

Quantum Cryptography in Minkowski Space

Talk at QCRYPT 2012, CQT Singapore
140011092012

Adrian Kent
Centre for Quantum Information and Foundations,
DAMTP, University of Cambridge
and
Perimeter Institute

Relativistic Cryptography: A Brief Partial History (from a personal perspective)

Classical Secure Coin Tossing in Minkowski Space: coin tossing is strictly weaker than bit commitment (AK 1998)

Classical Bit Commitment Schemes in Minkowski Space: secure against classical attacks and Mayers-Lo-Chau quantum attacks (AK 1999, 2005)

Unconditionally Secure Quantum Key Distribution Based on No-Signalling (Barrett-Hardy-AK 2005; with only 2 devices Barrett-Colbeck-AK 2012)

-> other protocols for Device-Independent Quantum Key Distribution (Acin, Gisin, Masanes, Scarani, Brunner, Massar, Pironio, Pino, Hanggi, Renner, Wolf,)

Quantum Tagging (Quantum Position Authentication in Minkowski Space)(Malaney,Buhrman-Chandran-Fehr-Gelles-Goyal-Ostrovsky-Schaffner,AK-Munro-Spiller 2006-11)

Position-Based Quantum Cryptography (Buhrman et al. 2010-11)

Unconditionally Secure Quantum Bit Commitment With Flying Qudits (AK 2011)

Unconditionally Secure Quantum Bit Commitment By Transmitting Measurement Outcomes (AK 2011)

Secure and Robust Transmission and Verification of Unknown Quantum States in Minkowski Space (AK-Massar-Silman 2012)

Relativistic Cryptography: A Brief Partial History (from a personal perspective)

Classical Secure Coin Tossing in Minkowski Space: coin tossing is strictly weaker than bit commitment (AK 1998)

Classical Bit Commitment Schemes in Minkowski Space: secure against classical attacks and Mayers-Lo-Chau quantum attacks (AK 1999, 2005)

Unconditionally Secure Quantum Key Distribution Based on No-Signalling (Barrett-Hardy-AK 2005; with only 2 devices Barrett-Colbeck-AK 2012)

-> other protocols for Device-Independent Quantum Key Distribution (Acin, Gisin, Masanes, Scarani, Brunner, Massar, Pironio, Pino, Hanggi, Renner, Wolf,)

Quantum Tagging (Quantum Position Authentication in Minkowski Space)(Malaney,Buhrman-Chandran-Fehr-Gelles-Goyal-Ostrovsky-Schaffner,AK-Munro-Spiller 2006-11)

Position-Based Quantum Cryptography (Buhrman et al. 2010-11)

Unconditionally Secure Quantum Bit Commitment With Flying Qudits (AK 2011)

Unconditionally Secure Quantum Bit Commitment By Transmitting Measurement Outcomes (AK 2011)

Secure and Robust Transmission and Verification of Unknown Quantum States in Minkowski Space (AK-Massar-Silman 2012)

(Figs from: *Quantum Tasks in Minkowski Space*, AK arxiv:1204.4022,
to appear in Classical and Quantum Gravity)

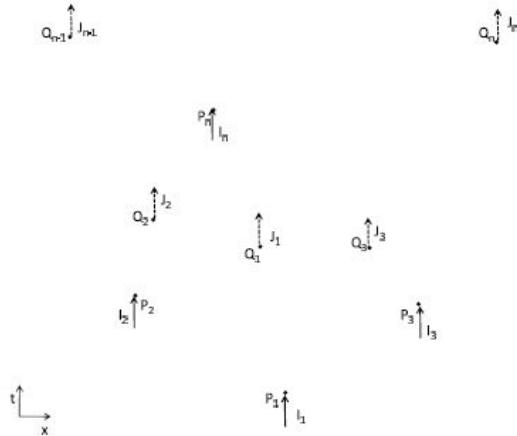


FIG. 1: An illustration of a relativistic quantum task in $1+1$ dimensions with no restrictions on the location of Alice's agents or their signalling, beyond those implied by Minkowski causality. Alice receives inputs I_1, \dots, I_m at points P_1, \dots, P_m . Following a prearranged protocol, she is required to calculate output points Q_1, \dots, Q_n and produce the output data J_1, \dots, J_n there.

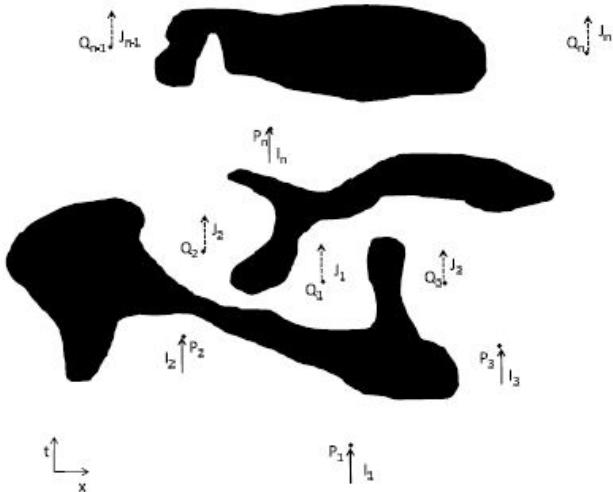


FIG. 9: An illustration of a relativistic quantum task in $1 + 1$ dimensions with restrictions on the location of Alice's agents. Alice receives inputs I_1, \dots, I_m at points P_1, \dots, P_m . Following a prearranged protocol, she is required to calculate output points Q_1, \dots, Q_n and produce the output data J_1, \dots, J_n there. Her agents may be located anywhere in space-time except for the darkened regions.

(from: *Quantum Tasks in Minkowski Space*, AK arxiv:1204.4022)

Bit commitment:

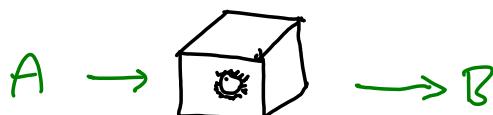
Alice wants to make an encrypted prediction, bit by bit.

