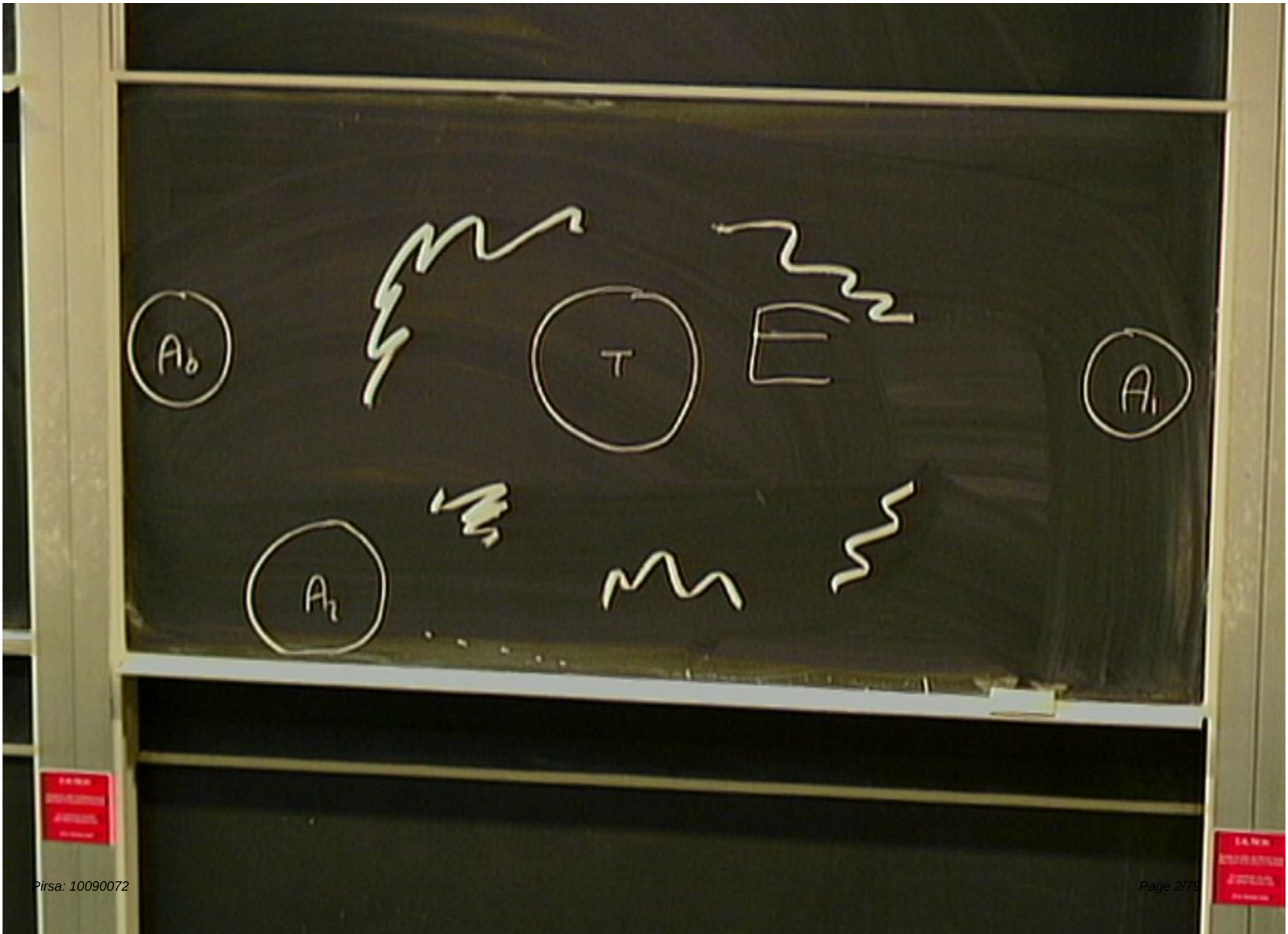
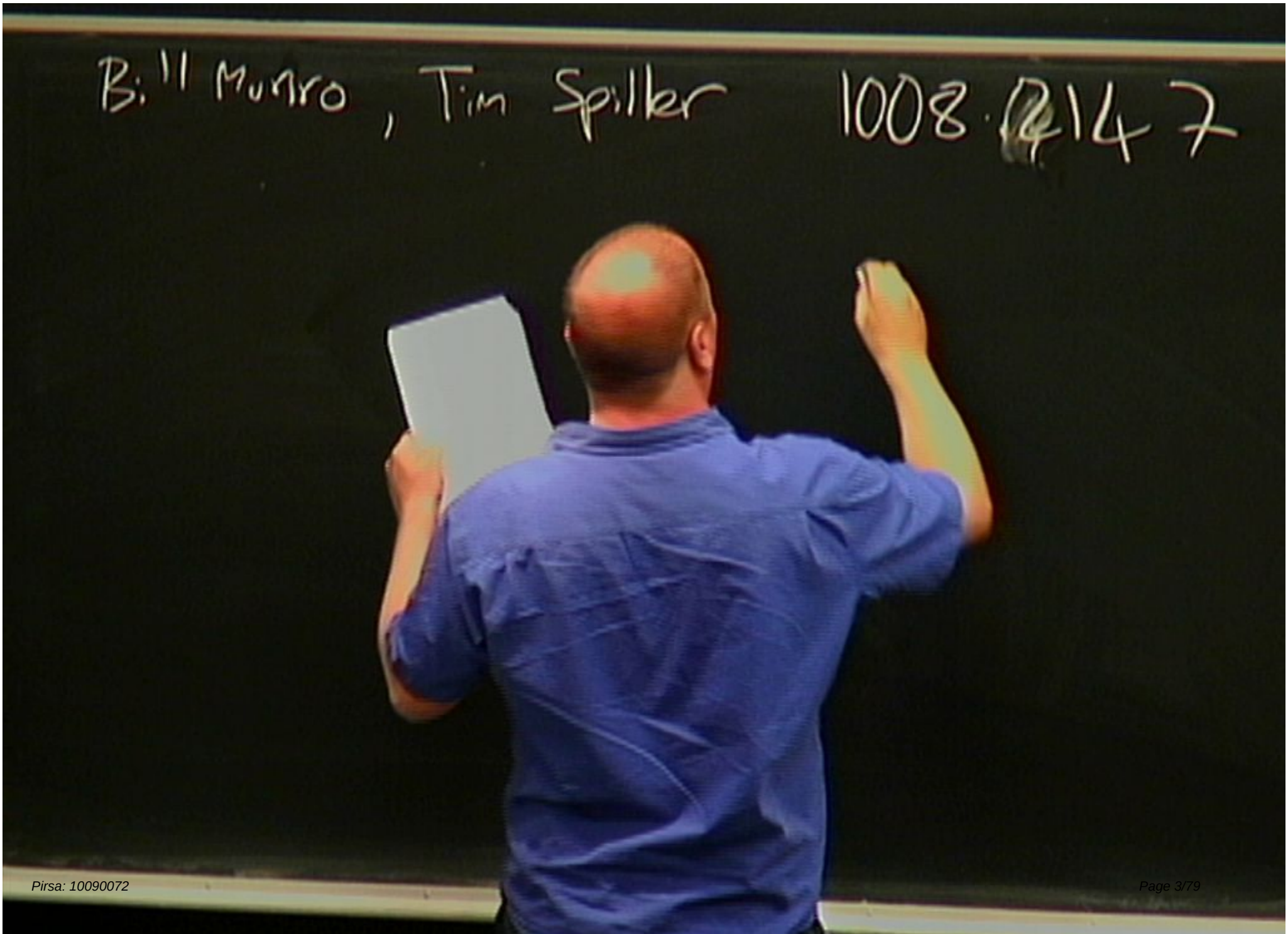
Title: Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signalling Constraints

Date: Sep 01, 2010 04:00 PM

URL: http://pirsa.org/10090072

Abstract: In this talk I review some joint work (arXiv:1008.2147) with Bill Munro and Tim Spiller on the task we call "quantum tagging", that is, authenticating the classical location of a classical tagging device by sending and receiving quantum signals from suitably located distant sites, in an environment controlled by an adversary whose quantum information processing and transmitting power is unbounded. Simple security models for this task will be presented. It will be shown that (among other protocols) recent protocols claimed to be unconditionally secure by Malaney and by Chandran et al. can in fact be broken by an adversary with pre-distributed entanglement using teleportation-based attacks. I also describe some protocols which cannot be broken by these specific attacks, but do not prove they are unconditionally secure. From a more foundational perspective, this work can be thought of (i) as an attempt to understand how and when we can know that something is somewhere, and (ii) an introduction to an interesting wider class of (im)possibility questions in relativistic quantum theory. If time permits, I will also touch on these topics.

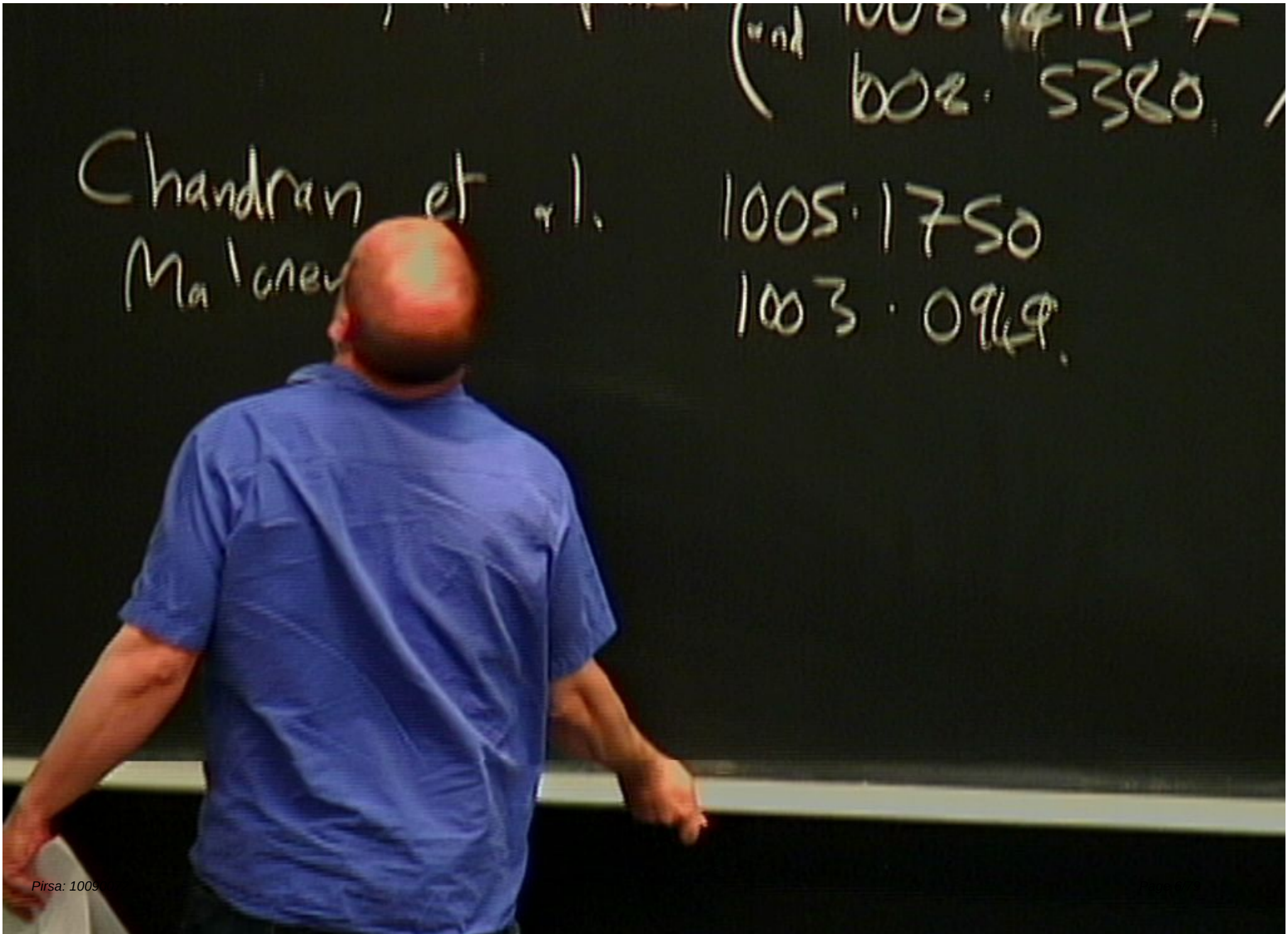

A_0
T
A_1
A_2


Bill Munro, Tim Spiller
1008.4147

Bill Munro, Tim Spiller (and 1008.4147
bor. 5380)

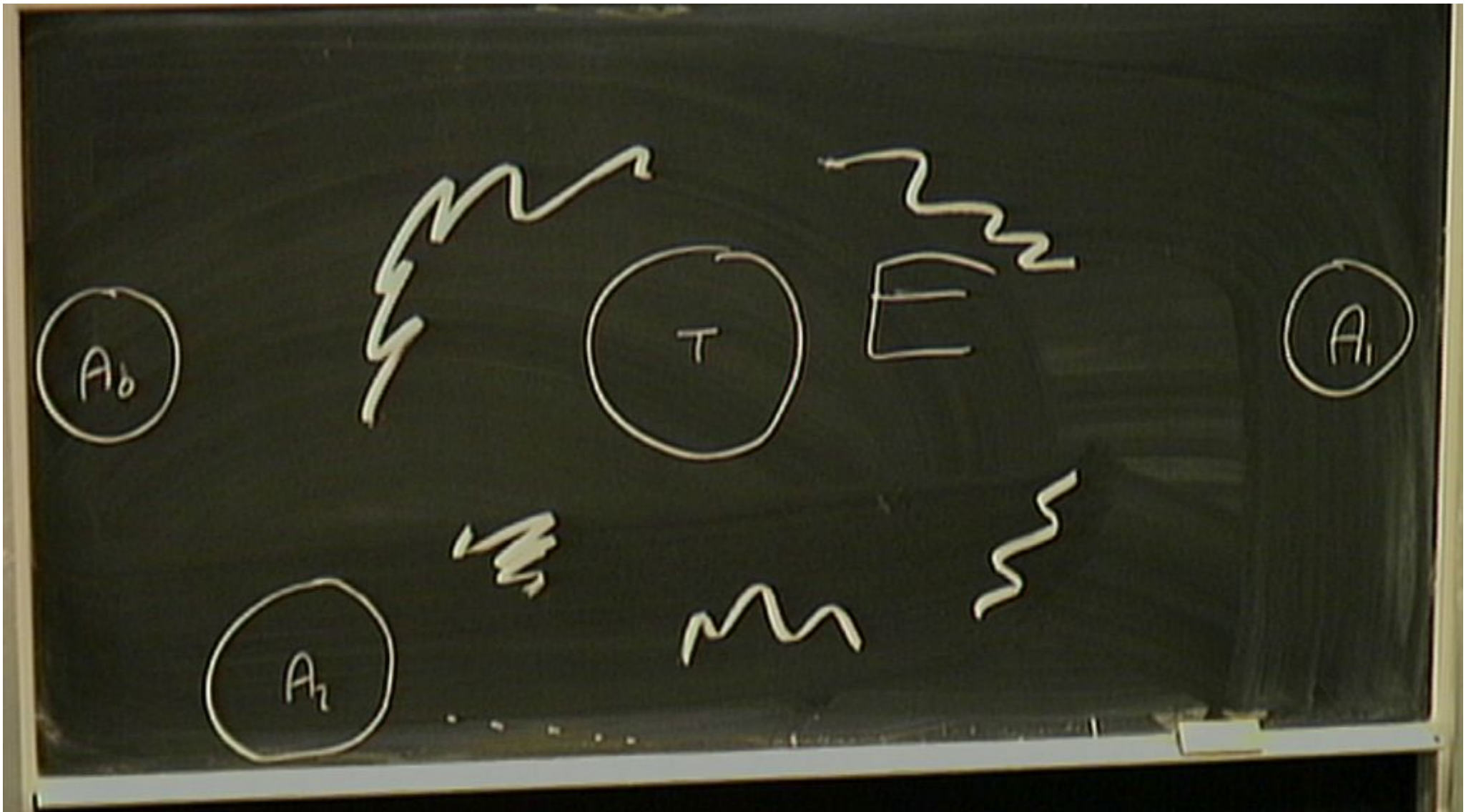
Bill Munro, Tim Spiller (and 1008.4147
bor. 5380)

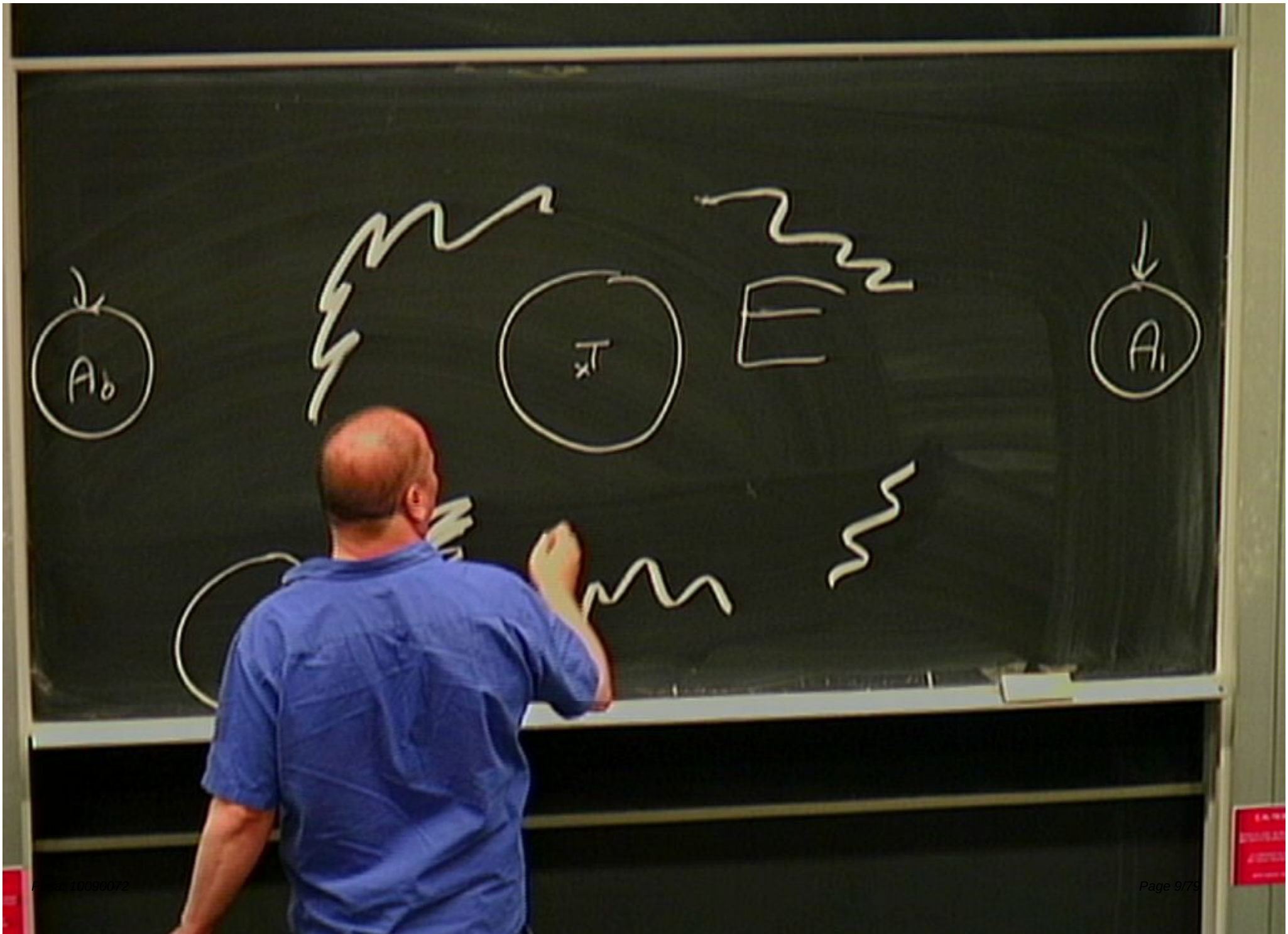
Chandran et al.

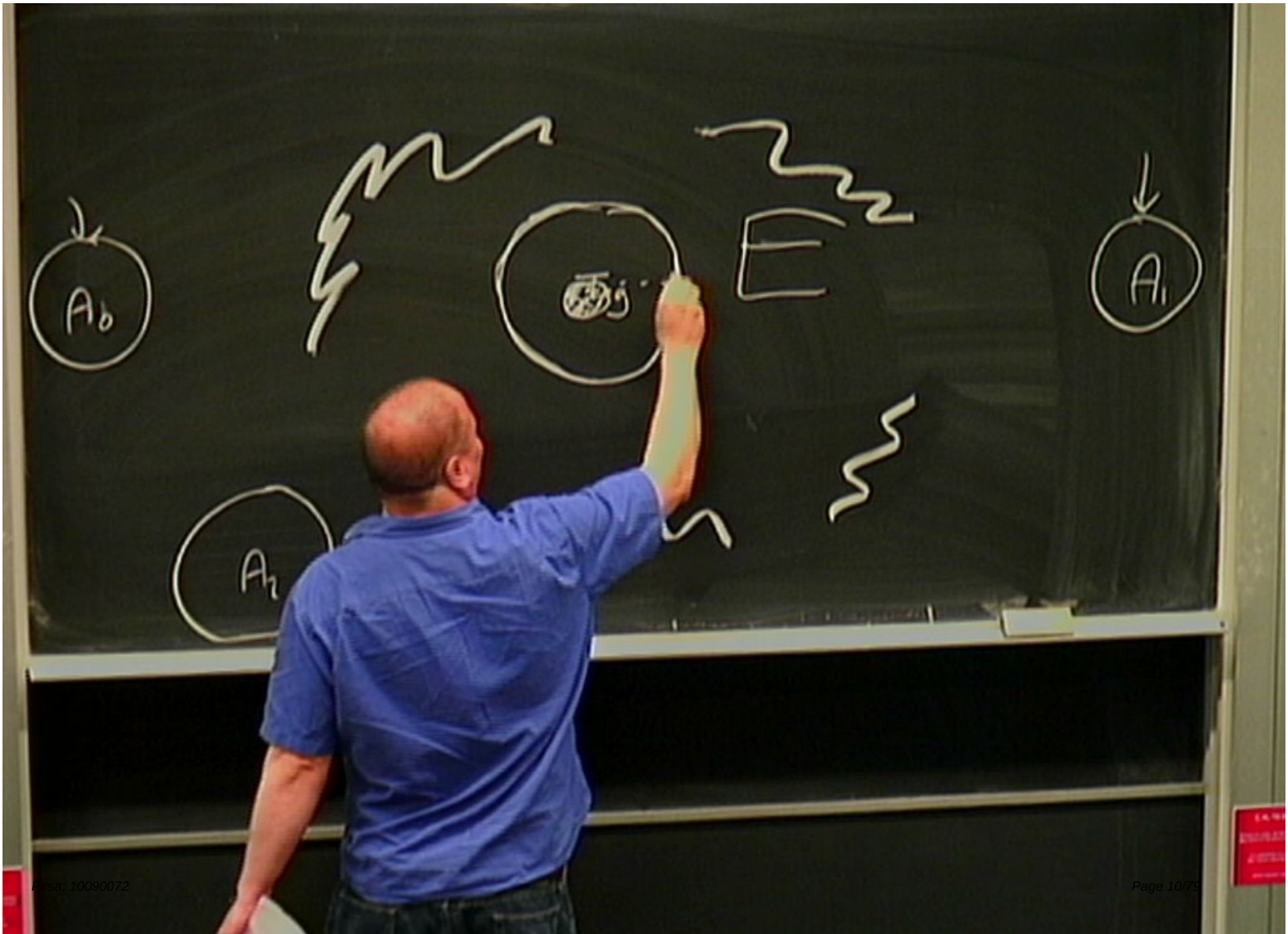

Chandran et al.
1005.1750
1003.0969

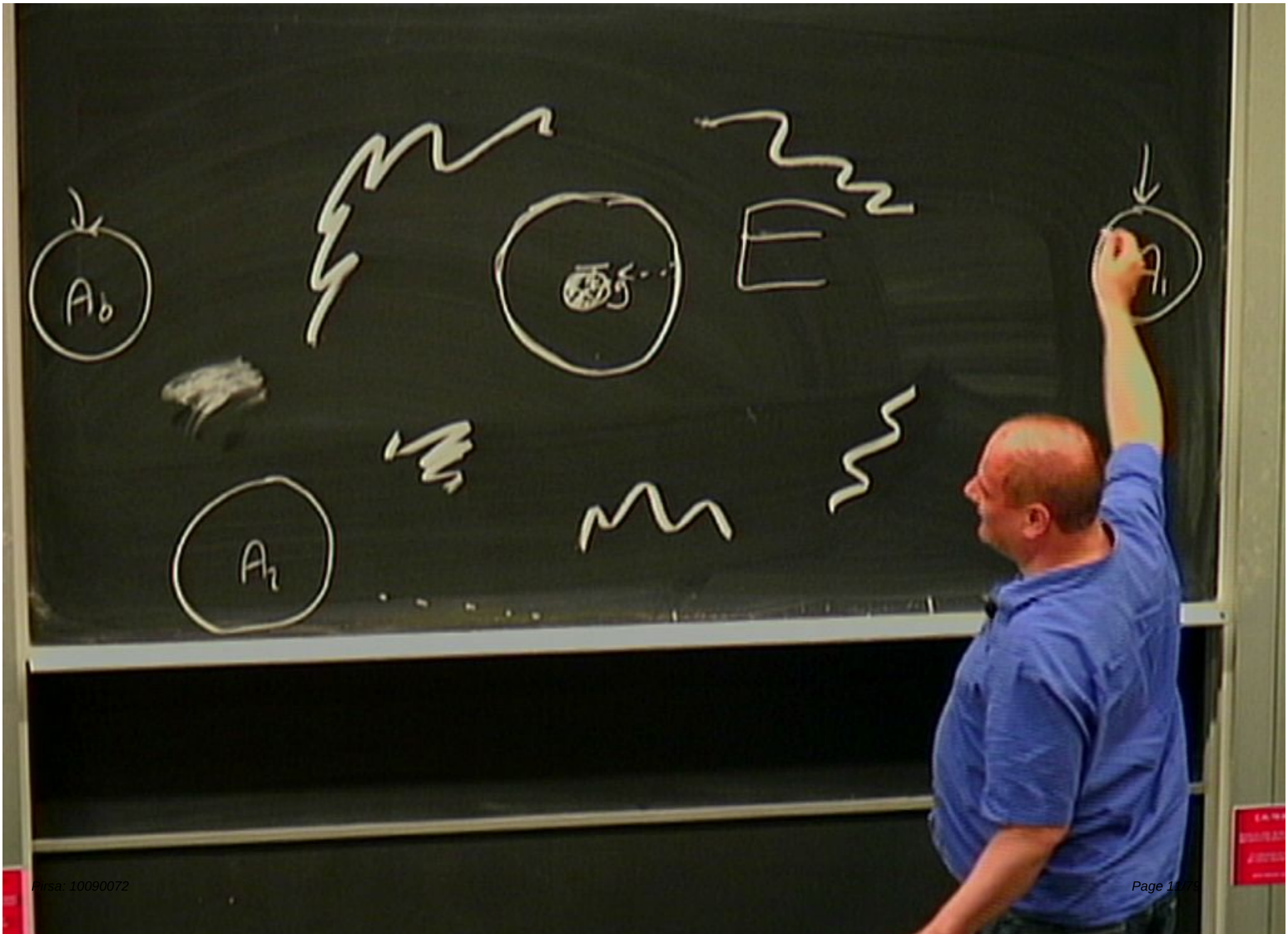
Bill Munro, Tim Spiller (and 1008.4147
bor. 5380.)

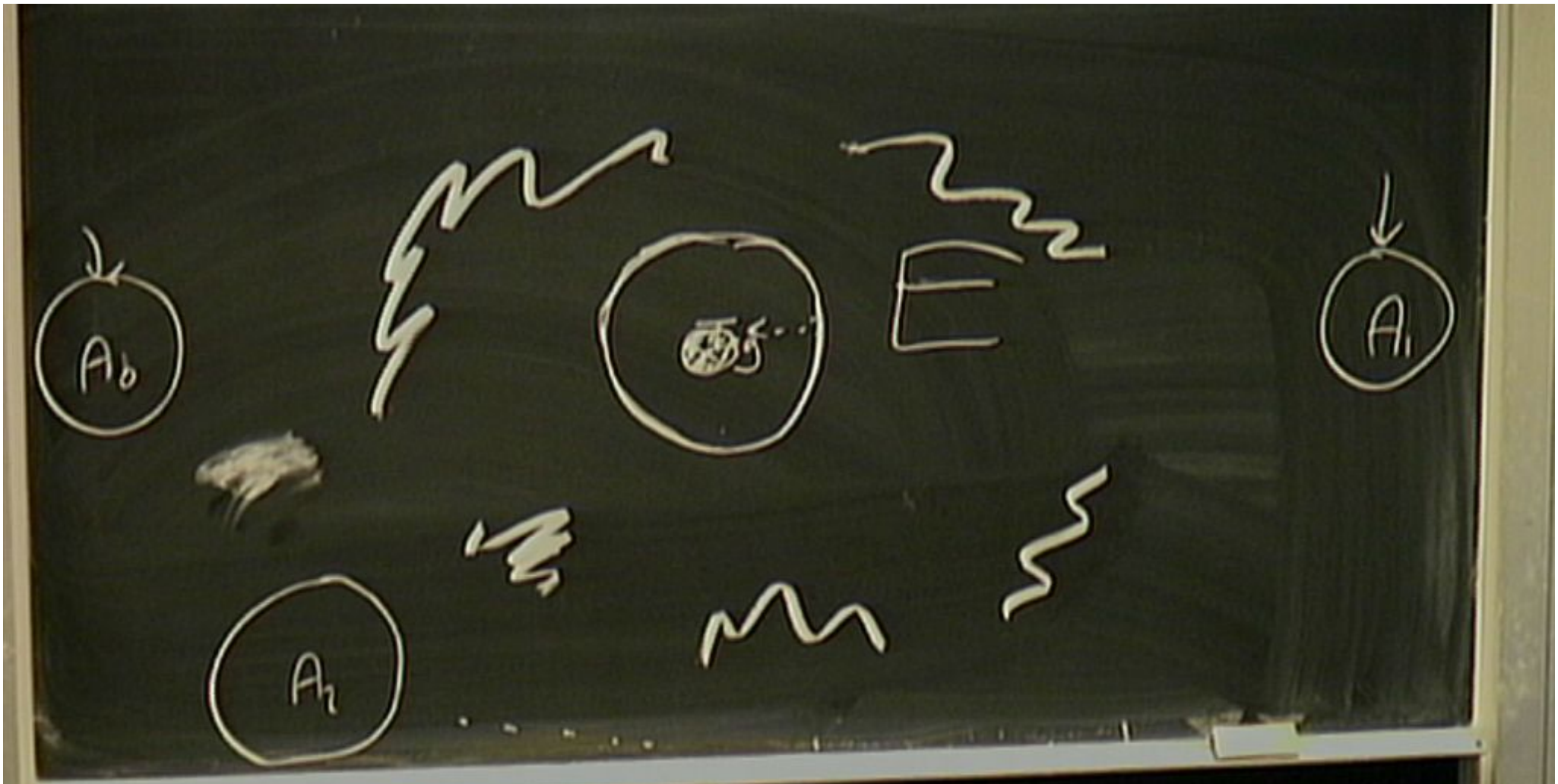
Chandran et al. 1005.1750
Maloney 1003.0949.


A_0
T
E
A_1
A_2


A_0
π
A_1


A0
E
A1
A2


A_0
E
A_1
A_2


A_0
E
A_1
A_2

Alice's task: wants to authenticate location of T.

Eve's aim:

Alice's task: wants to authenticate location of T.

Eve's aim:

Alice's task: wants to authenticate location of T.

Eve's aim: wants to simulate "spoof" T to A so Alice falsely believes it's at correct location.

Alice's task: wants to authenticate location of T.

Eve's aim: wants to simulate "spoof" T to A so Alice falsely believes it's at correct location.

A_i cryptographically secure.

Alice's task: wants to authenticate location of T.

Eve's aim: wants to simulate "spoof" T to A so Alice falsely believes it's at correct location.

A_i cryptographically secure.

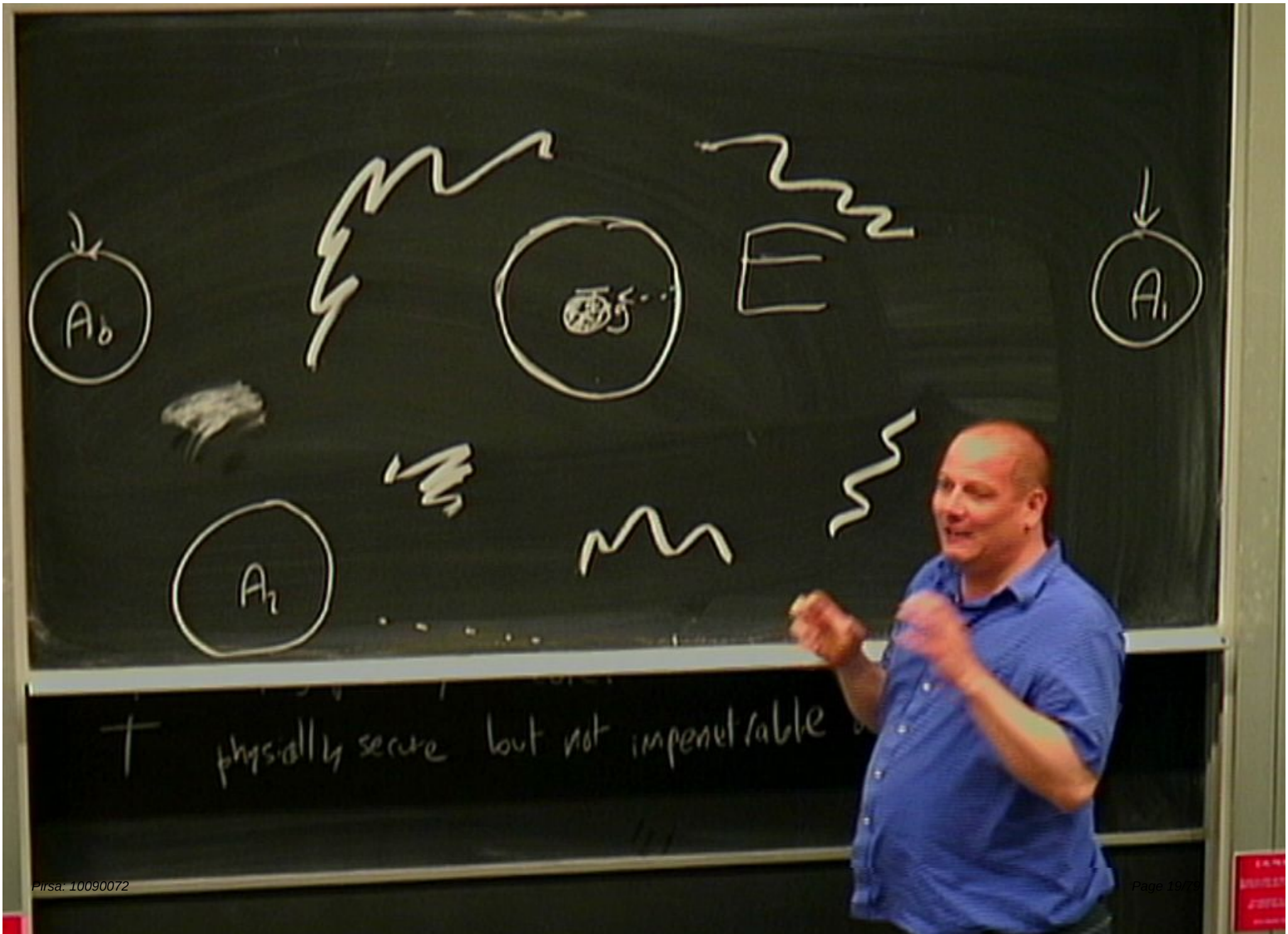
T physically secure but not impenetrable

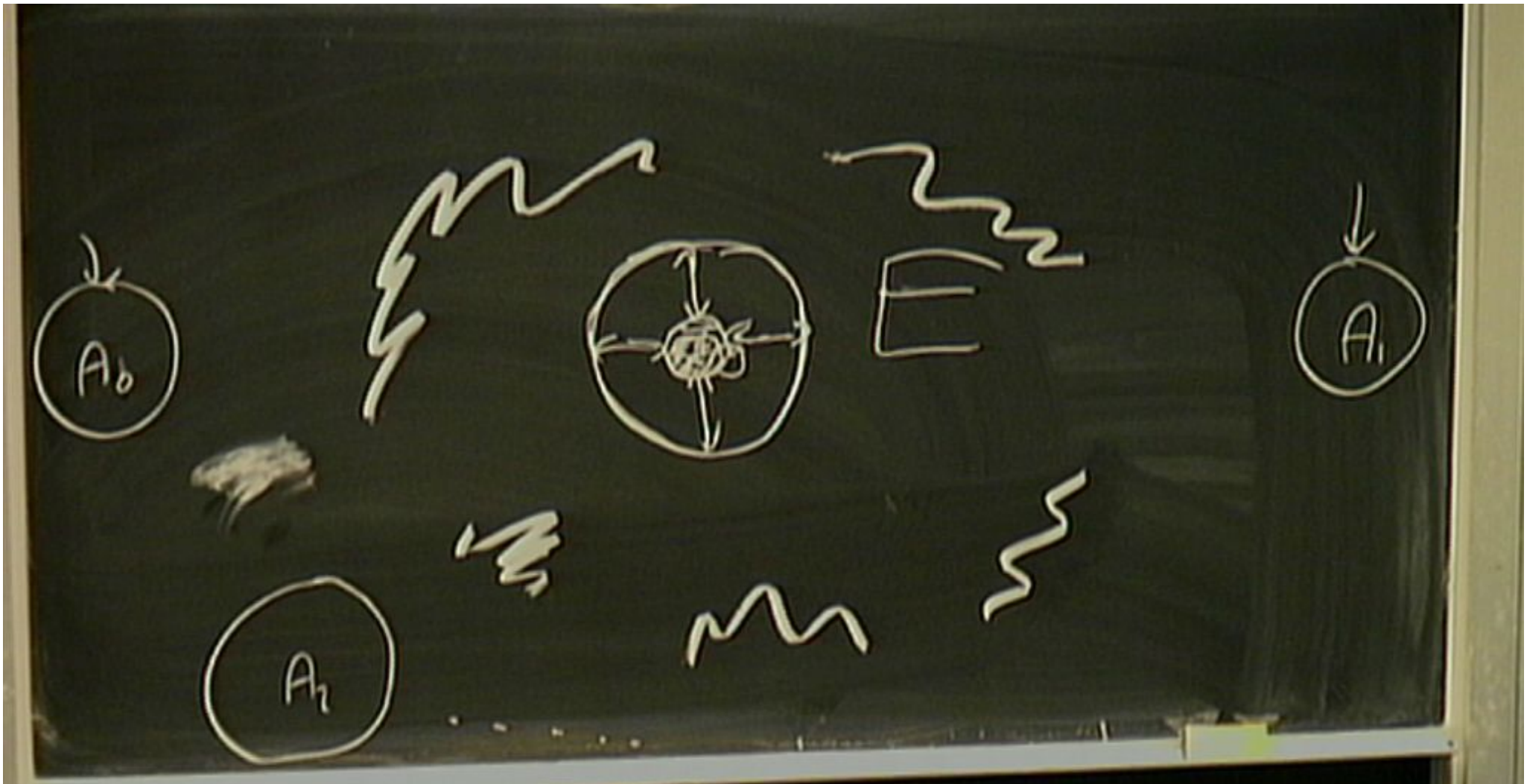
Alice's task: wants to authenticate location of T.

Eve's aim: wants to simulate "spoof" T to A so Alice falsely believes it's at correct location.

A_i cryptographically secure.

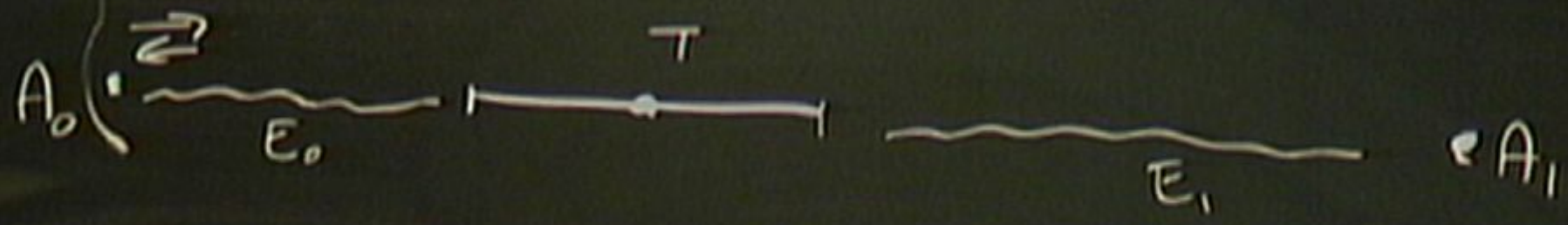
T physically secure but not impenetrable or cryptographically


A_0
E
A_1
A_2
physically secure but not impenetrable

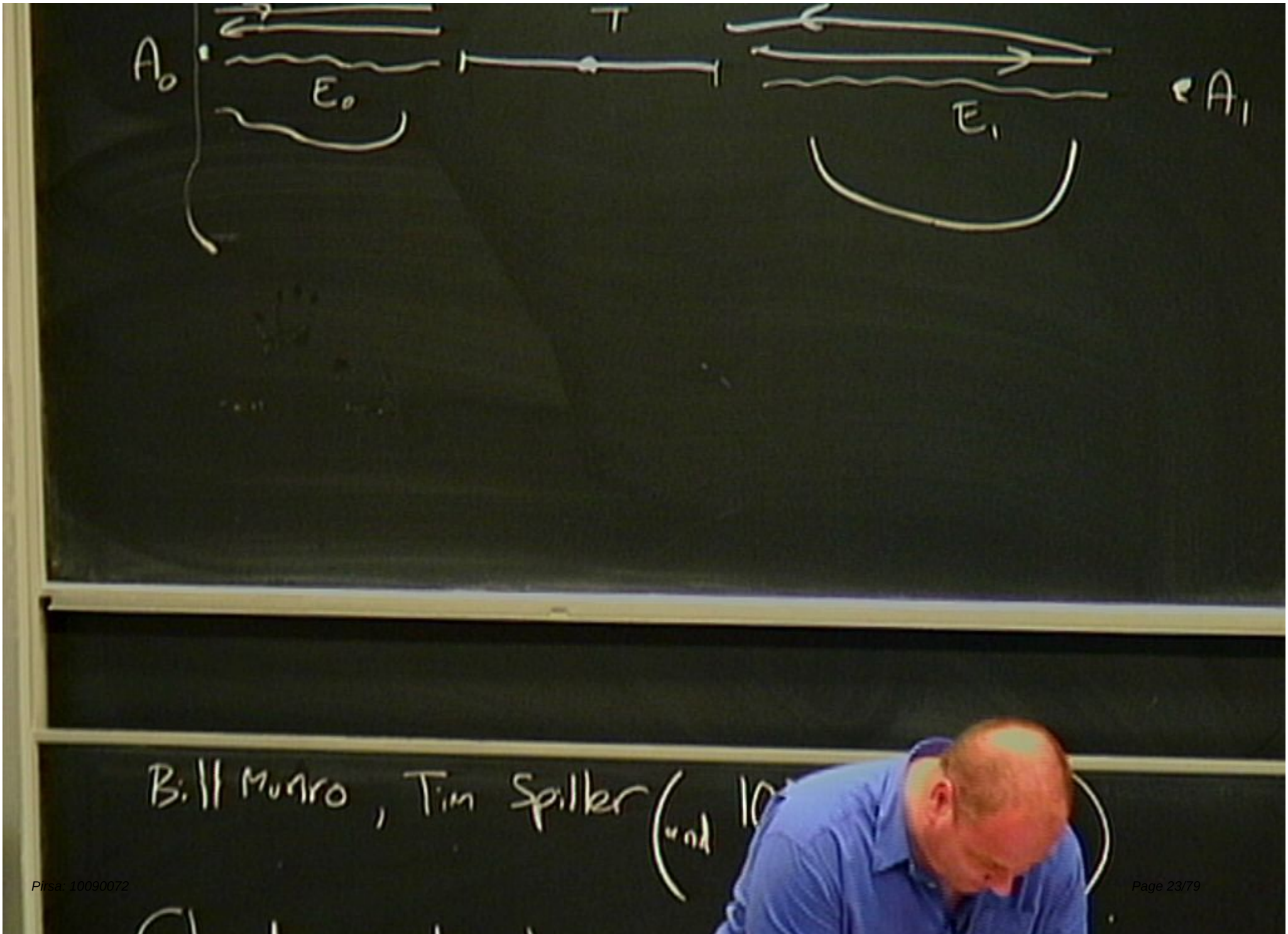


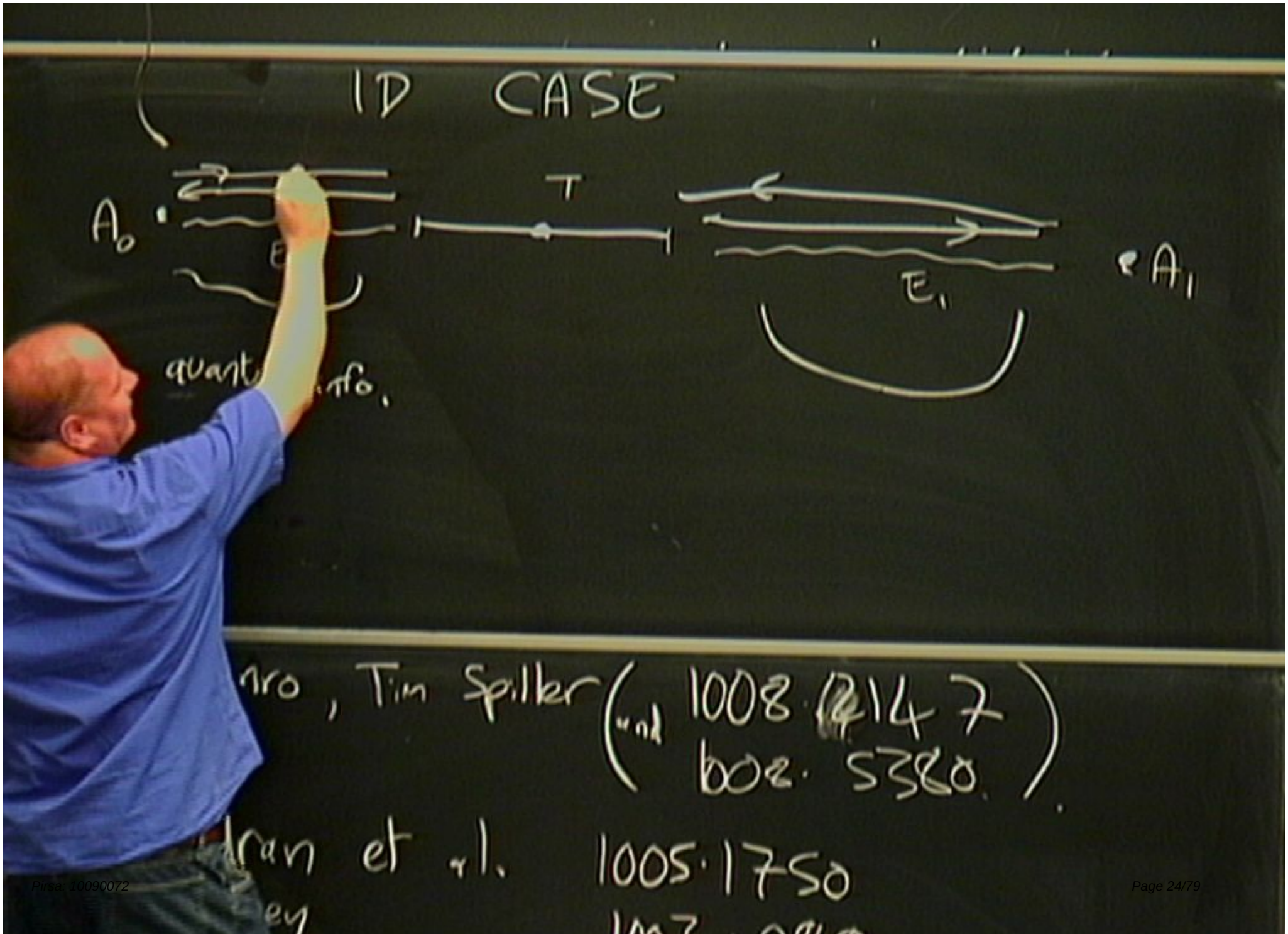
physically secure but not impenetrable a cryptographically secure.

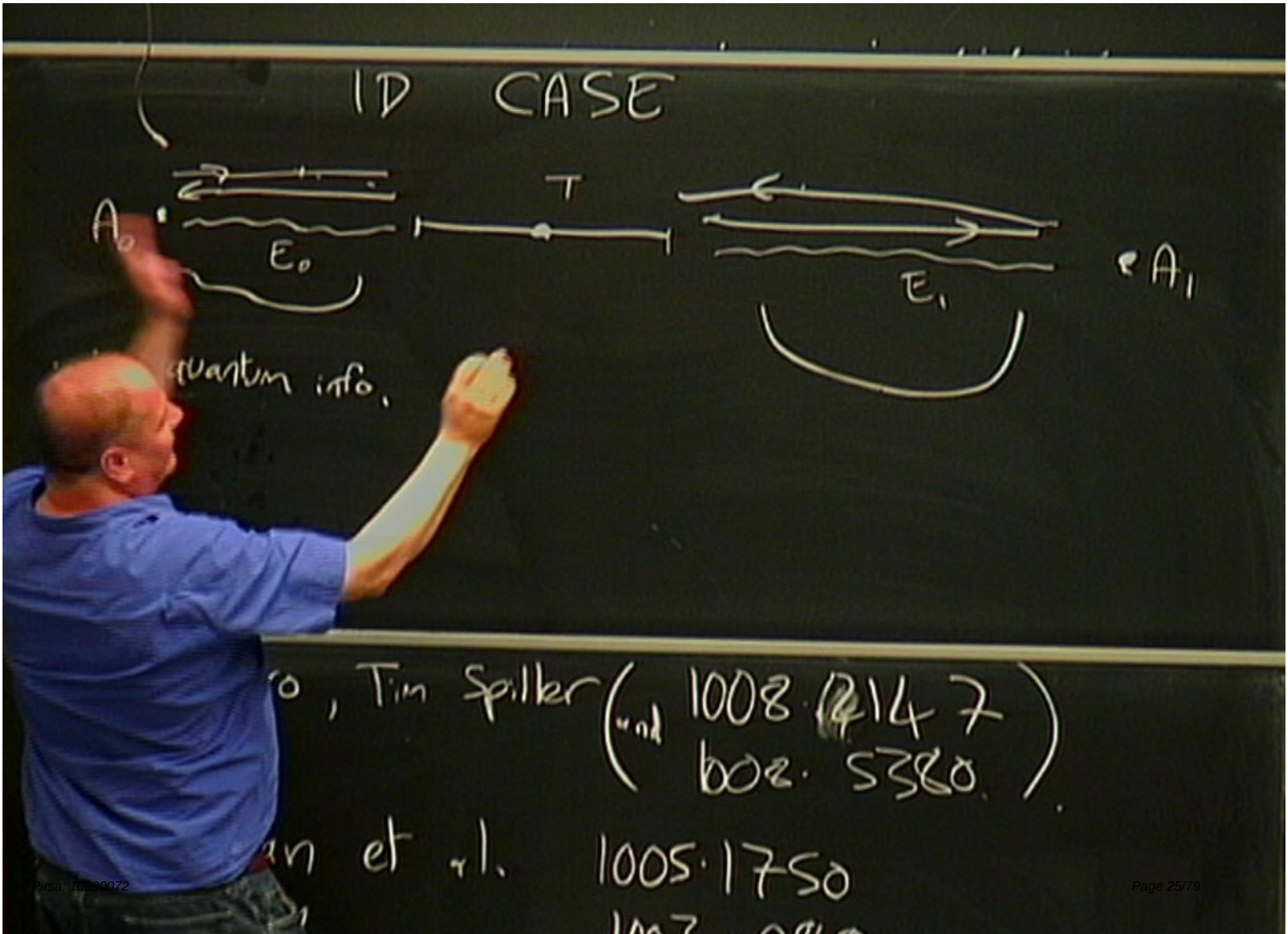
1D CASE

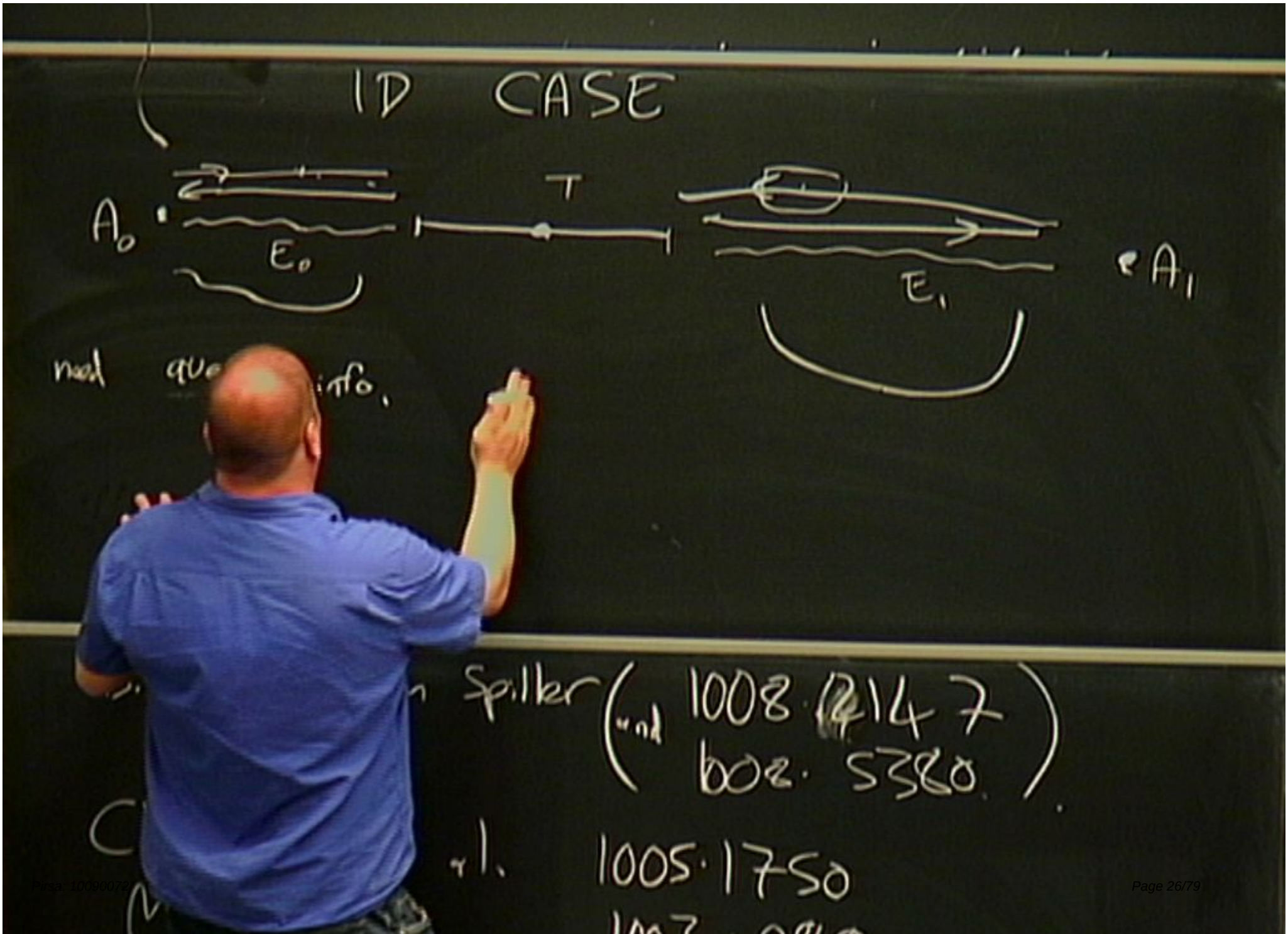


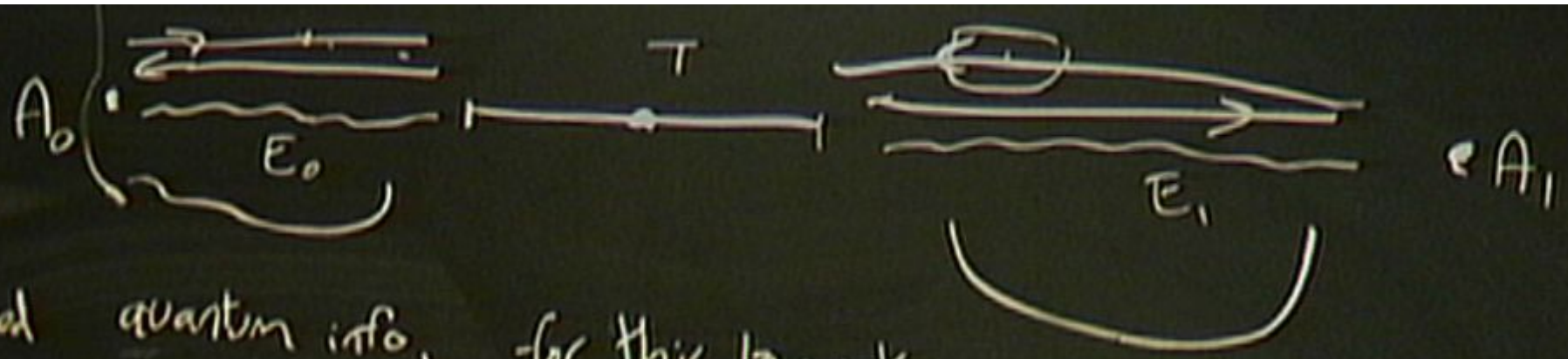
o, Tim Spiller (and 1008 (414 7
boz. 5380)


A_0
E_0
T
E_1
A_1
Bill Munro, Tim Spiller


1D CASE
A_0
T
E_1
A_1
quant info.
, Tim Spiller
1008.4147
bo2.5380
et al. 1005.1750


1D CASE
T
A_0
E_0
E_1
A_1
quantum info.
o, Tim Spiller (and 1008.4147
bor. 5380).
n et al. 1005.1750


1D CASE
A_0
E_0
T
E_1
A_1
need que info.
Spiller
1008.4147
boz. 5380
1005.1750



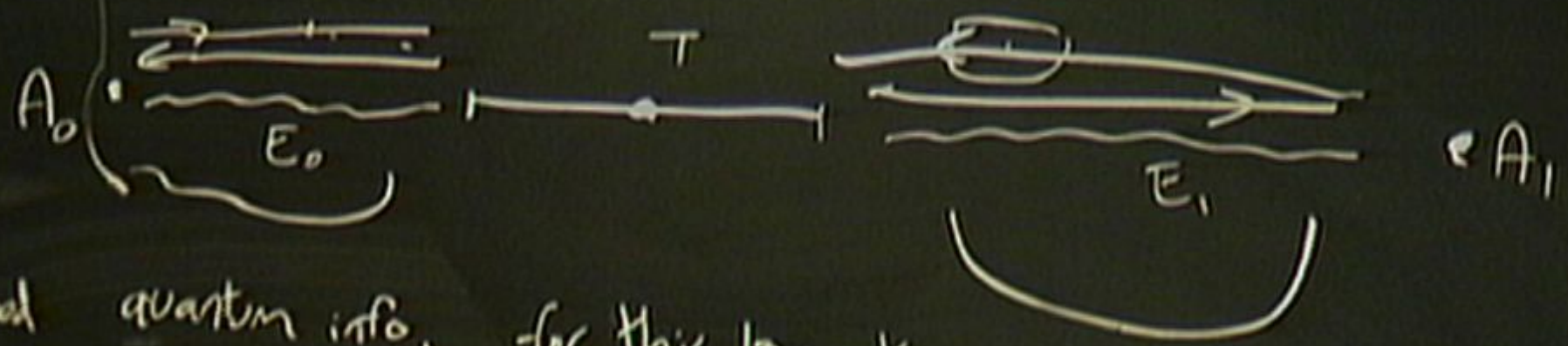
need quantum info. for this to work

Bill Munro, Tim Spiller (and 1008.4147 bor. 5380).

Chandran et al. 1005.1750

Maloney 1003.[illegible]

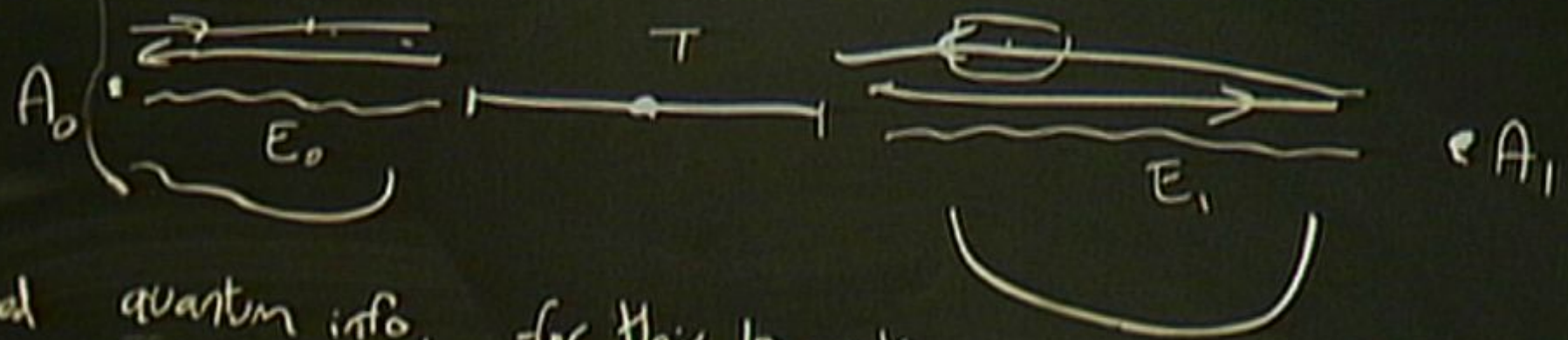
1D CASE



need quantum info. for this to work

Bill Munro, Tim Spiller (and 1008.2147)

1D CASE

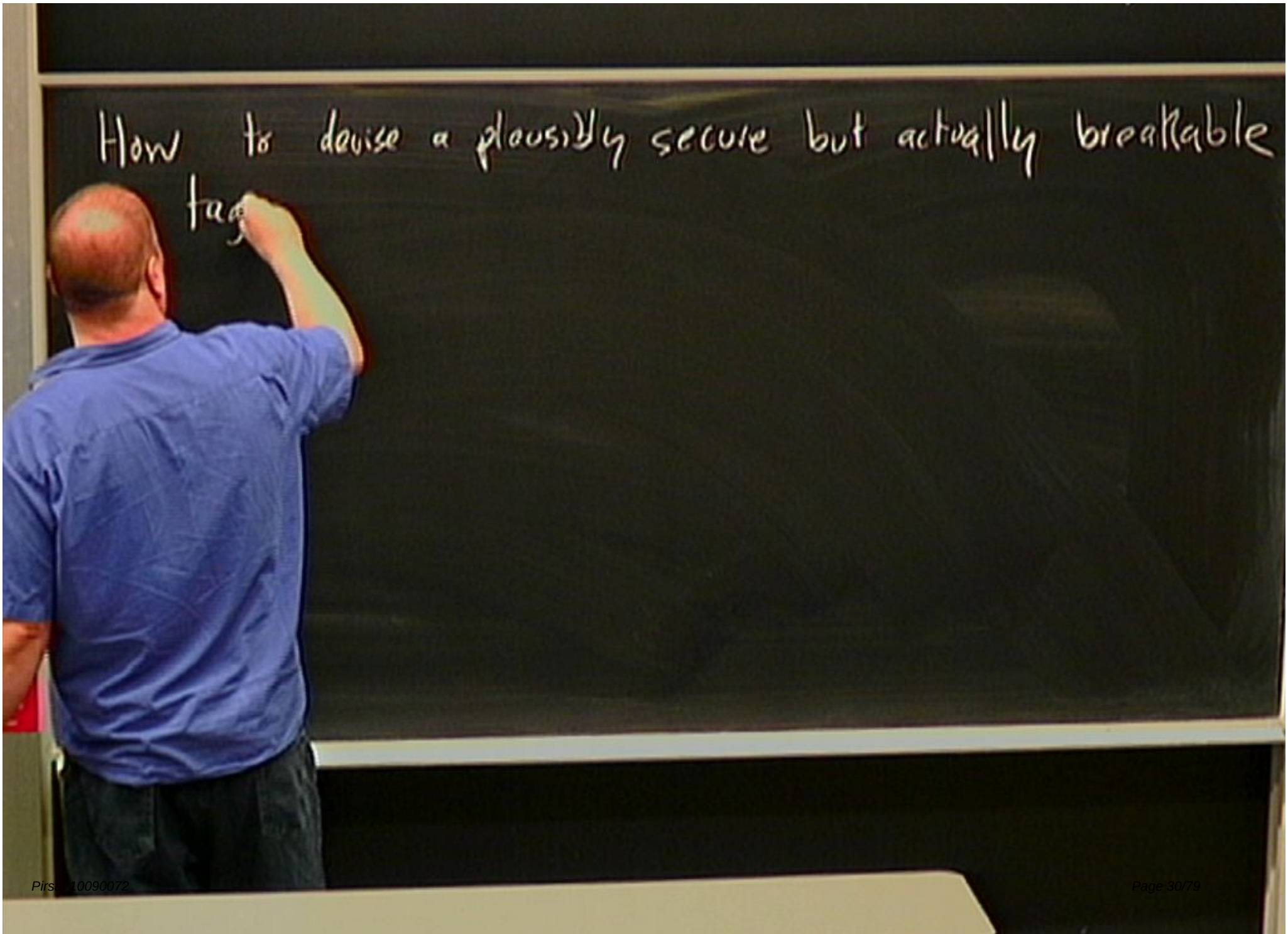


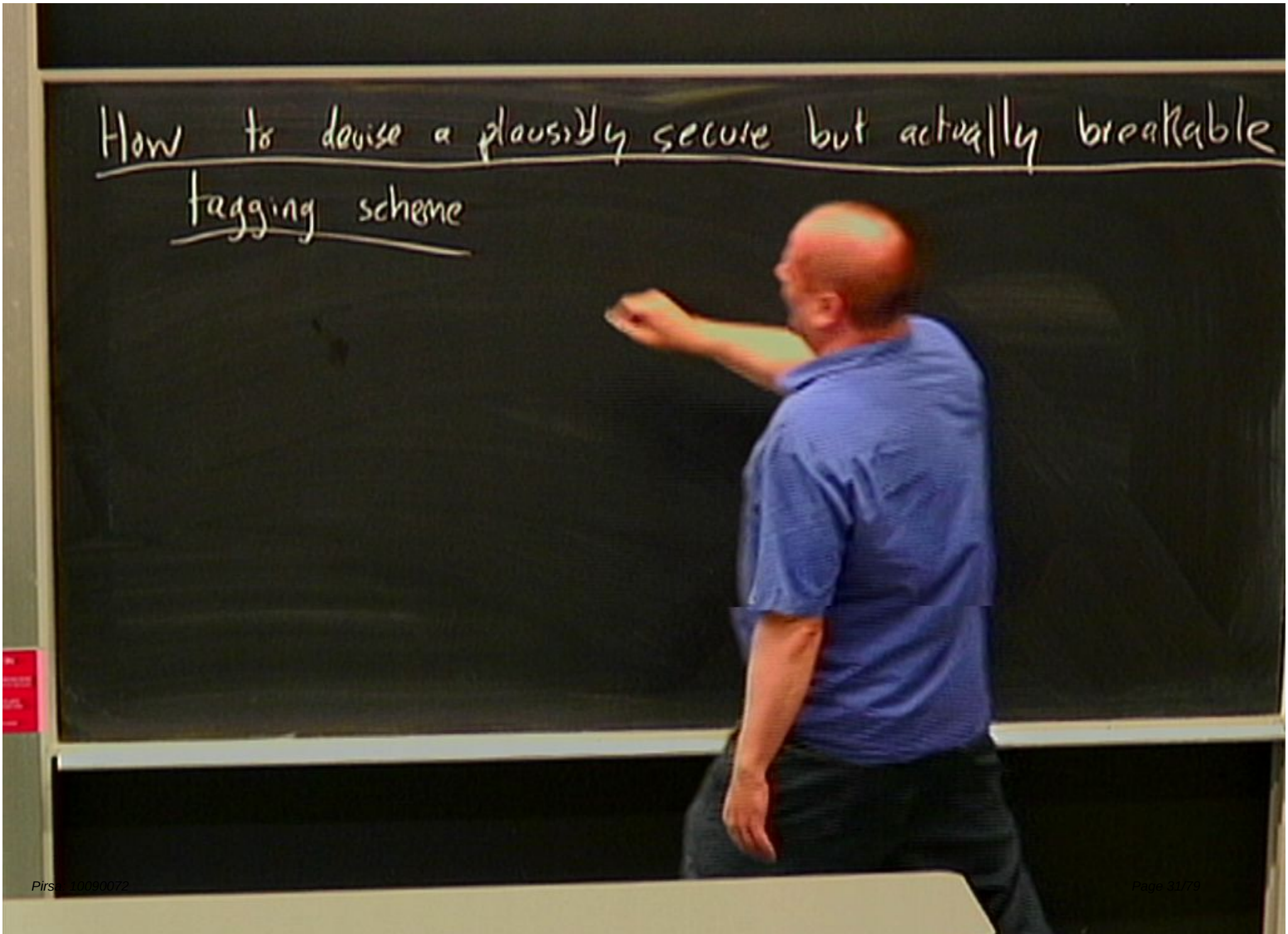
need quantum info. for this to work

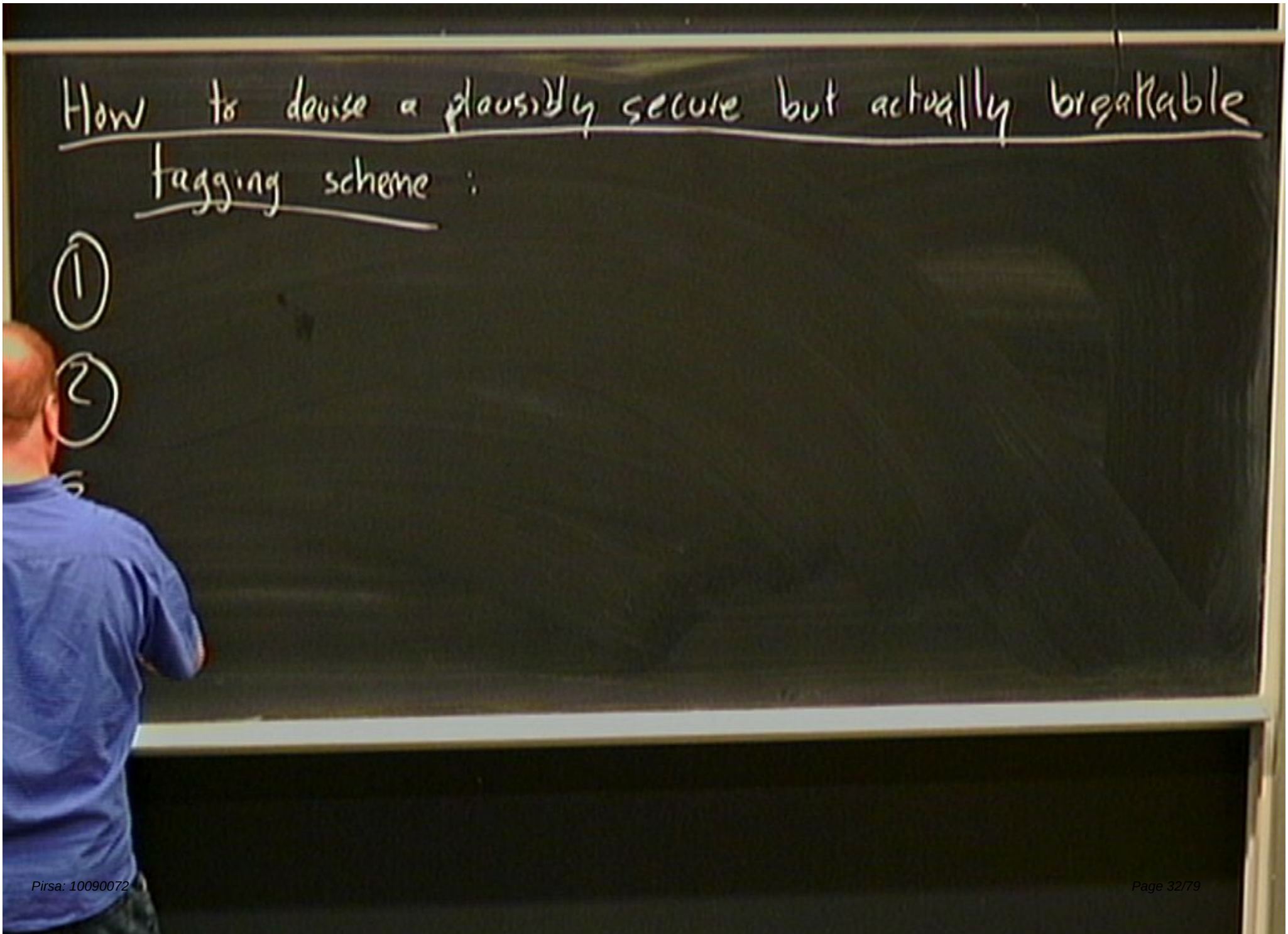
need non-signalling

...

Bill Munro, Tim Spiller (and 1008.0147)

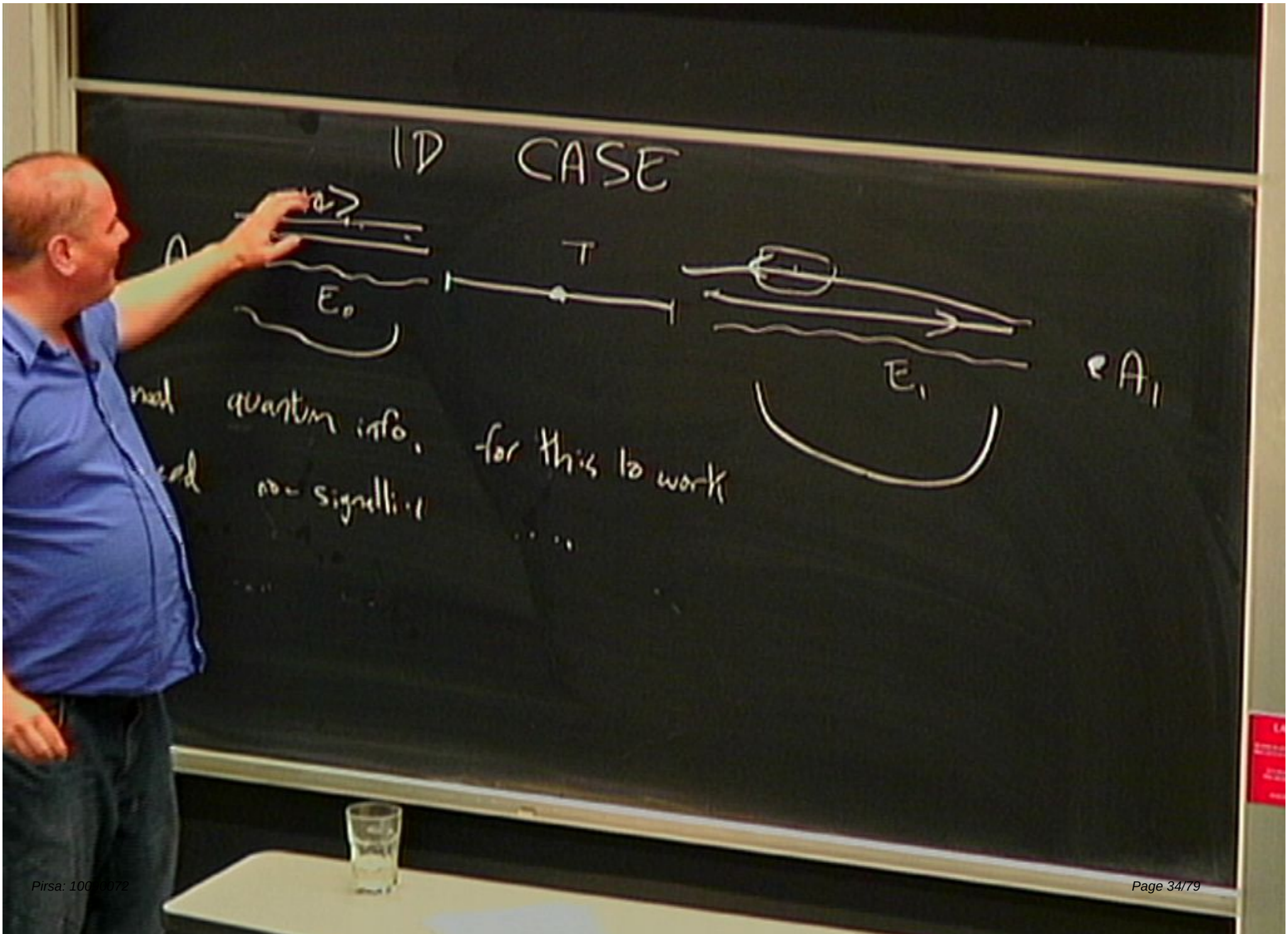

How to devise a plausibly secure but actually breakable
tag


How to devise a plausibly secure but actually breakable
tagging scheme

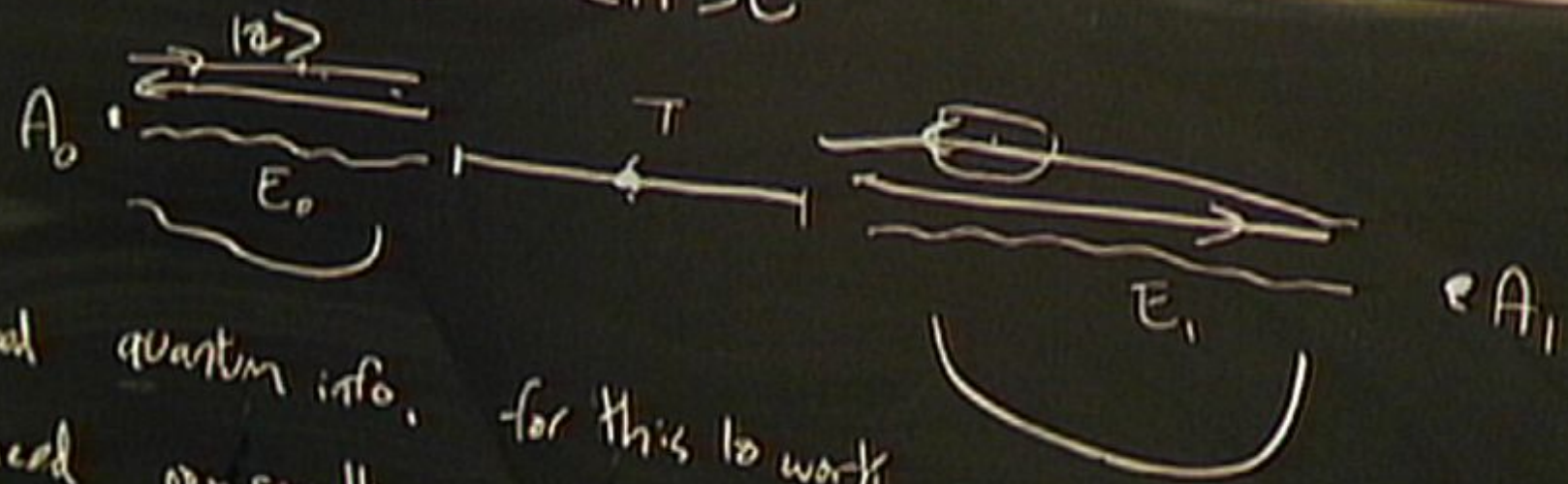

How to devise a plausibly secure but actually breakable tagging scheme :
1
2

How to devise a plausibly secure but actually breakable tagging scheme:

1


1D CASE
T
E_0
E_1
quantum info.
for this to work
no-signalling

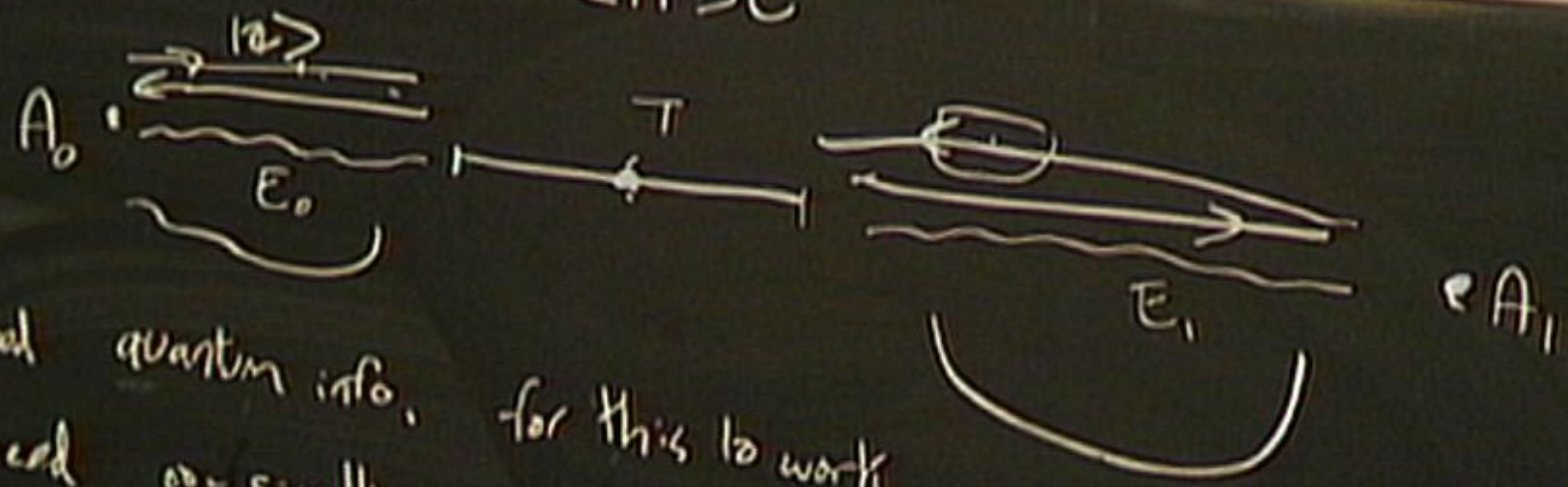
1D CASE



need quantum info. for this to work

need non-signalling

1D CASE

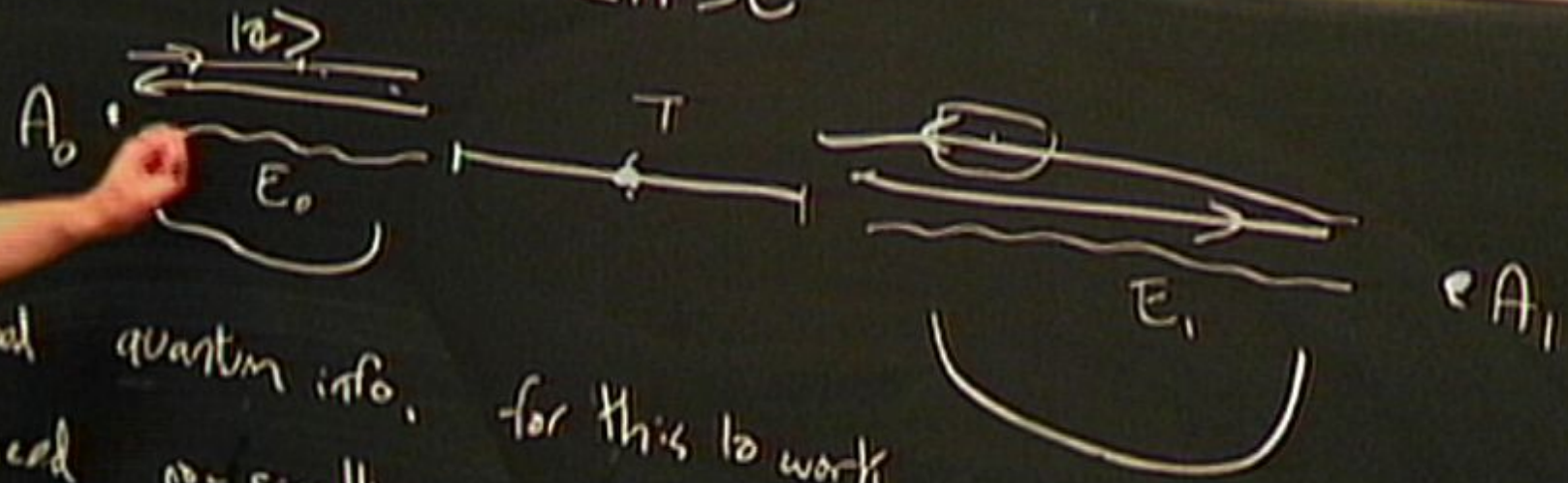


need quantum info. for this to work

need non-signalling

Naive intuition (from no-cloning) is that q. info

1D CASE



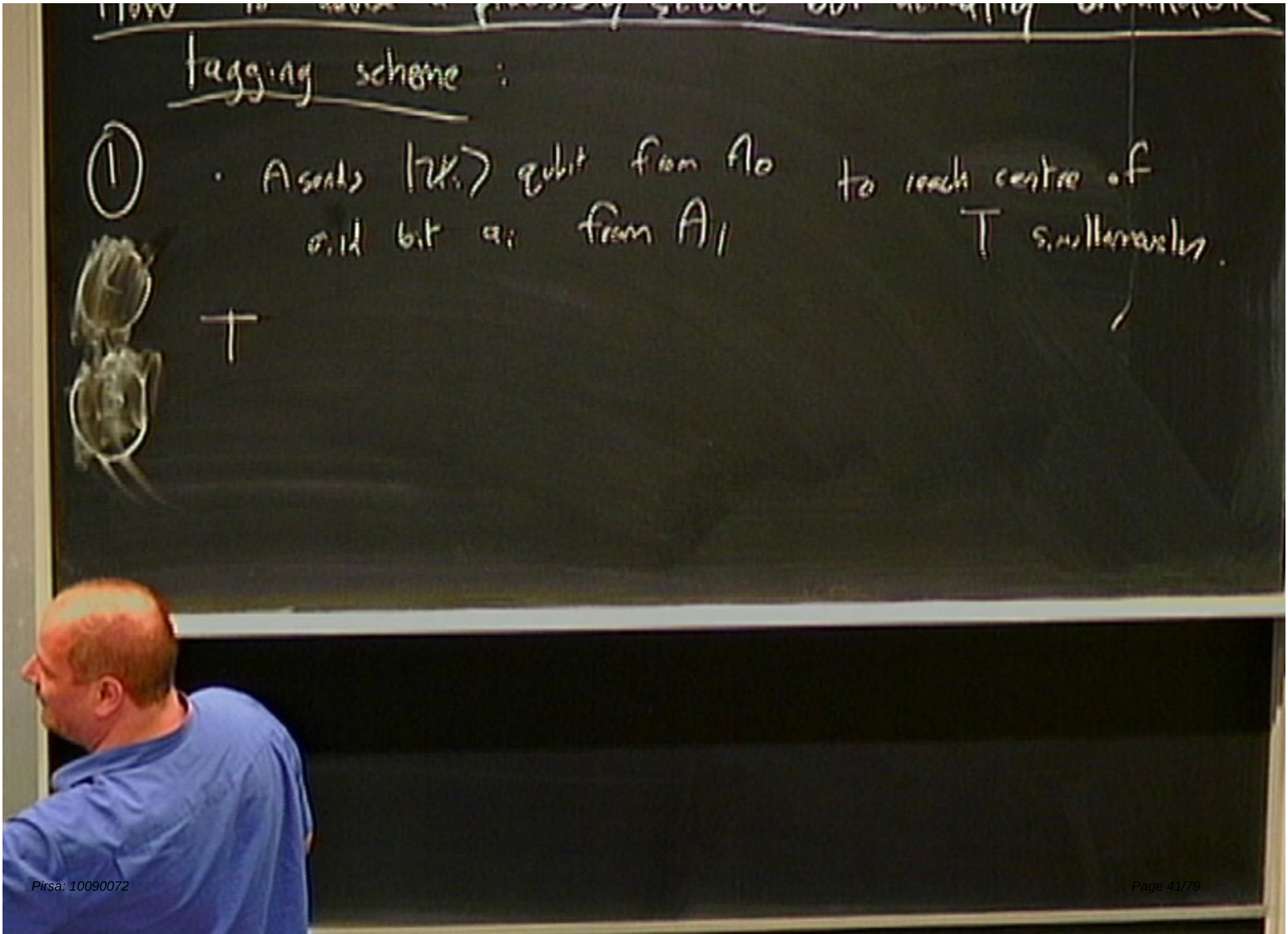
need quantum info. for this to work

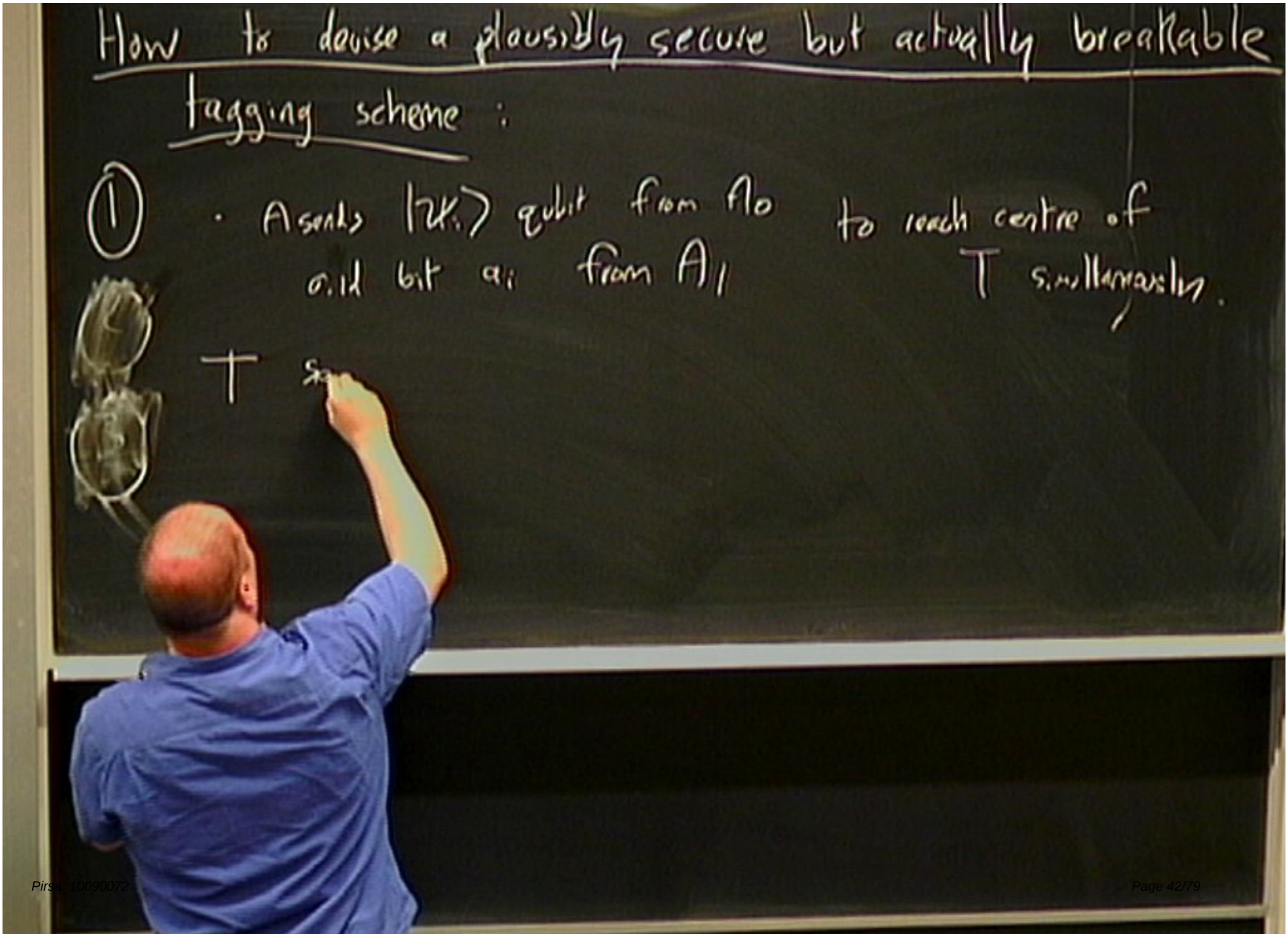
need non-signalling

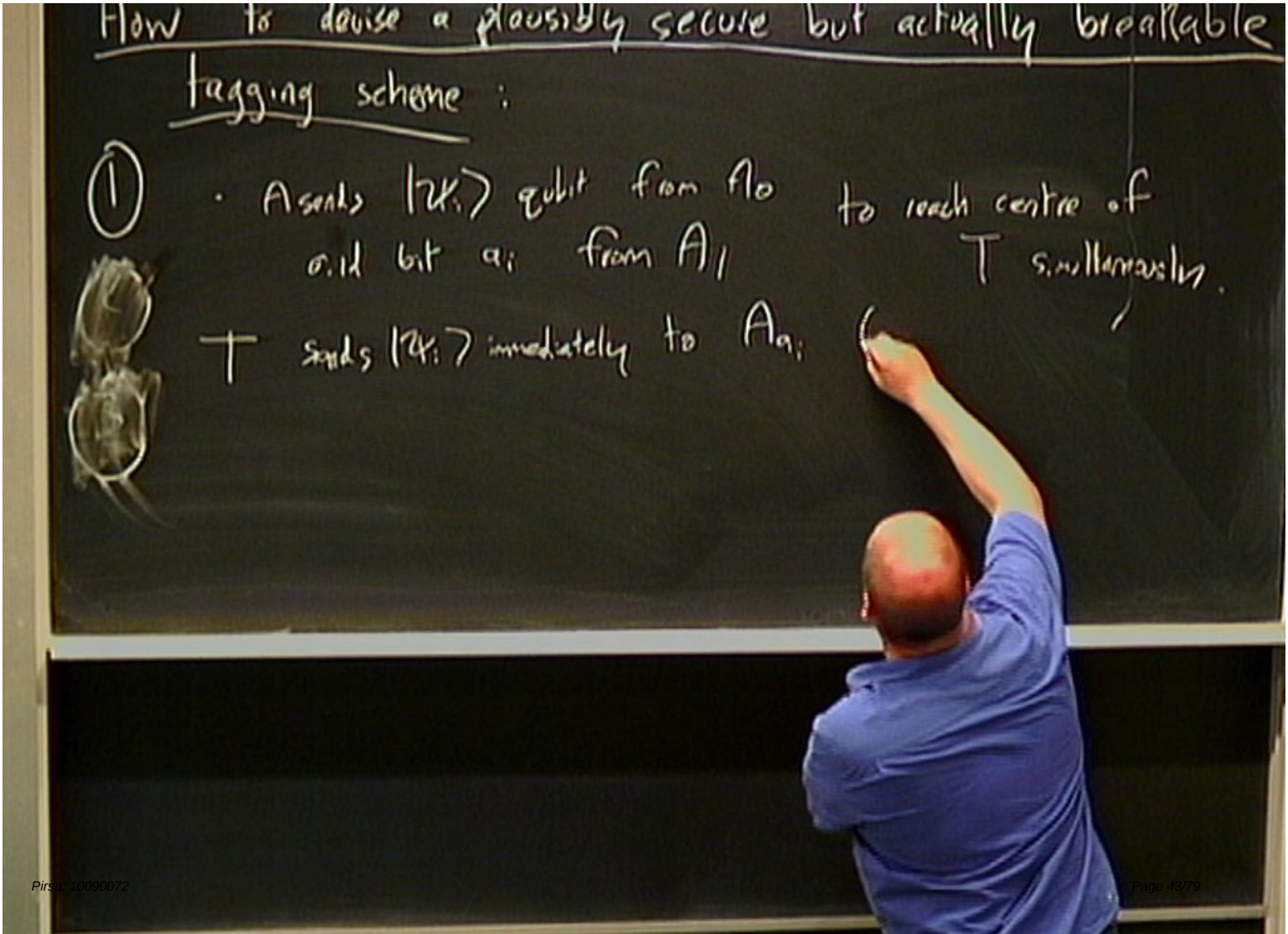
Naive intuition (from no-cloning) is that q. info follows a definite trajectory

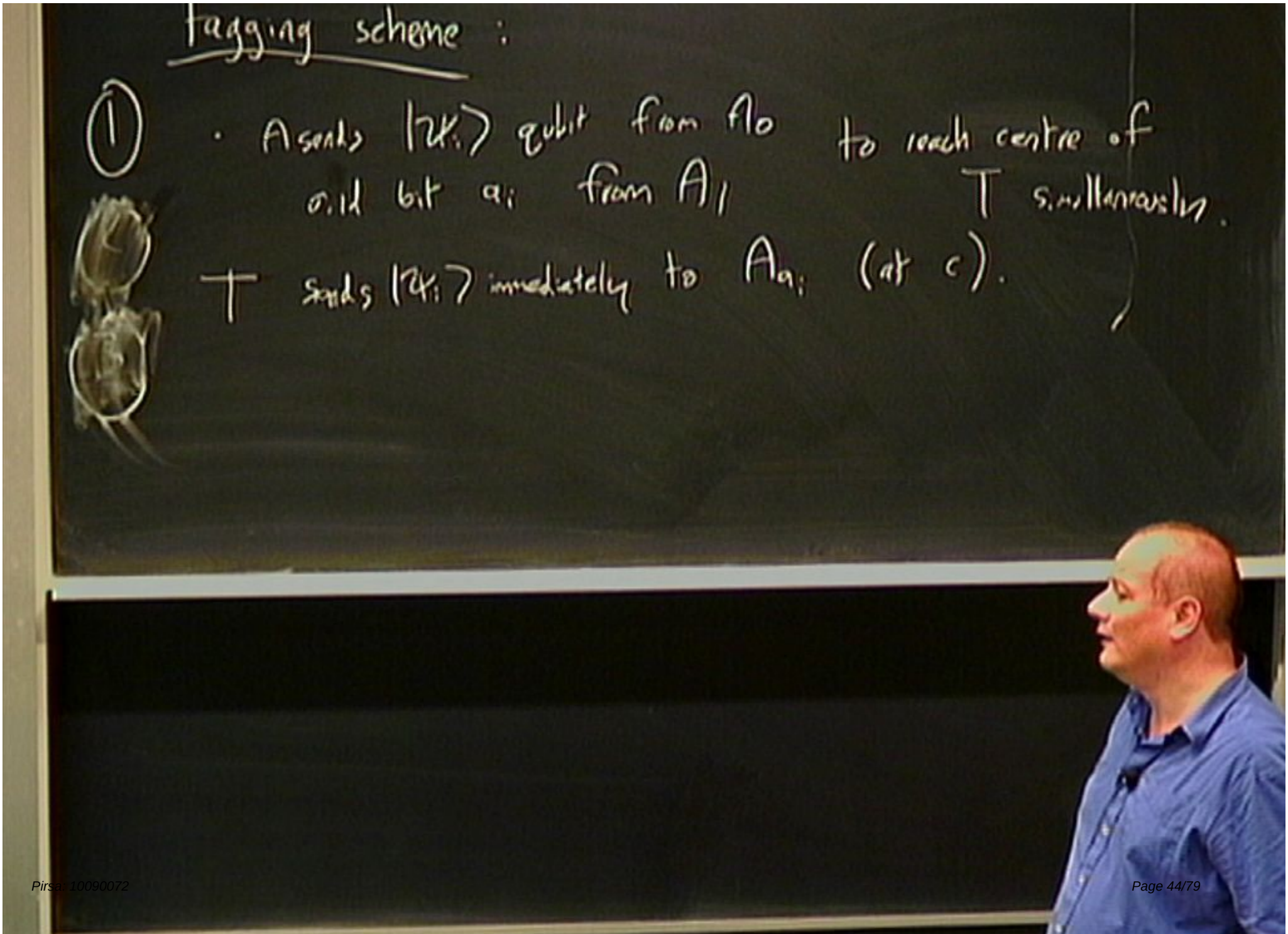
How to devise a plausibly secure but actually breakable tagging scheme :

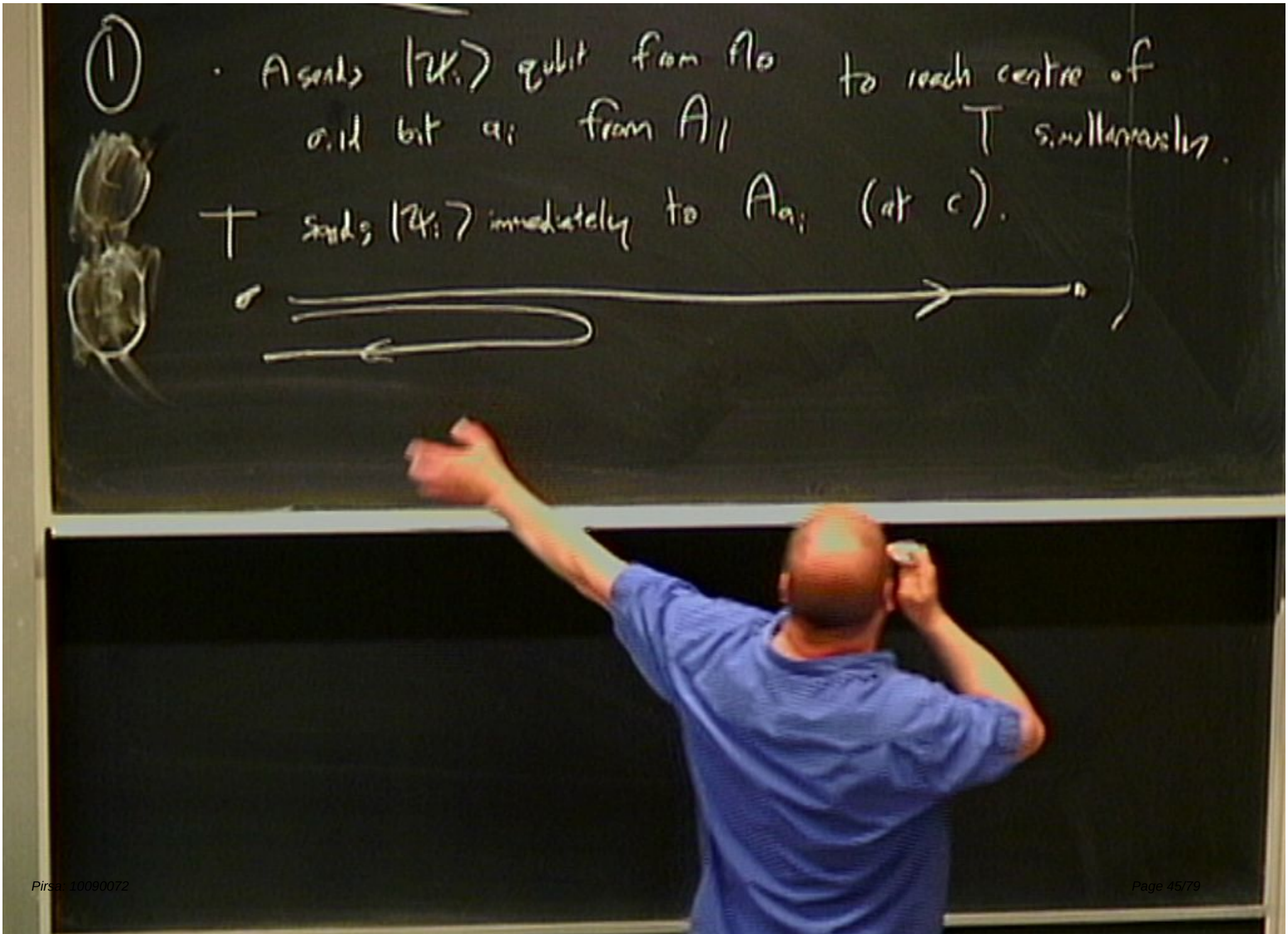
(1) · A sends $|\psi_i\rangle$ qubit from A_0
o.id bit a_i from A_1


tagging scheme :
1
· A sends |ψ_i⟩ qubit from A_0 to each centre of
and bit a_i from A_1 T simultaneously.
T


How to devise a plausibly secure but actually breakable
tagging scheme :
1
· A sends |ψ_i⟩ qubit from A_0 to reach centre of
o.id bit a_i from A_1 T simultaneously.
T


How to devise a plausibly secure but actually breakable
tagging scheme :
1
· A sends |ψ_i⟩ qubit from A_0 to reach centre of
o.id bit a_i from A_1 T simultaneously.
T sends |ψ_i⟩ immediately to A_{a_i}

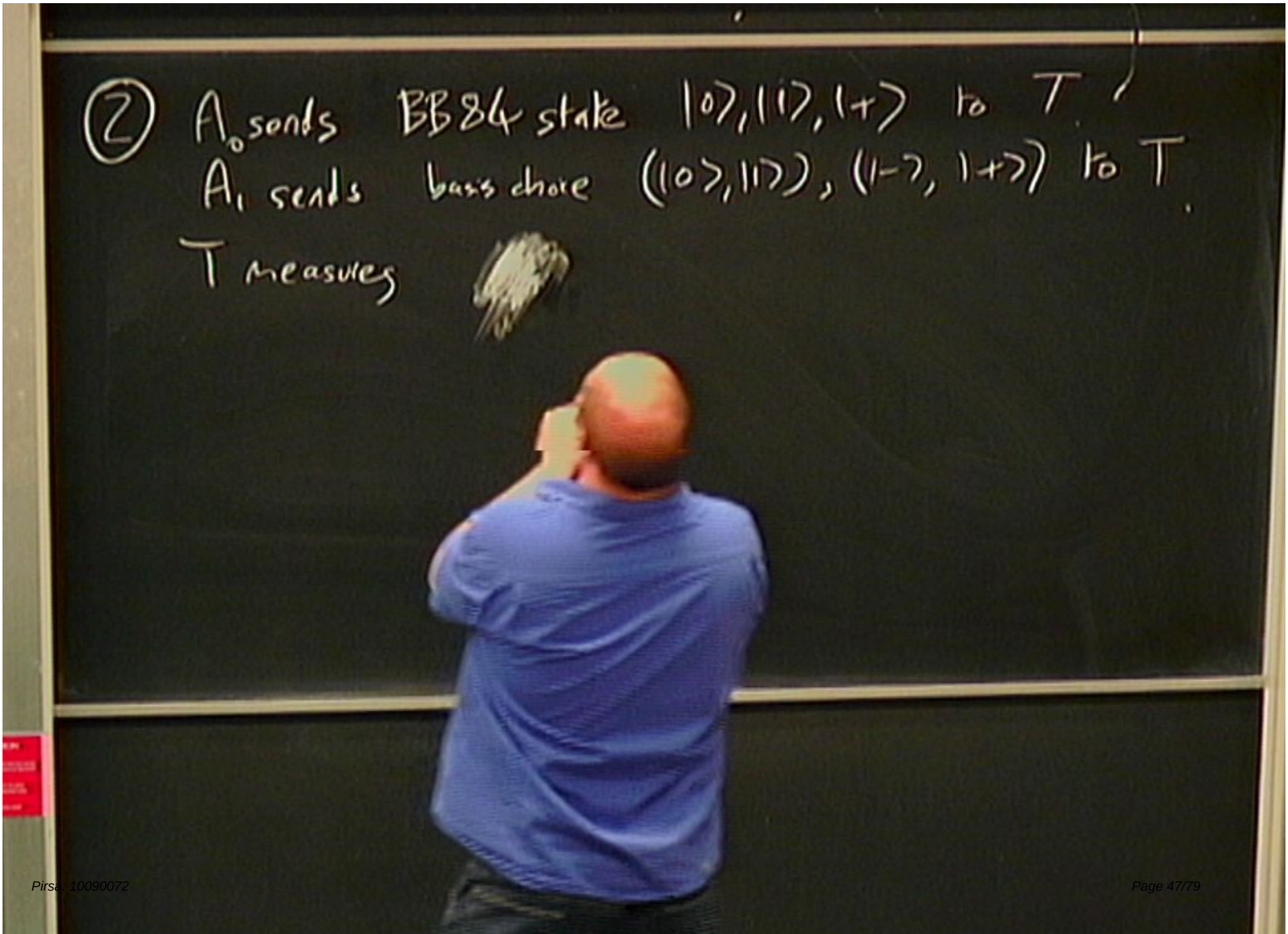

Tagging scheme :
1
· A sends |ψ_i⟩ qubit from A_0 to reach centre of
o.id bit a_i from A_1 T simultaneously.
T sends |ψ_i⟩ immediately to A_{a_i} (at c).


1
· A sends |ψ_i⟩ qubit from A_0 to reach centre of
o.ld bit a_i from A_1 T simultaneously.
T sends |ψ_i⟩ immediately to A_{a_i} (at c).

How to devise a plausibly secure but actually breakable tagging scheme:

(1) · A sends $|\psi_i\rangle$ qubit from A_0 to reach centre of and bit a_i from A_1 T simultaneously.

T sends $|\psi_i\rangle$ immediately to A_{a_i} (at c).


② A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.
A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.
T measures

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result.

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result.

(3) $\longrightarrow$ $\longleftarrow$

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.
A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.
T measures and broadcasts result.

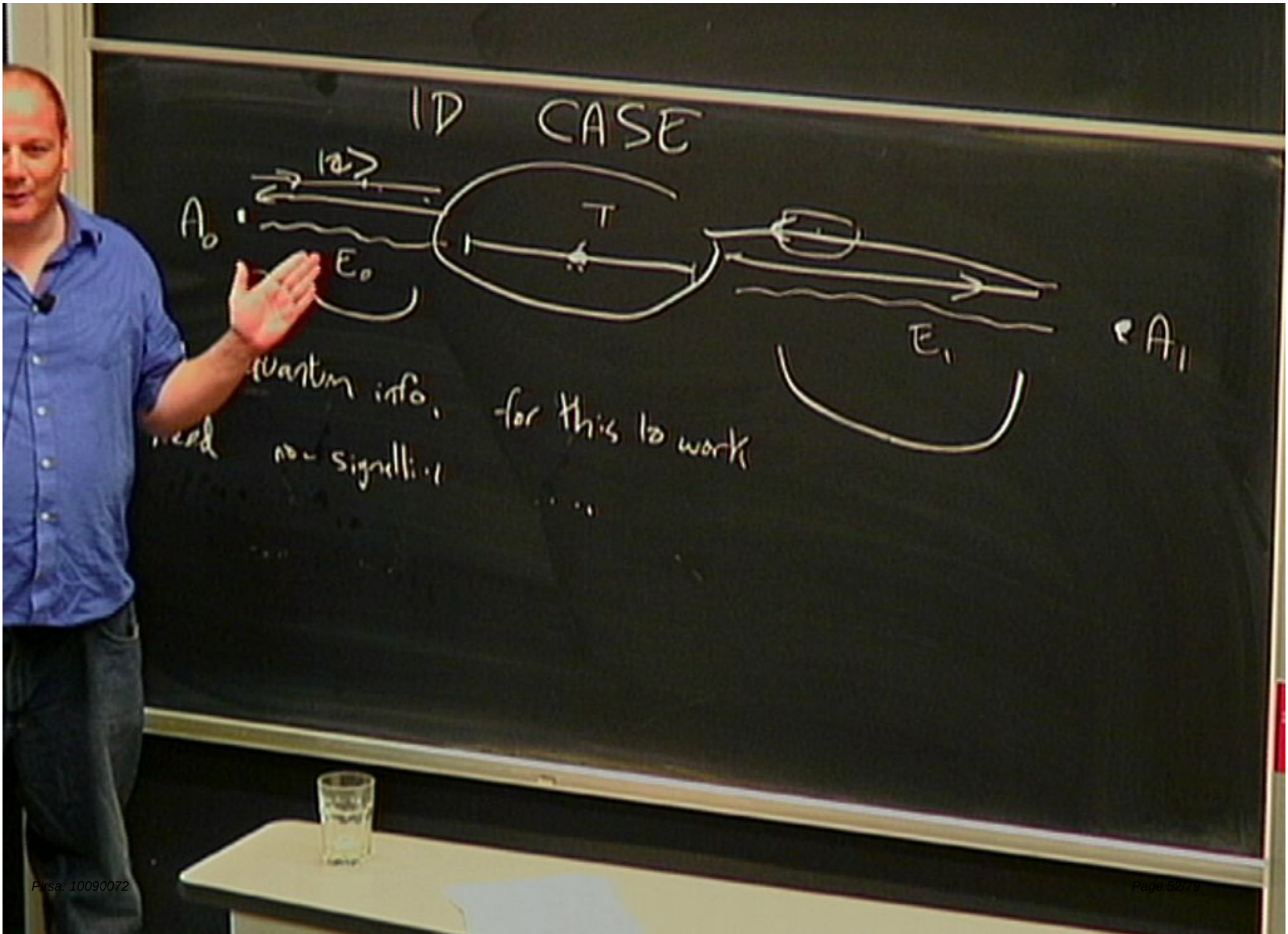
(3) $A_0 \longrightarrow$ $\longleftarrow A_1$

A_0 and A_1

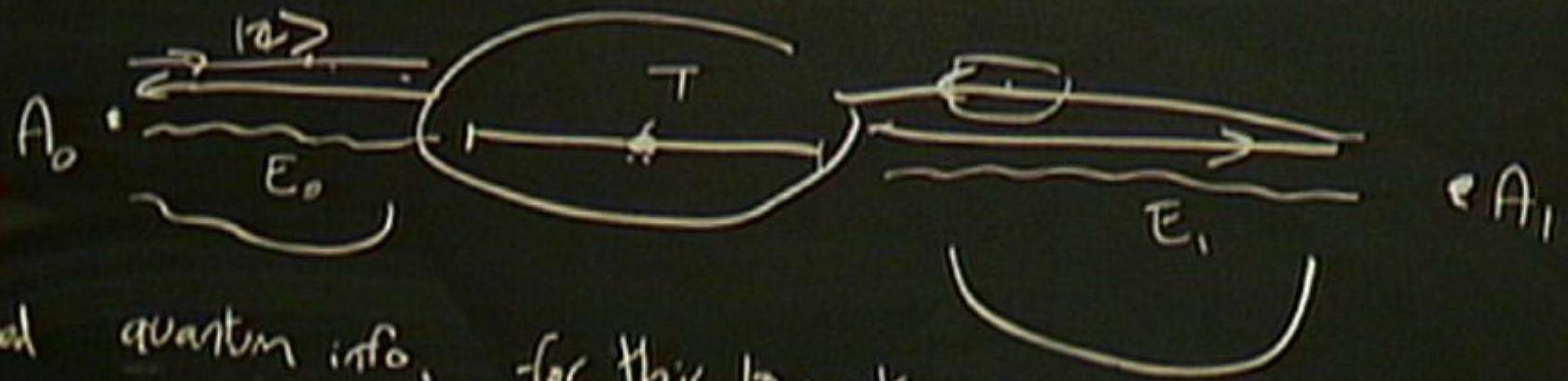
(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.
A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.
T measures and broadcasts result. A checks timings + statistics.

(3) $A_0 \longrightarrow$ $\longleftarrow A_1$

A_0 and A_1

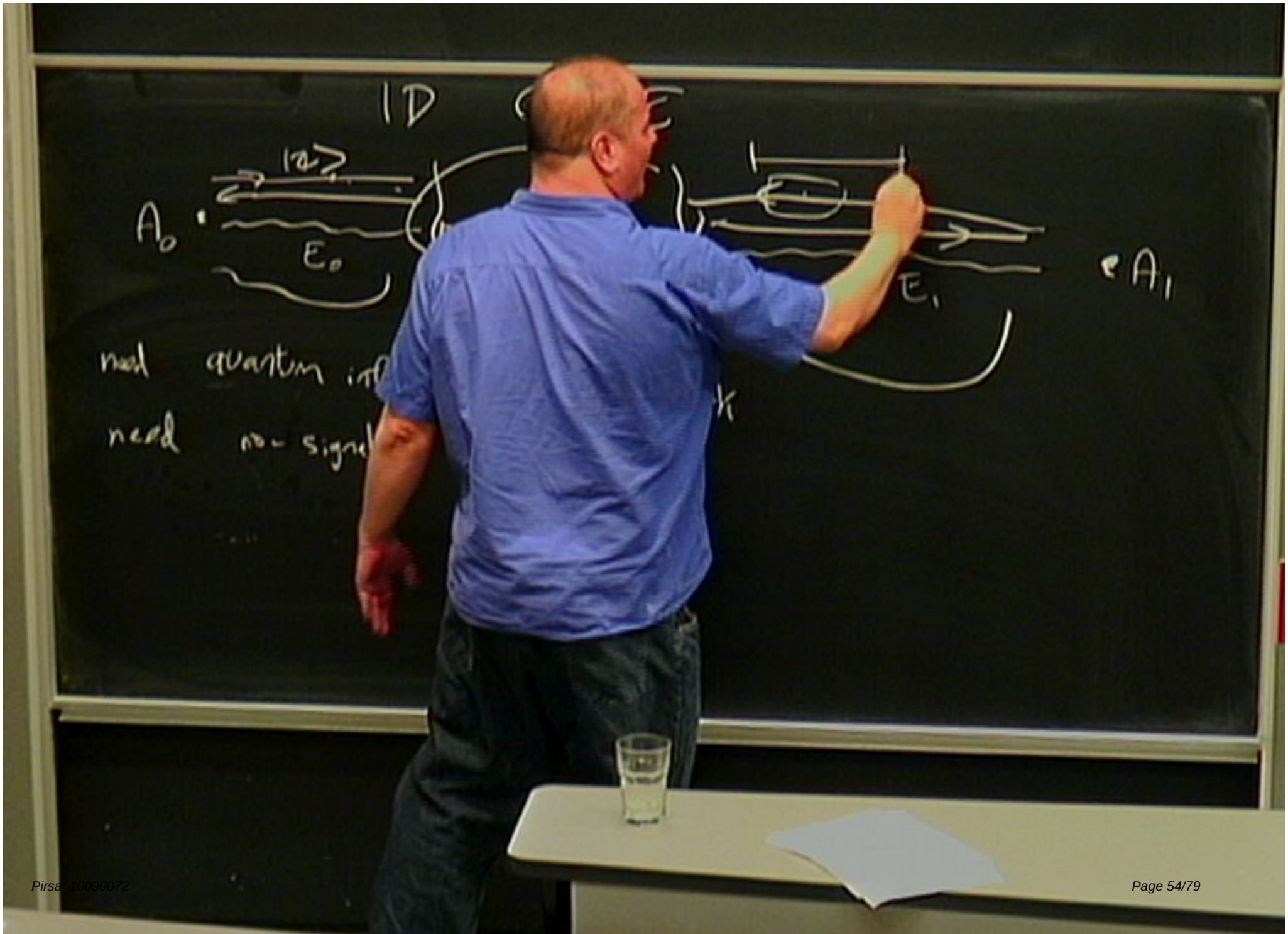

1D CASE
$|\alpha\rangle$
A_0
E_0
T
E_1
A_1
quantum info.
for this to work
need
non-signalling

1D CASE

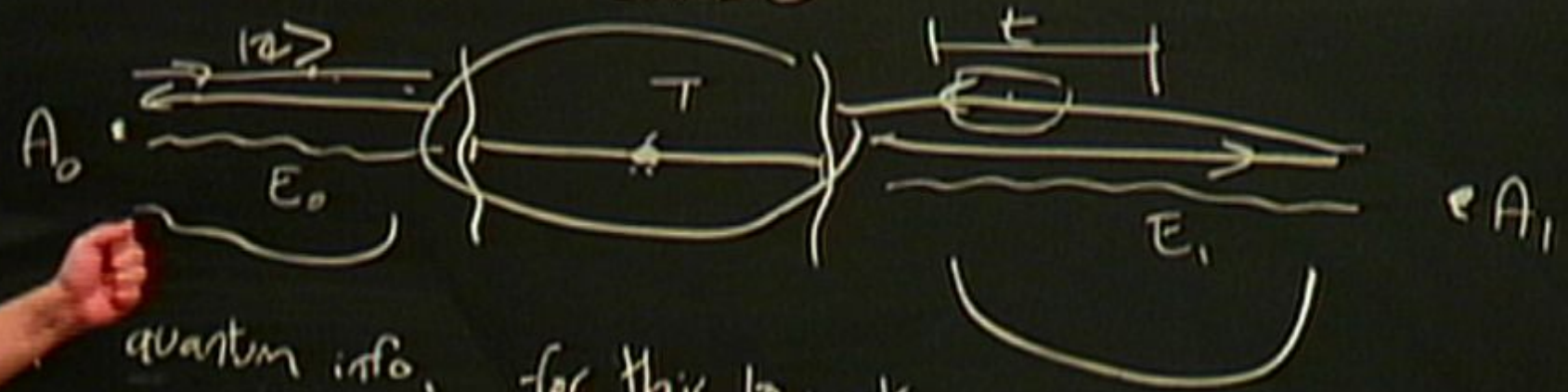


need quantum info. for this to work

need non-signalling

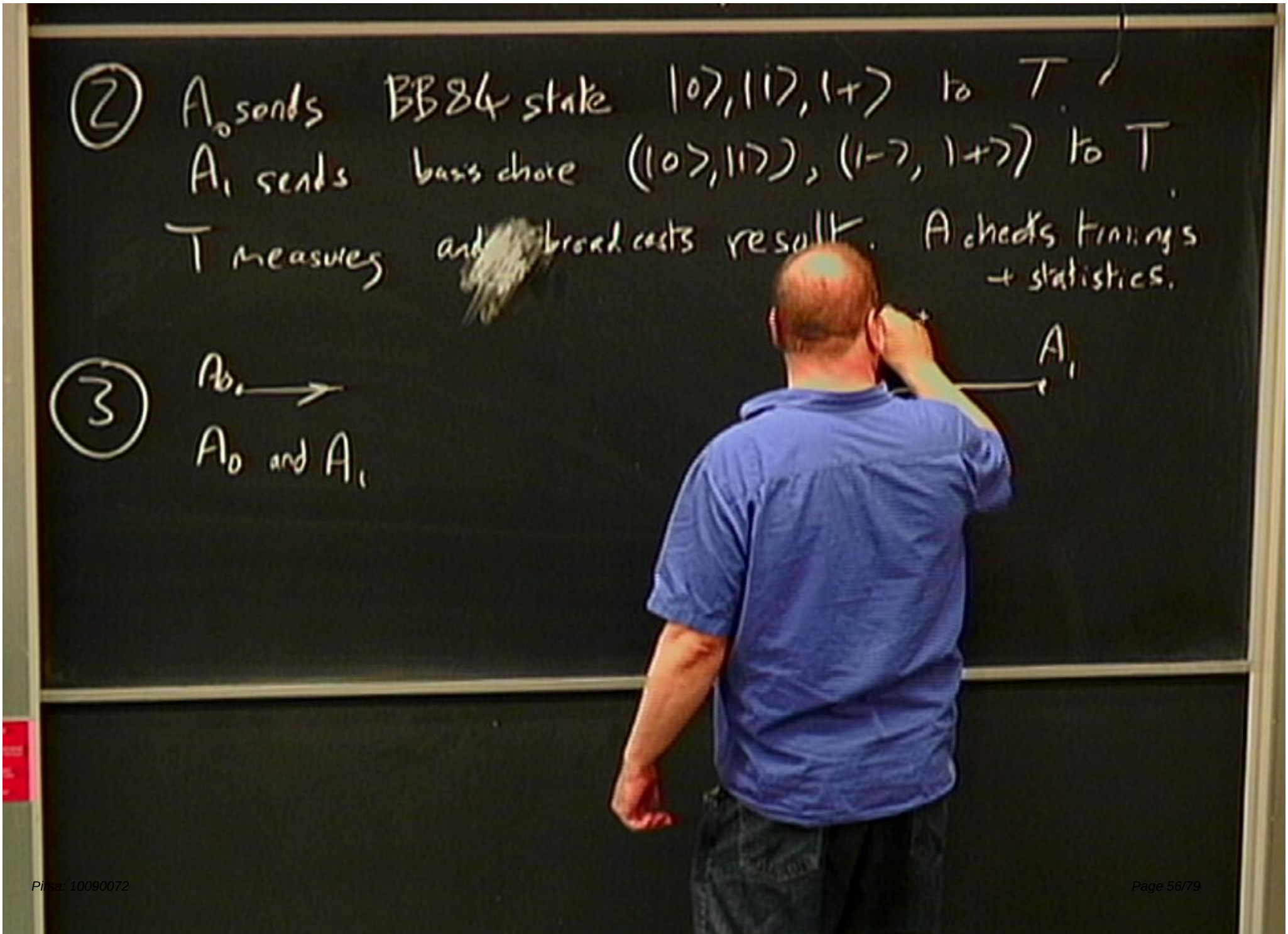

1D
$|\alpha\rangle$
A_0
E_0
E_1
A_1
need quantum
need no-signal

1D CASE



quantum info. for this to work

need non-signalling

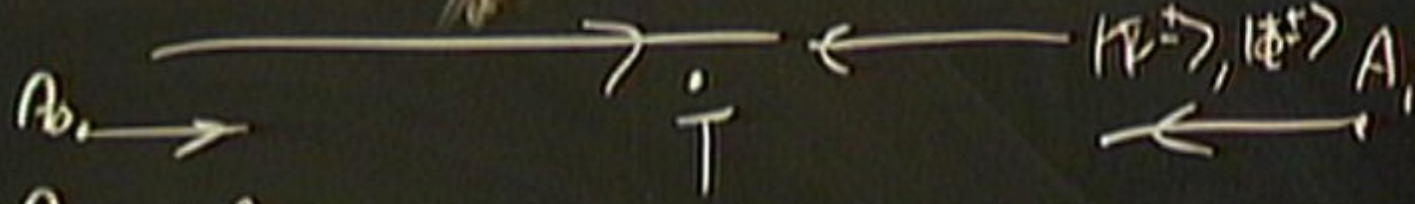

2
A0 sends BB84 state |0⟩, |1⟩, |+⟩ to T
A1 sends basis choice (|0⟩, |1⟩), (|−⟩, |+⟩) to T
T measures and broadcasts result. A checks timings + statistics.
3
A0 →
A0 and A1
A1

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result. A checks timings + statistics

(3)



A_0 and A_1

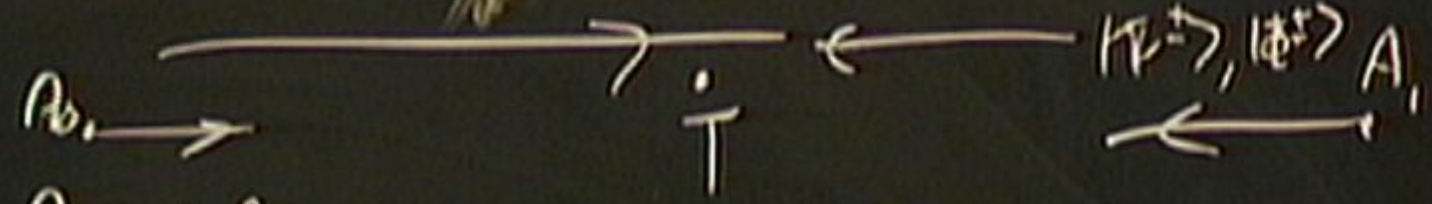
T Bell state measures + broadcasts answer

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T. Chandran et al.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result. A checks timings + statistics.

(3)



A_0 and A_1

T Bell state measures + broadcasts answer.

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T. Chandran et al.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result. A checks timings + statistics.

(3)

$$\begin{tikzcd} A_0 \arrow[rr] & & T & & A_1 \arrow[ll] \arrow[lll, "|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle"'] \end{tikzcd}$$

Malaney.

A_0 and A_1

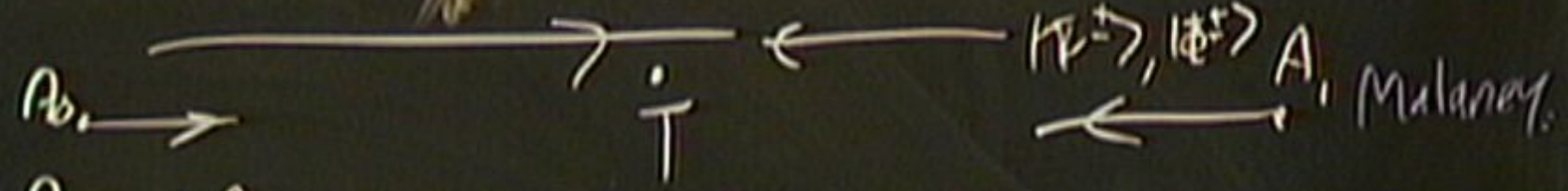
T Bell state measures + broadcasts answer.

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T. Chandran et al.

A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result. A checks timings + statistics.

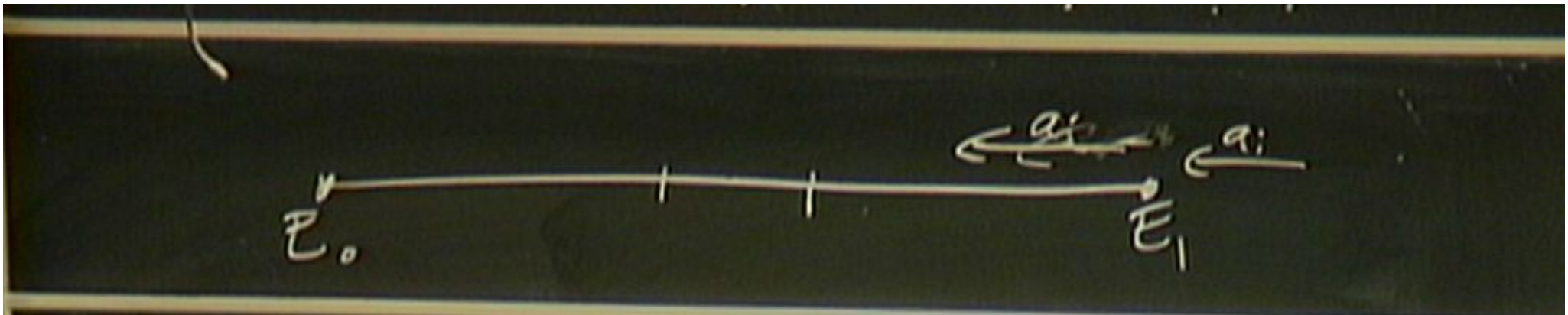
(3)



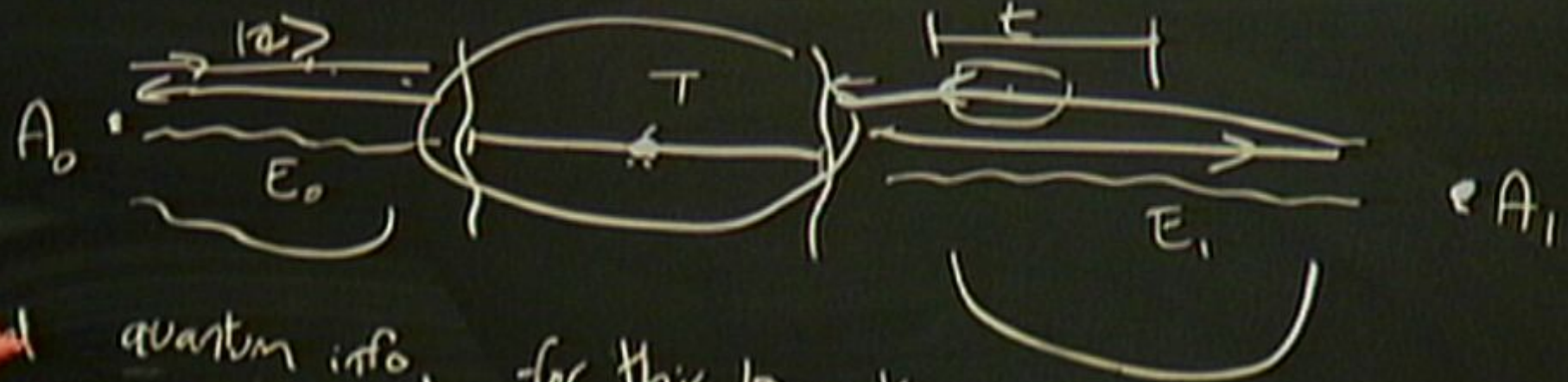
Malaney.

A_0 and A_1

T Bell state measures + broadcasts answer.



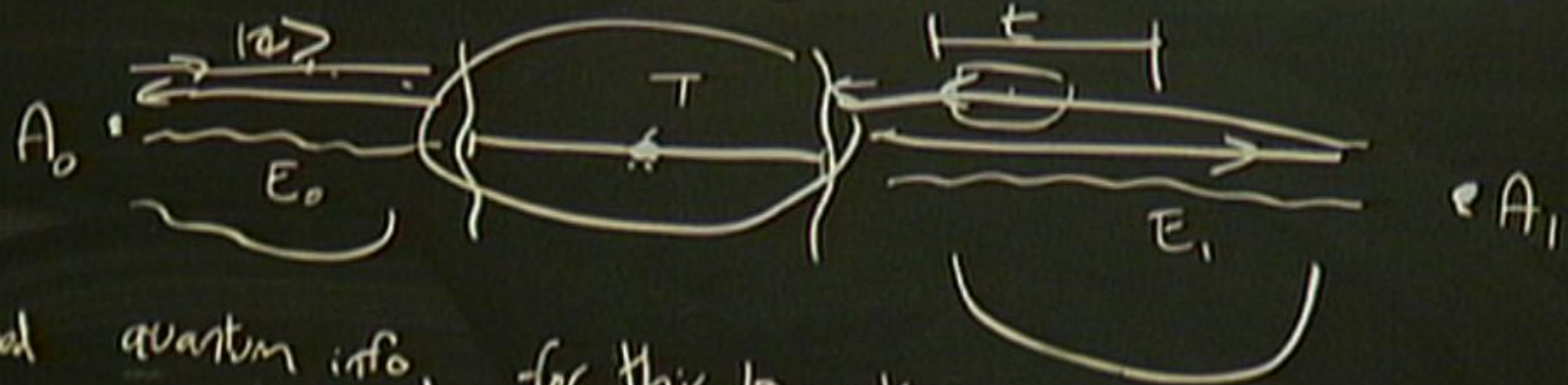
1D CASE



quantum info. for this to work

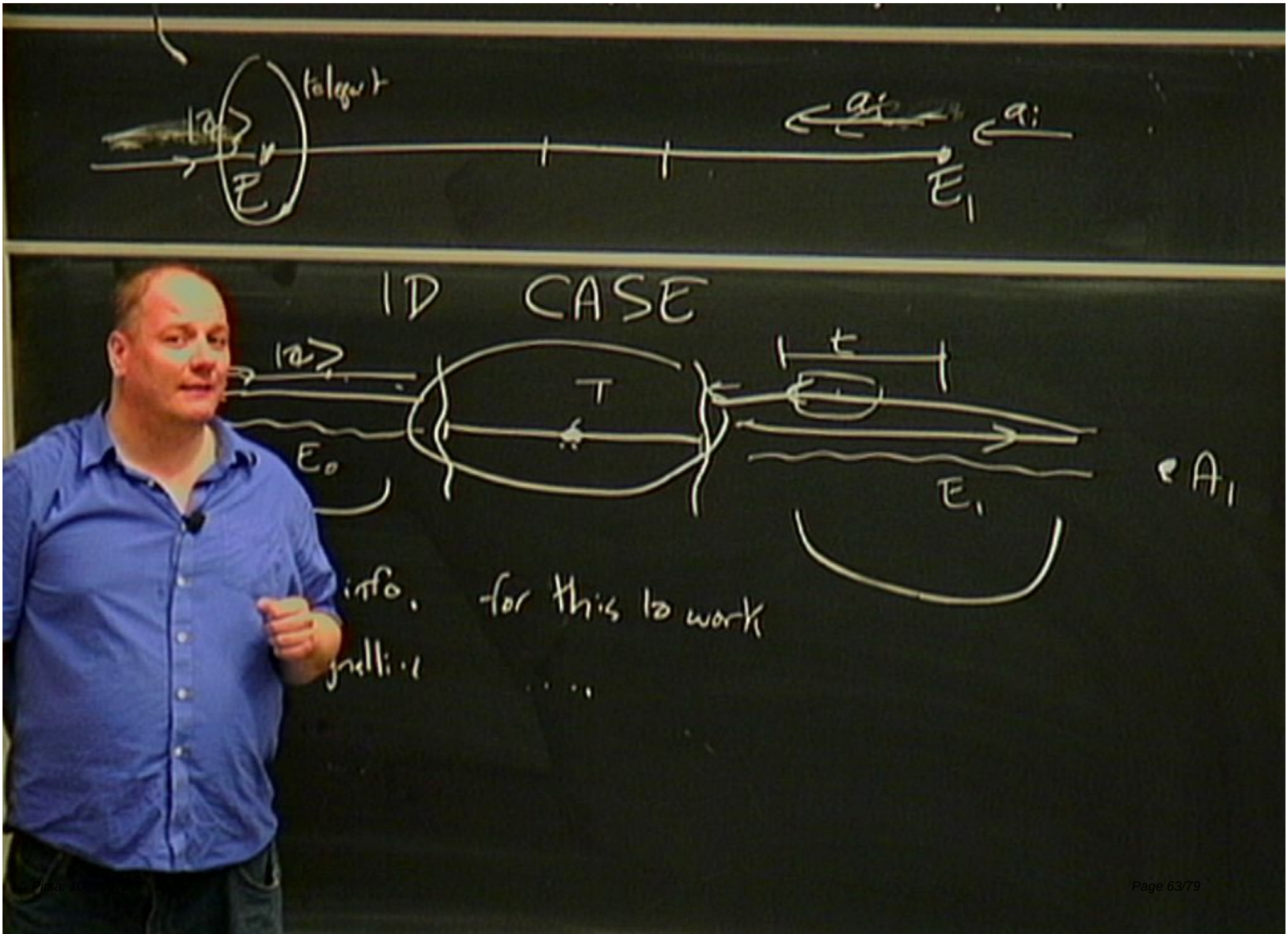
need no-signalling

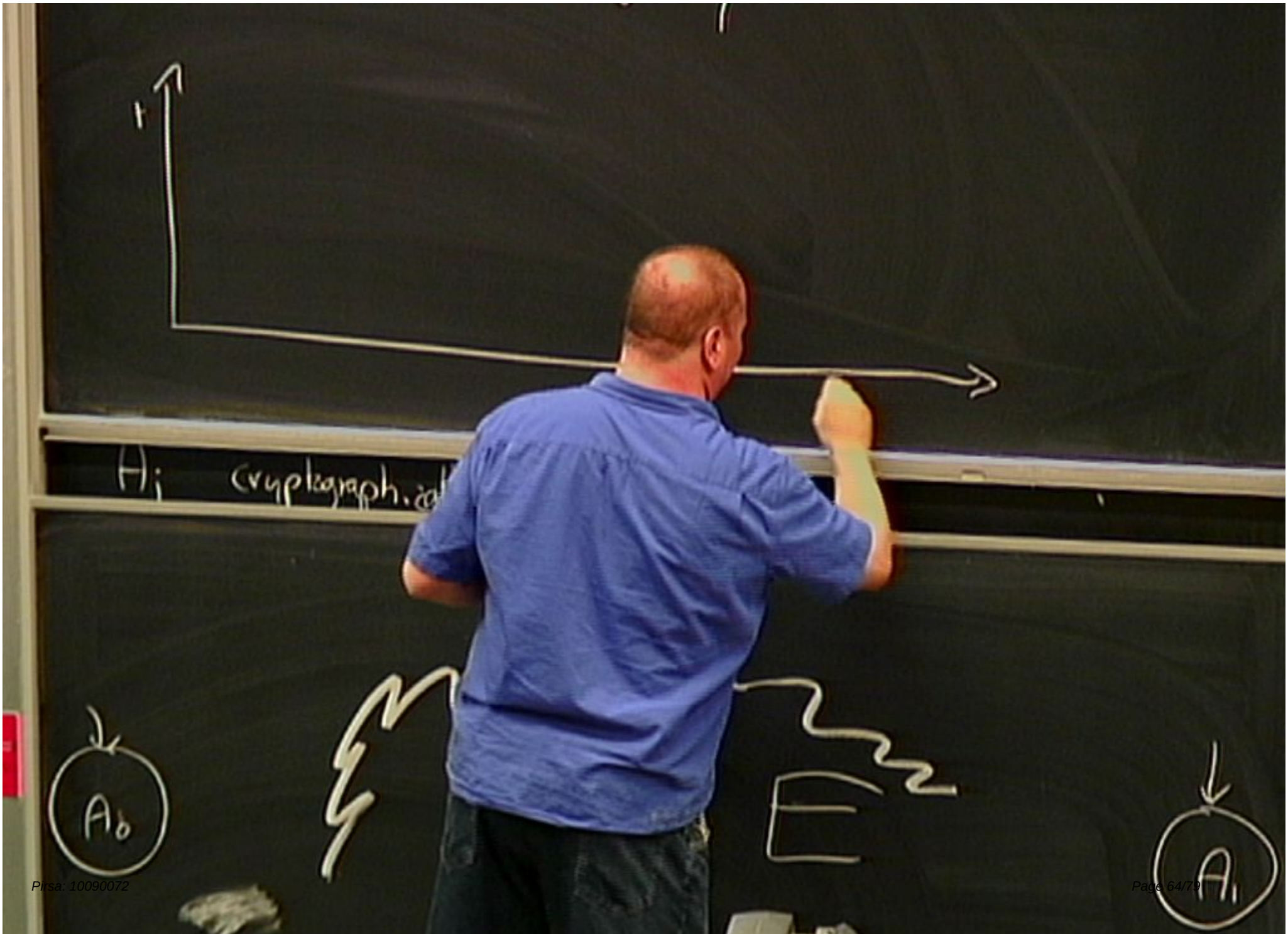
1D CASE

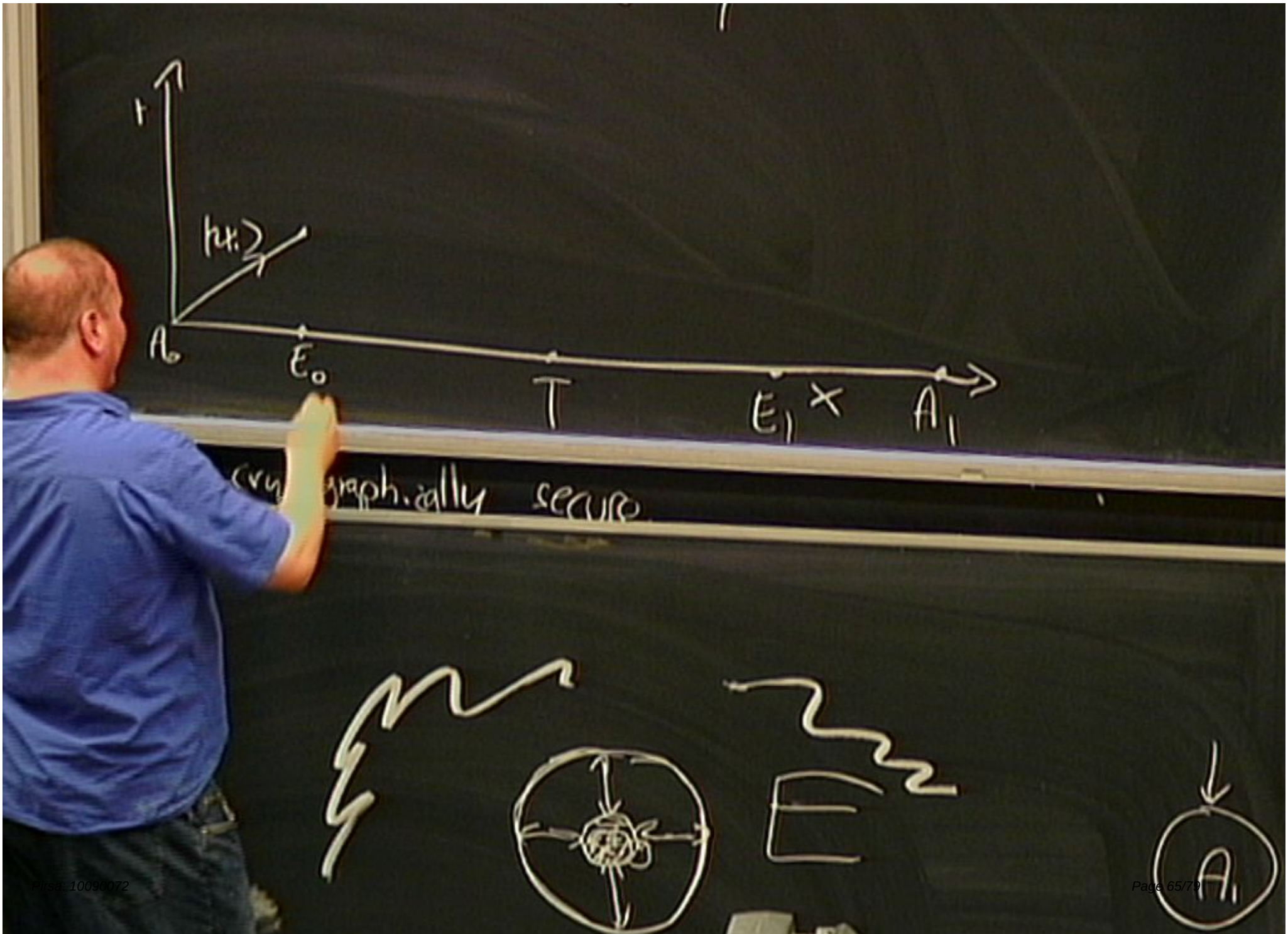


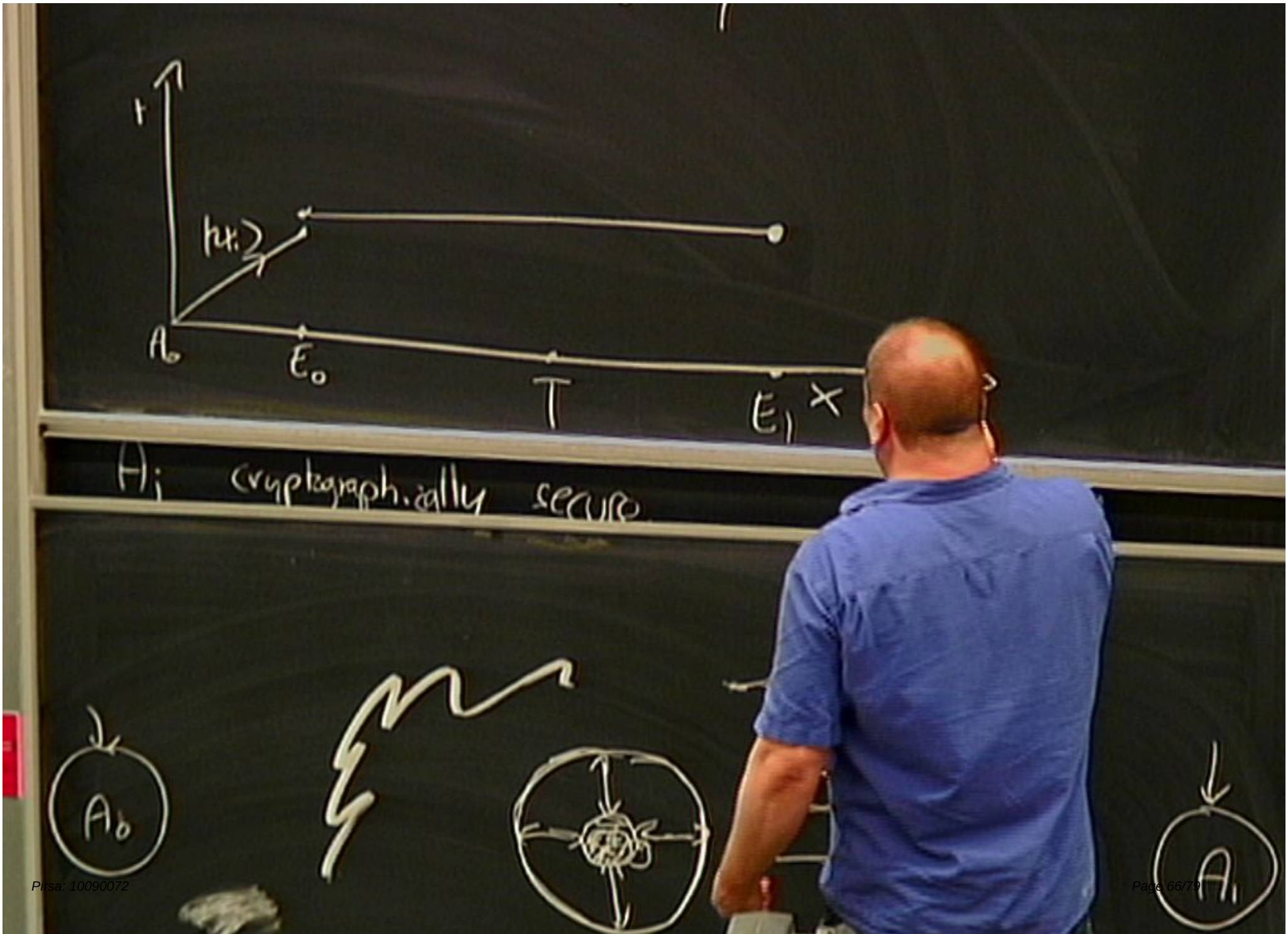
need quantum info. for this to work

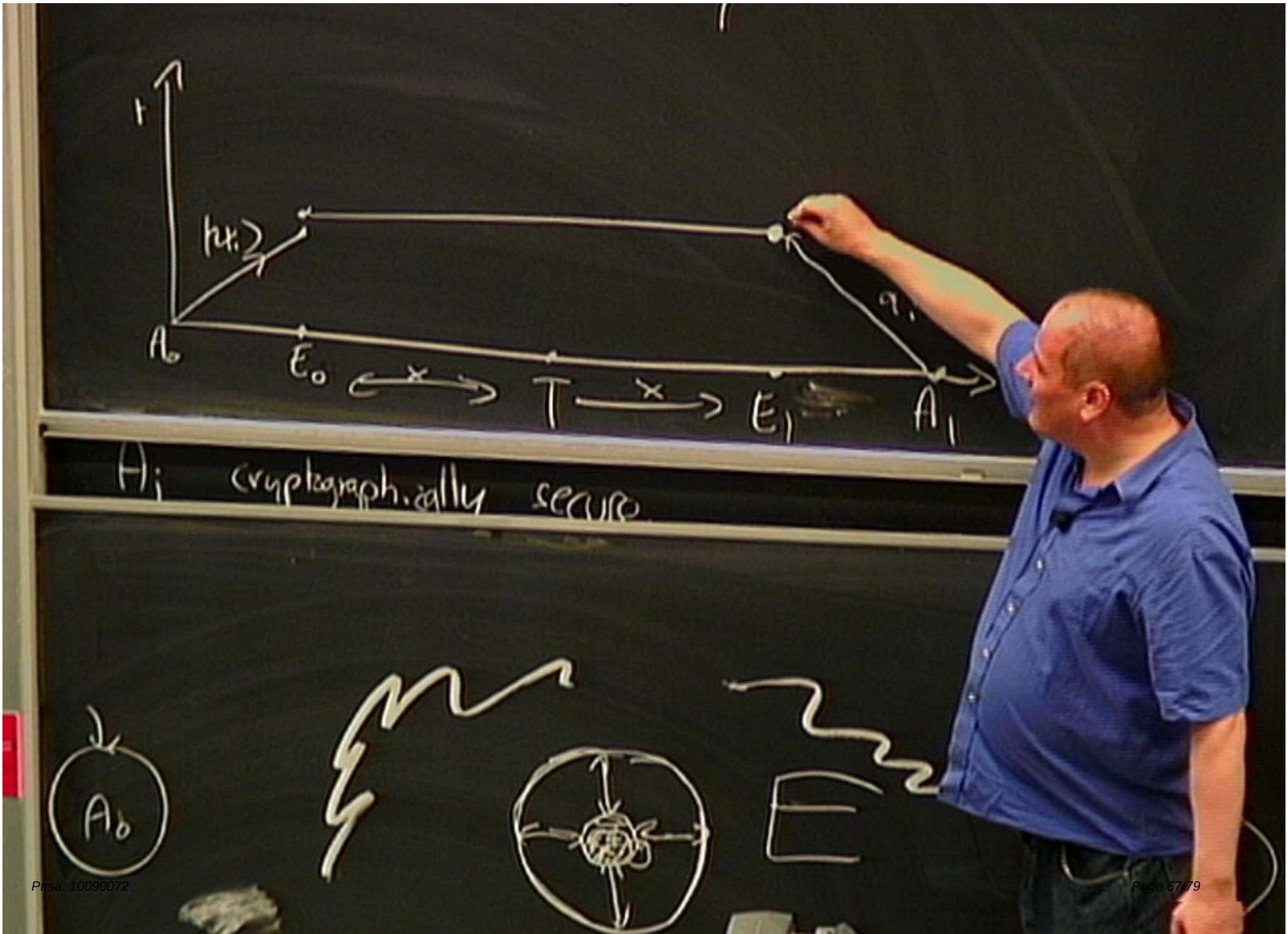
need non-signalling ...


1D CASE
T
E₀
E₁
A₁
for this to work

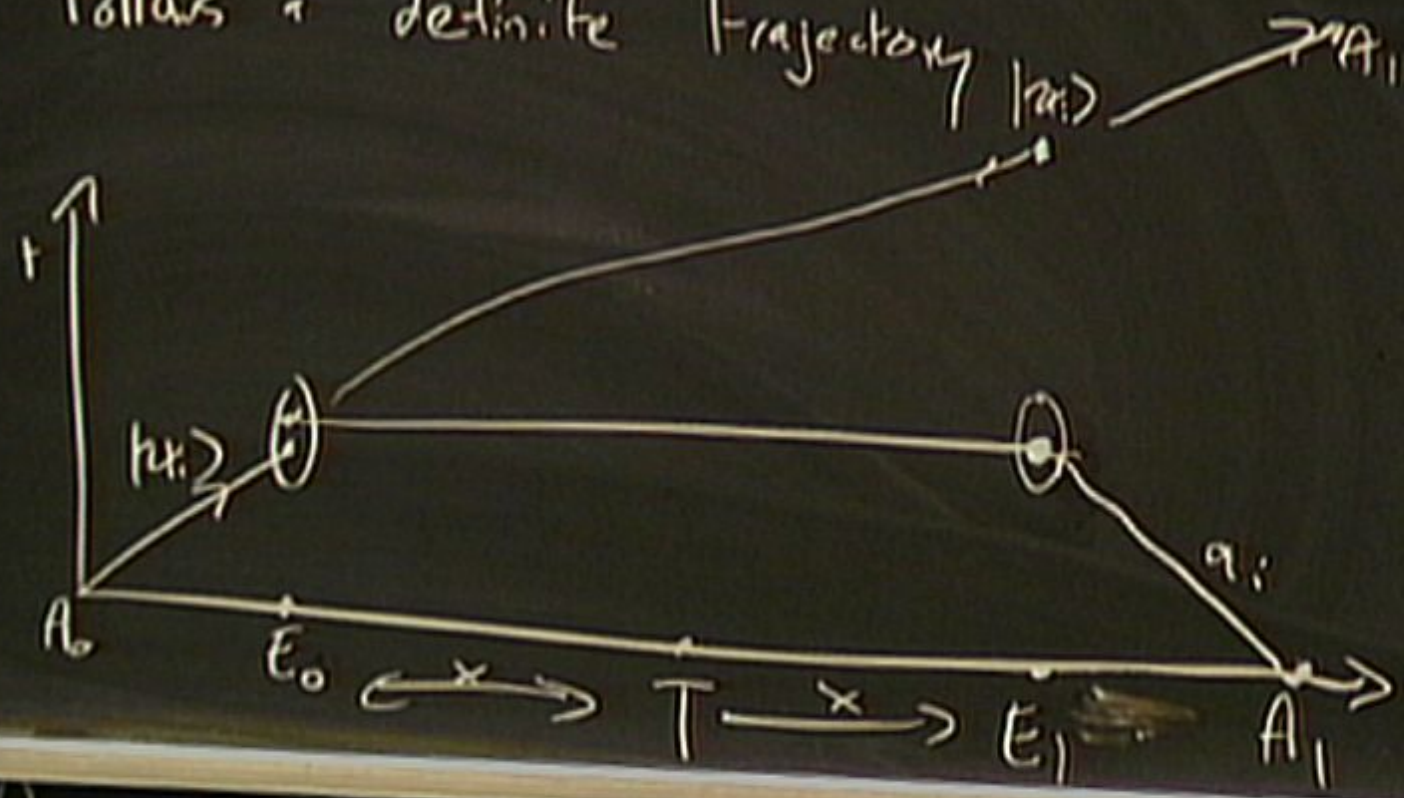

Hi cryptograph.
A0
E
A1


1
A0
E0
T
E1
x
A1
secure
A1

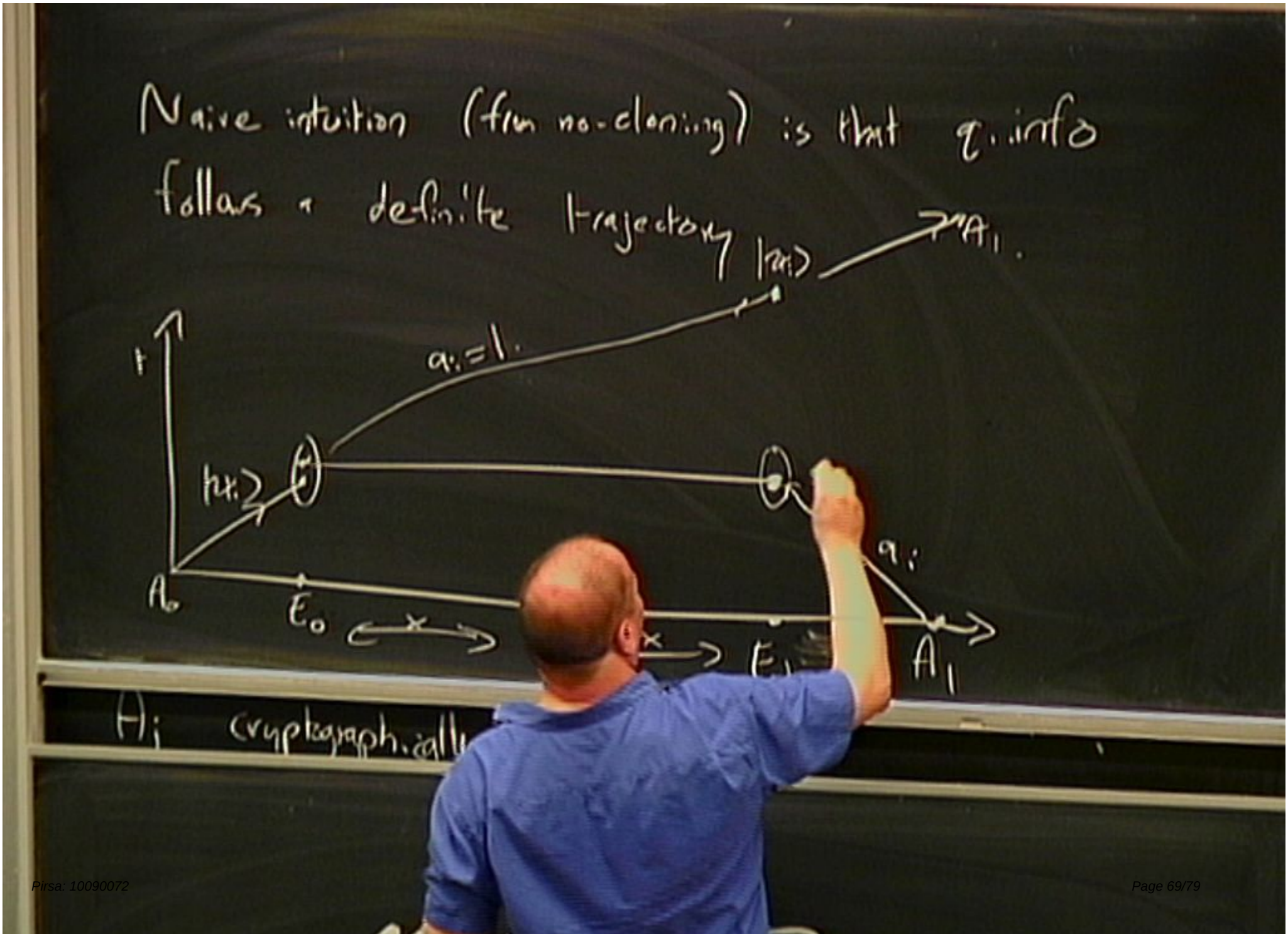

A_0
E_0
T
E_1
x
A_i cryptographically secure
A_0
A_1


A_0
E_0
T
E_1
A_1
A_i cryptographically secure
A_0
E

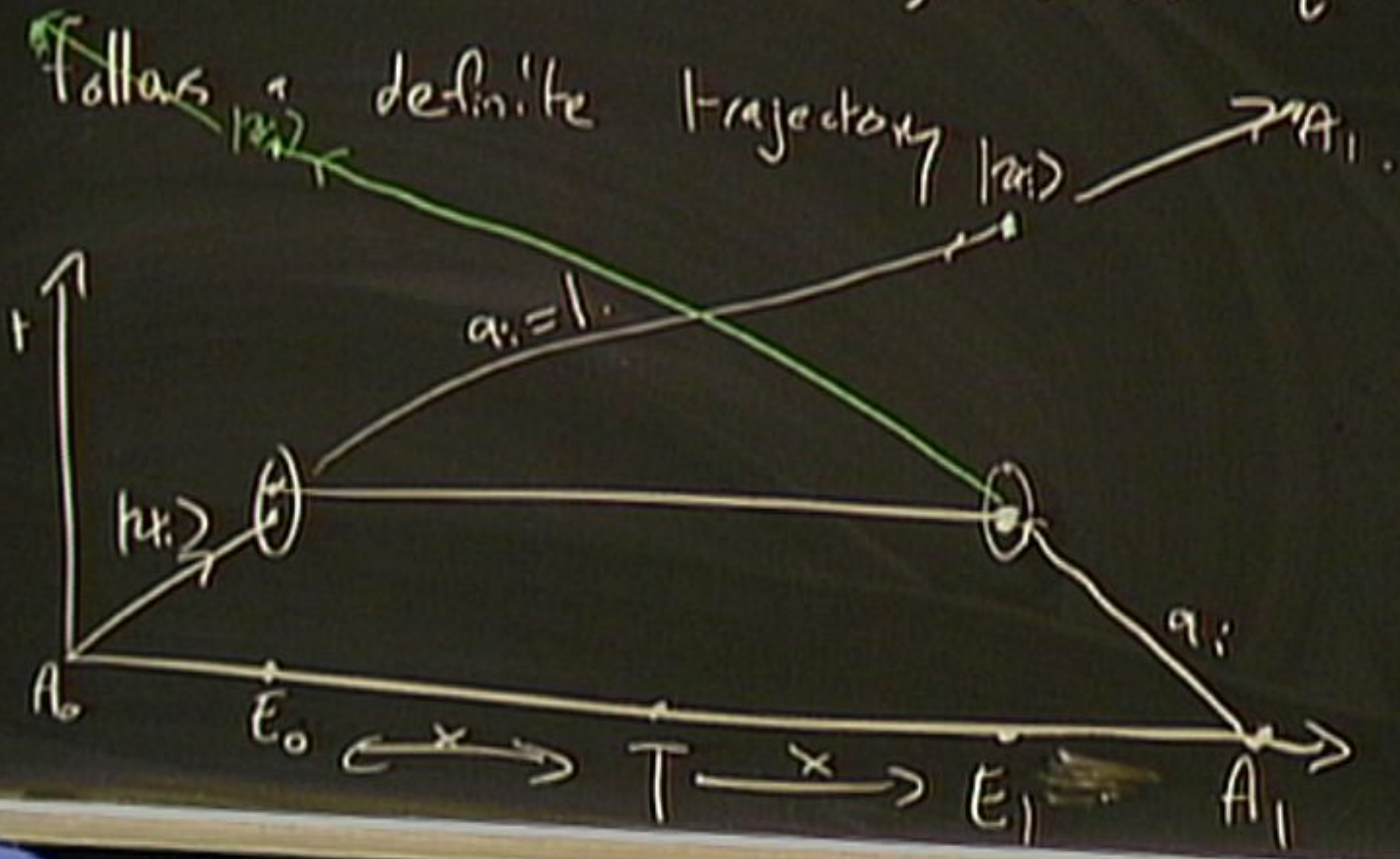
Naive intuition (from no-cloning) is that q. info follows a definite trajectory



A_i cryptographically secure

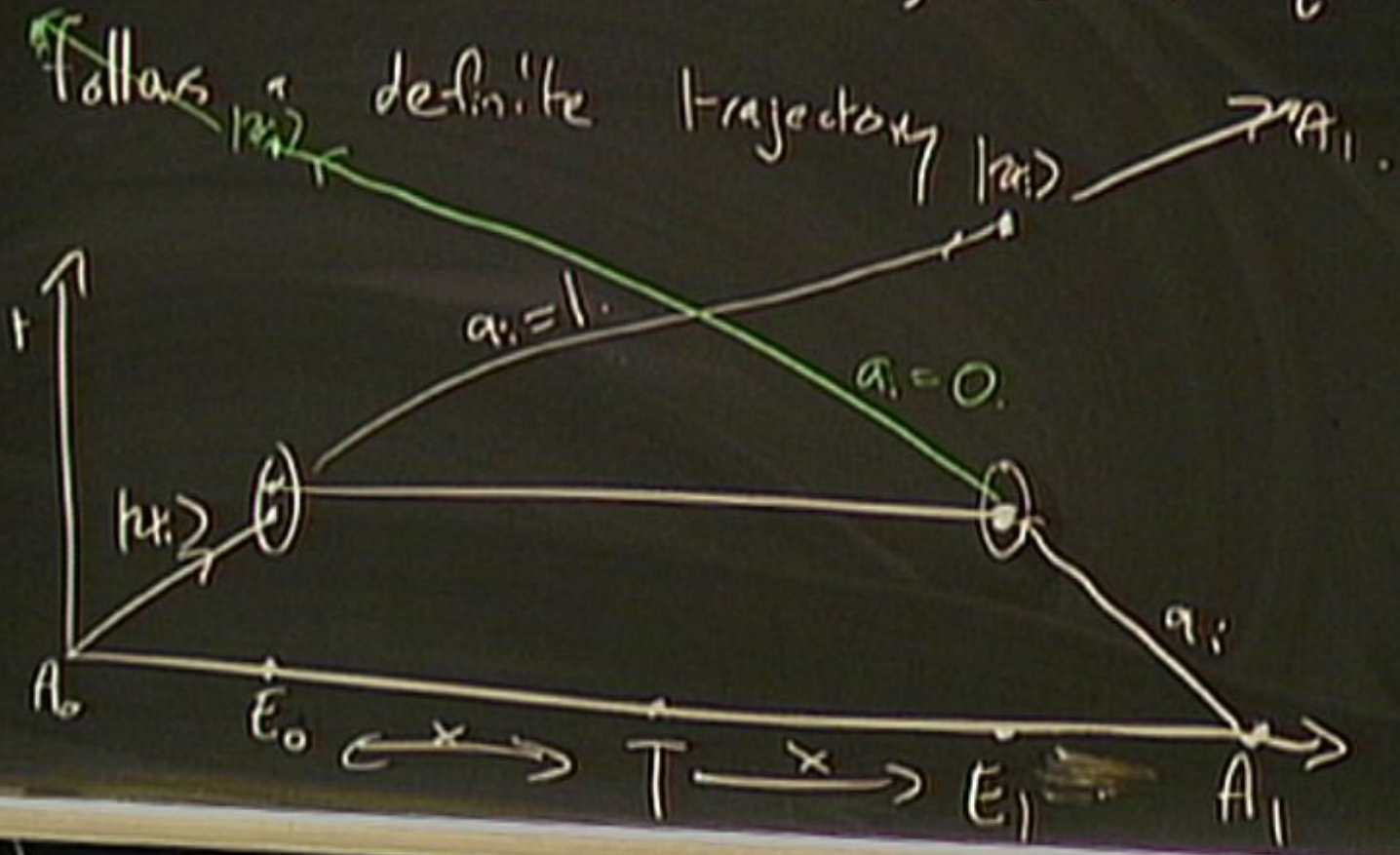

Naive intuition (from no-cloning) is that q. info
follows a definite trajectory
$|x_i\rangle$
A_1
$a_i = 1$
$|x_i\rangle$
a_i
A_0
E_0
E_1
A_1
A_i cryptographically

Naive intuition (from no-cloning) is that q. info follows a definite trajectory

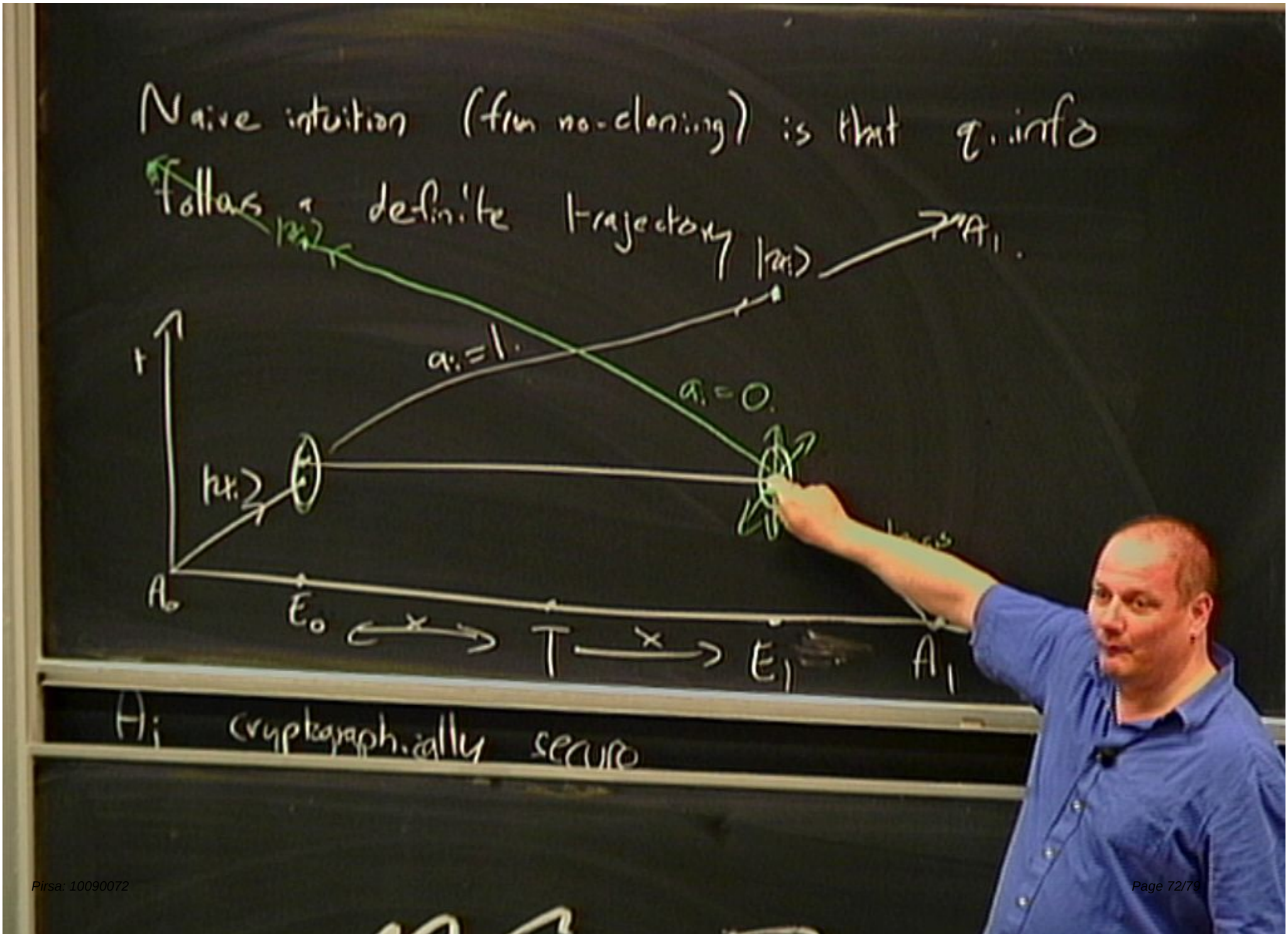


cryptographically secure

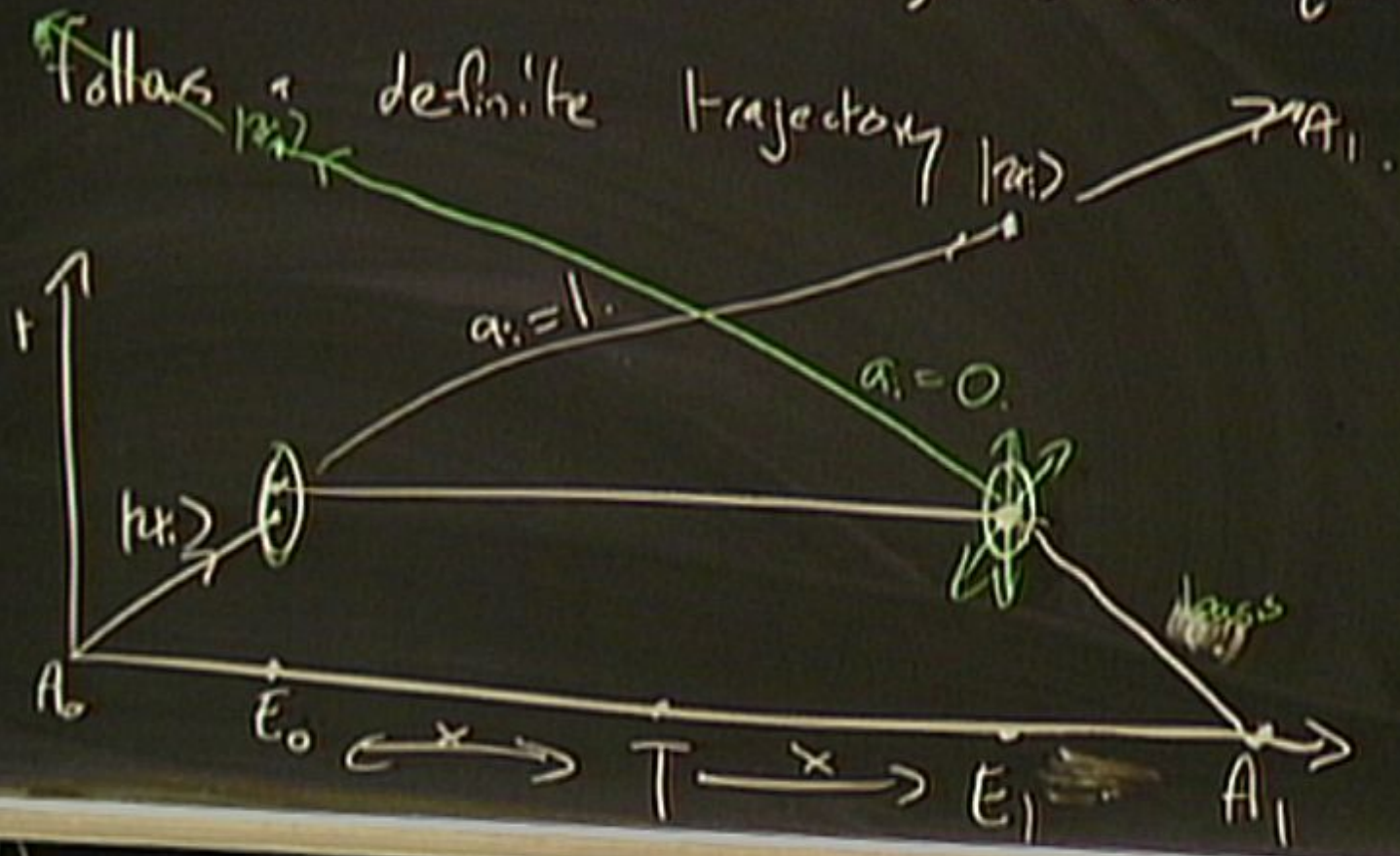
Naive intuition (from no-cloning) is that q. info follows a definite trajectory



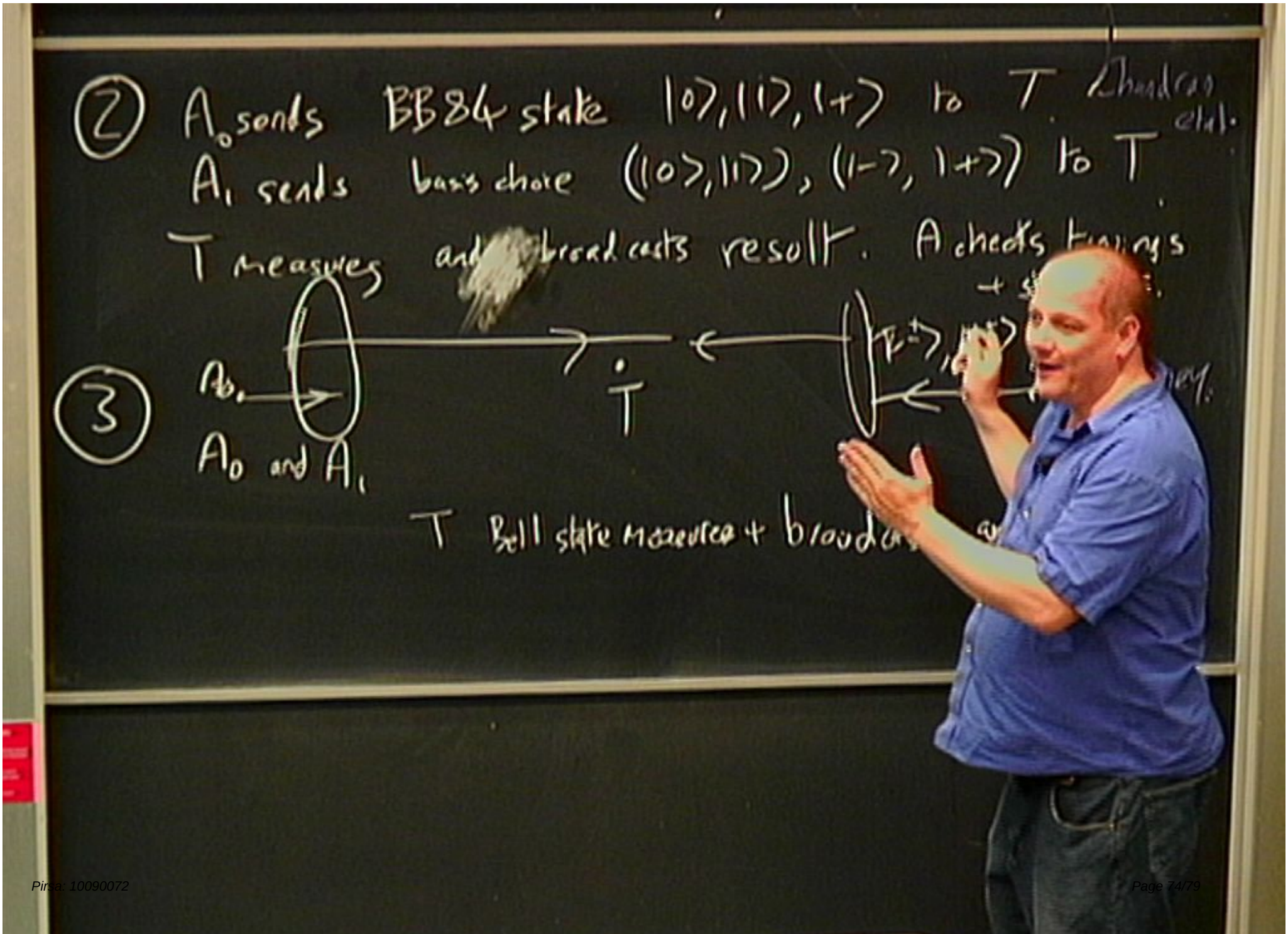
A_i cryptographically secure


Naive intuition (from no-cloning) is that q. info
follows a definite trajectory
$|\alpha_1\rangle$
$|\alpha_1\rangle$
A_1
$a_1 = 1$
$a_1 = 0$
$|\alpha_1\rangle$
A_0
E_0
T
E_1
A_1
A_i cryptographically secure

Naive intuition (from no-cloning) is that q. info follows a definite trajectory



A_i cryptographically secure

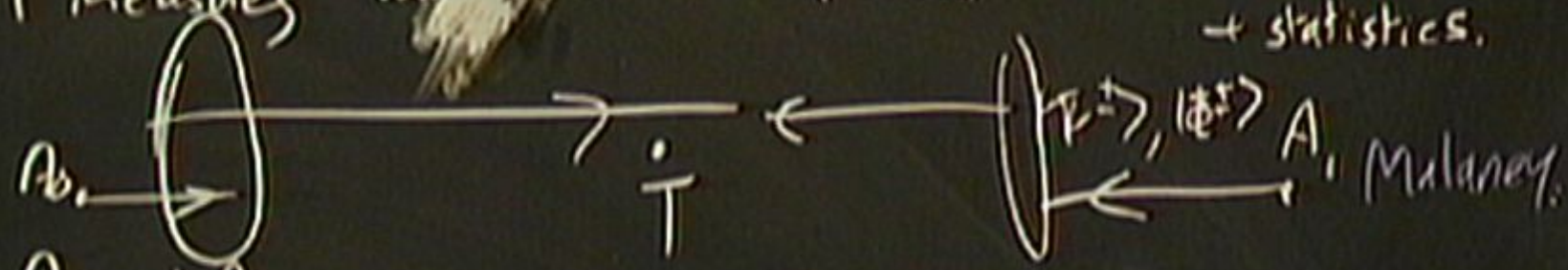

② A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T
A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T
T measures and broadcasts result.
③ A_0
A_0 and A_1
T
T Bell state measurement + broadcast

(2) A_0 sends BB84 state $|0\rangle, |1\rangle, |+\rangle$ to T. Chandran et al.

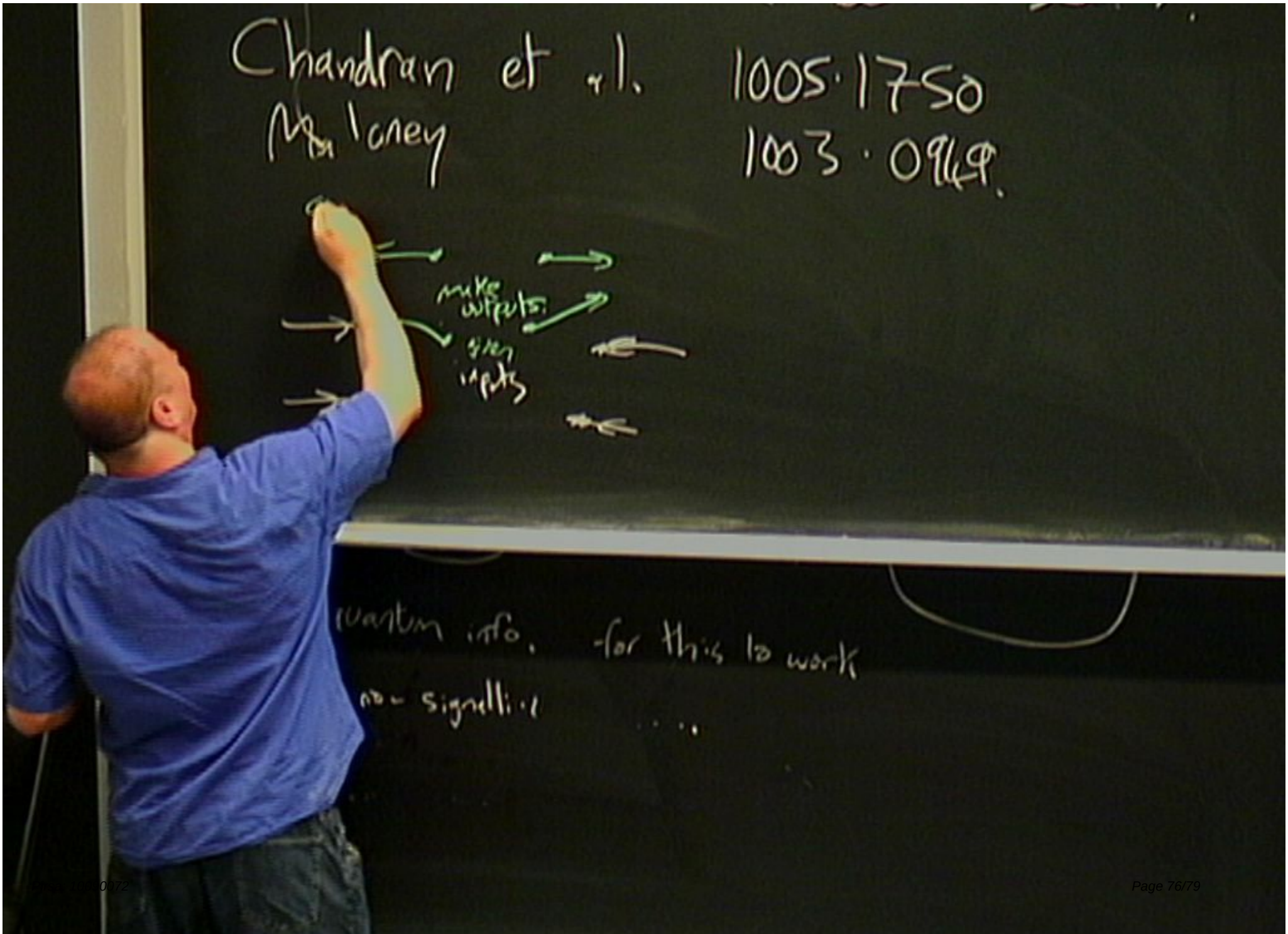
A_1 sends basis choice $(|0\rangle, |1\rangle), (|-\rangle, |+\rangle)$ to T.

T measures and broadcasts result. A checks timings + statistics.

(3)



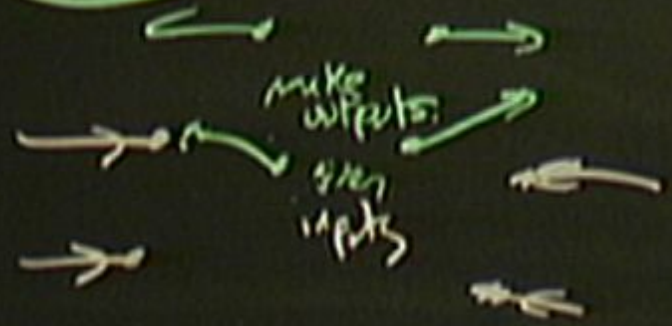
T Bell state measures + broadcasts answer.


Chandran et al. 1005.1750
Mahoney 1003.0969
make outputs
given inputs
quantum info. - for this to work
non-signalling

Chandran et al. 1005.1750

Mahoney 1003.0969.

can you?



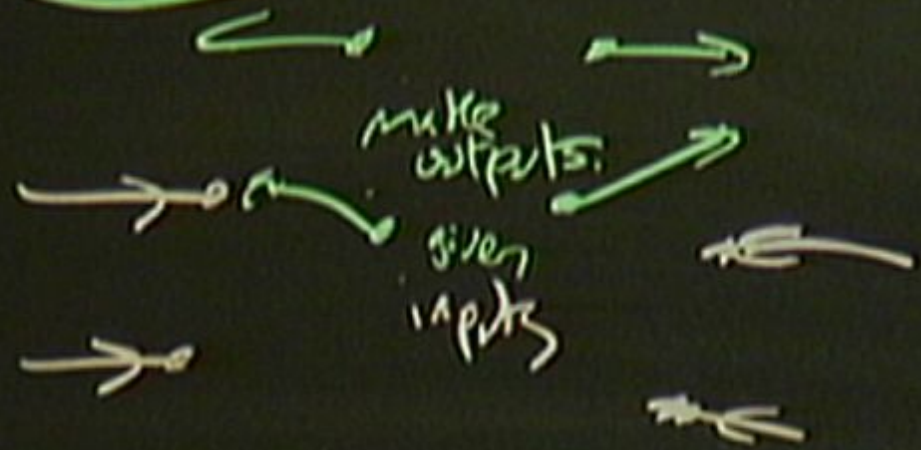
need quantum info. for this to work

need non-signalling ...

Chandran et al. 1005.1750

Mahaney 1003.0949

convex?



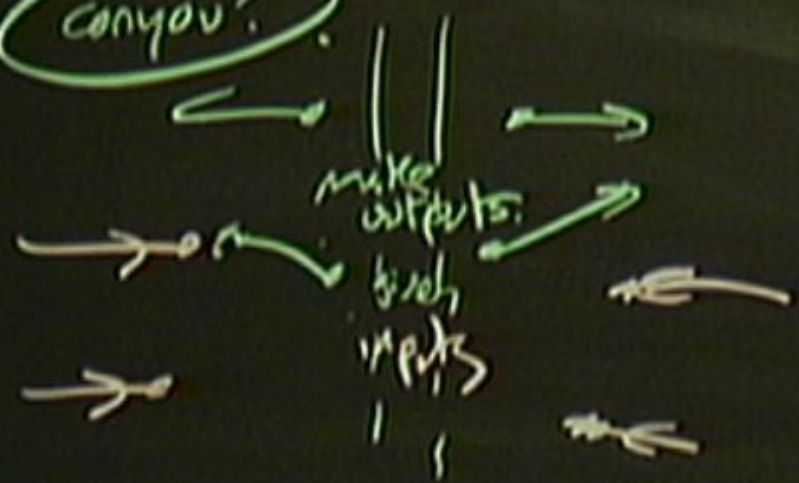
need quantum info. - for this to work

(hep-th/0608.5380)

Chandran et al. 1005.1750

McInerney 1003.0969

convex?



given control of $R \subseteq M^4$

quantum info. - for this to work

need no-signalling