on the first particle and obtained the outcome x_1, he is supposed to measure X on the second particle; if he obtained the outcome x_2, he is supposed to measure Y on the second particle.
- If he measured Y on the first particle and obtained the outcome y_1, he is supposed to apply the unitary transformation U_1 to the second particle; if he obtained the outcome y_2, he is supposed to apply the unitary transformation U_2.
- After performing the required operation, he is supposed to return the second particle to Alice.

Bit Commitment

It would seem at first sight that Bob has to actually perform a measurement on the first channel particle and obtain a particular outcome before he can apply the protocol to the second particle, given that he only has access to one channel particle at a time, so an EPR cheating strategy is excluded. But this is not so.

Bit Commitment

Bob's strategy is the following: He applies the EPR strategy discussed above for two alternative measurements to the first channel particle. For the second channel particle, he applies the following unitary transformation on the tensor product of the Hilbert spaces of his ancillas and the channel particle, where the state of the second channel particle is denoted by $|\phi\rangle$, and the state of the pointer ancilla for the second channel particle is denoted by $|q_0\rangle$ (a second die particle is not required):

Bit Commitment

$$|d_X\rangle|p_1\rangle|\phi\rangle|q_0\rangle \xrightarrow{U_C} |d_X\rangle|p_1\rangle \otimes U_X|\phi\rangle|q_0\rangle$$

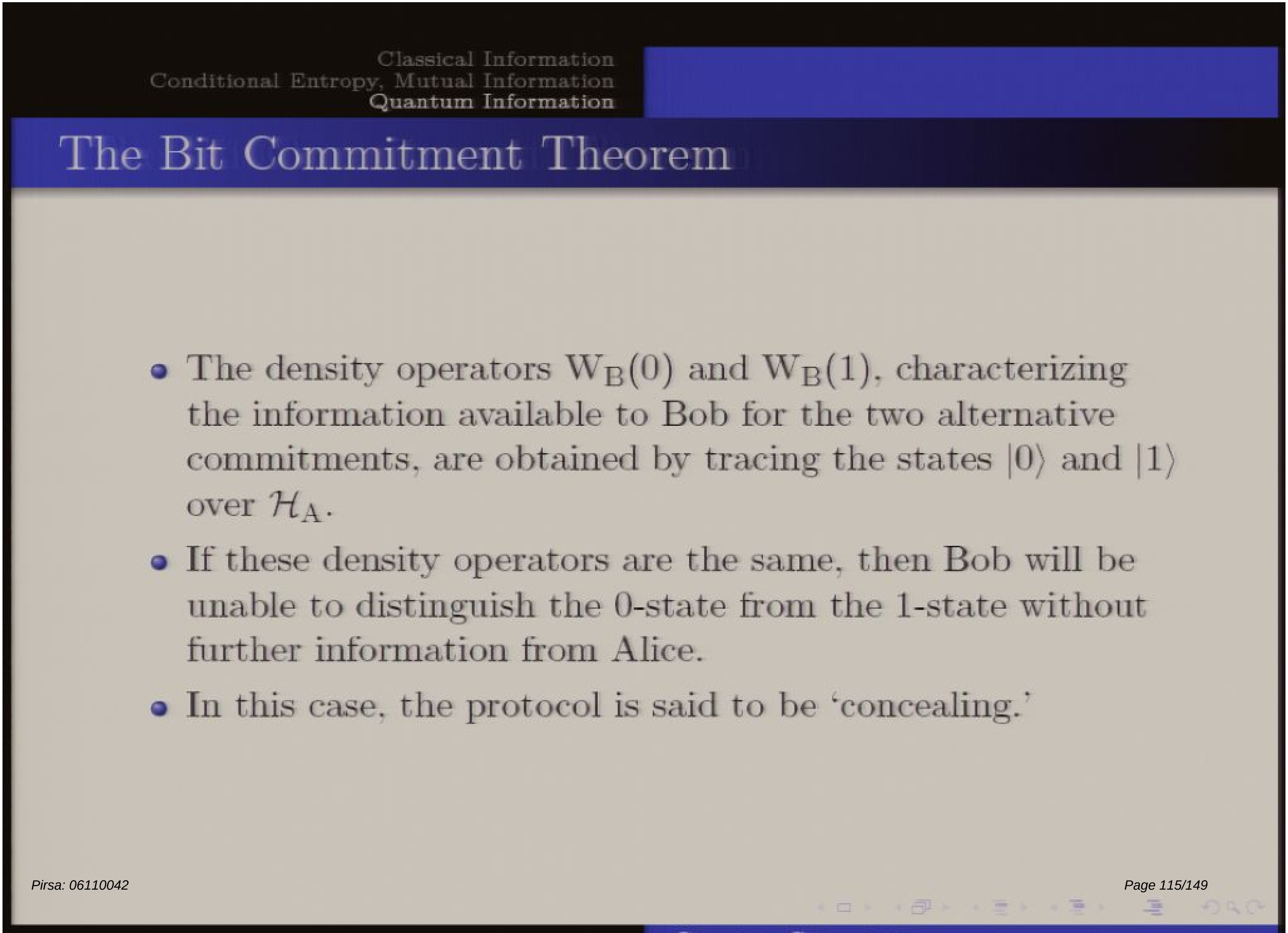
$$|d_X\rangle|p_2\rangle|\phi\rangle|q_0\rangle \xrightarrow{U_C} |d_X\rangle|p_2\rangle \otimes U_Y|\phi\rangle|q_0\rangle$$

$$|d_Y\rangle|p_1\rangle|\phi\rangle|q_0\rangle \xrightarrow{U_C} |d_Y\rangle|p_1\rangle \otimes U_1|\phi\rangle|q_0\rangle$$

$$|d_Y\rangle|p_2\rangle|\phi\rangle|q_0\rangle \xrightarrow{U_C} |d_Y\rangle|p_2\rangle \otimes U_2|\phi\rangle|q_0\rangle$$

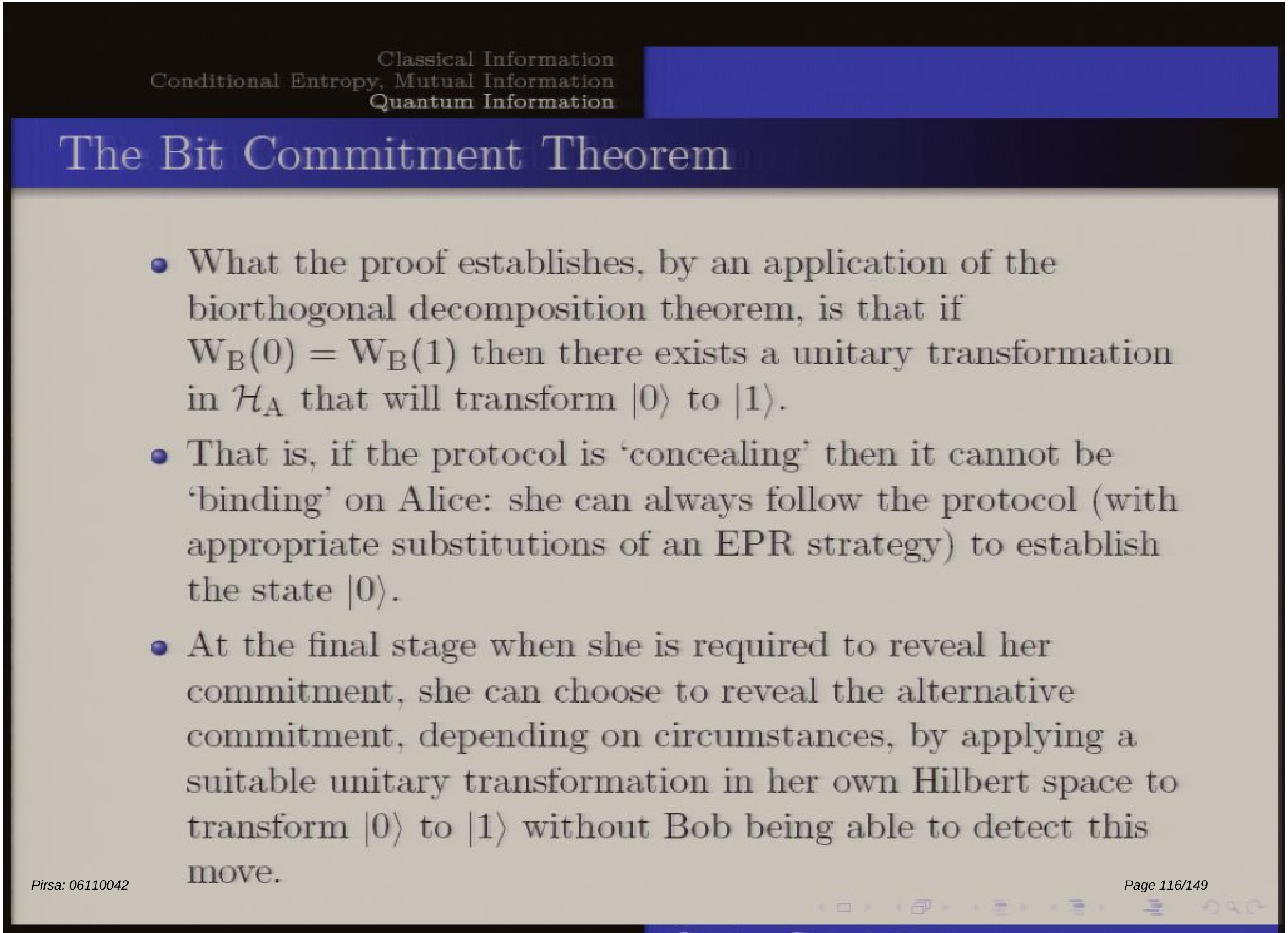
The Bit Commitment Theorem

Since an EPR cheating strategy can always be applied without detection, the proof of the quantum bit commitment theorem assumes that at the end of the commitment stage the composite system consisting of Alice's ancillas, the n channel particles, and Bob's ancillas will be represented by some composite entangled state $|0\rangle$ or $|1\rangle$, depending on whether Alice intends to reveal 0 or 1 on a Hilbert space $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$, where $\mathcal{H}_{\mathrm{A}}$ is the Hilbert space of the particles in Alice's possession at that stage (Alice's ancillas and the channel particles retained by Alice, if any), and $\mathcal{H}_{\mathrm{B}}$ is the Hilbert space of the particles in Bob's possession at that stage (Bob's ancillas and the channel particles retained by Bob, if any).



The Bit Commitment Theorem

- The density operators $\mathrm{W_B}(0)$ and $\mathrm{W_B}(1)$, characterizing the information available to Bob for the two alternative commitments, are obtained by tracing the states $|0\rangle$ and $|1\rangle$ over $\mathcal{H}_{\mathrm{A}}$.
- If these density operators are the same, then Bob will be unable to distinguish the 0-state from the 1-state without further information from Alice.
- In this case, the protocol is said to be 'concealing.'



The Bit Commitment Theorem

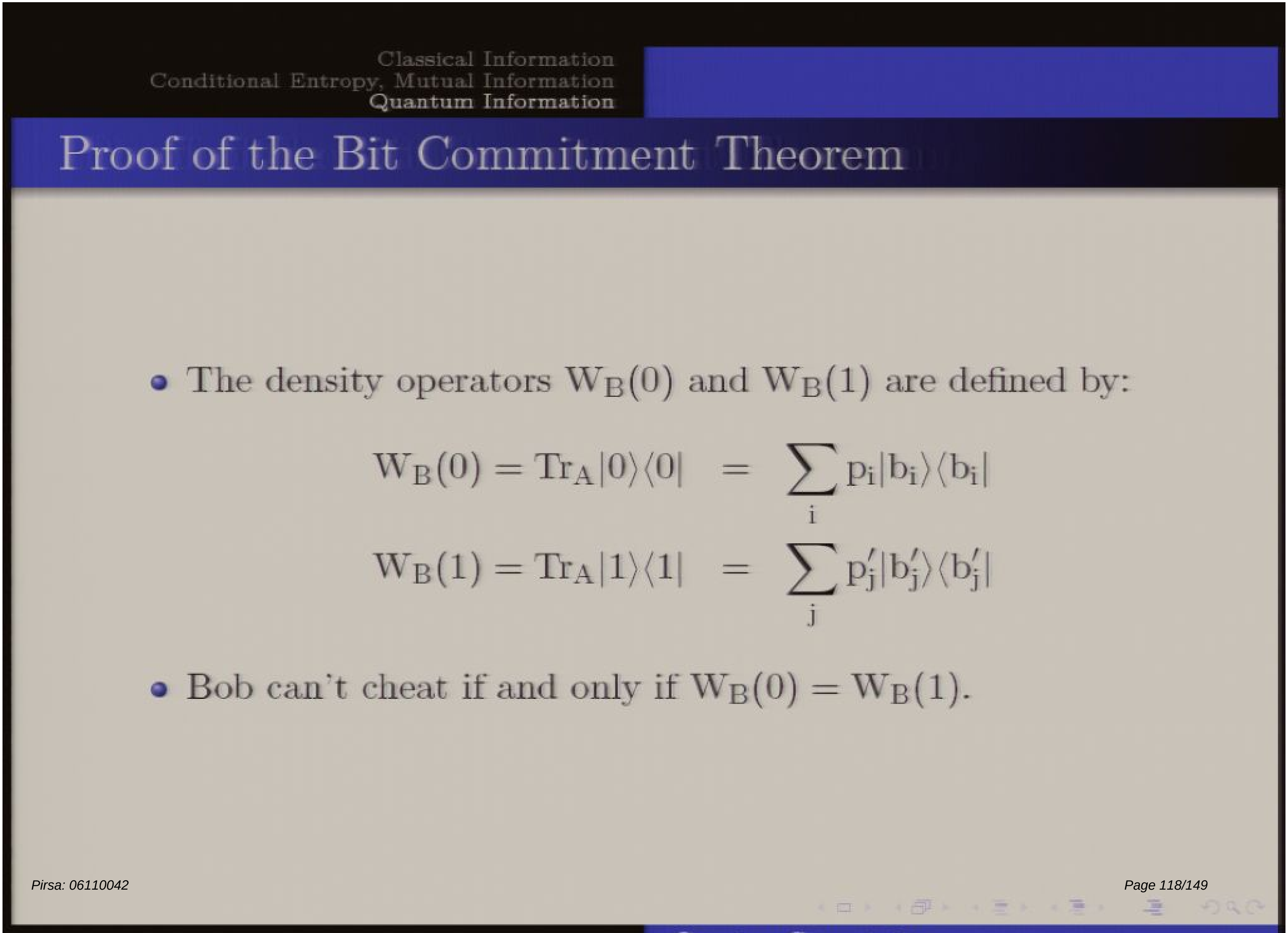
- What the proof establishes, by an application of the biorthogonal decomposition theorem, is that if $\mathrm{W_B}(0) = \mathrm{W_B}(1)$ then there exists a unitary transformation in $\mathcal{H}_\mathrm{A}$ that will transform $|0\rangle$ to $|1\rangle$.
- That is, if the protocol is 'concealing' then it cannot be 'binding' on Alice: she can always follow the protocol (with appropriate substitutions of an EPR strategy) to establish the state $|0\rangle$.
- At the final stage when she is required to reveal her commitment, she can choose to reveal the alternative commitment, depending on circumstances, by applying a suitable unitary transformation in her own Hilbert space to transform $|0\rangle$ to $|1\rangle$ without Bob being able to detect this move.

Proof of the Bit Commitment Theorem

In the Schmidt decomposition, the states $|0\rangle$ and $|1\rangle$ can be expressed as:

$$
\begin{aligned}
|0\rangle &= \sum_{i} \sqrt{p_i}|a_i\rangle|b_i\rangle \\
|1\rangle &= \sum_{j} \sqrt{p_j'}|a_j'\rangle|b_j'\rangle
\end{aligned}
$$

where $\{|a_i\rangle\}, \{|a_j'\rangle\}$ are two orthonormal sets of states in $\mathcal{H}_A$, and $\{|b_i\rangle\}, \{|b_j'\rangle\}$ are two orthonormal sets in $\mathcal{H}_B$.



Proof of the Bit Commitment Theorem

- The density operators $W_B(0)$ and $W_B(1)$ are defined by:

$$\begin{aligned} W_B(0) = \mathrm{Tr}_A|0\rangle\langle 0| &= \sum_i p_i|b_i\rangle\langle b_i| \\ W_B(1) = \mathrm{Tr}_A|1\rangle\langle 1| &= \sum_j p'_j|b'_j\rangle\langle b'_j| \end{aligned}$$

- Bob can't cheat if and only if $W_B(0) = W_B(1)$.

The Bit Commitment Theorem

- By the spectral theorem, the decompositions:

$$\begin{aligned} W_B(0) &= \sum_i p_i |b_i\rangle\langle b_i| \\ W_B(1) &= \sum_j p'_j |b'_j\rangle\langle b'_j| \end{aligned}$$

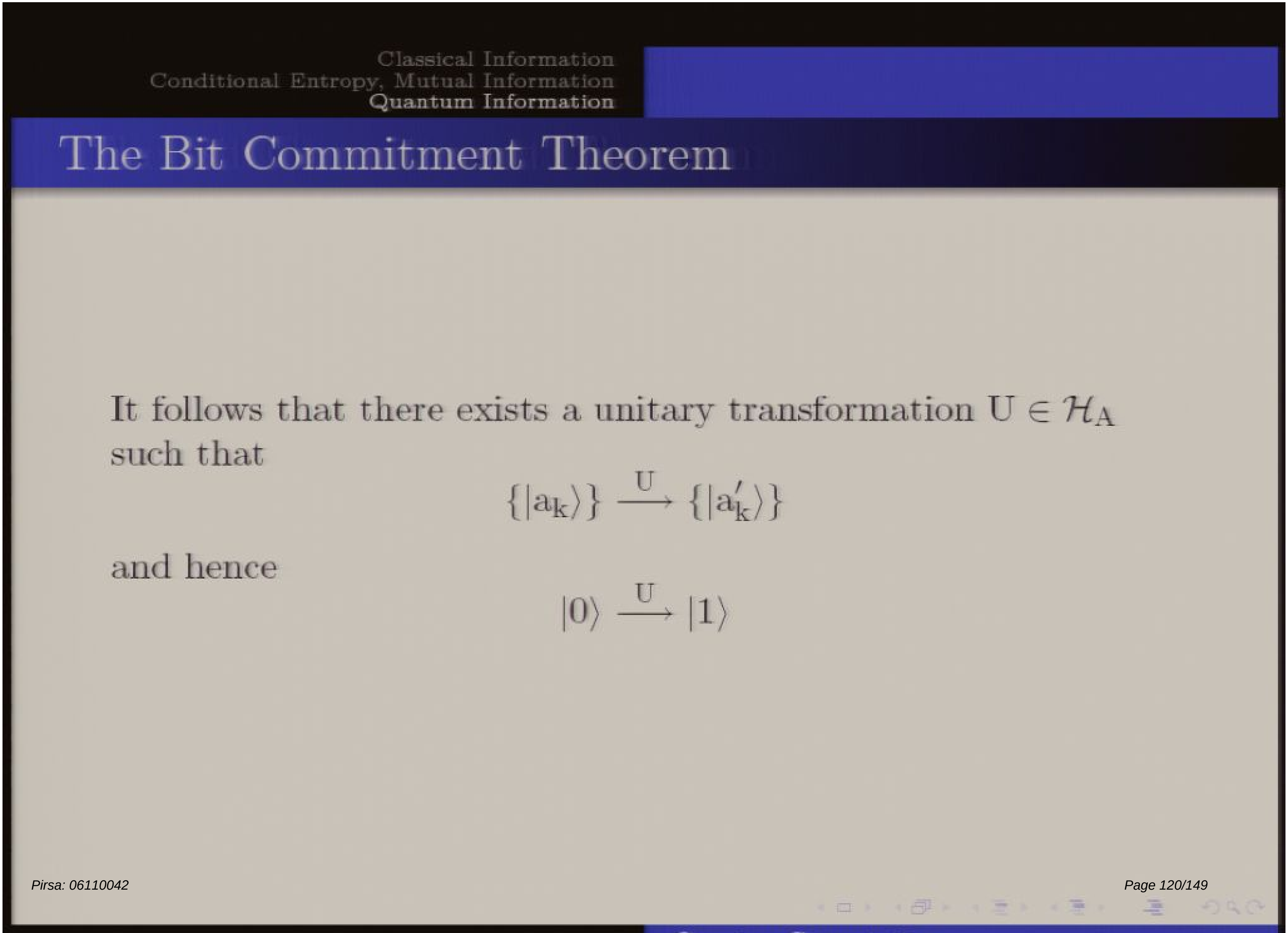
  are unique for the nondegenerate case, where the p_i are all distinct and the p'_j are all distinct.

- The condition $W_B(0) = W_B(1)$ implies that for all k:

$$\begin{aligned} p_i &= p'_i \\ |b_i\rangle &= |b'_i\rangle \end{aligned}$$

  and so

$$|0\rangle = \sum_i \sqrt{p_i} |a_i\rangle |b_i\rangle$$



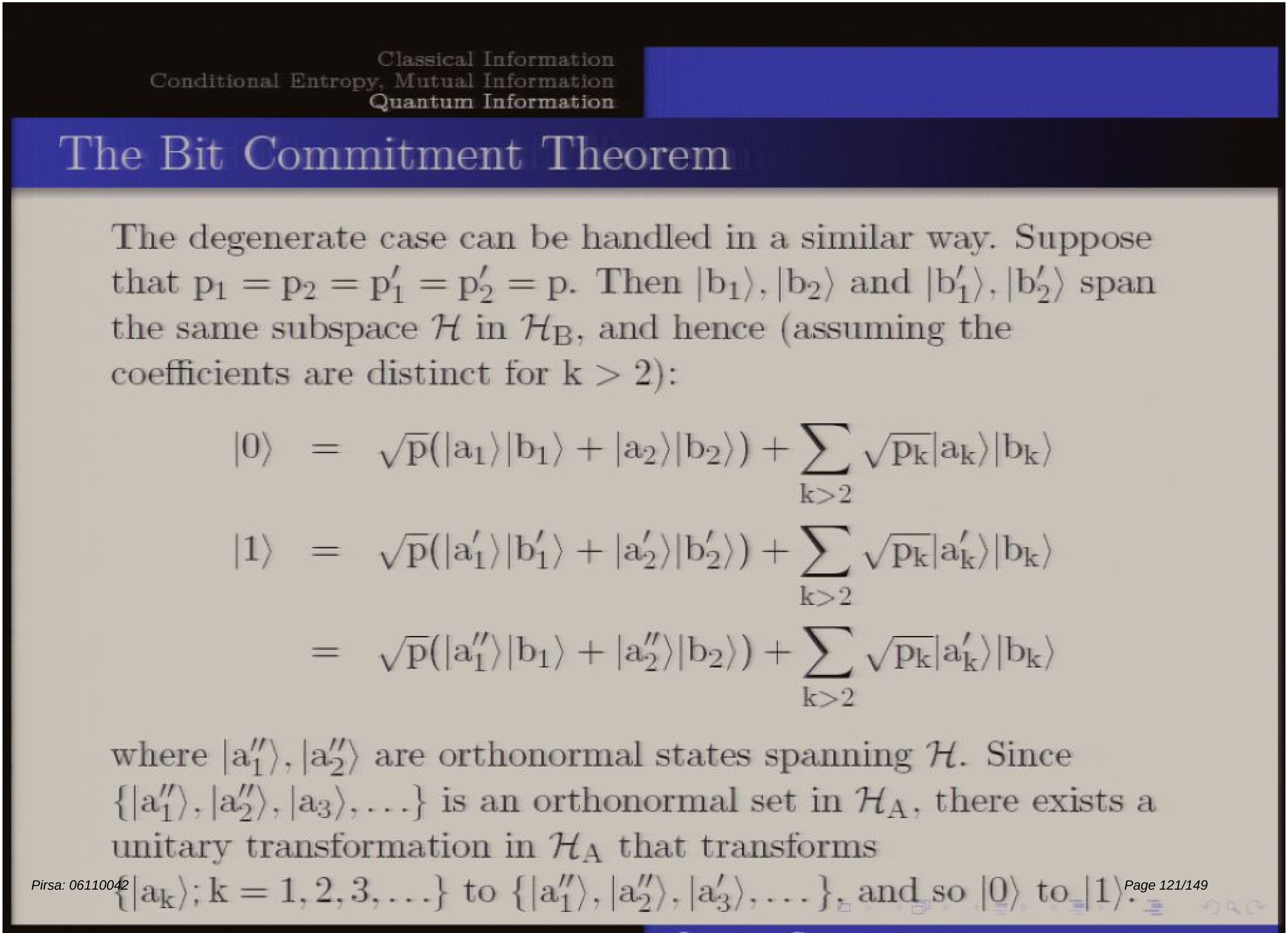
The Bit Commitment Theorem

It follows that there exists a unitary transformation $\mathrm{U} \in \mathcal{H}_\mathrm{A}$ such that

$$\{|\mathrm{a_k}\rangle\} \xrightarrow{\mathrm{U}} \{|\mathrm{a'_k}\rangle\}$$

and hence

$$|0\rangle \xrightarrow{\mathrm{U}} |1\rangle$$



The Bit Commitment Theorem

The degenerate case can be handled in a similar way. Suppose that $p_1 = p_2 = p'_1 = p'_2 = p$. Then $|b_1\rangle, |b_2\rangle$ and $|b'_1\rangle, |b'_2\rangle$ span the same subspace $\mathcal{H}$ in $\mathcal{H}_B$, and hence (assuming the coefficients are distinct for $k > 2$):

$$\begin{aligned}
|0\rangle &= \sqrt{p}(|a_1\rangle|b_1\rangle + |a_2\rangle|b_2\rangle) + \sum_{k>2} \sqrt{p_k}|a_k\rangle|b_k\rangle \\
|1\rangle &= \sqrt{p}(|a'_1\rangle|b'_1\rangle + |a'_2\rangle|b'_2\rangle) + \sum_{k>2} \sqrt{p_k}|a'_k\rangle|b_k\rangle \\
&= \sqrt{p}(|a''_1\rangle|b_1\rangle + |a''_2\rangle|b_2\rangle) + \sum_{k>2} \sqrt{p_k}|a'_k\rangle|b_k\rangle
\end{aligned}$$

where $|a''_1\rangle, |a''_2\rangle$ are orthonormal states spanning $\mathcal{H}$. Since $\{|a''_1\rangle, |a''_2\rangle, |a_3\rangle, \ldots\}$ is an orthonormal set in $\mathcal{H}_A$, there exists a unitary transformation in $\mathcal{H}_A$ that transforms $\{|a_k\rangle; k = 1, 2, 3, \ldots\}$ to $\{|a''_1\rangle, |a''_2\rangle, |a'_3\rangle, \ldots\}$, and so $|0\rangle$ to $|1\rangle$.

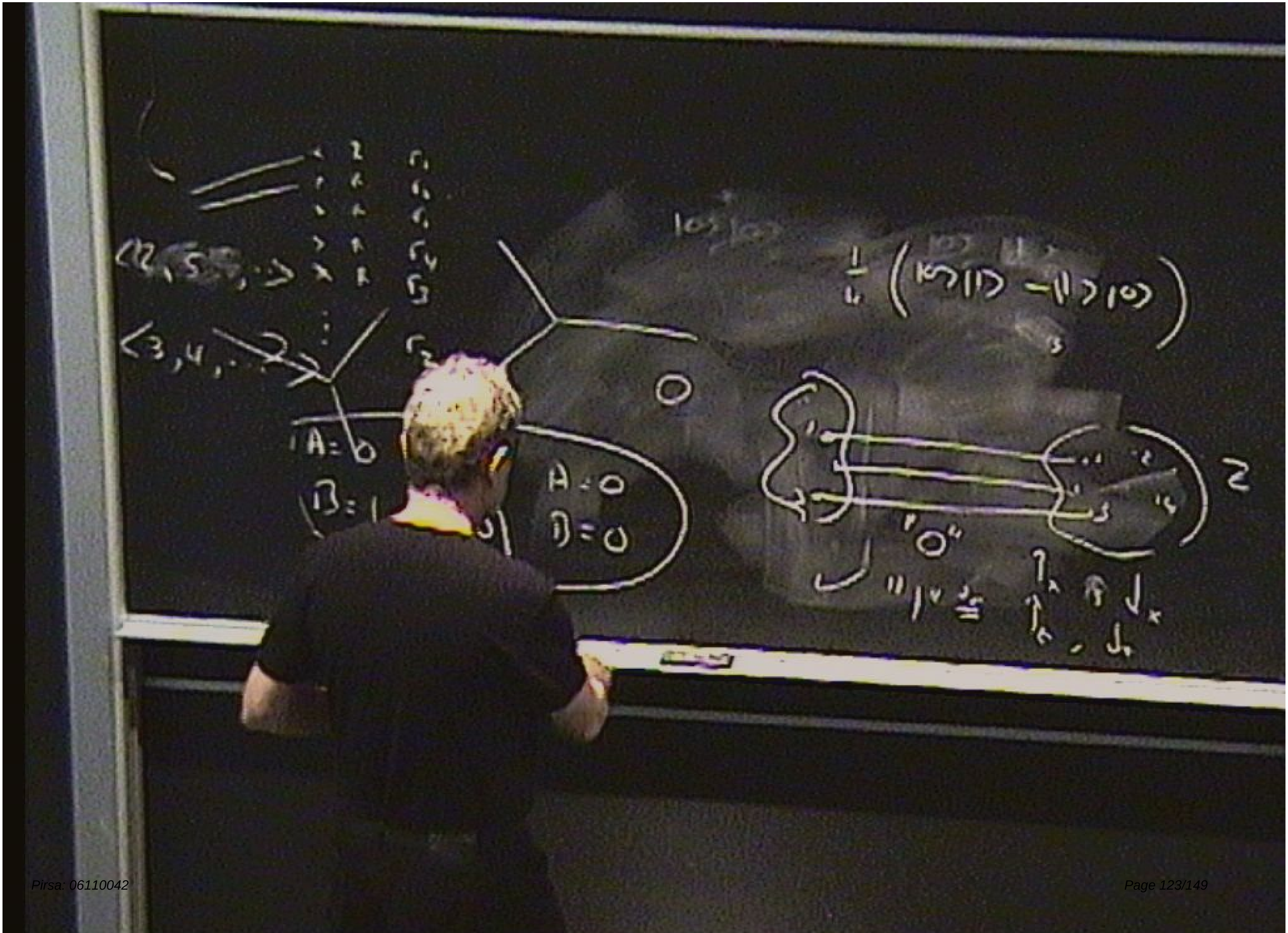
An Illuminating Example

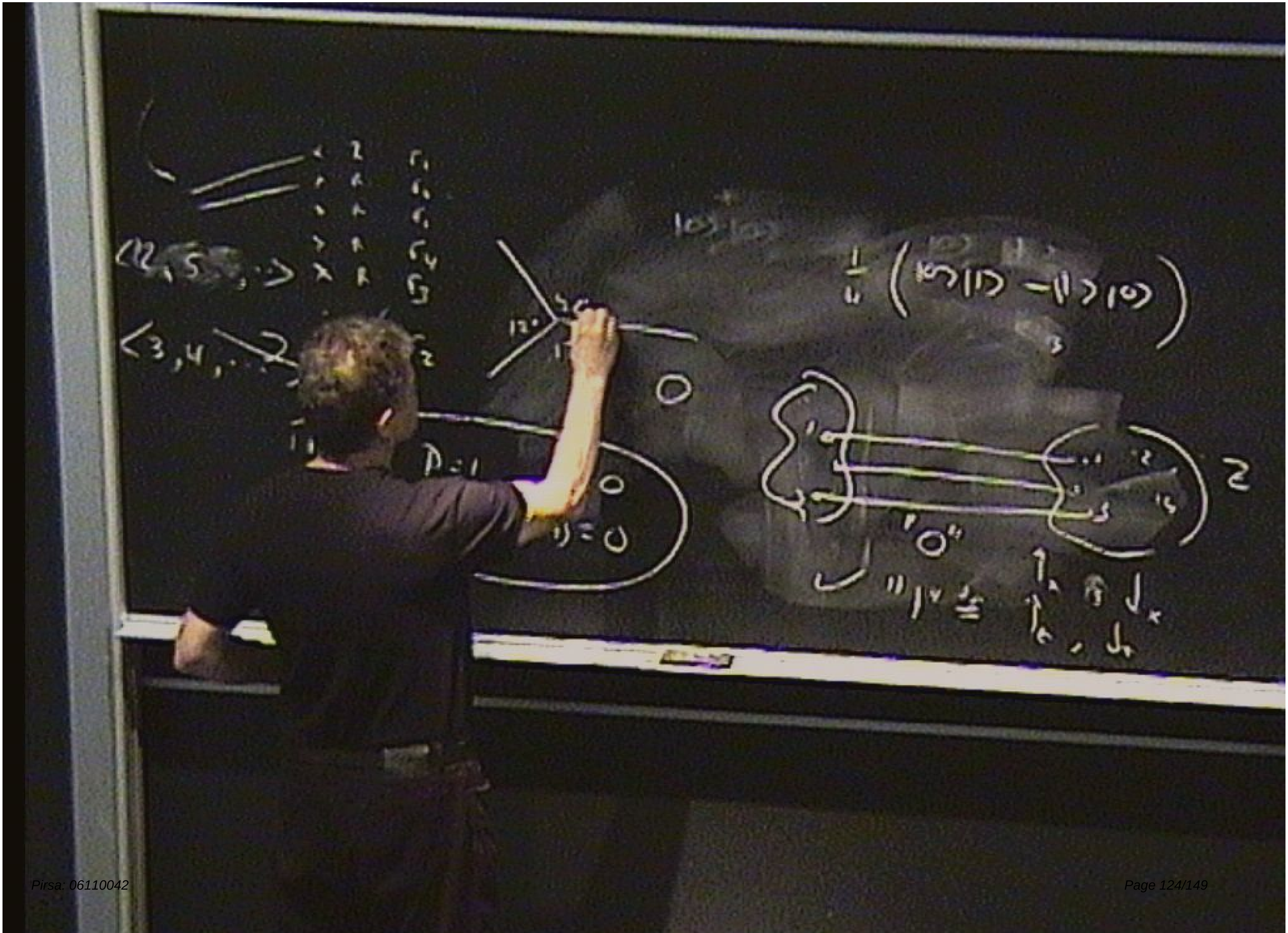
- Suppose Alice is required to send Bob a channel particle C in an equal weight mixture of the qubit states:

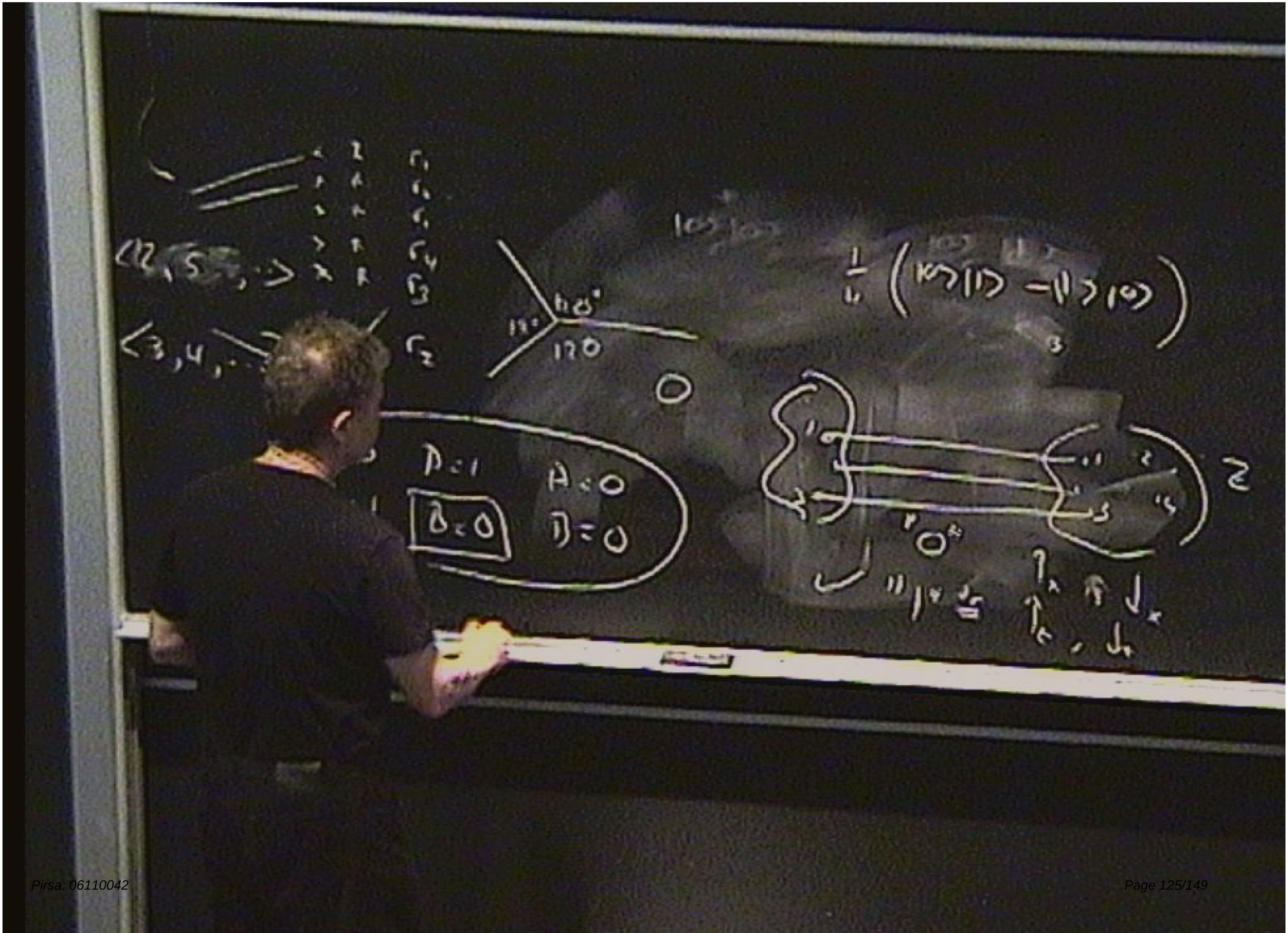
$$\begin{aligned} |c_0\rangle &= |0\rangle \\ |c_2\rangle &= -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ |c_4\rangle &= -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \end{aligned}$$

if she commits to 0, and an equal weight mixture of the qubit states:

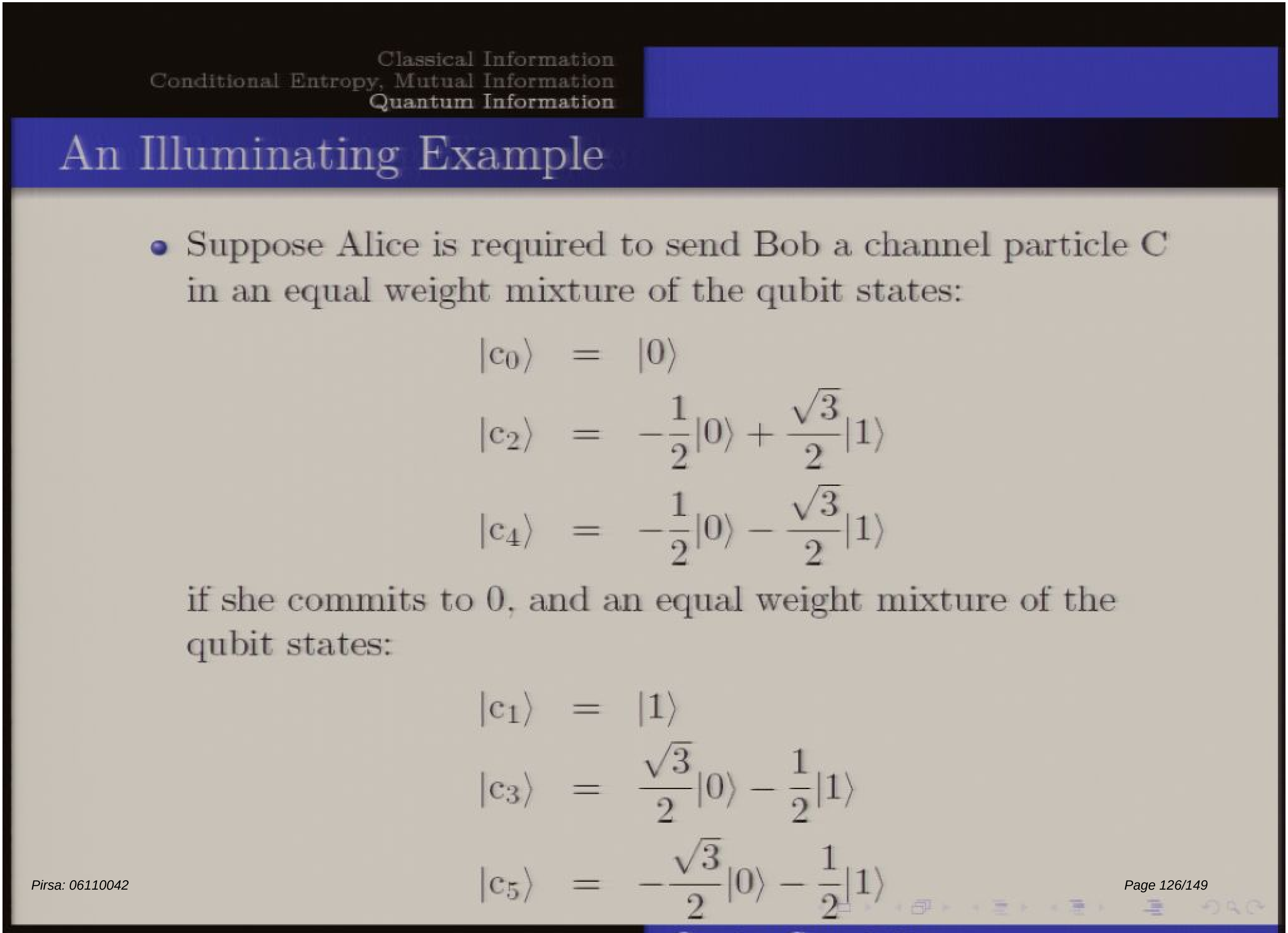
$$\begin{aligned} |c_1\rangle &= |1\rangle \\ |c_3\rangle &= \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \\ |c_5\rangle &= -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \end{aligned}$$


⟨3,4,...⟩
A=0
B=1
A=0
B=0
0
1/√2 (|0⟩|1⟩ − |1⟩|0⟩)
Z
"0"
"1" ≐ ↑x ⊗ ↓x
↑z , ↓z


1/4 (|0⟩|1⟩ − |1⟩|0⟩)
Z
"O"
D=1
O
<3, 4, …>



<2,5,...>
<3,4,...>
G1
G2
G3
G4
G5
120°
120
120
0
$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$
3
P=1
$\boxed{B=0}$
A=0
B=0
1
2
3
4
Z



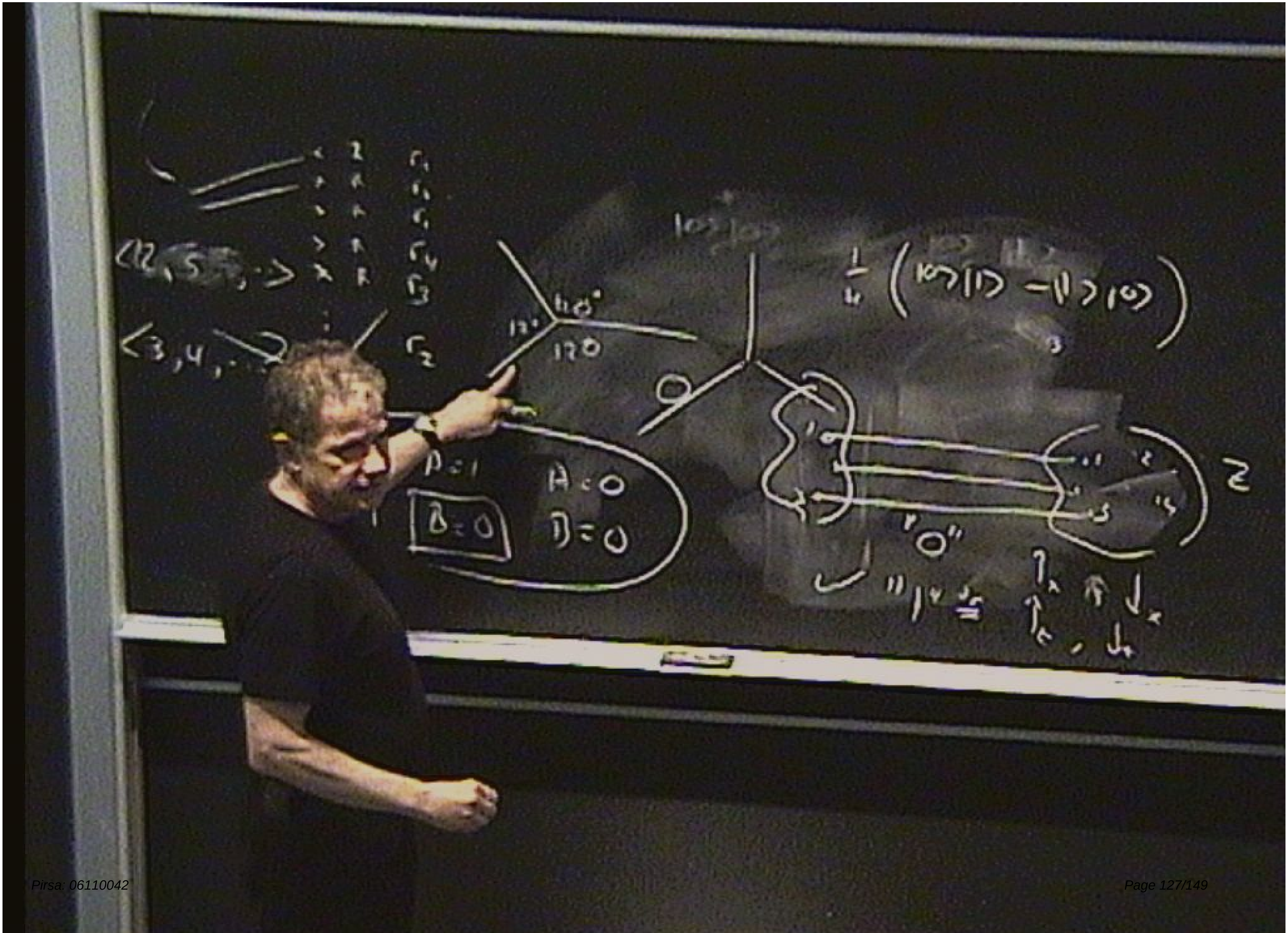
An Illuminating Example

- Suppose Alice is required to send Bob a channel particle C in an equal weight mixture of the qubit states:

$$\begin{aligned} |c_0\rangle &= |0\rangle \\ |c_2\rangle &= -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ |c_4\rangle &= -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \end{aligned}$$

if she commits to 0, and an equal weight mixture of the qubit states:

$$\begin{aligned} |c_1\rangle &= |1\rangle \\ |c_3\rangle &= \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \\ |c_5\rangle &= -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \end{aligned}$$



120°
120°
120
1/√2 (|0⟩|1⟩ − |1⟩|0⟩)
A=0
B=0
B=0
"0"
Z

An Illuminating Example

- Suppose Alice is required to send Bob a channel particle C in an equal weight mixture of the qubit states:

$$\begin{aligned}|c_0\rangle &= |0\rangle\\ |c_2\rangle &= -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\\ |c_4\rangle &= -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\end{aligned}$$

if she commits to 0, and an equal weight mixture of the qubit states:

$$\begin{aligned}|c_1\rangle &= |1\rangle\\ |c_3\rangle &= \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\\ |c_5\rangle &= -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\end{aligned}$$

An Illuminating Example

- Suppose Alice tries to implement an EPR cheating strategy by preparing the entangled state of a system AC:

$$|0\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4\rangle|\mathrm{c}_4\rangle)$$

  where $\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\}$ is an orthonormal basis in the 3-dimensional Hilbert space $\mathcal{H}^{\mathrm{A}}$ of a suitable ancilla system A.

- If Alice could transform the state $|0\rangle$ to the state:

$$|1\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle)$$

  where $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ is another orthonormal basis in $\mathcal{H}^{\mathrm{A}}$, by a local unitary transformation in $\mathcal{H}^{\mathrm{A}}$, she could delay her commitment to the opening stage.

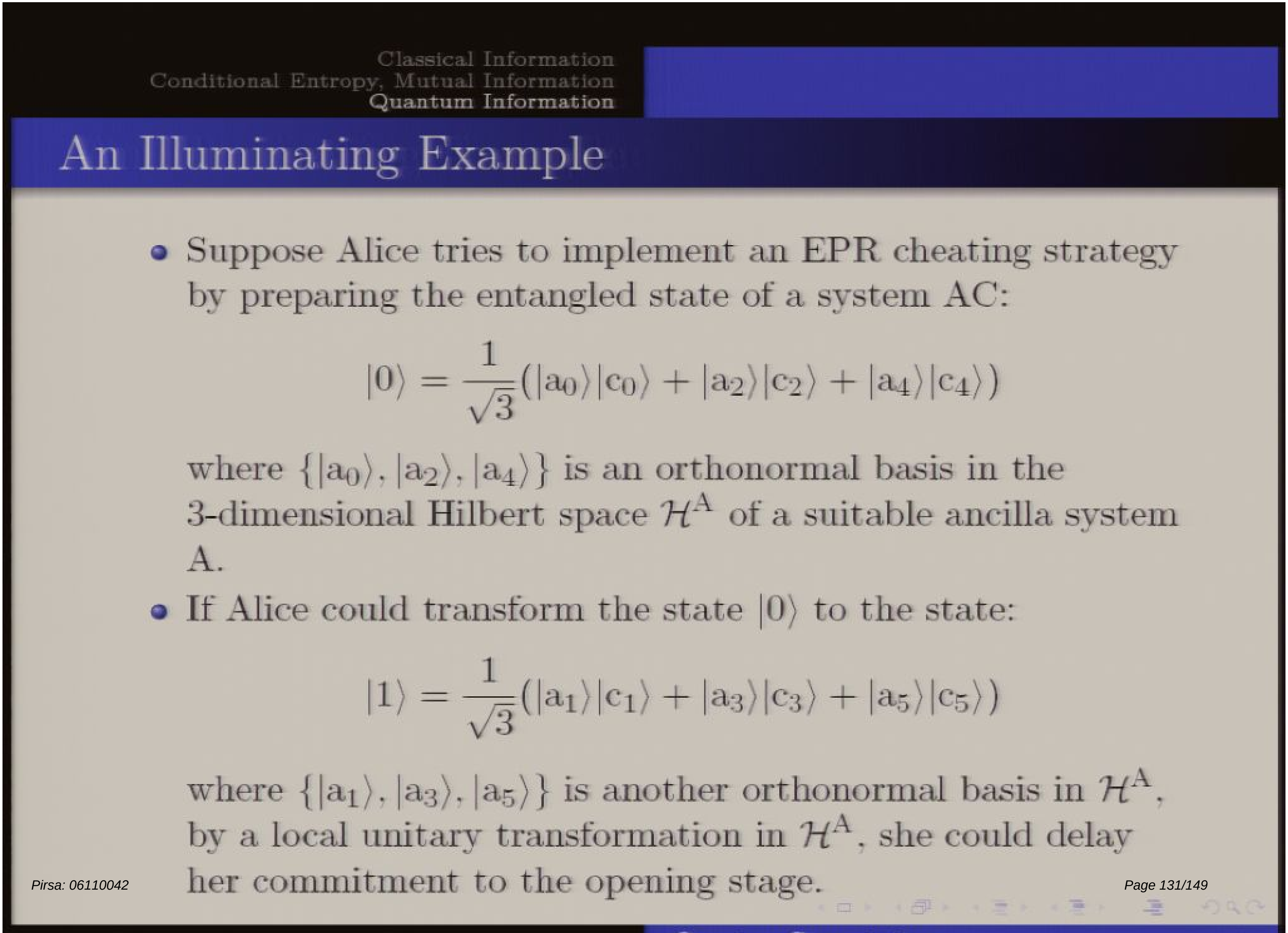
An Illuminating Example

- Suppose Alice is required to send Bob a channel particle C in an equal weight mixture of the qubit states:

$$\begin{aligned} |c_0\rangle &= |0\rangle \\ |c_2\rangle &= -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \\ |c_4\rangle &= -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \end{aligned}$$

if she commits to 0, and an equal weight mixture of the qubit states:

$$\begin{aligned} |c_1\rangle &= |1\rangle \\ |c_3\rangle &= \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \\ |c_5\rangle &= -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \end{aligned}$$



An Illuminating Example

- Suppose Alice tries to implement an EPR cheating strategy by preparing the entangled state of a system AC:

$$|0\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4\rangle|\mathrm{c}_4\rangle)$$

  where $\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\}$ is an orthonormal basis in the 3-dimensional Hilbert space $\mathcal{H}^{\mathrm{A}}$ of a suitable ancilla system A.

- If Alice could transform the state $|0\rangle$ to the state:

$$|1\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle)$$

  where $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ is another orthonormal basis in $\mathcal{H}^{\mathrm{A}}$, by a local unitary transformation in $\mathcal{H}^{\mathrm{A}}$, she could delay her commitment to the opening stage.

An Illuminating Example

- If, at that stage, she decides to commit to 0, she measures the observable with eigenstates $\{|a_0\rangle, |a_2\rangle, |a_4\rangle\}$. If she decides to commit to 1, she performs the local unitary transformation taking the state $|0\rangle$ to the state $|1\rangle$ and measures the observable with eigenstates $\{|a_1\rangle, |a_3\rangle, |a_5\rangle\}$.

An Illuminating Example

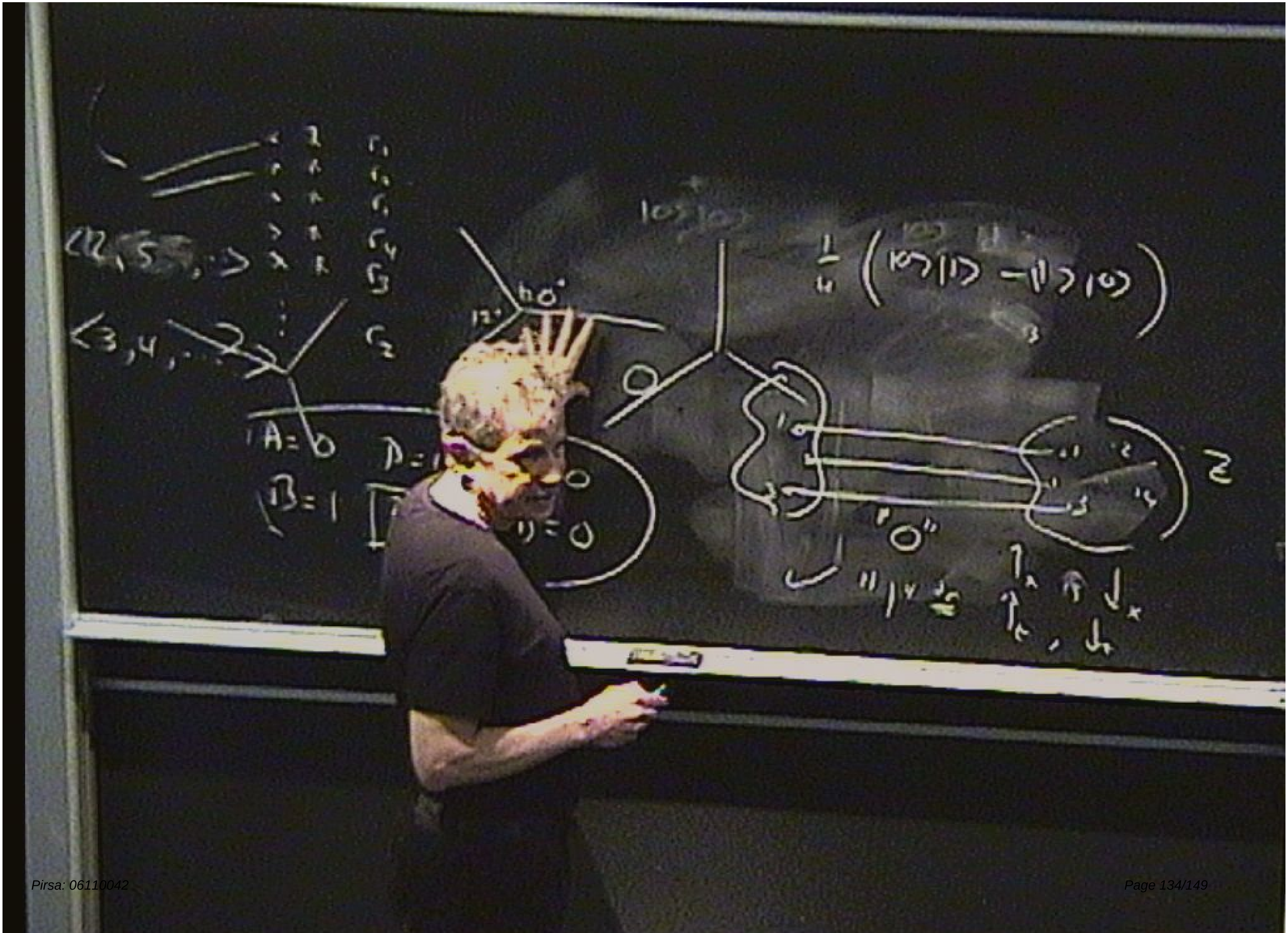
- Now, $|0\rangle$ can be expressed as:

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{3}}\left(|\mathrm{a}_0\rangle\frac{|\mathrm{c}_3\rangle-|\mathrm{c}_5\rangle}{\sqrt{3}}+|\mathrm{a}_2\rangle\frac{|\mathrm{c}_1\rangle-|\mathrm{c}_3\rangle}{\sqrt{3}}+|\mathrm{a}_4\rangle\frac{|\mathrm{c}_5\rangle-|\mathrm{c}_1\rangle}{\sqrt{3}}\right) \\ &= \frac{1}{\sqrt{3}}\left(\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}|\mathrm{c}_1\rangle+\frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}|\mathrm{c}_3\rangle+\frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}|\mathrm{c}_5\rangle\right) \end{aligned}$$

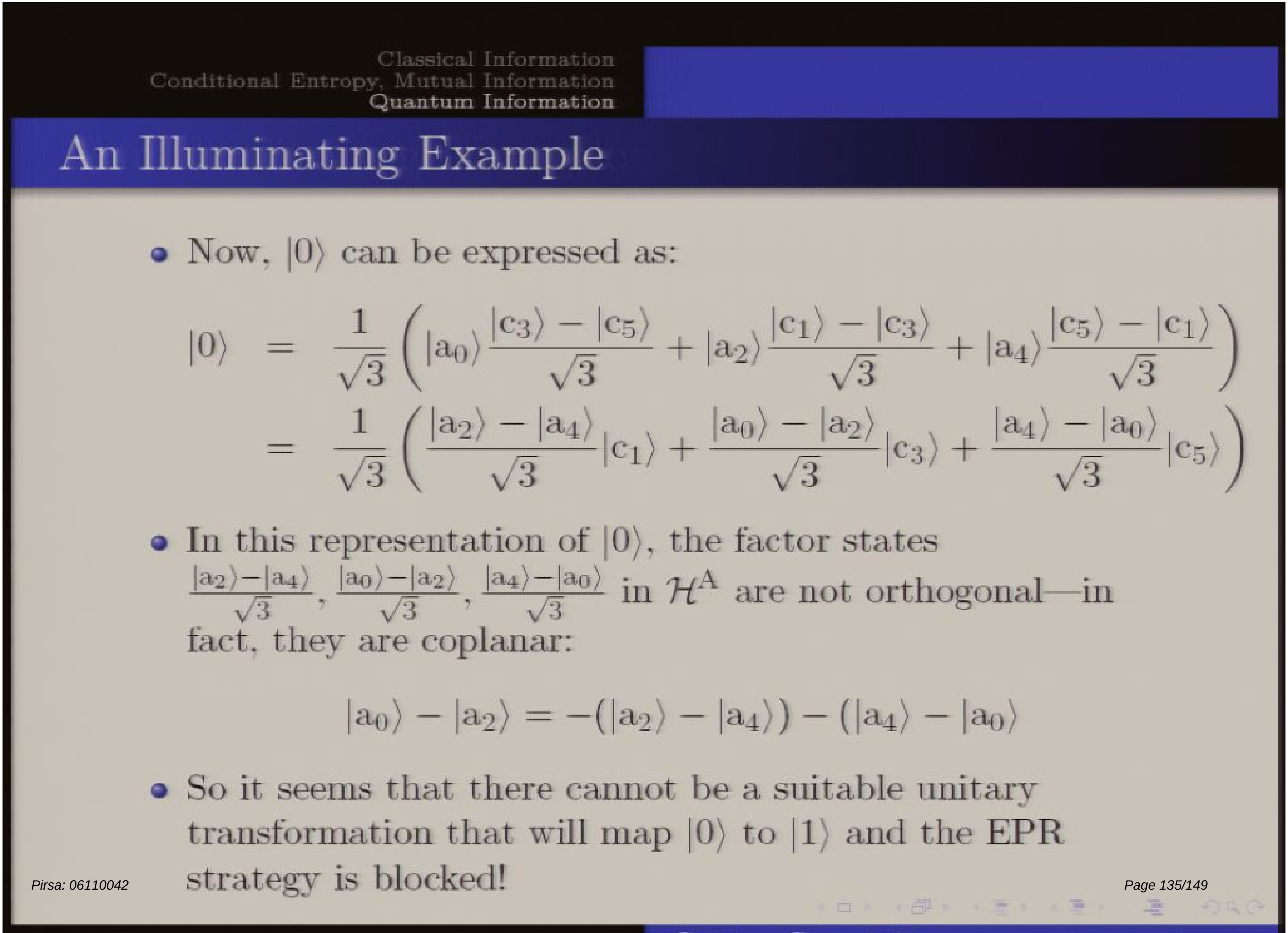
- In this representation of $|0\rangle$, the factor states $\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}$ in $\mathcal{H}^{\mathrm{A}}$ are not orthogonal—in fact, they are coplanar:

$$|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle=-(|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle)-(|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle)$$

- So it seems that there cannot be a suitable unitary transformation that will map $|0\rangle$ to $|1\rangle$ and the EPR strategy is blocked!



⟨2,5,...⟩
⟨3,4,...⟩
A=0
B=1
B=1
1/4 (|0⟩|1⟩ − |1⟩|0⟩)
"0"
Z



An Illuminating Example

- Now, $|0\rangle$ can be expressed as:

$$\begin{aligned}|0\rangle &= \frac{1}{\sqrt{3}}\left(|\mathrm{a}_0\rangle\frac{|\mathrm{c}_3\rangle-|\mathrm{c}_5\rangle}{\sqrt{3}}+|\mathrm{a}_2\rangle\frac{|\mathrm{c}_1\rangle-|\mathrm{c}_3\rangle}{\sqrt{3}}+|\mathrm{a}_4\rangle\frac{|\mathrm{c}_5\rangle-|\mathrm{c}_1\rangle}{\sqrt{3}}\right)\\ &= \frac{1}{\sqrt{3}}\left(\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}|\mathrm{c}_1\rangle+\frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}|\mathrm{c}_3\rangle+\frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}|\mathrm{c}_5\rangle\right)\end{aligned}$$

- In this representation of $|0\rangle$, the factor states $\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}$ in $\mathcal{H}^{\mathrm{A}}$ are not orthogonal—in fact, they are coplanar:

$$|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle = -(|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle)-(|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle)$$

- So it seems that there cannot be a suitable unitary transformation that will map $|0\rangle$ to $|1\rangle$ and the EPR strategy is blocked!

An Illuminating Example

- Suppose Alice tries to implement an EPR cheating strategy by preparing the entangled state of a system AC:

$$|0\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4\rangle|\mathrm{c}_4\rangle)$$

  where $\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\}$ is an orthonormal basis in the 3-dimensional Hilbert space $\mathcal{H}^{\mathrm{A}}$ of a suitable ancilla system A.

- If Alice could transform the state $|0\rangle$ to the state:

$$|1\rangle = \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle)$$

  where $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ is another orthonormal basis in $\mathcal{H}^{\mathrm{A}}$, by a local unitary transformation in $\mathcal{H}^{\mathrm{A}}$, she could delay her commitment to the opening stage.

An Illuminating Example

- Now, $|0\rangle$ can be expressed as:

$$
\begin{aligned}
|0\rangle &= \frac{1}{\sqrt{3}}\left(|\mathrm{a}_0\rangle\frac{|\mathrm{c}_3\rangle-|\mathrm{c}_5\rangle}{\sqrt{3}}+|\mathrm{a}_2\rangle\frac{|\mathrm{c}_1\rangle-|\mathrm{c}_3\rangle}{\sqrt{3}}+|\mathrm{a}_4\rangle\frac{|\mathrm{c}_5\rangle-|\mathrm{c}_1\rangle}{\sqrt{3}}\right)\\
&= \frac{1}{\sqrt{3}}\left(\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}|\mathrm{c}_1\rangle+\frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}|\mathrm{c}_3\rangle+\frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}|\mathrm{c}_5\rangle\right)
\end{aligned}
$$

- In this representation of $|0\rangle$, the factor states $\frac{|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle}{\sqrt{3}}, \frac{|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle}{\sqrt{3}}$ in $\mathcal{H}^{\mathrm{A}}$ are not orthogonal—in fact, they are coplanar:

$$|\mathrm{a}_0\rangle-|\mathrm{a}_2\rangle=-(|\mathrm{a}_2\rangle-|\mathrm{a}_4\rangle)-(|\mathrm{a}_4\rangle-|\mathrm{a}_0\rangle)$$

- So it seems that there cannot be a suitable unitary transformation that will map $|0\rangle$ to $|1\rangle$ and the EPR strategy is blocked!

An Illuminating Example

- Of course, this is not the case. To see that there is such a unitary transformation, note that $|0\rangle$ and $|1\rangle$ can be expressed in the Schmidt decomposition as:

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}\left(\frac{2|a_0\rangle - |a_2\rangle - |a_4\rangle}{\sqrt{6}}|c_0\rangle + \frac{|a_2\rangle - |a_4\rangle}{\sqrt{2}}|c_1\rangle\right) \\ |1\rangle &= \frac{1}{\sqrt{2}}\left(\frac{|a_3\rangle - |a_5\rangle}{\sqrt{2}}|c_0\rangle + \frac{-2|a_1\rangle + |a_3\rangle + |a_5\rangle}{\sqrt{6}}|c_1\rangle\right) \end{aligned}$$

An Illuminating Example

- Clearly, there exists a unitary transformation U in $\mathcal{H}^{\mathrm{A}}$ such that:

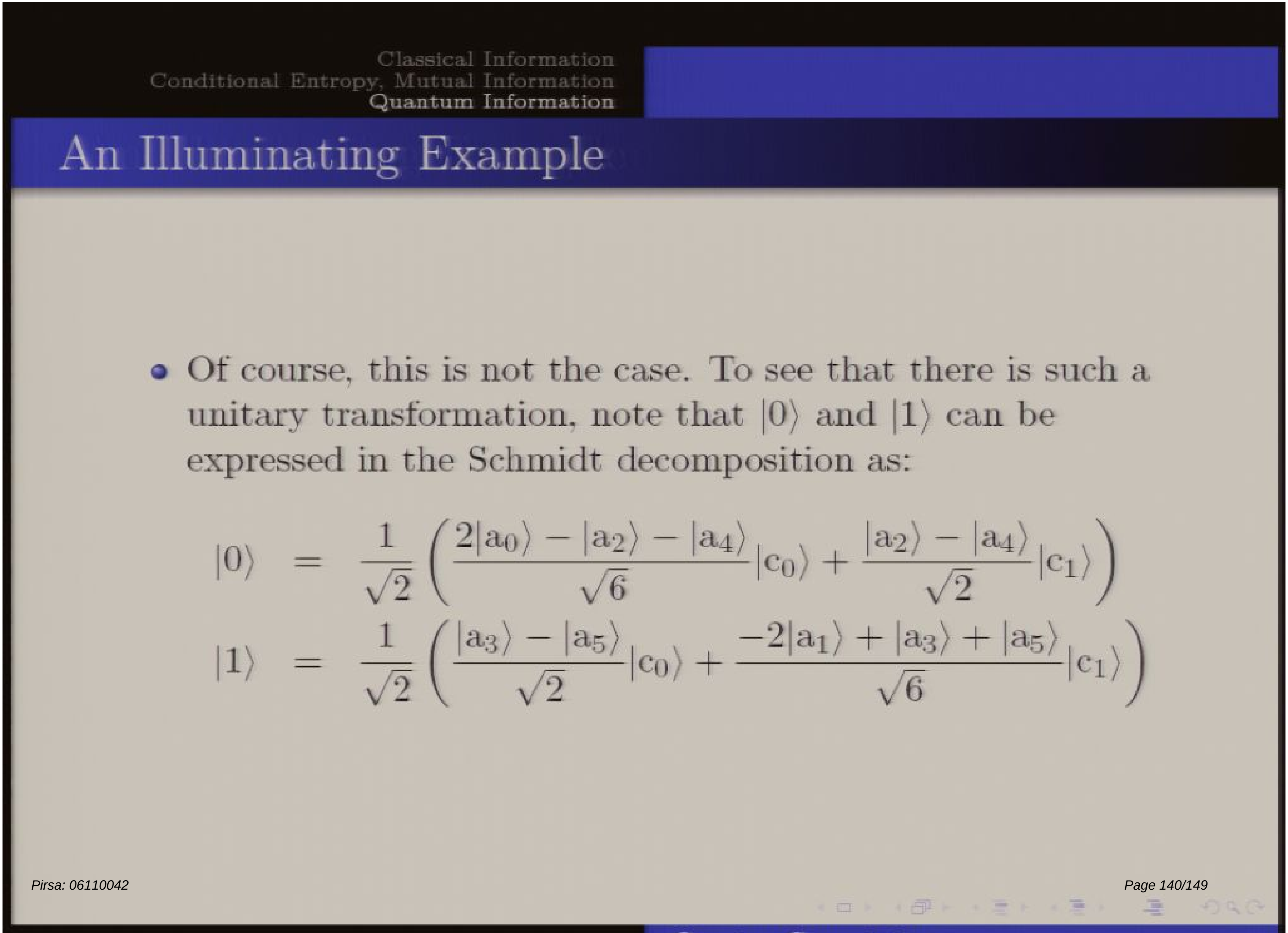
$$|0\rangle \xrightarrow{\mathrm{U}} |1\rangle$$

- It follows that:

$$\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\} \xrightarrow{\mathrm{U}} \{|\mathrm{a}_0'\rangle, |\mathrm{a}_2'\rangle, |\mathrm{a}_4'\rangle\}$$

where $\{|\mathrm{a}_0'\rangle, |\mathrm{a}_2'\rangle, |\mathrm{a}_4'\rangle\}$ is a basis in $\mathcal{H}^{\mathrm{A}}$, and so

$$\begin{aligned} |1\rangle &= \frac{1}{\sqrt{3}}(|\mathrm{a}_0'\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2'\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4'\rangle|\mathrm{c}_4\rangle) \\ &= \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle) \end{aligned}$$



An Illuminating Example

- Of course, this is not the case. To see that there is such a unitary transformation, note that $|0\rangle$ and $|1\rangle$ can be expressed in the Schmidt decomposition as:

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}\left(\frac{2|\mathrm{a}_0\rangle - |\mathrm{a}_2\rangle - |\mathrm{a}_4\rangle}{\sqrt{6}}|\mathrm{c}_0\rangle + \frac{|\mathrm{a}_2\rangle - |\mathrm{a}_4\rangle}{\sqrt{2}}|\mathrm{c}_1\rangle\right) \\ |1\rangle &= \frac{1}{\sqrt{2}}\left(\frac{|\mathrm{a}_3\rangle - |\mathrm{a}_5\rangle}{\sqrt{2}}|\mathrm{c}_0\rangle + \frac{-2|\mathrm{a}_1\rangle + |\mathrm{a}_3\rangle + |\mathrm{a}_5\rangle}{\sqrt{6}}|\mathrm{c}_1\rangle\right) \end{aligned}$$

An Illuminating Example

- Clearly, there exists a unitary transformation U in $\mathcal{H}^{\mathrm{A}}$ such that:

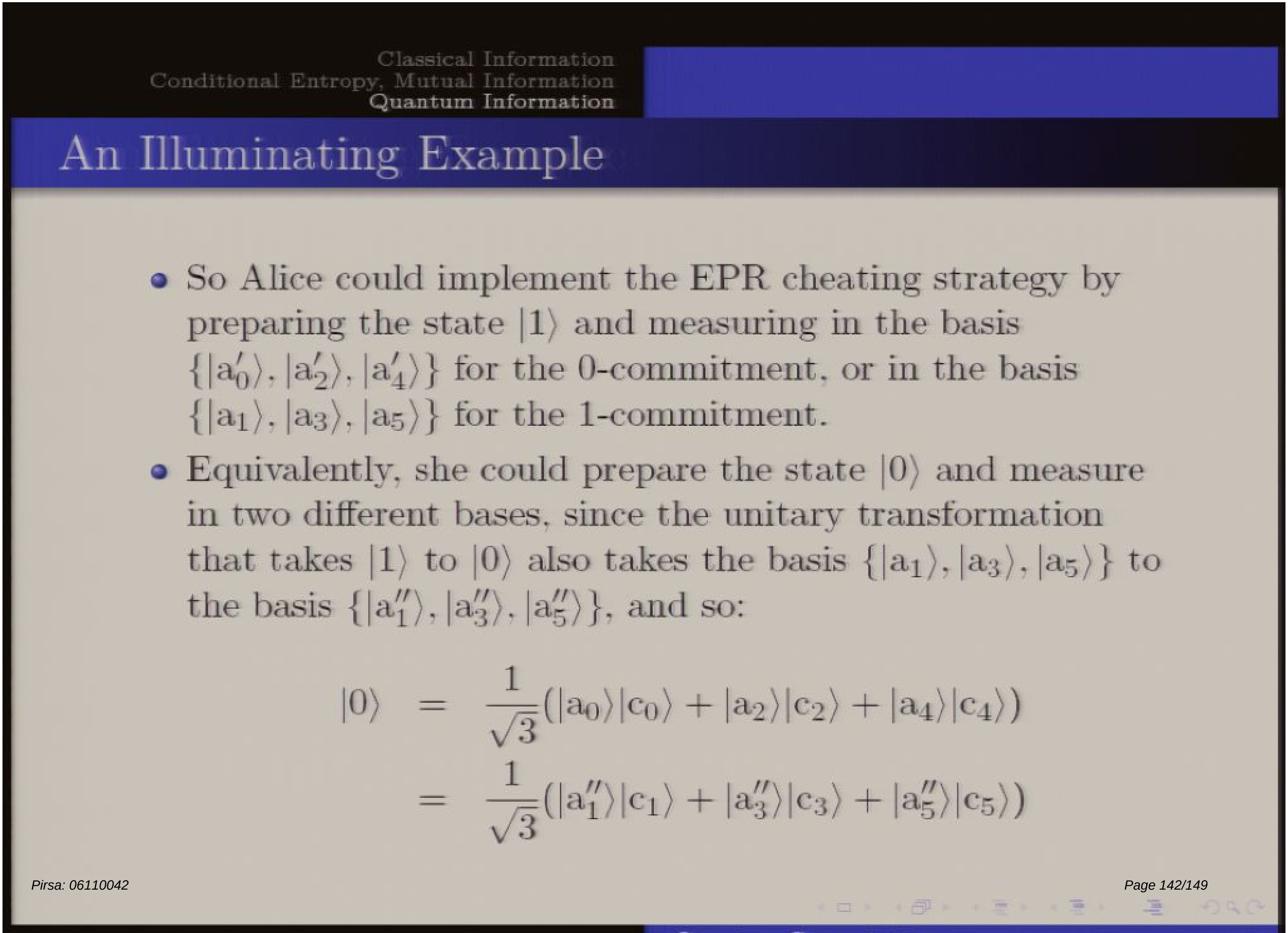
$$|0\rangle \xrightarrow{\mathrm{U}} |1\rangle$$

- It follows that:

$$\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\} \xrightarrow{\mathrm{U}} \{|\mathrm{a}'_0\rangle, |\mathrm{a}'_2\rangle, |\mathrm{a}'_4\rangle\}$$

where $\{|\mathrm{a}'_0\rangle, |\mathrm{a}'_2\rangle, |\mathrm{a}'_4\rangle\}$ is a basis in $\mathcal{H}^{\mathrm{A}}$, and so

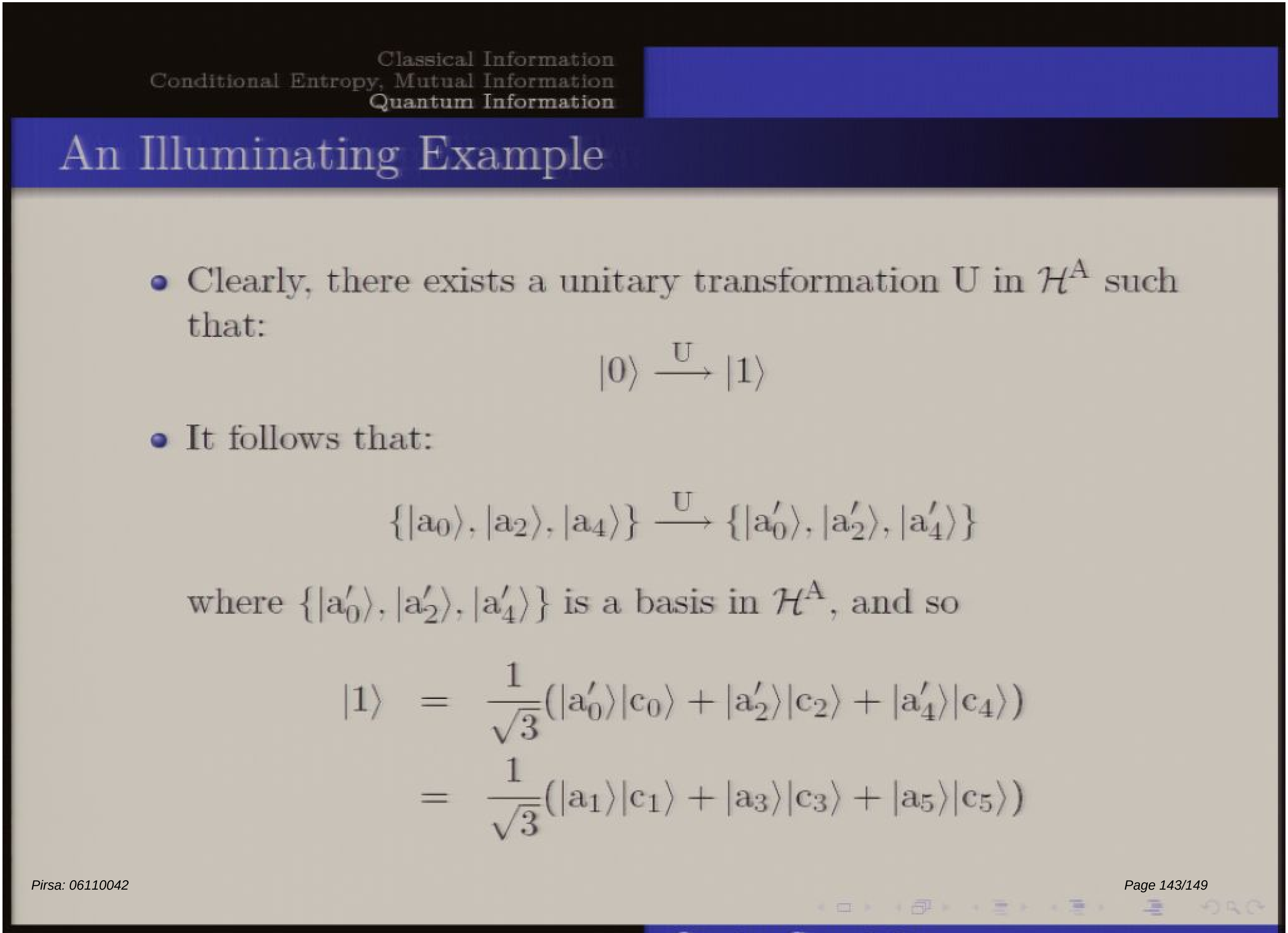
$$\begin{aligned} |1\rangle &= \frac{1}{\sqrt{3}}(|\mathrm{a}'_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}'_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}'_4\rangle|\mathrm{c}_4\rangle) \\ &= \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle) \end{aligned}$$



An Illuminating Example

- So Alice could implement the EPR cheating strategy by preparing the state $|1\rangle$ and measuring in the basis $\{|\mathrm{a}'_0\rangle, |\mathrm{a}'_2\rangle, |\mathrm{a}'_4\rangle\}$ for the 0-commitment, or in the basis $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ for the 1-commitment.
- Equivalently, she could prepare the state $|0\rangle$ and measure in two different bases, since the unitary transformation that takes $|1\rangle$ to $|0\rangle$ also takes the basis $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ to the basis $\{|\mathrm{a}''_1\rangle, |\mathrm{a}''_3\rangle, |\mathrm{a}''_5\rangle\}$, and so:

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{3}}(|\mathrm{a}_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4\rangle|\mathrm{c}_4\rangle) \\ &= \frac{1}{\sqrt{3}}(|\mathrm{a}''_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}''_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}''_5\rangle|\mathrm{c}_5\rangle) \end{aligned}$$



An Illuminating Example

- Clearly, there exists a unitary transformation U in $\mathcal{H}^{\mathrm{A}}$ such that:

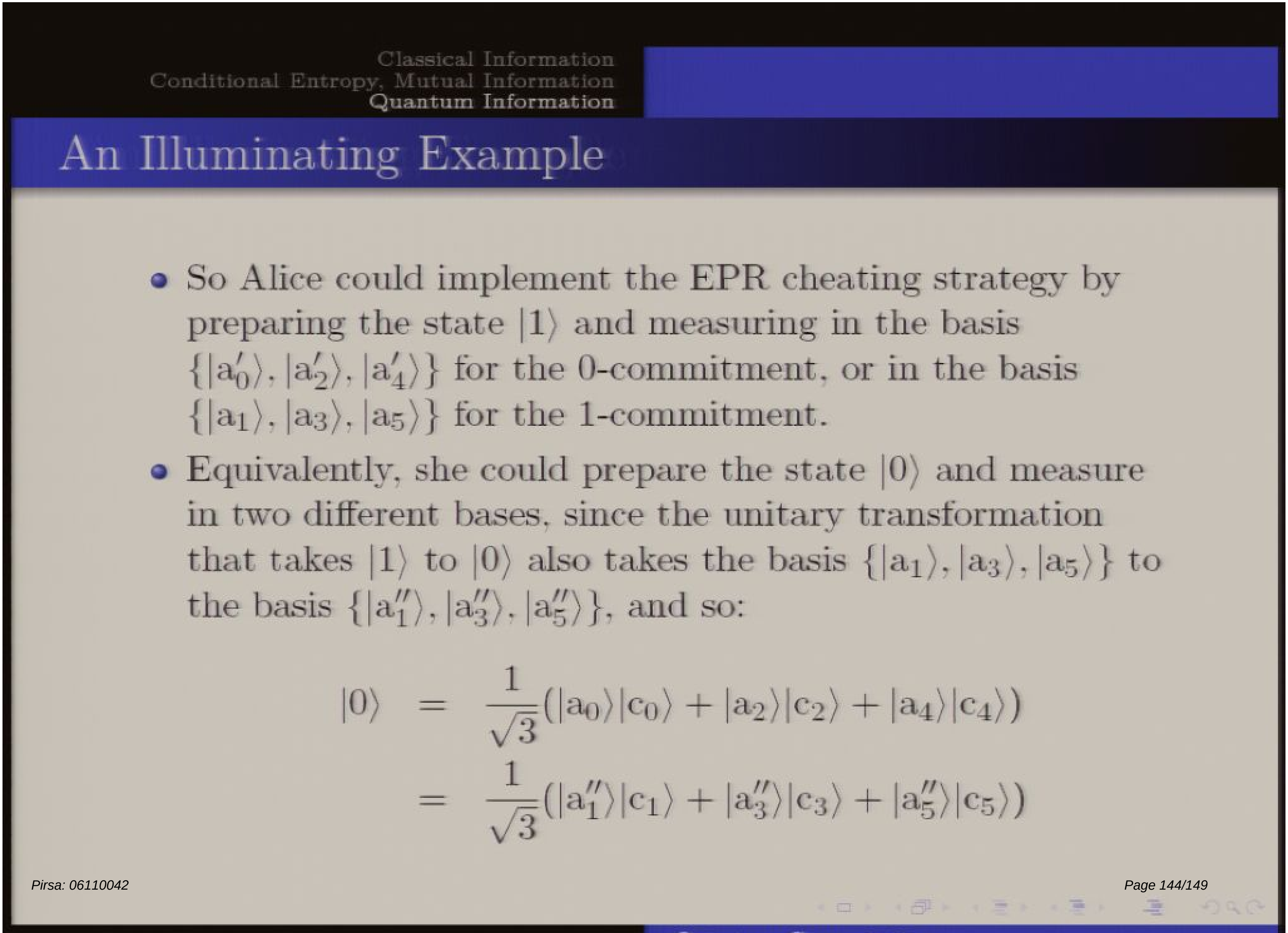
$$|0\rangle \xrightarrow{\mathrm{U}} |1\rangle$$

- It follows that:

$$\{|\mathrm{a}_0\rangle, |\mathrm{a}_2\rangle, |\mathrm{a}_4\rangle\} \xrightarrow{\mathrm{U}} \{|\mathrm{a}_0'\rangle, |\mathrm{a}_2'\rangle, |\mathrm{a}_4'\rangle\}$$

where $\{|\mathrm{a}_0'\rangle, |\mathrm{a}_2'\rangle, |\mathrm{a}_4'\rangle\}$ is a basis in $\mathcal{H}^{\mathrm{A}}$, and so

$$\begin{aligned} |1\rangle &= \frac{1}{\sqrt{3}}(|\mathrm{a}_0'\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2'\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4'\rangle|\mathrm{c}_4\rangle) \\ &= \frac{1}{\sqrt{3}}(|\mathrm{a}_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}_5\rangle|\mathrm{c}_5\rangle) \end{aligned}$$



An Illuminating Example

- So Alice could implement the EPR cheating strategy by preparing the state $|1\rangle$ and measuring in the basis $\{|\mathrm{a}'_0\rangle, |\mathrm{a}'_2\rangle, |\mathrm{a}'_4\rangle\}$ for the 0-commitment, or in the basis $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ for the 1-commitment.
- Equivalently, she could prepare the state $|0\rangle$ and measure in two different bases, since the unitary transformation that takes $|1\rangle$ to $|0\rangle$ also takes the basis $\{|\mathrm{a}_1\rangle, |\mathrm{a}_3\rangle, |\mathrm{a}_5\rangle\}$ to the basis $\{|\mathrm{a}''_1\rangle, |\mathrm{a}''_3\rangle, |\mathrm{a}''_5\rangle\}$, and so:

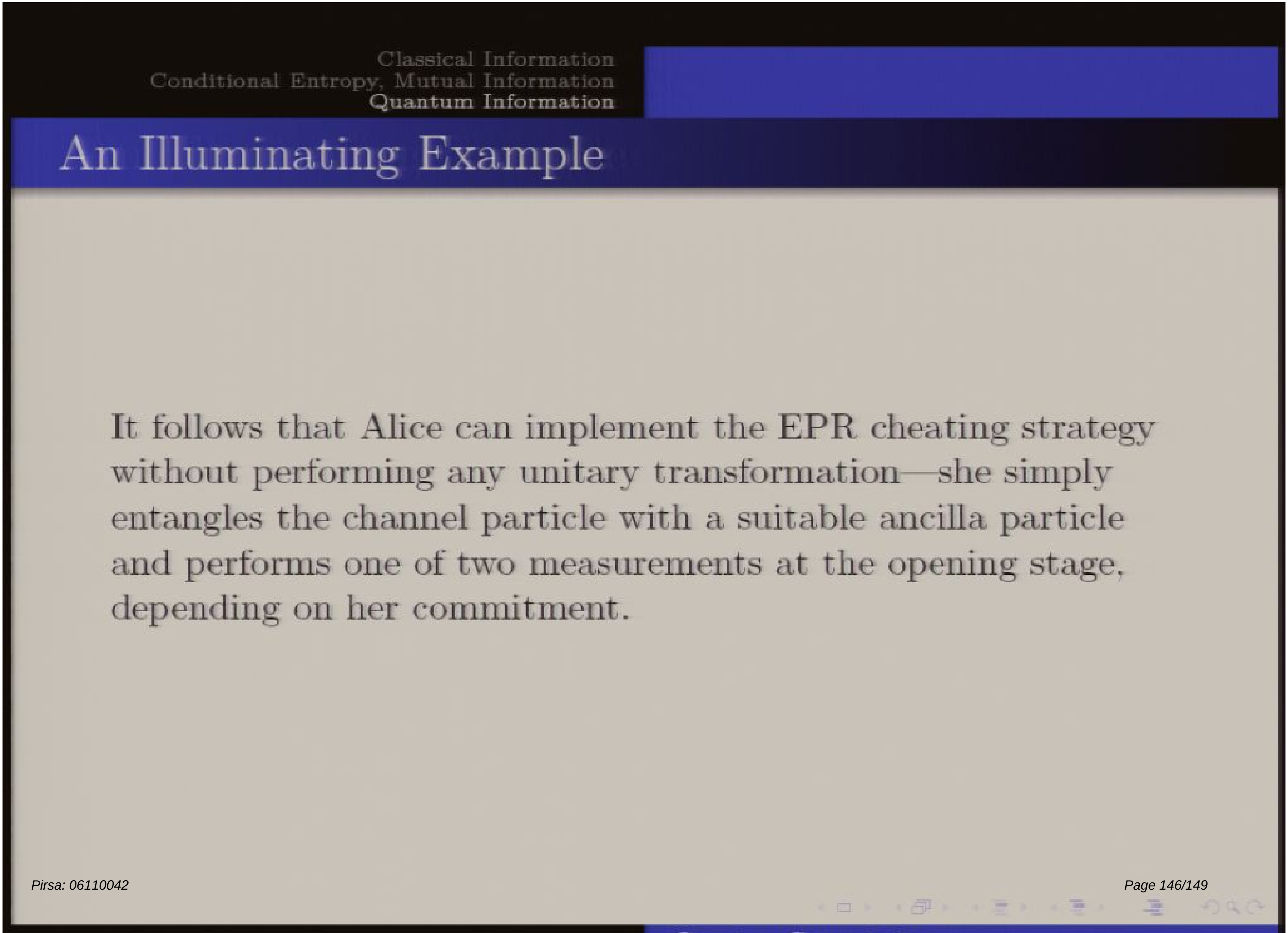
$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{3}}(|\mathrm{a}_0\rangle|\mathrm{c}_0\rangle + |\mathrm{a}_2\rangle|\mathrm{c}_2\rangle + |\mathrm{a}_4\rangle|\mathrm{c}_4\rangle) \\ &= \frac{1}{\sqrt{3}}(|\mathrm{a}''_1\rangle|\mathrm{c}_1\rangle + |\mathrm{a}''_3\rangle|\mathrm{c}_3\rangle + |\mathrm{a}''_5\rangle|\mathrm{c}_5\rangle) \end{aligned}$$

An Illuminating Example

- A calculation shows that:

$$
\begin{aligned}
|a_1''\rangle &= \frac{1}{3}\Big(|a_0\rangle + (1+\sqrt{3})|a_2\rangle + (1-\sqrt{3})|a_4\rangle\Big)\\
|a_3''\rangle &= \frac{1}{3}\Big((1+\sqrt{3})|a_0\rangle + (1-\sqrt{3})|a_2\rangle + |a_4\rangle\Big)\\
|a_5''\rangle &= \frac{1}{3}\Big(1-\sqrt{3})|a_0\rangle + |a_2\rangle + (1+\sqrt{3})|a_4\rangle\Big)
\end{aligned}
$$

- In effect, if Alice prepares the entangled state $|0\rangle$ and measures the ancilla A in the $\{|a_0\rangle, |a_2\rangle, |a_4\rangle\}$ basis, she steers the channel particle into a mixture of nonorthogonal states $\{|c_0\rangle, |c_2\rangle, |c_4\rangle\}$. If she measures in the $\{|a_1''\rangle, |a_3''\rangle, |a_5''\rangle\}$ basis, she steers the channel particle into a mixture of nonorthogonal states $\{|c_1\rangle, |c_3\rangle, |c_5\rangle\}$.



An Illuminating Example

It follows that Alice can implement the EPR cheating strategy without performing any unitary transformation—she simply entangles the channel particle with a suitable ancilla particle and performs one of two measurements at the opening stage, depending on her commitment.

An Illuminating Example

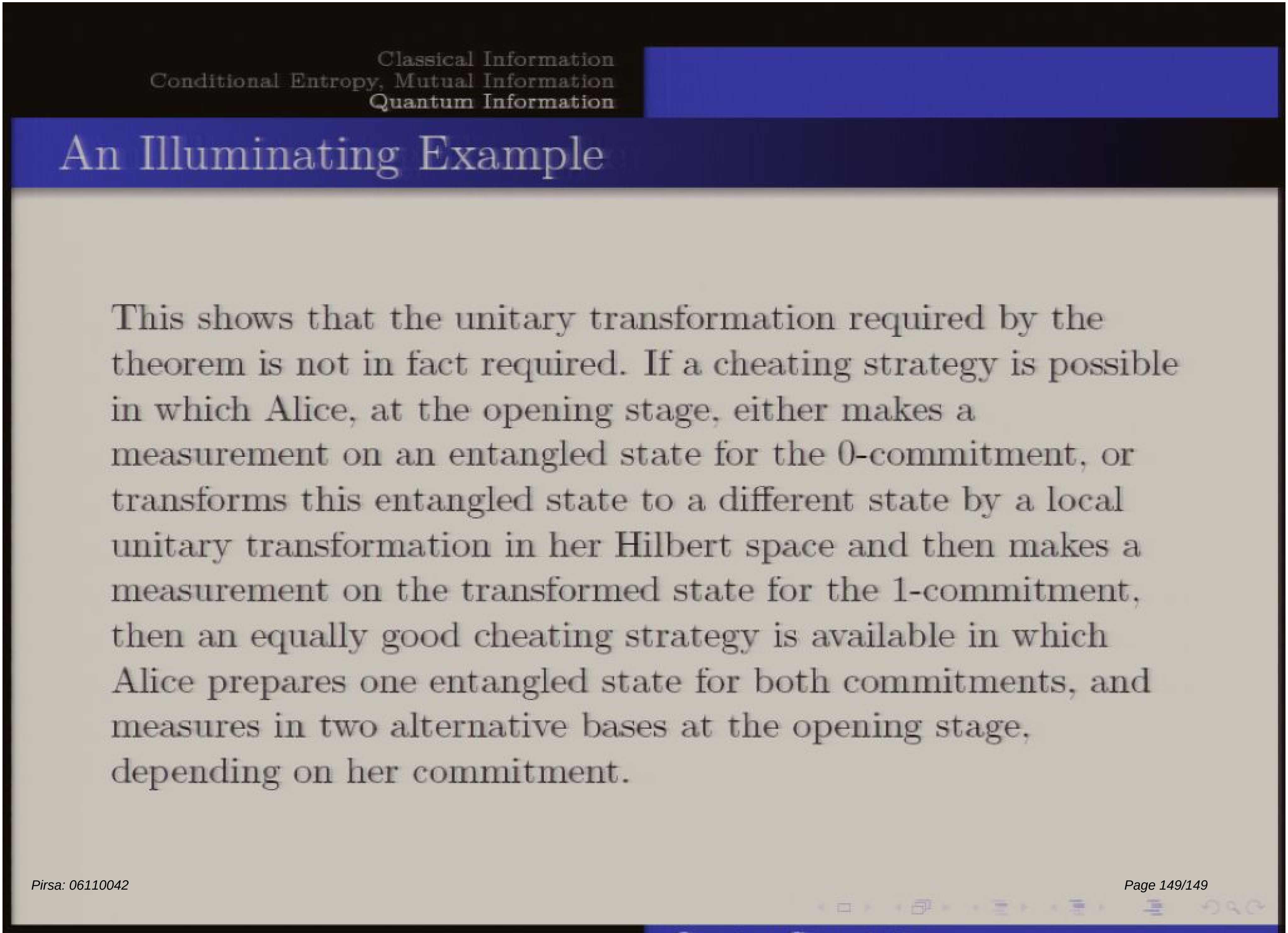
This shows that the unitary transformation required by the theorem is not in fact required. If a cheating strategy is possible in which Alice, at the opening stage, either makes a measurement on an entangled state for the 0-commitment, or transforms this entangled state to a different state by a local unitary transformation in her Hilbert space and then makes a measurement on the transformed state for the 1-commitment, then an equally good cheating strategy is available in which Alice prepares one entangled state for both commitments, and measures in two alternative bases at the opening stage, depending on her commitment.

Quantum Computation: Deutsch’s XOR algorithm

- $\mathrm{B} = \{0, 1\}$ a Boolean algebra
- Given a ‘black box’ or oracle that computes a function

$$\mathrm{f} : \mathrm{B} \rightarrow \mathrm{B} \tag{8}$$

  we are required to determine whether the function is ‘constant’ (takes the same value for both inputs) or “balanced’ (takes a different value for each input).
- Classically, the only way to do this would be to consult the oracle twice, for the input values 0 and 1, and compare the outputs.



An Illuminating Example

This shows that the unitary transformation required by the theorem is not in fact required. If a cheating strategy is possible in which Alice, at the opening stage, either makes a measurement on an entangled state for the 0-commitment, or transforms this entangled state to a different state by a local unitary transformation in her Hilbert space and then makes a measurement on the transformed state for the 1-commitment, then an equally good cheating strategy is available in which Alice prepares one entangled state for both commitments, and measures in two alternative bases at the opening stage, depending on her commitment.