She needs a guarantee that the recipient, Bob, cannot decrypt her prediction until she gives him the key -- extra data.

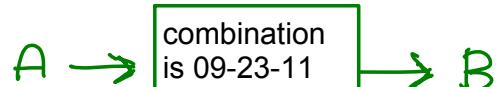
He needs a guarantee that she is genuinely committed and cannot change her prediction, for instance by having two different keys that will reveal two different predictions.

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

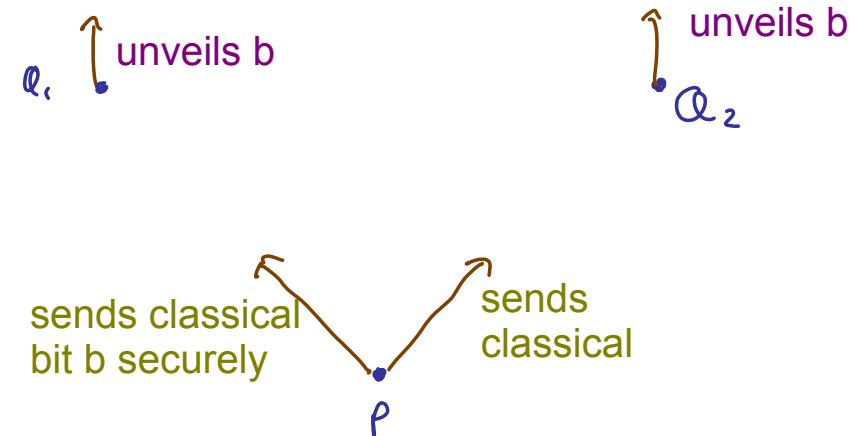
Commitment



Unveiling



Defining bit commitment in Minkowski space



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

If Alice's agents at Q₁ and Q₂ have no correlated information other than b, they cannot coordinate a cheating attack.

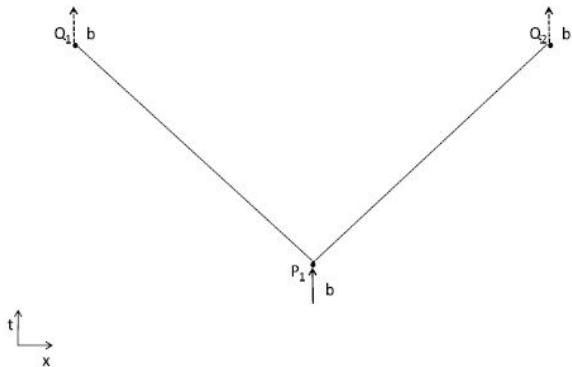
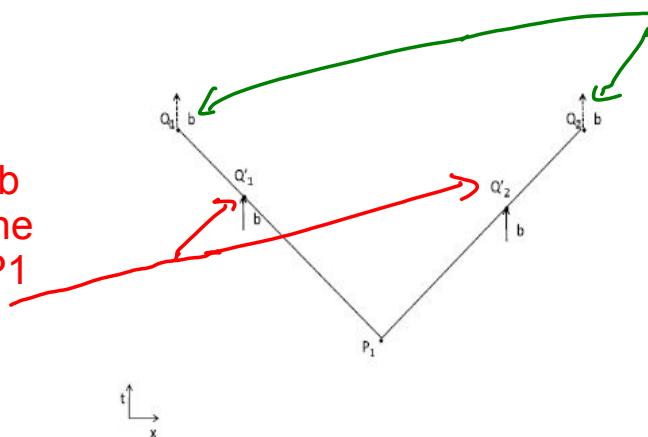


FIG. 7: A classical relativistic bit commitment protocol in $1 + 1$ dimensions represented in our framework. Alice learns the bit b at point P_1 . She is required to send the encrypted bit to her agents at Q_1 and Q_2 , points lightlike separated from P_1 in different directions. Her agents decrypt the bit and give it to Bob's agents at Q_1 and Q_2 . Note that while this protocol does indeed allow Bob to infer some constraints on Alice's acquisition of b , it does *not* guarantee to Bob that she was committed by the point P_1 .

(from: *Quantum Tasks in Minkowski Space*, AK arxiv:1204.4022)

Alice obtains the bit b
only at two sites in the
future light cone of P_1
(perhaps via
computations or
from natural events)

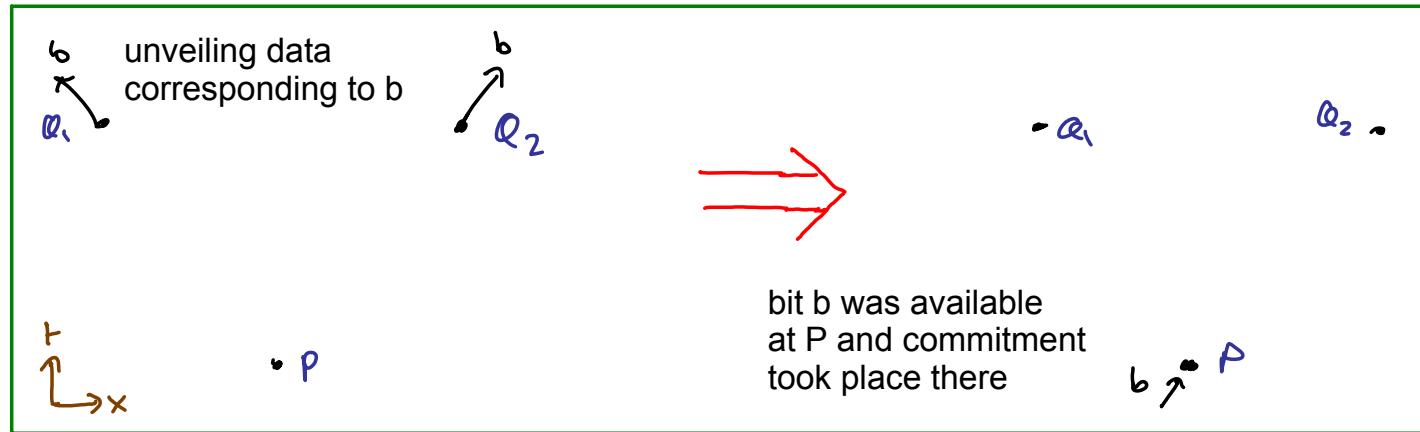


b is unveiled at Q_1 and
 Q_2 - but Alice neither
knew it nor was committed
at P_1 .

FIG. 8: Defeating the classical relativistic bit commitment protocol described in Figure 7. Alice learns the bit b independently at points Q'_1 and Q'_2 . She sends the bit to her agents at Q_1 and Q_2 , who give it to Bob's agents at Q_1 and Q_2 . Alice's unveiling is apparently valid, but she did *not* have the bit b available at the point P_1 , and so clearly was not committed there.

(from: *Quantum Tasks in Minkowski Space*, AK arxiv:1204.4022)

What we need -- which the bit commitment protocols I will describe provably provide -- is security defined appropriately for Minkowski space



That is, in these tasks, Alice's valid unveiling of b at Q₁, Q₂ guarantees that she already had committed herself at P. Her optimal unveiling probabilities for 0 and 1 obey $p_0 + p_1 < 1$ and later arriving data cannot

To decrypt 0, Alice returns ψ somewhere on this ray

Q_0

$\psi?$

To commit 0, Alice sends ψ at light speed securely* along this ray

*secure fibre, teleportation, ...
cf AK-Massar-Silman 1208.0745

To decrypt 1, Alice returns ψ somewhere on this ray

Q_1

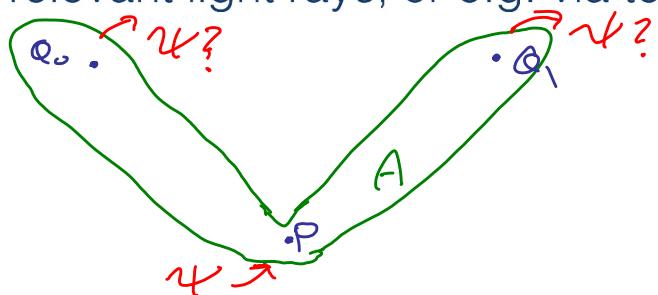
$\psi?$

To commit 1, Alice sends ψ at light speed securely along this ray

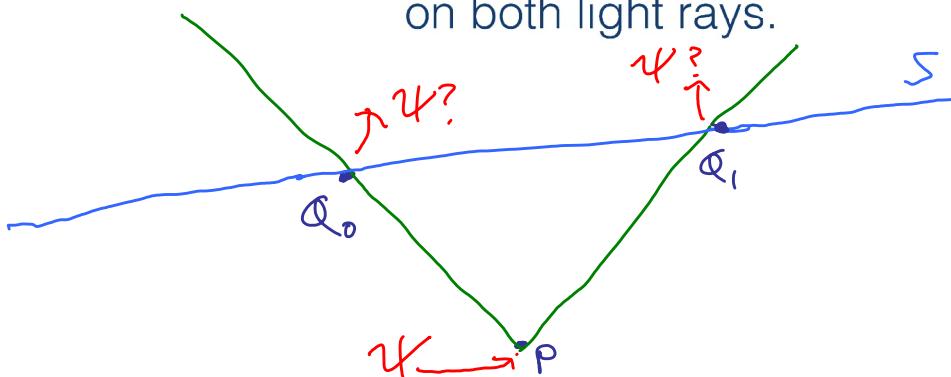
P

Bob gives Alice state ψ at P

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)

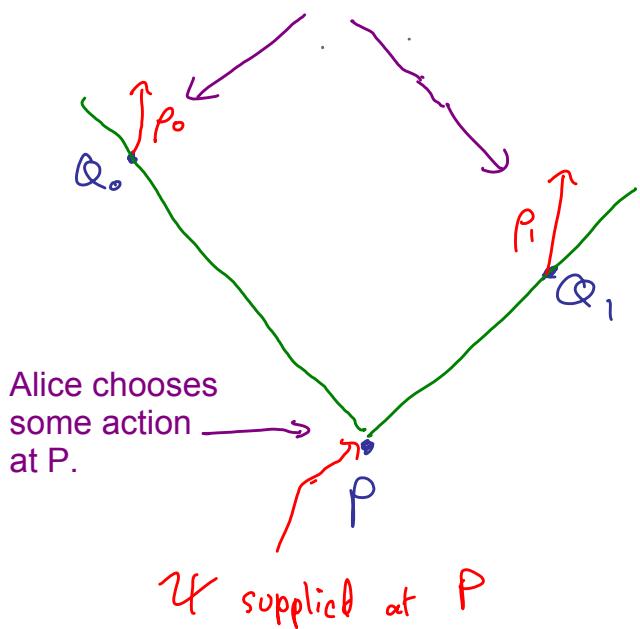


Security against Alice: ensured by the no-summoning theorem -- she cannot return ψ independently at points on both light rays.

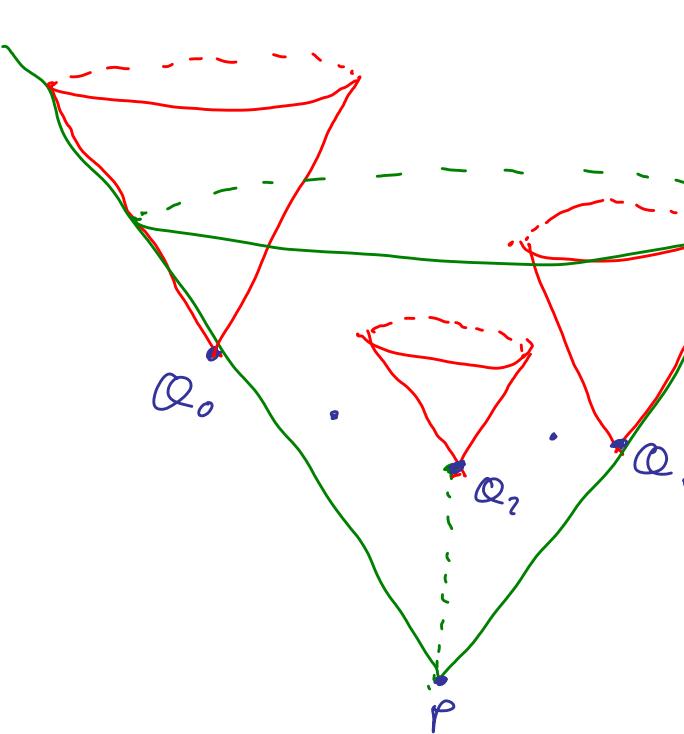


More precisely, we can quantify the security in terms of the dimension d of the space of the unknown state: Alice's cheating probability is bounded by $O(1/d)$.

Optimal states A can return
given her actions chosen at P



$$\begin{aligned}
 & P(\text{Bob accepts unveiling at } Q_0) + \\
 & P(\text{Bob accepts unveiling at } Q_1) \\
 = & \langle \psi | \rho_0 | \psi \rangle + \langle \psi | \rho_1 | \psi \rangle \\
 \leqslant & 1 + \frac{2}{d+1} \\
 & \text{Alice's "wiggle room" decays exponentially in \#qubits = log } d
 \end{aligned}$$



Any 2 points
on distinct light
rays through P
are spacelike
separated

This works in 3+1 dimensions also -- and now each possible light like direction can code for a different data value, so the amount of data committed is bounded only by the precision of Alice's transmission and Bob's measurement.

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.

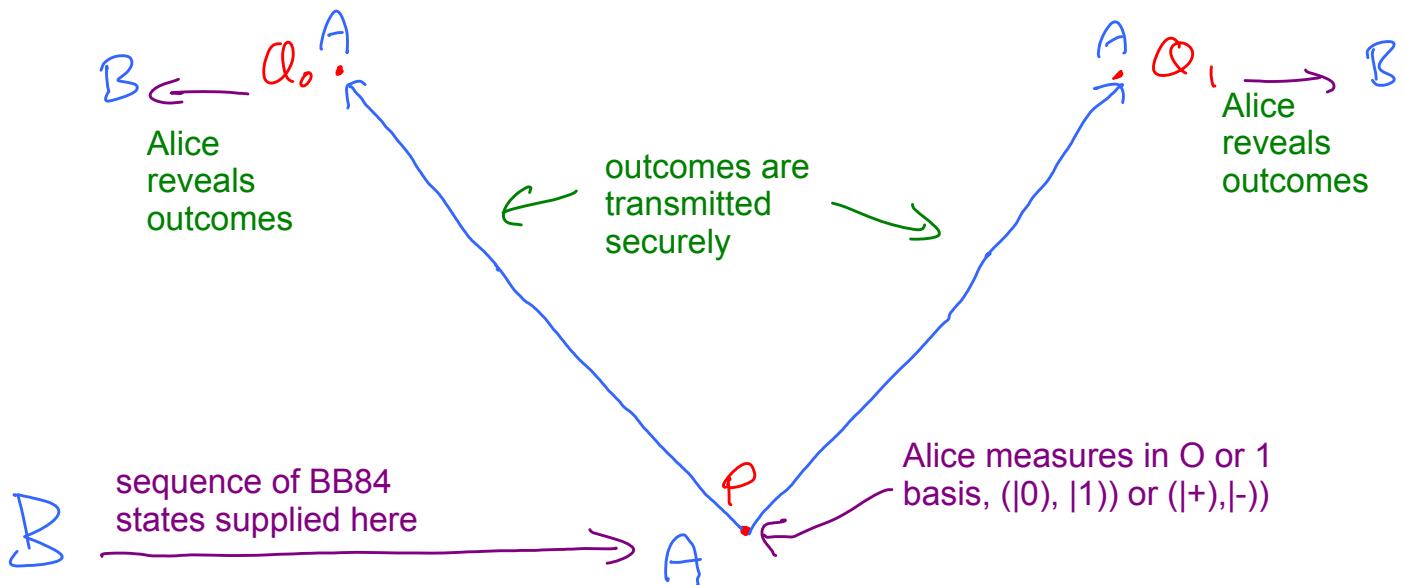
In particular, it assumes that, if there is a unitary map taking a 0 commitment to a 1 commitment, known to Alice, she can implement it physically -- and so cheat by altering her commitments.

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.

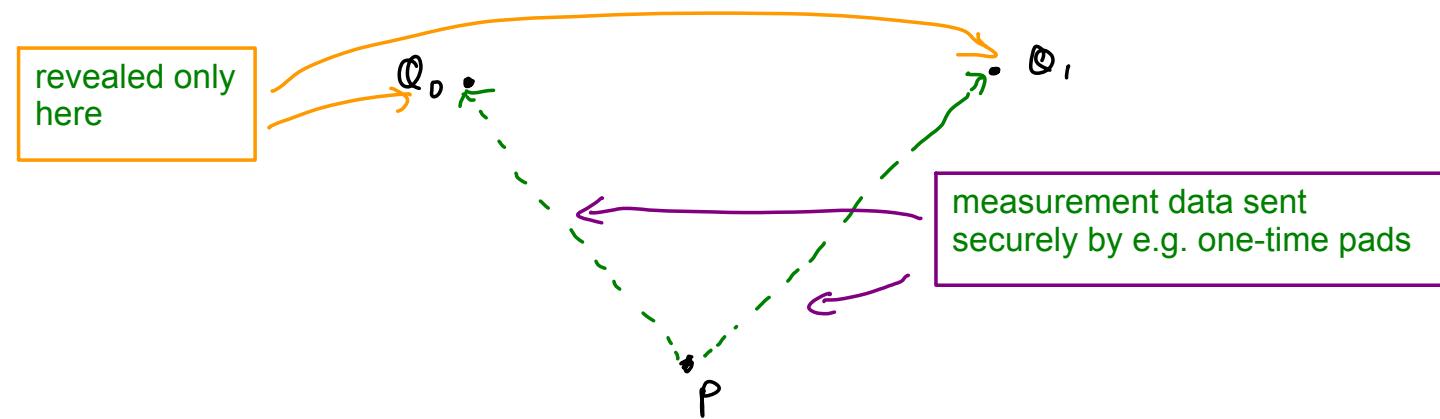
Unconditionally secure bit commitment by transmitting measurement outcomes (AK, arxiv:1108.2879, PRL to appear)

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.



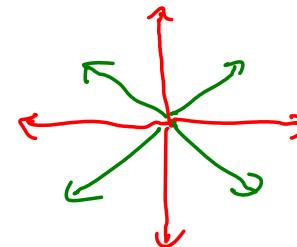
Security discussion (see the two papers already mentioned 1108.2879, 1204.4022
see also Kaniewski-Tomamichael-Hanggi-Wehner 1206.1740, Croke-AK
1208.1458).

Security against Bob: ensured because Alice sends all data securely, e.g. using one-time pads. In a rather appealingly Zen sense, in this and the previous protocol, Alice commits herself without actually giving Bob anything at all until she unveils.



Security against Alice: ensured because any nonzero probability p of her being able to unveil both 0 and 1 implies her being able to report credible measurement outcomes for each BB84 state in both complementary bases -- and in particular to identify the state correctly in its own basis.

Alice's optimal probability for doing this, for any given state, is $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$, obtained by the POVM



BB84 states
POVM operators

Collective operations on N states give Alice no advantage.

Any collective operation applied to any given list of input states (where the states are listed in some arbitrary order) defines a PO on the N th state for each possible set of guesses on the first N states. No PO can give Alice greater confidence than $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$ in the guess on the N th state. So, whatever the success rate for the first $(N-1)$ guesses, the N -th guess has success probability bounded by $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$ and the overall success rate is thus bounded by $\left(\frac{1}{2}(1 + \frac{1}{\sqrt{2}})\right)^N$.

General Quantum Tasks In Minkowski Space

$|q_i\rangle$
 S_i

Given inputs in the form of quantum states $|q_i\rangle$ 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}
 $|q_{i+1}\rangle$
 S_{i+1}

General Quantum Tasks In Minkowski Space

$|q_i\rangle$
 s_i
 Q_i

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

$|q_{i+1}\rangle$
 s_{i+1}
 Q_{i+1}

$|q_i\rangle$
 s_i
 P_i

Given inputs in the form of quantum states $|q_i\rangle$ 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}
 $|q_{i+1}\rangle$
 s_{i+1}



General Quantum Tasks In Minkowski Space

$|q_i\rangle$
 $E = -s_i$
 Q_i

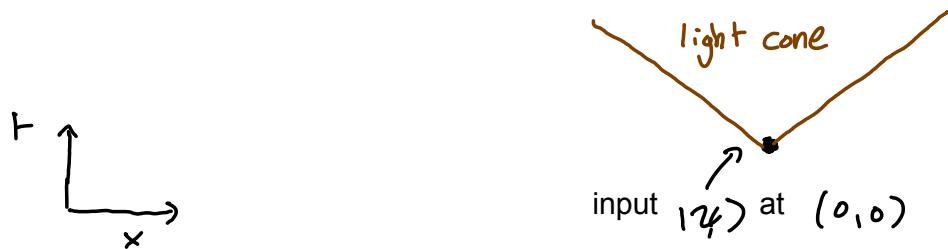


$|q_i\rangle$
 s_i
 P_i

$|q_{i+1}\rangle$
 s'_{i+1}
 Q_{i+1}

P_{i+1}
 $|q_{i+1}\rangle$
 s_{i+1}

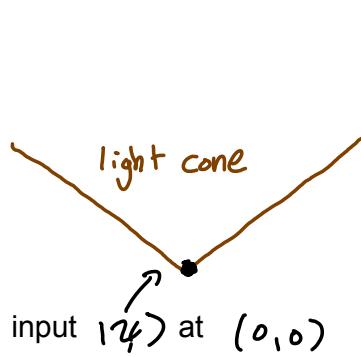
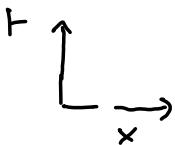
An Interesting Example: Returning an Unknown State

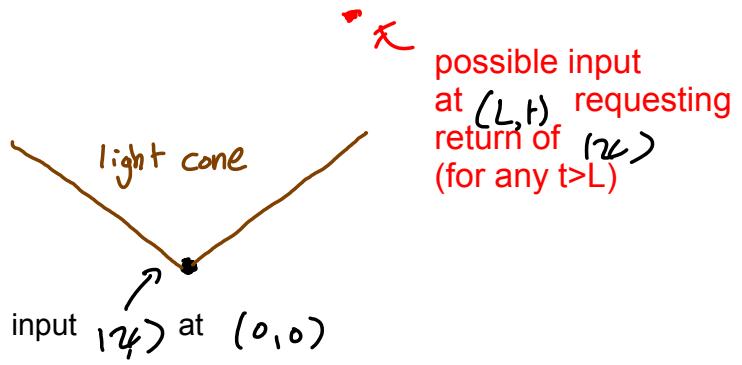
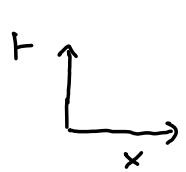


requires output
of $h\psi$ at $(-L, t+2L)$

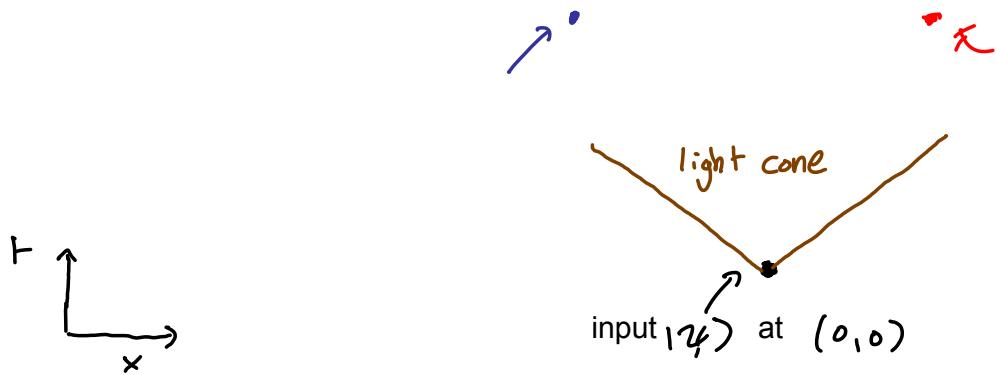


possible input
at $(-L, r)$ requesting
return of ψ
(for any $t > L$)

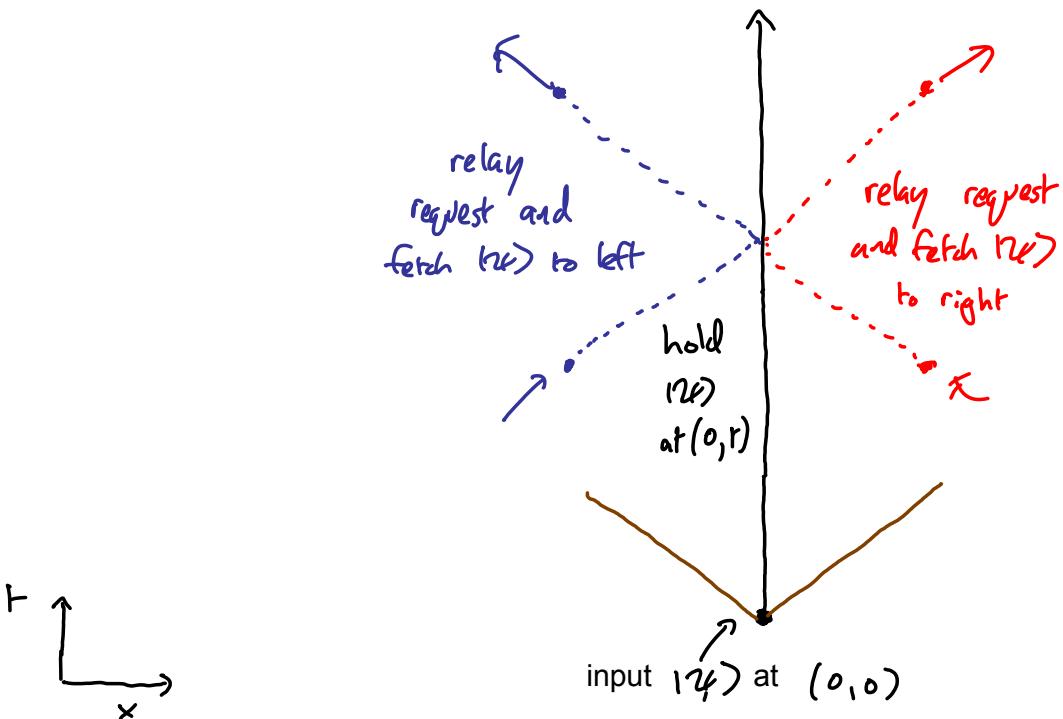




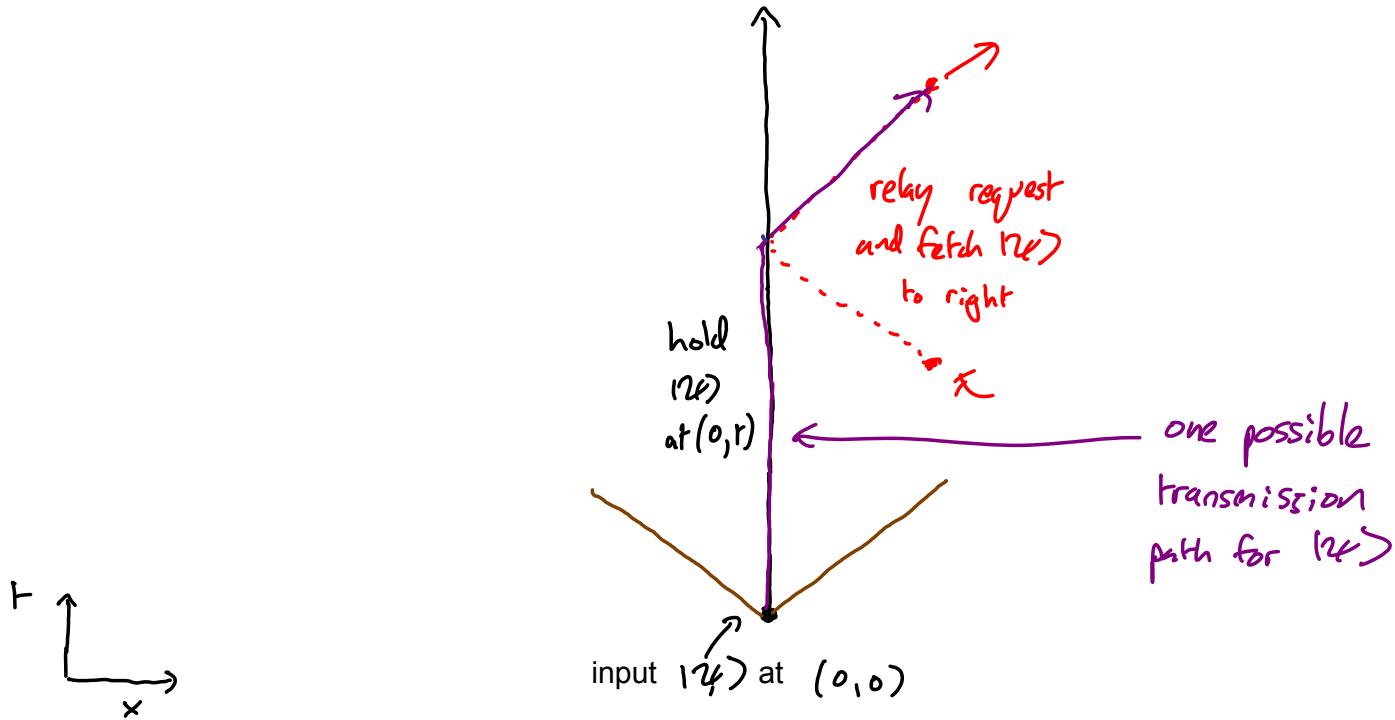
Only one request
will be made, but
when and on which
side isn't known



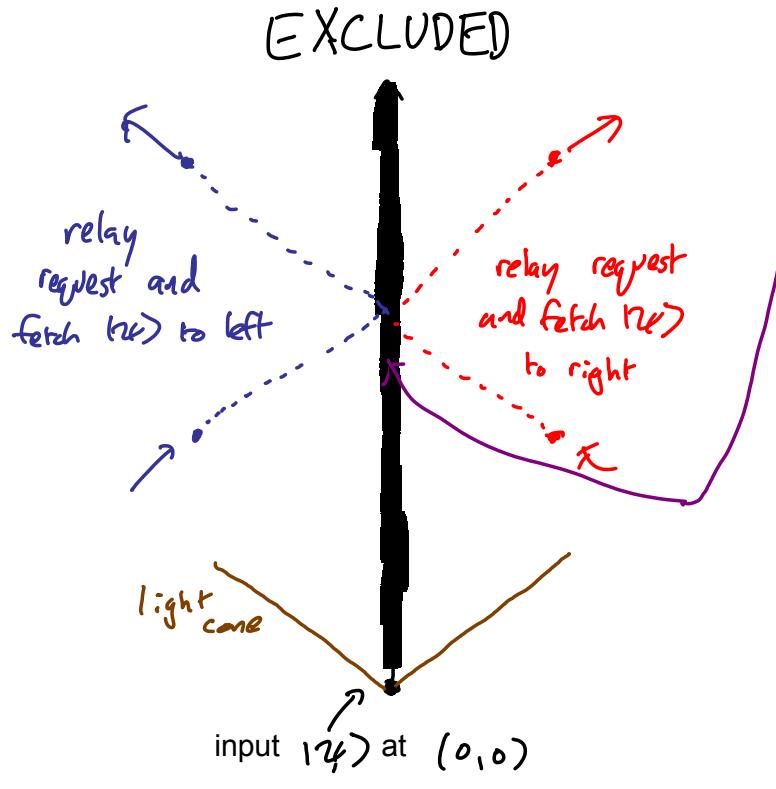
Simple solution to this task



Simple solution to this task



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



This strategy no longer works:
can't hold $|w\rangle$ at $(0,t)$ awaiting signal.

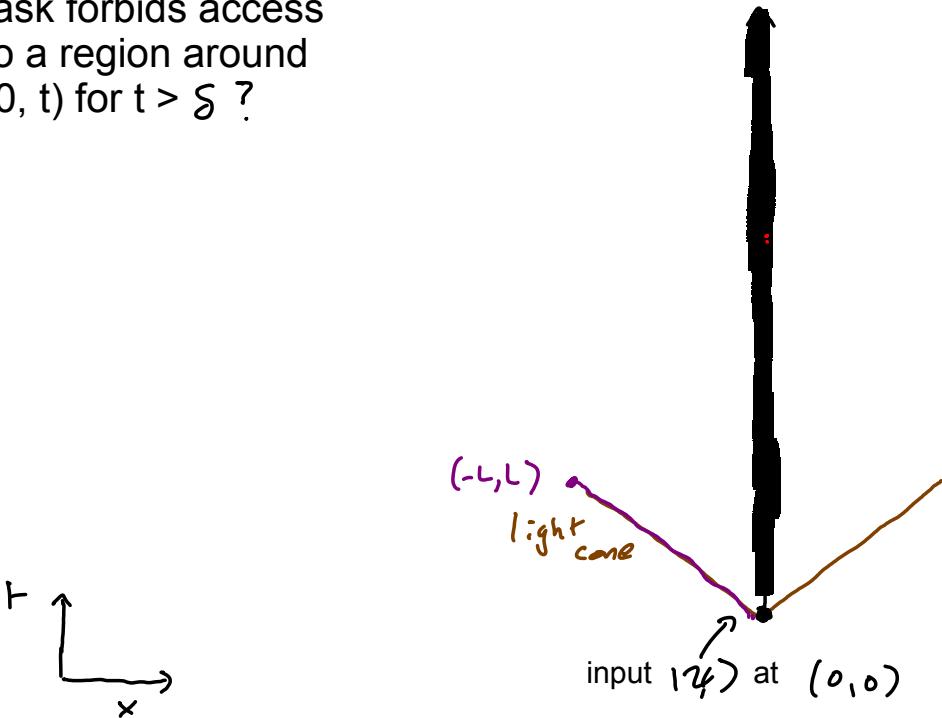
And holding $|w\rangle$ on either the left or right of the excluded region doesn't work either:
the output on the opposite side would arrive

But what if the task forbids access to a region around $(0, t)$ for $t > \mathcal{S}$?

EXCLUDED

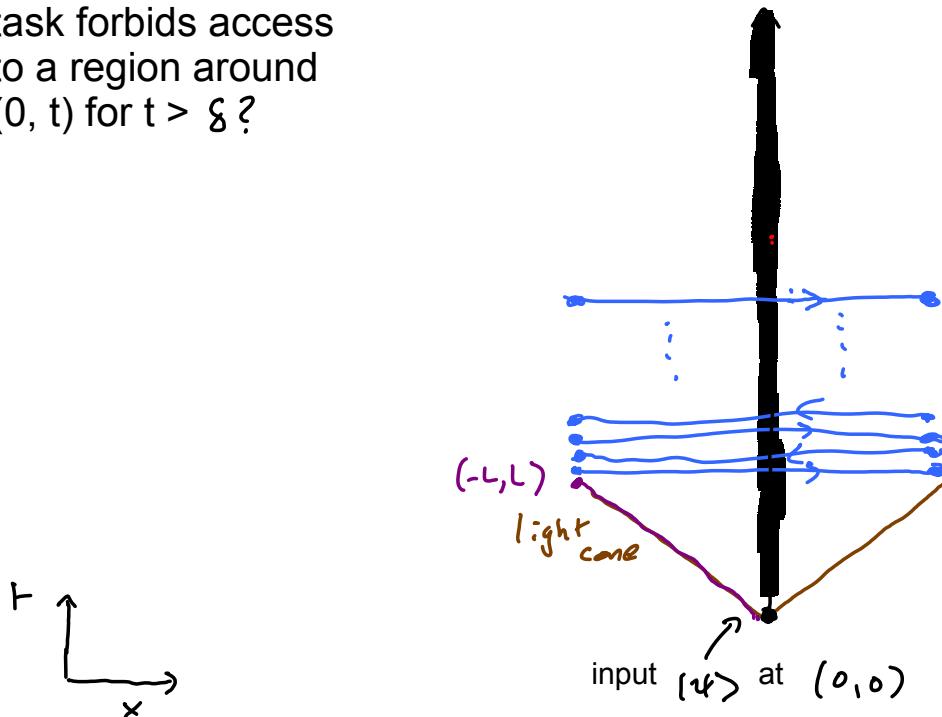
There is nonetheless a simple solution:

- 1) send ψ to (say) the point $(-L, L)$.



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

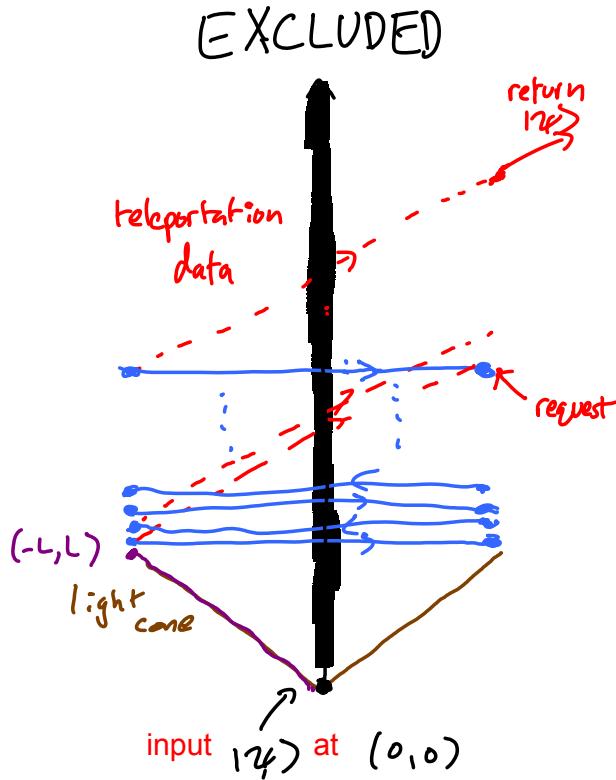
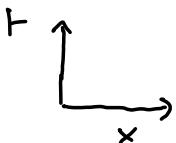
EXCLUDED



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.

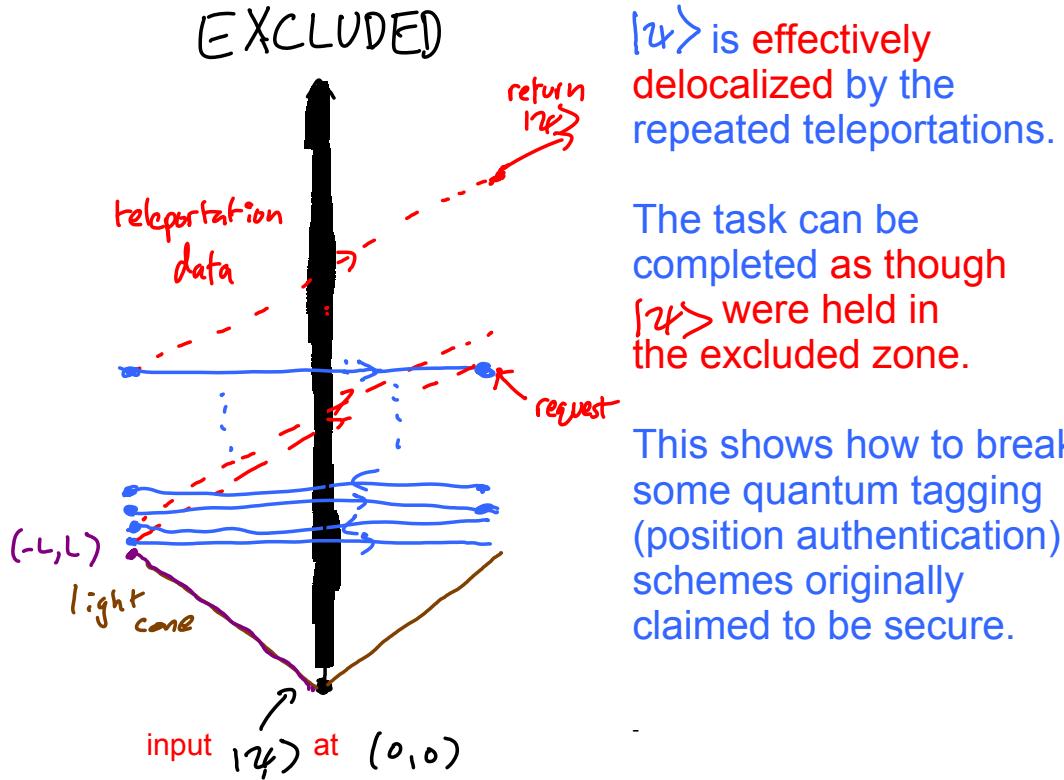
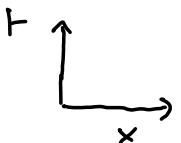
But what if the task forbids access to a region around $(0, t)$ for $t > \delta$?



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 task forbids access to a region around $(0, t)$ for $t > \delta$?



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).**
- 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.

Quantum Tagging References

- ▶ KMSB (2006): AK, Munro, Spiller, Beausoleil, "Tagging Systems", US patent 2006/0022832
- ▶ Malaney (2009): Phys Rev A 81 042319 and arxiv 1004.2689
- ▶ CFGGO (2010): Chandran, Fehr, Gelles, Goyal, Ostrovsky arxiv: 1005.1750
- ▶ KMS (2010): AK, