

Title: Quantum Tasks in Minkowski Space

Date: Jun 28, 2012 02:30 PM

URL: <http://pirsa.org/12060062>

Abstract: <span>The fundamental properties of quantum information and its applications to computing and cryptography have been greatly illuminated by considering information-theoretic tasks that are provably possible or impossible within non-relativistic quantum mechanics.&nbsp; In this talk I describe a general framework for defining tasks within (special) relativistic quantum theory and illustrate it with examples from relativistic quantum cryptography.</span>

# Quantum Tasks in Minkowski Space

Talk at RQI-North, Perimeter Institute  
143028062012

Adrian Kent  
University of Cambridge and Perimeter Institute

(based on arxiv:1204.4022, to appear in special relativistic quantum information issue of Classical and Quantum Gravity, and earlier papers)

1 / 41



# General Quantum Tasks In Minkowski Space

$| \psi_i \rangle$   
 $S_i$  →  $P_i$

Given inputs in the form of quantum states  $| \psi_i \rangle$  and classical data  $S_i$  at locations  $P_i$ , where neither the locations nor the classical or quantum data are generally known in advance.

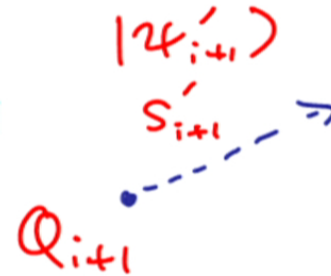
$P_{i+1}$  ←  $| \psi_{i+1} \rangle$   
 $S_{i+1}$



# General Quantum Tasks In Minkowski Space



Required to produce outputs in the form of quantum states  $|\psi_i\rangle$  and classical data  $S'_i$  at locations  $Q_i$ , where the output data and locations generally depend on the input data and locations.



Given inputs in the form of quantum states  $|\psi_i\rangle$  and classical data  $S_i$  at locations  $P_i$ , where neither the locations nor the classical or quantum data are generally known in advance.



# General Quantum Tasks In Minkowski Space



Required to produce outputs in the form of quantum states  $|\psi'_i\rangle$  and classical data  $S'_i$  at locations  $Q_i$ , where the output data and locations generally depend on the input data and locations.

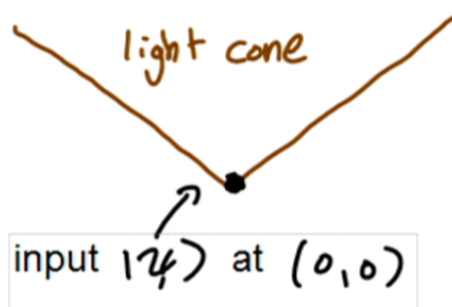
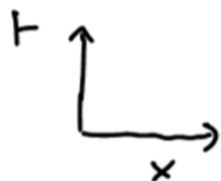


Given inputs in the form of quantum states  $|\psi_i\rangle$  and classical data  $S_i$  at locations  $P_i$ , where neither the locations nor the classical or quantum data are generally known in advance.

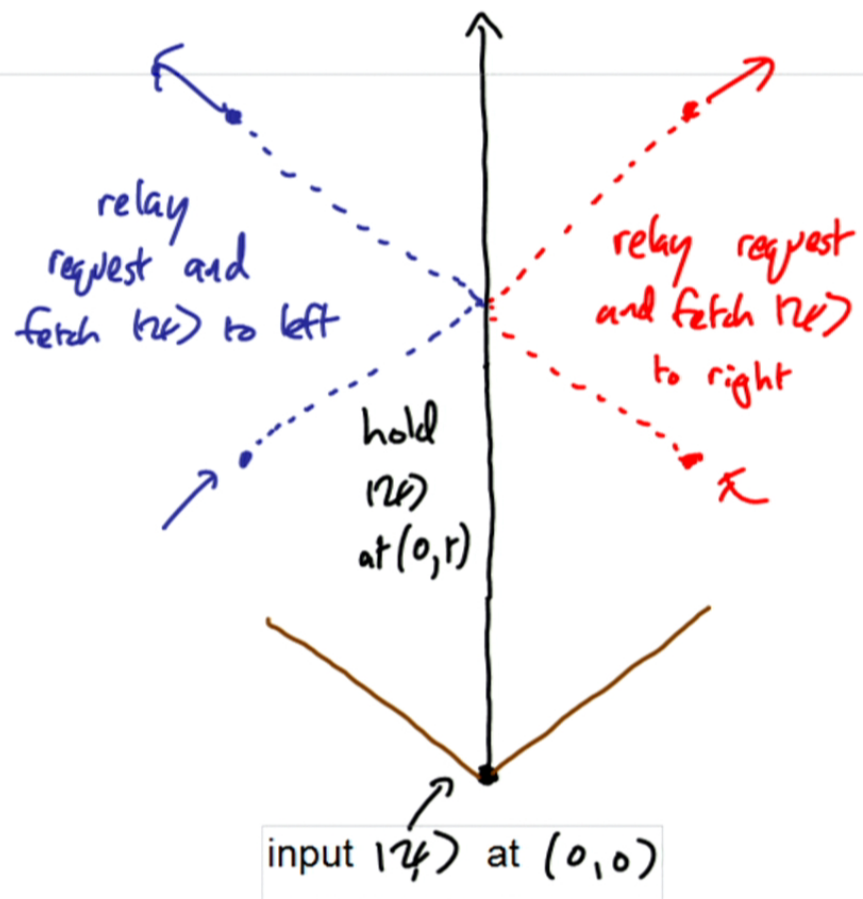


requires output  
of  $h\psi\rangle$  at  $(-L, t+2L)$

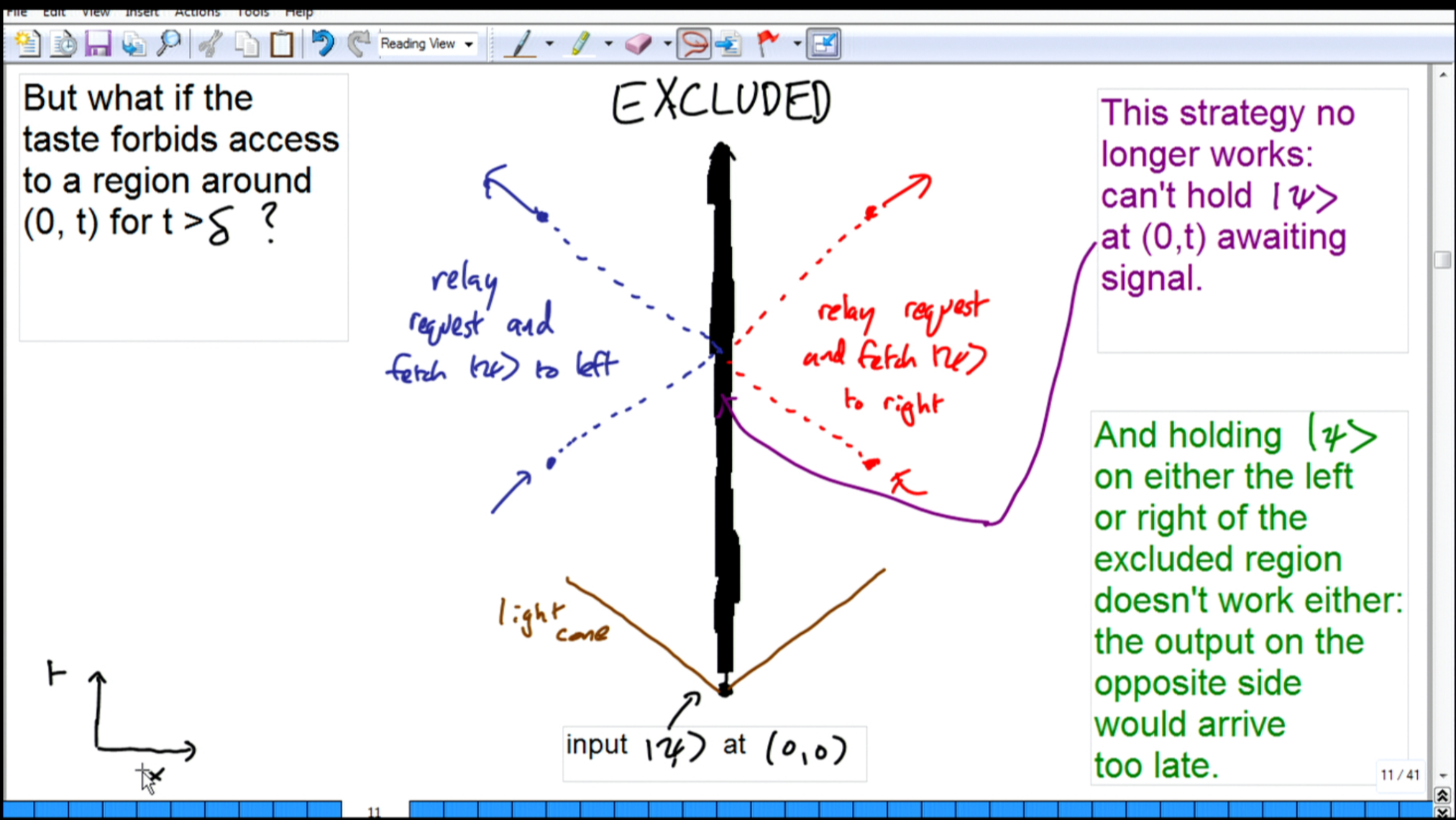
possible input  
at  $(-L, t)$  requesting  
return of  
(for any  $t > 0$ )

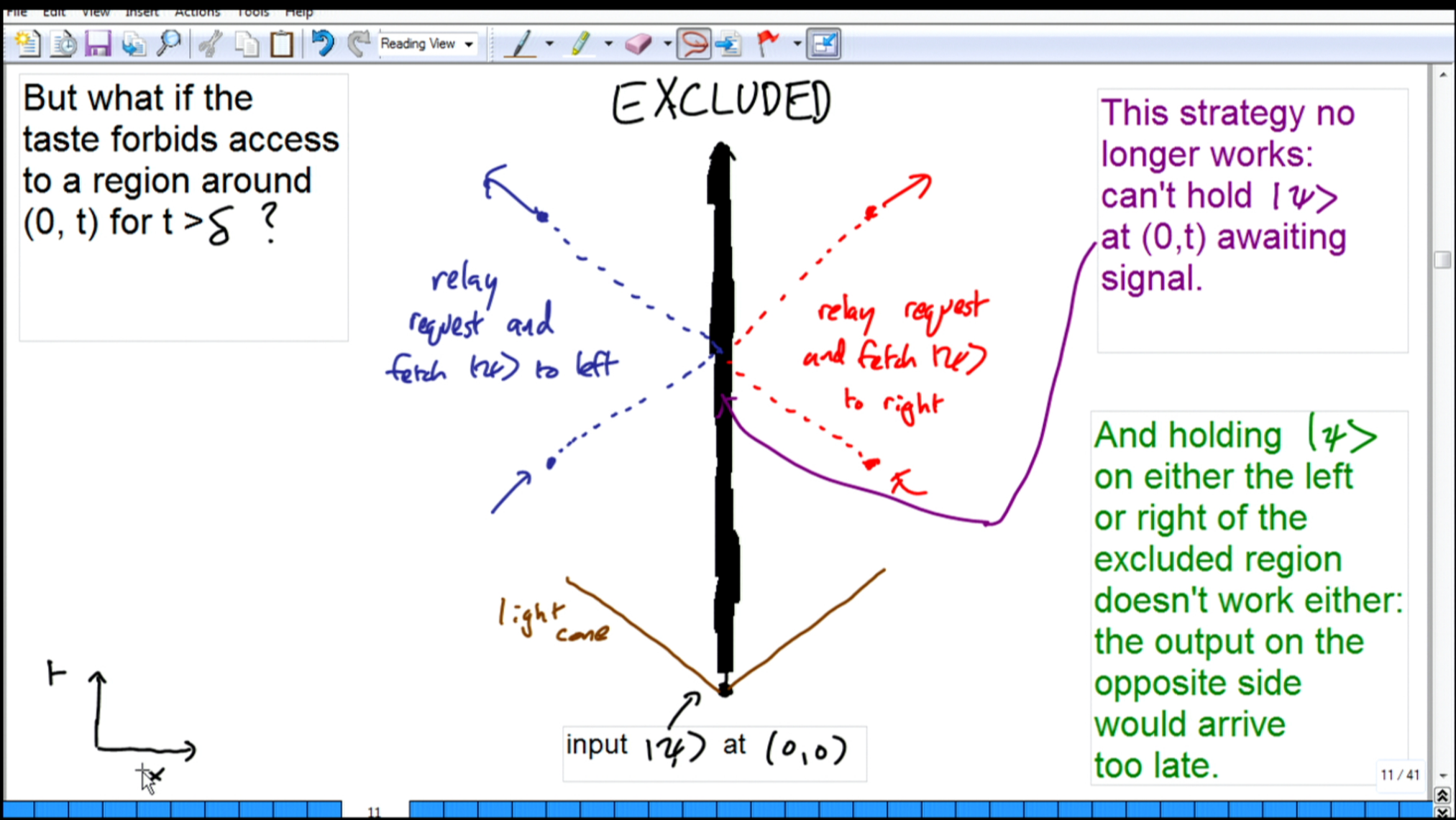


## Simple solution to this task









But what if the taste forbids access to a region around  $(0, t)$  for  $t > \delta$ ?

EXCLUDED

There is nonetheless a simple solution:

1) send  $|u\rangle$  to (say) the point  $(-L, L)$ .



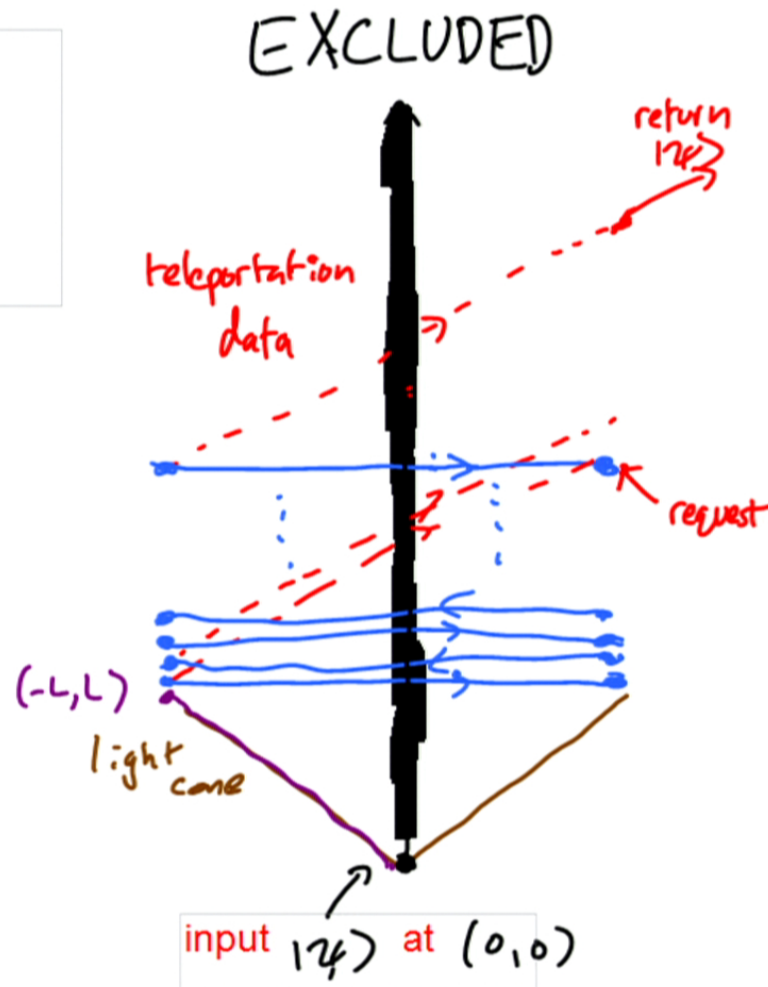
$(-L, L)$

light cone

input  $|u\rangle$  at  $(0, 0)$



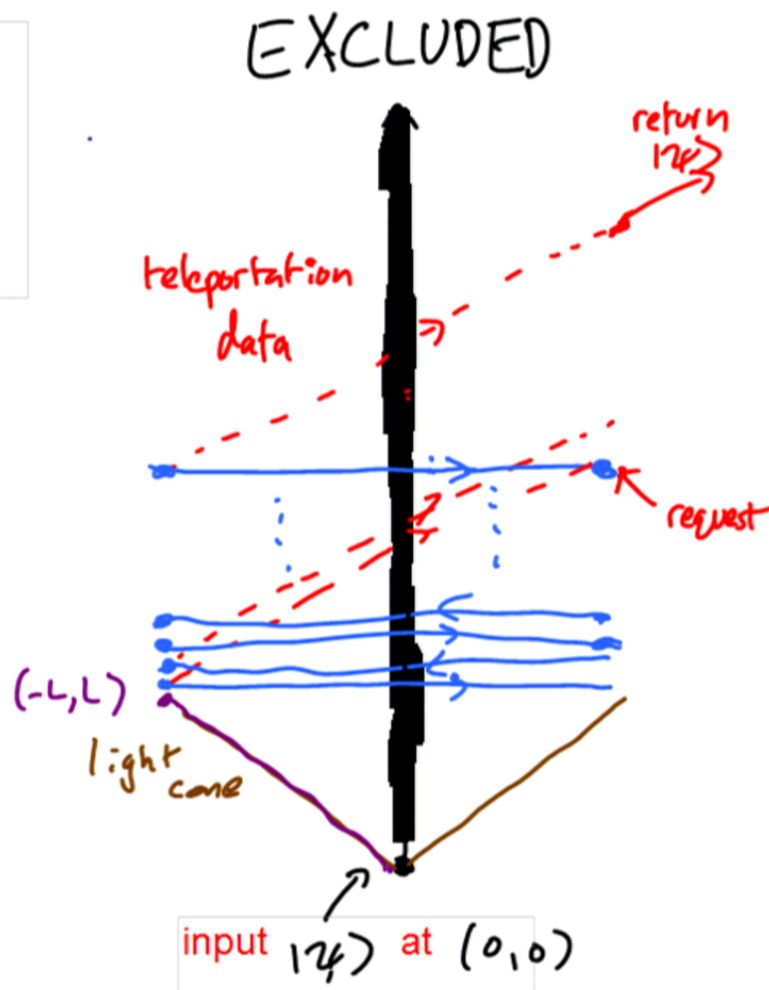
But what if the  
taste forbids access  
to a region around  
 $(0, t)$  for  $t > \delta$ ?



There is nonetheless  
a simple solution:

- 1) send  $|\psi\rangle$  to (say) the point  $(-L, L)$ .
- 2) repeatedly "teleport" the quantum state  $|\psi\rangle$  back and forth between  $(-L, t)$  and  $(L, t)$  without waiting for the classical correction data.
- 3) on the side a request arrives, stop "teleporting", wait for classical correction data, create and return  $|\psi\rangle$ .

But what if the  
taste forbids access  
to a region around  
(0, t) for  $t > \delta$ ?



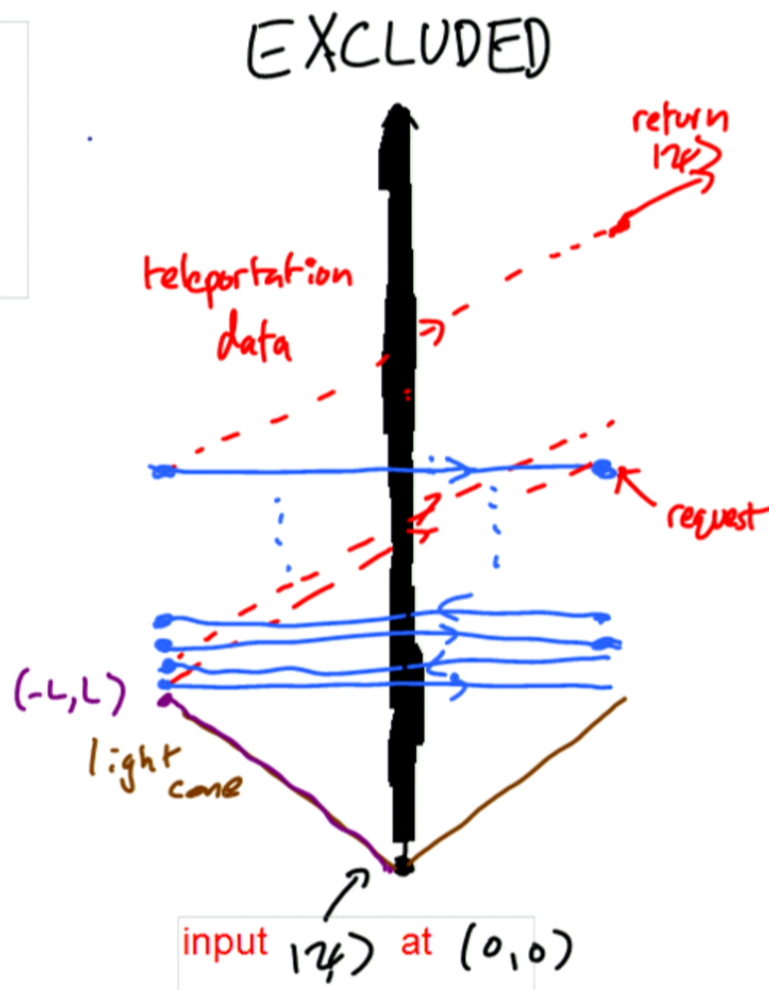
$|\psi\rangle$  is effectively  
delocalized by the  
repeated teleportations.

The task can be  
completed as though  
 $|\psi\rangle$  were held in  
the excluded zone.

This shows how to break  
some quantum tagging  
(position authentication)  
schemes originally  
claimed to be secure.

(AK-W.Munro-T.Spiller  
2010)

But what if the  
taste forbids access  
to a region around  
(0, t) for  $t > \delta$ ?



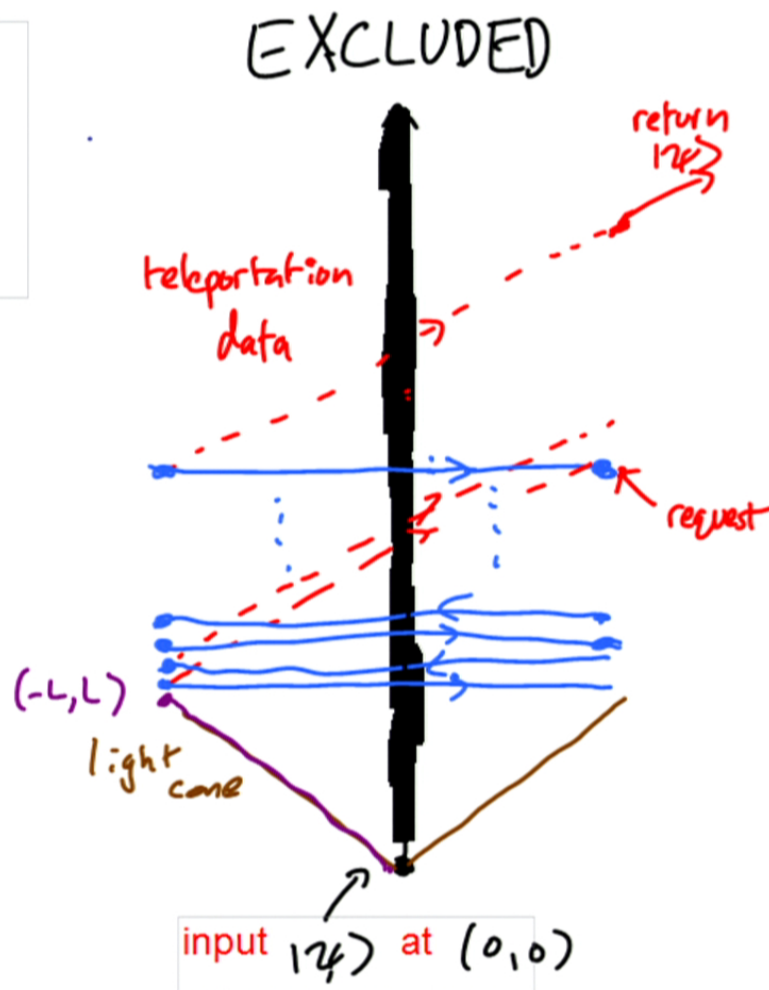
$|\psi\rangle$  is effectively  
delocalized by the  
repeated teleportations.

The task can be  
completed as though  
 $|\psi\rangle$  were held in  
the excluded zone.

This shows how to break  
some quantum tagging  
(position authentication)  
schemes originally  
claimed to be secure.

(AK-W.Munro-T.Spiller  
2010)

But what if the  
taste forbids access  
to a region around  
(0, t) for  $t > \delta$ ?



$|\psi\rangle$  is effectively  
delocalized by the  
repeated teleportations.

The task can be  
completed as though  
 $|\psi\rangle$  were held in  
the excluded zone.

This shows how to break  
some quantum tagging  
(position authentication)  
schemes originally  
claimed to be secure.

(AK-W.Munro-T.Spiller  
2010)



# A Brief History of Quantum Tagging

- Independently invented by KMSB (2002, patent 2006), CFGGO (2010) (who used the name quantum position-verification, and extended to more general position-based quantum cryptography), Malaney (2009).
- Various tagging schemes proposed: CFGGO and Malaney schemes claimed proven secure, but **broken by teleportation attacks (KMS 2010)**. New schemes proposed by KMS 2010 (security left open) and LL 2010 (security conjectured).
- (Im)possibility of security turns out to depend crucially on subtleties in the properties assumed for the tag: in particular, whether Eve can read information from within it. **Secure quantum tagging is possible if the tag can keep secret data shared with Alice (K 2010). (Cf. Thomas Jennewein's talk)**
- **For tags that cannot hold secrets, a large class of tagging schemes including KMS 2010 and LL 2010 are provably insecure (BCFGGOS, 2010) -- a beautiful result that relies on earlier work by Vaidman (2003) on non-local quantum measurements.**

# A Brief History of Quantum Tagging

- Independently invented by KMSB (2002, patent 2006), CFGGO (2010) (who used the name quantum position-verification, and extended to more general position-based quantum cryptography), Malaney (2009).
- Various tagging schemes proposed: CFGGO and Malaney schemes claimed proven secure, but **broken by teleportation attacks (KMS 2010)**. New schemes proposed by KMS 2010 (security left open) and LL 2010 (security conjectured).
- (Im)possibility of security turns out to depend crucially on subtleties in the properties assumed for the tag: in particular, whether Eve can read information from within it. **Secure quantum tagging is possible if the tag can keep secret data shared with Alice (K 2010). (Cf. Thomas Jennewein's talk)**
- **For tags that cannot hold secrets, a large class of tagging schemes including KMS 2010 and LL 2010 are provably insecure (BCFGGOS, 2010) -- a beautiful result that relies on earlier work by Vaidman (2003) on non-local quantum measurements.**



File Edit View Insert Actions Tools Help

Reading View

Our operational test for locating a quantum state **failed**. The location can't be pinned down by remote requests, even when the timings are precisely stipulated.

That's a problem for some cryptographic tagging schemes, but raises an interesting question -- what constraints **are** there on producing an unknown state when requested?

One very simple but, it turns out, very useful example of a constraint is given by the "no-summoning theorem"  
(AK, arxiv:1101.4612, to appear in Quantum Information Processing)

18 / 41

The image is a screenshot of a presentation slide displayed within a software application. The application's interface includes a menu bar at the top with options: File, Edit, View, Insert, Actions, Tools, and Help. Below the menu bar is a toolbar with various icons for document manipulation, such as opening, saving, and searching. The slide itself has a white background and contains three paragraphs of text. The first paragraph is in blue, the second in green, and the third in brown. The text discusses quantum state localization and cryptographic tagging schemes. The slide is framed by a grey border, and a mouse cursor is visible in the bottom-left corner of the slide area. In the bottom-right corner of the slide, there is a small box indicating the slide number '18 / 41'. At the very bottom of the application window, a blue progress bar is visible, with the number '18' centered below it.

File Edit View Insert Actions Tools Help

Reading View

Our operational test for locating a quantum state **failed**. The location can't be pinned down by remote requests, even when the timings are precisely stipulated.

That's a problem for some cryptographic tagging schemes, but raises an interesting question -- what constraints **are** there on producing an unknown state when requested?

One very simple but, it turns out, very useful example of a constraint is given by the "no-summoning theorem"  
(AK, arxiv:1101.4612, to appear in Quantum Information Processing)

18 / 41

18



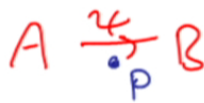
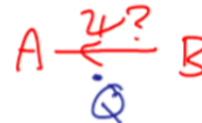
## An example of a relativistic quantum impossibility: Summoning a quantum state

Consider two agencies, Alice and Bob, with independent secure networks and (here we idealise for now) representatives everywhere in space-time.

Alice prepares a localised physical state unknown to Bob and gives him it at point P.

At some point Q, in the causal future of P, not known in advance by Bob, Alice **summons** -- i.e. asks Bob to return -- the state.

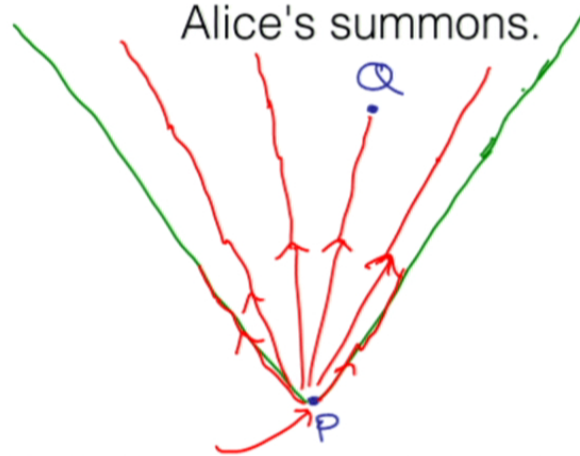
N.B.



# Summoning in classical theories

Given an unknown classical state at point  $P$  in Minkowski space, Bob can (in principle) measure it precisely, broadcast the information in all directions, and reconstruct the state at any point  $Q$  in the causal future of  $P$  -- and so comply with

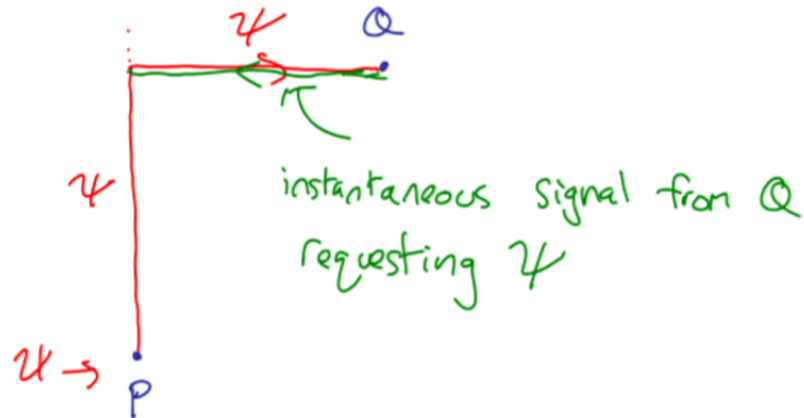
Alice's summons.



# Summoning in non-relativistic quantum mechanics

Given an unknown quantum state  $\psi$  at a point  $P=(x,t)$  in Galilean space-time, Bob can hold the state at position  $x$ , wait for a summons at  $Q=(y,t')$  (where  $t'>t$ ), instantaneously send a signal to  $(x,t')$  requesting the state, and instantaneously send the state back to  $Q$ , and so comply with the summons.

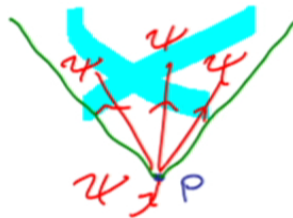
Unknown state  
supplied here



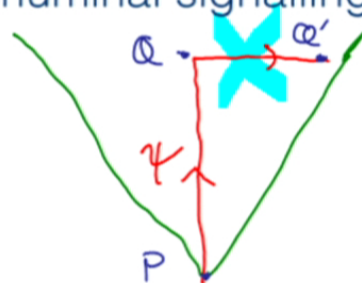


## No summoning in relativistic quantum theory

Given an unknown quantum state  $\psi$  at point P in Minkowski space-time, Bob cannot precisely identify it or copy it (because of the no-cloning theorem).

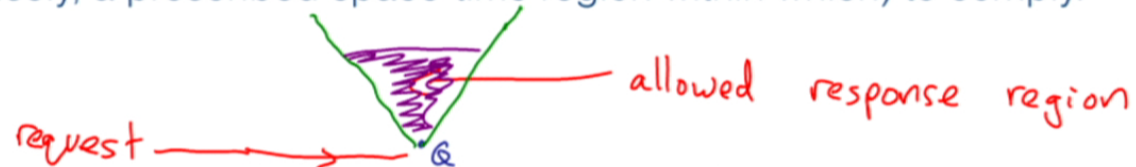


If he holds it at a possible summoning point Q in the causal future of P, he cannot send it to another space like separated possible summoning point Q' (because of the no-superluminal signalling principle).



## No approximate summoning in relativistic quantum theory

- A more realistic version of the task would allow Bob some time (more precisely, a prescribed space-time region within which) to comply.



- Also, realistically, we could allow him margin for errors - ok to return approximately the same state (i.e. with fidelity close to 1 to the original)
- Under these definitions, summoning is realistically (not just ideally) possible in non-relativistic quantum mechanics or relativistic classical mechanics.
- But there are non-trivial bounds on the fidelity of approximate cloning. Removing our idealizations doesn't affect the main conclusion. No-approximate-cloning plus no-signalling imply no-approximate-summoning in relativistic quantum theory.



# No-summoning and quantum cryptography

(arxiv:1101.4620, see also 1102.2816)

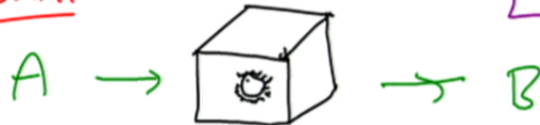
One dramatic example of the power of the no-summoning theorem is a simple and practical solution to the long-standing problem of unconditionally secure quantum bit commitment.

**Bit commitment:** Alice wants to make an encrypted prediction. She needs a guarantee that the recipient (Bob) cannot decrypt her prediction until she gives him a key - extra data.

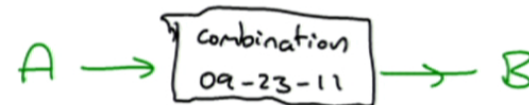
He needs a guarantee that she is genuinely committed and cannot change her prediction, for instance by having two different keys that will decrypt two different predictions.

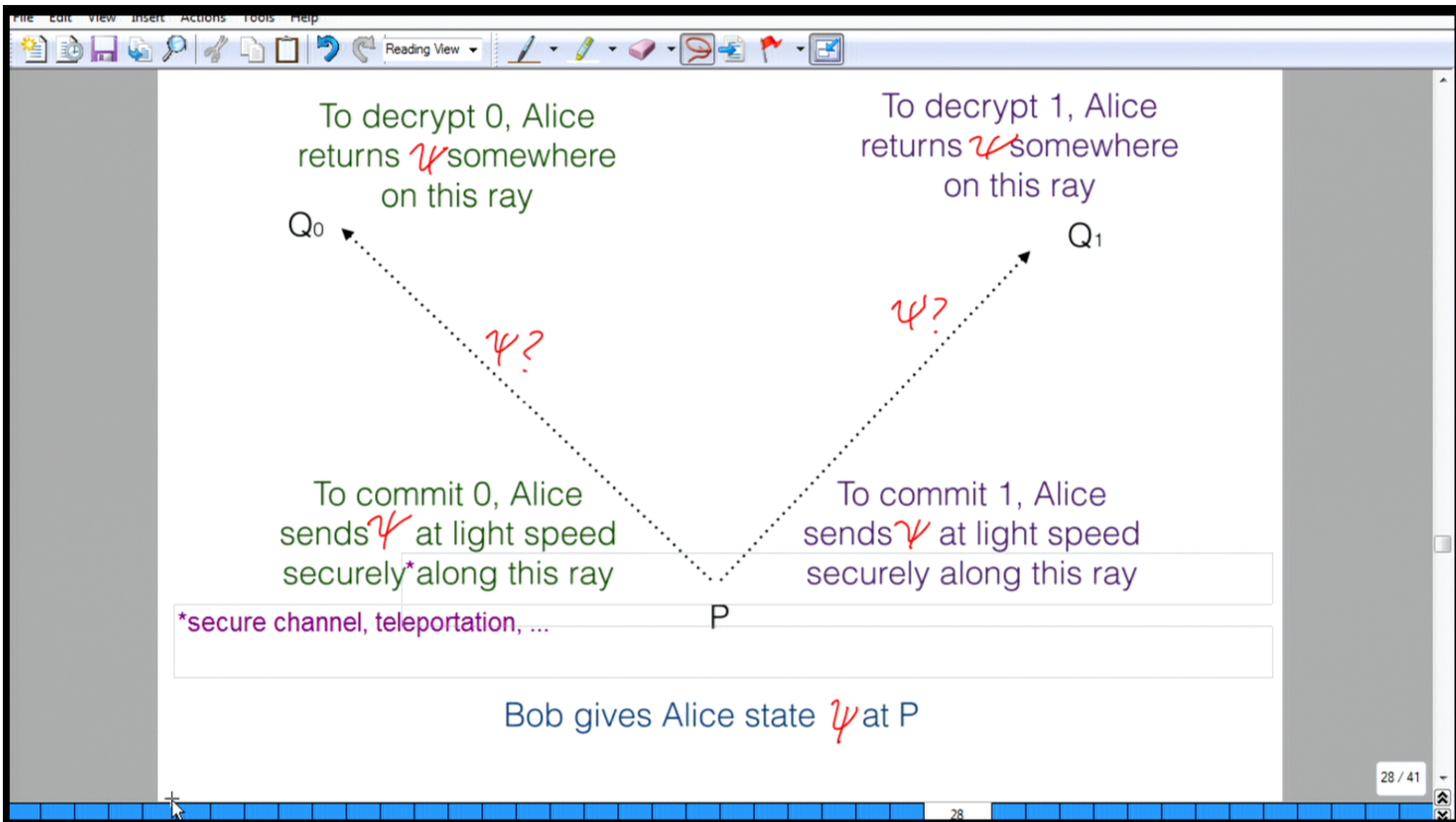
They both ideally want these guarantees based only on the laws of physics.

commit

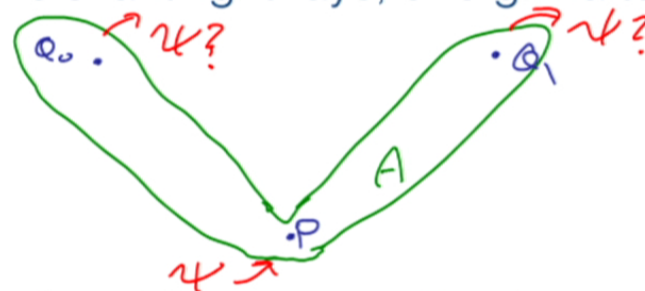


unveil

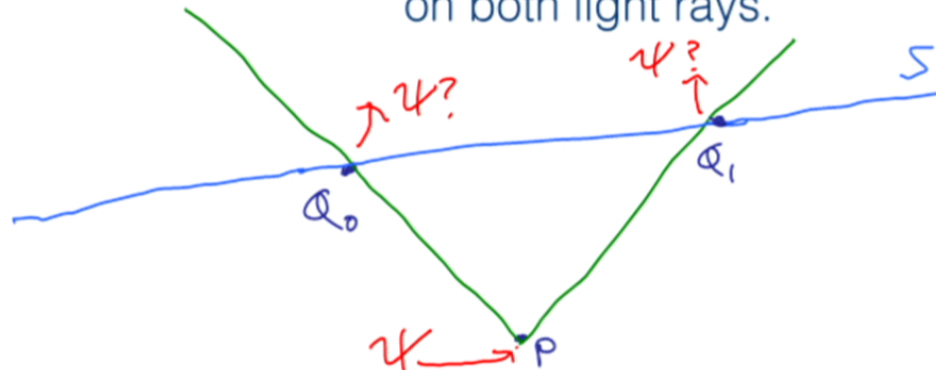




Security against Bob: ensured since Alice sends the state securely (either because she controls a region around the relevant light rays, or e.g. via teleportation)



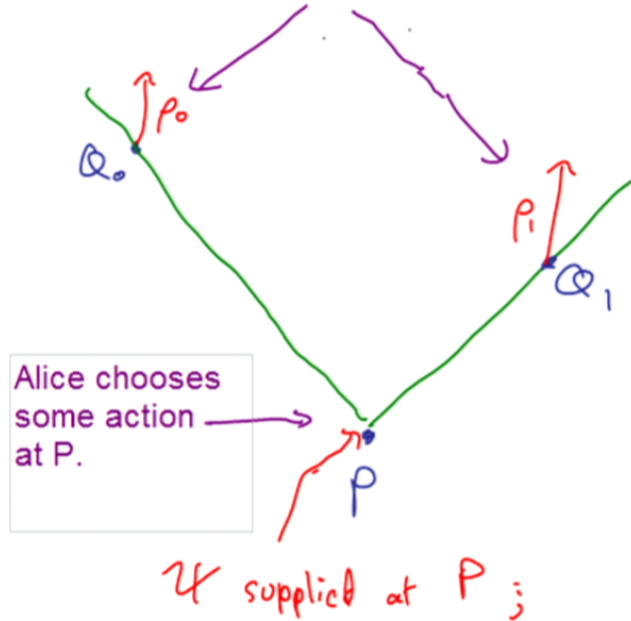
Security against Alice: ensured by the no-summoning theorem -- she cannot return  $\psi$  independently at points on both light rays.





More precisely, we can quantify the security in terms of the dimension  $d$  of the space of the unknown state: Alice's cheating probability is bounded by  $O(1/d)$ .

Optimal states A can return given her actions chosen at P

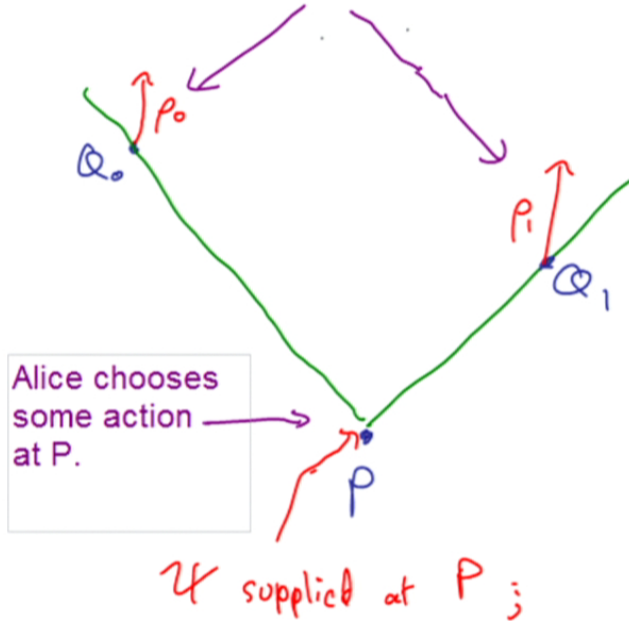


$$\begin{aligned}
 &P(\text{Bob accepts unveiling at } Q_0) + \\
 &P(\text{Bob accepts unveiling at } Q_1) \\
 &= \langle U | P_0 | U \rangle + \langle U | P_1 | U \rangle \\
 &\leq 1 + \frac{2}{d+1}
 \end{aligned}$$

Alice's "wiggle room" decays exponentially in #qubits =  $\log(d)$

More precisely, we can quantify the security in terms of the dimension  $d$  of the space of the unknown state: Alice's cheating probability is bounded by  $O(1/d)$ .

Optimal states A can return given her actions chosen at P



$$\begin{aligned}
 &P(\text{Bob accepts unveiling at } Q_0) + \\
 &P(\text{Bob accepts unveiling at } Q_1) \\
 &= \langle \mathcal{U} | p_0 | \mathcal{U} \rangle + \langle \mathcal{U} | p_1 | \mathcal{U} \rangle \\
 &\leq 1 + \frac{2}{d+1}
 \end{aligned}$$

Alice's "wiggle room" decays exponentially in #qubits =  $\log(d)$

The image is a screenshot of a presentation slide displayed within a software window. The window has a menu bar at the top with 'File', 'Edit', 'View', 'Insert', 'Actions', 'Tools', and 'Help'. Below the menu bar is a toolbar with various icons for navigation and editing. The slide itself has a white background with a green title and blue body text. The title is 'No contradiction with the Mayers-Lo-Chau no-go theorem'. The body text consists of three paragraphs. The first paragraph states that Mayers and Lo-Chau's result shows that unconditionally secure bit commitment is impossible for a large class of quantum protocols, but the proof makes some tacit assumptions. The second paragraph explains that the proof assumes that if there is a unitary map taking a 0 commitment to a 1 commitment, known to Alice, she can implement it physically and cheat by altering her commitments. The third paragraph states that in their protocol, Alice does know the relevant unitary, which takes a qudit going along one light ray to the same qudit going along another. A final line of text, in red, states that this unitary cannot be implemented physically as it would violate causality, so the Mayers-Lo-Chau cheating strategy doesn't apply. The slide is numbered 32 / 41 in the bottom right corner. The software window has a blue status bar at the bottom.

## No contradiction with the Mayers-Lo-Chau no-go theorem

Mayers and Lo-Chau's celebrated result shows that unconditionally secure bit commitment is impossible for a large class of quantum protocols -- but the proof makes some tacit assumptions.

In particular, it assumes that, if there is a unitary map taking a 0 commitment to a 1 commitment, known to Alice, she can implement it physically -- and so cheat by altering her commitments.

In our protocol Alice does know the relevant unitary -- which takes a qudit going along one light ray to the same qudit going along another.

But this unitary cannot be implemented physically, as it would violate causality. So the Mayers-Lo-Chau cheating strategy doesn't apply.

32 / 41



The image is a screenshot of a presentation slide displayed within a software window. The window has a menu bar at the top with 'File', 'Edit', 'View', 'Insert', 'Actions', 'Tools', and 'Help'. Below the menu bar is a toolbar with various icons for navigation and editing. The slide content is centered on a white background with green and blue text. The title is in green, and the body text is in blue, except for a concluding sentence in red. The slide is numbered 32 / 41 in the bottom right corner.

## No contradiction with the Mayers-Lo-Chau no-go theorem

Mayers and Lo-Chau's celebrated result shows that unconditionally secure bit commitment is impossible for a large class of quantum protocols -- but the proof makes some tacit assumptions.

In particular, it assumes that, if there is a unitary map taking a 0 commitment to a 1 commitment, known to Alice, she can implement it physically -- and so cheat by altering her commitments.

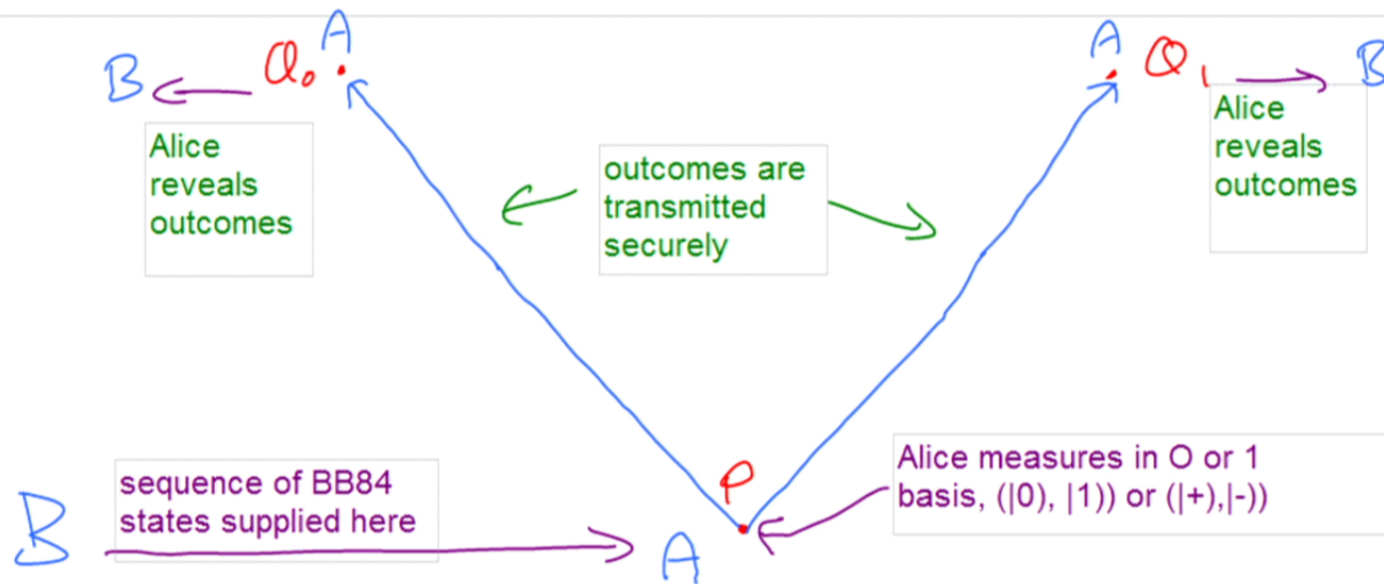
In our protocol Alice does know the relevant unitary -- which takes a qudit going along one light ray to the same qudit going along another.

But this unitary cannot be implemented physically, as it would violate causality. So the Mayers-Lo-Chau cheating strategy doesn't apply.

32 / 41

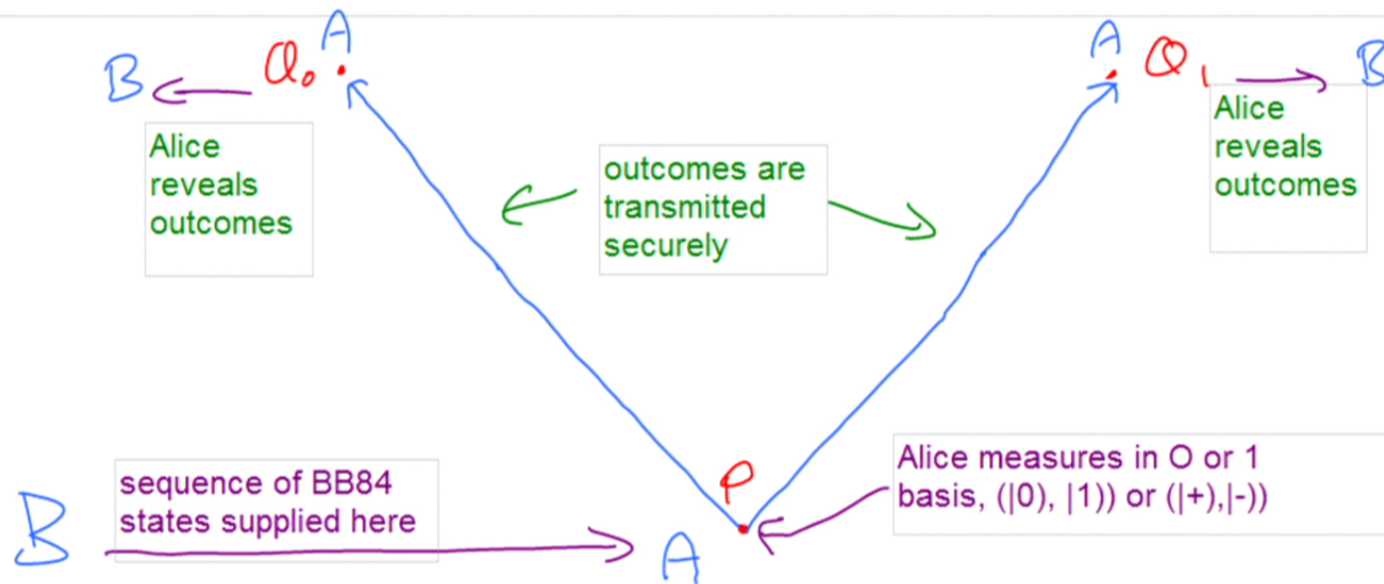
## Another recent development (AK, arxiv:1108.2879 )

Unconditionally secure bit commitment in Minkowski space can also be implemented by transmitting measurement outcomes on an unknown quantum state - i.e. without any need for Alice to transmit quantum states even over short distances.



## Another recent development (AK, arxiv:1108.2879 )

Unconditionally secure bit commitment in Minkowski space can also be implemented by transmitting measurement outcomes on an unknown quantum state - i.e. without any need for Alice to transmit quantum states even over short distances.





# Defining bit commitment in Minkowski space

$Q_1$  unveils  $b$

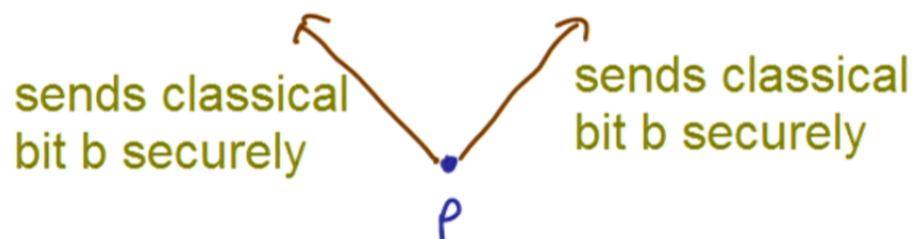


$Q_2$  unveils  $b$



$P$  sends classical bit  $b$  securely

$P$  sends classical bit  $b$  securely



Notice that even simple classical bit commitment protocols can appear superficially secure.

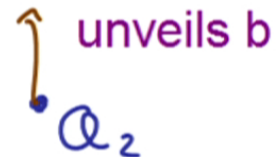
If Alice's agents at  $Q_1$  and  $Q_2$  have no correlated information other than  $b$ , they cannot coordinate a cheating attack.

# Defining bit commitment in Minkowski space

$Q_1$  unveils  $b$



$Q_2$  unveils  $b$

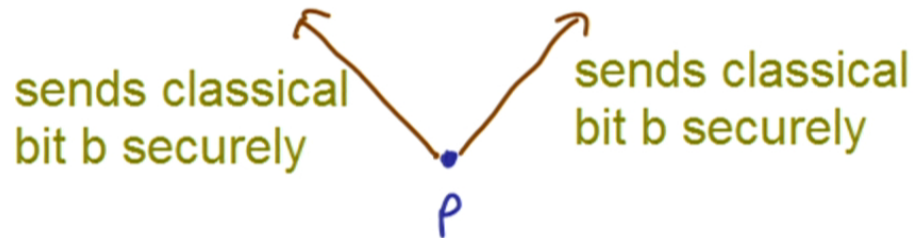


Notice that even simple classical bit commitment protocols can **appear** superficially secure.

sends classical bit  $b$  securely

$P$

sends classical bit  $b$  securely



If Alice's agents at  $Q_1$  and  $Q_2$  have no correlated information other than  $b$ , they cannot coordinate a cheating attack.



# Defining bit commitment in Minkowski space

$Q_1$  unveils  $b$



$Q_2$  unveils  $b$

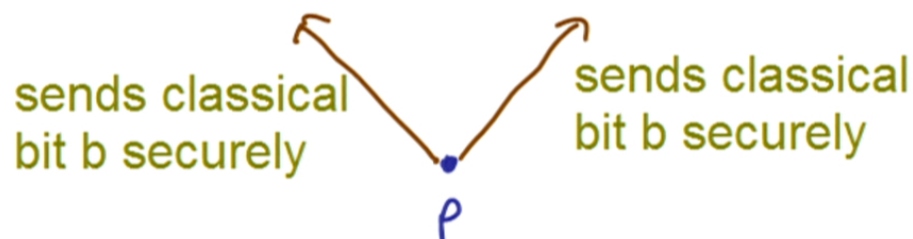


Notice that even simple classical bit commitment protocols can **appear** superficially secure.

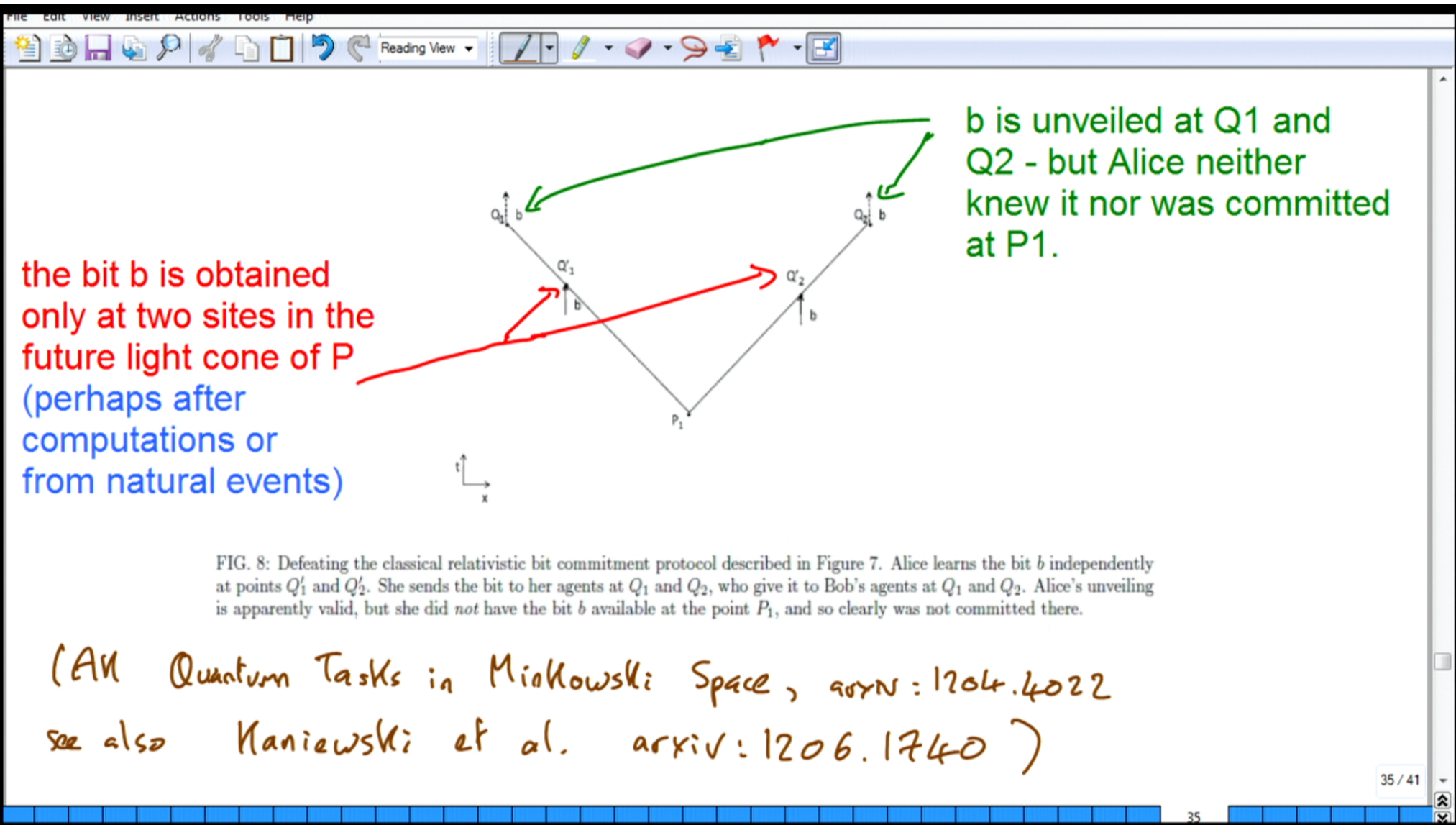
sends classical bit  $b$  securely

$P$

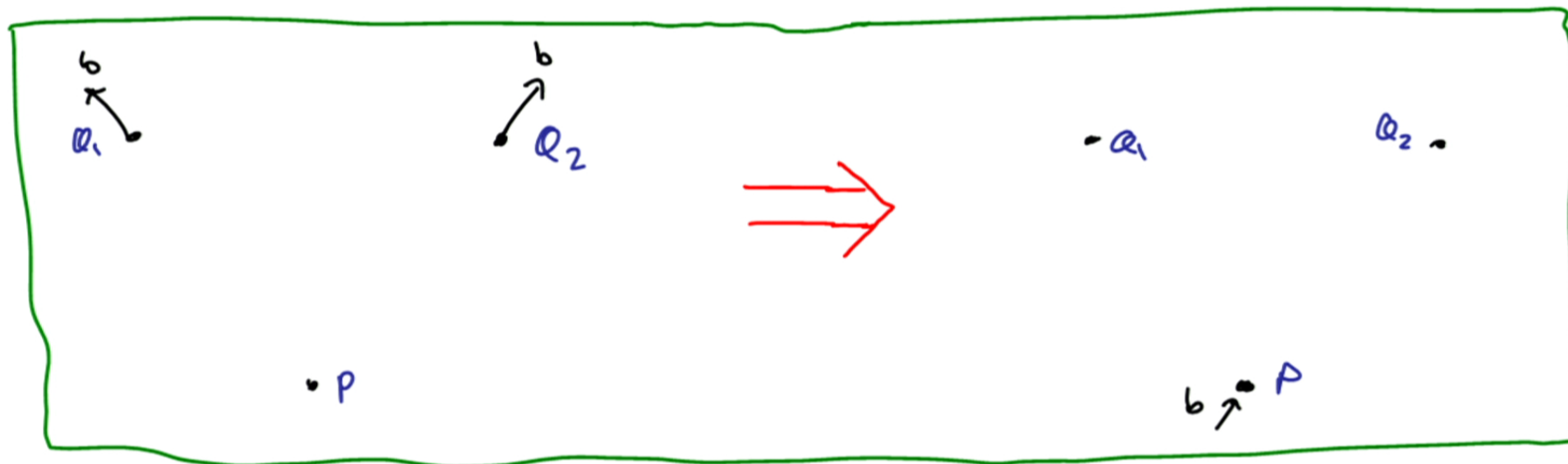
sends classical bit  $b$  securely



If Alice's agents at  $Q_1$  and  $Q_2$  have no correlated information other than  $b$ , they cannot coordinate a cheating attack.

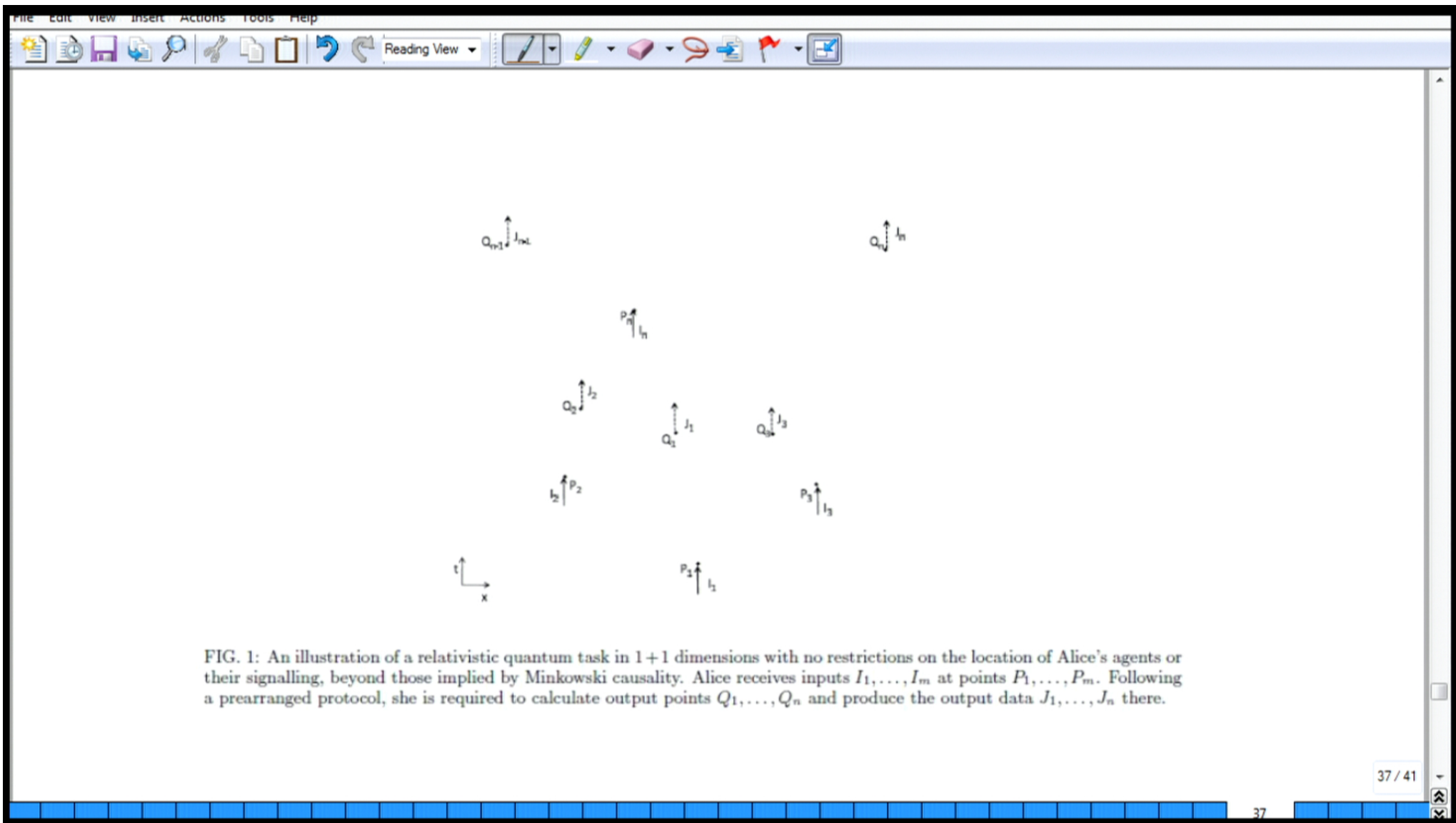


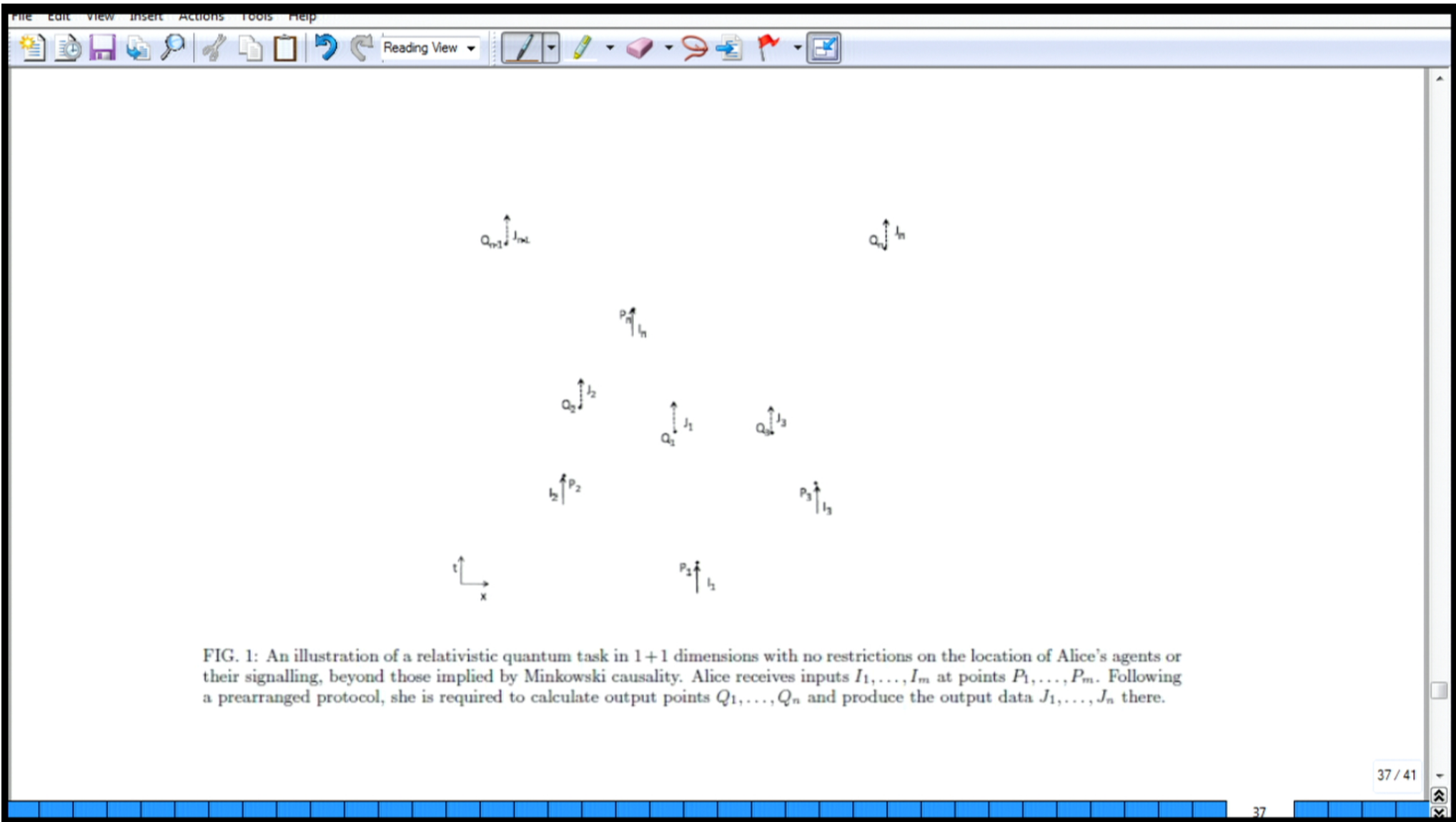
What we need, and the bit commitment protocols described earlier provide, is a Minkowski task based form of security:

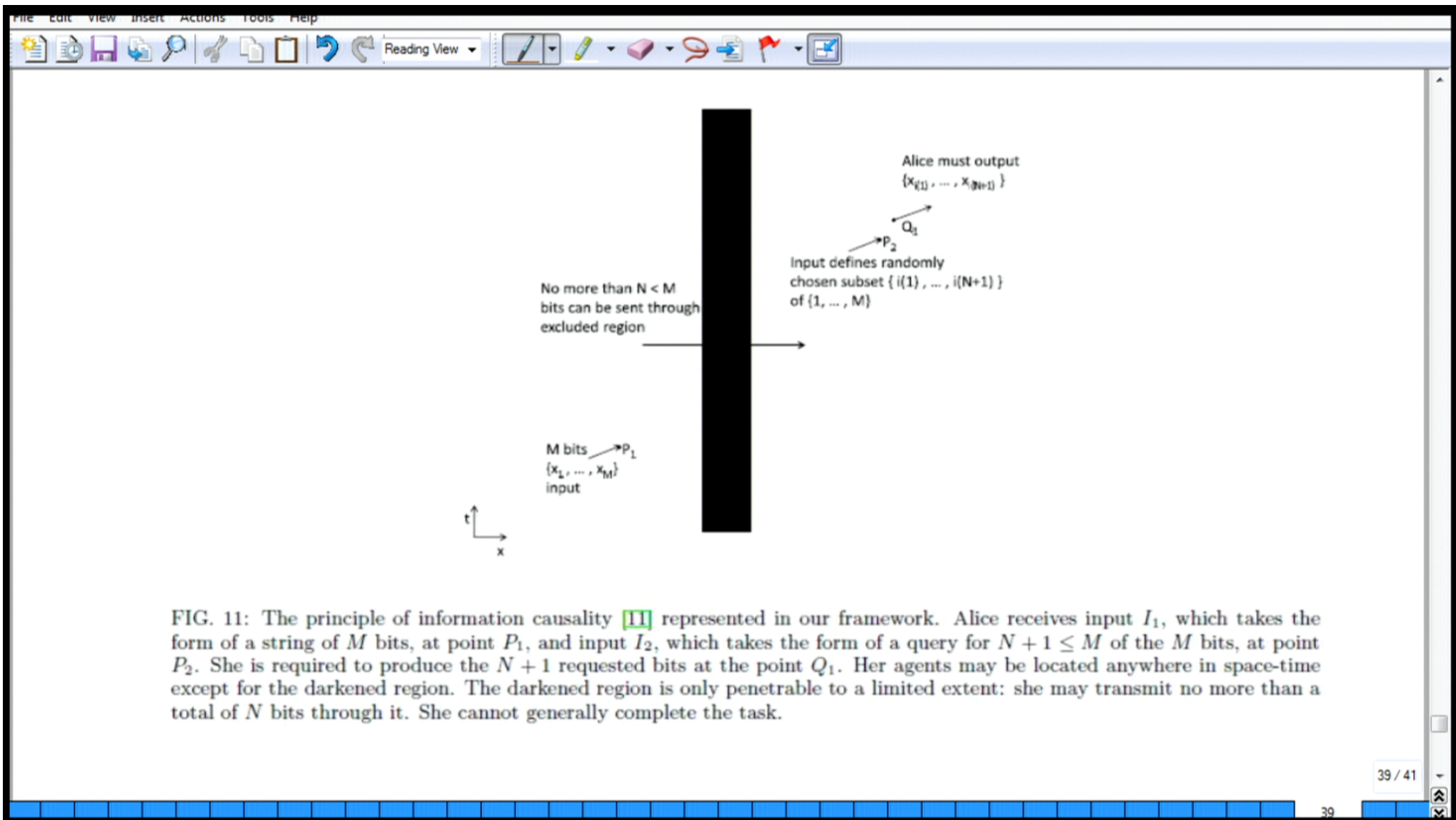


That is, Alice's valid unveiling of  $b$  at  $Q_1$ ,  $Q_2$  guarantees that she already had, and committed herself to, the bit  $b$  at  $P$

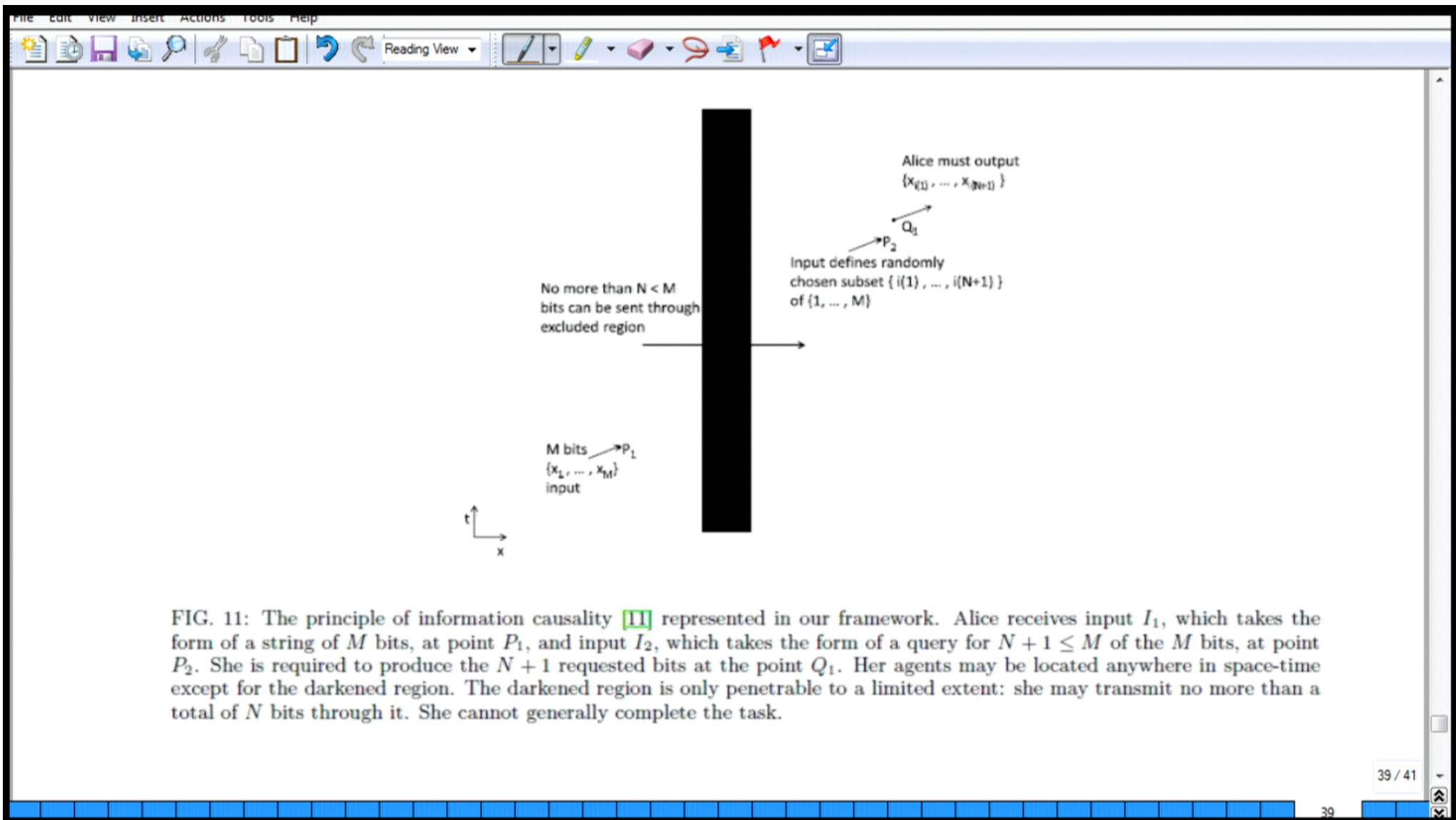












File Edit View Insert Actions Tools Help

Reading View

## Summary

- We can learn new features of relativistic quantum theory by considering intrinsically relativistic and quantum tasks.
- Summoning is a simple example, which singles out relativistic quantum theory from NRQM or relativistic classical mechanics.
- It's cryptographically powerful, with a direct application to quantum bit commitment; it also allows other relativistic cryptographic tasks to be implemented securely.
- Quantum tagging and position-based quantum cryptography are further natural applications, with intriguing (and practically relevant) possibilities and impossibilities. (Also, "location-oblivious data transfer", AK PRA 84 01238 (2011).)
- There are surely many other interesting tasks, many open questions, and many new quantum cryptographic and computational applications.

40 / 41

40

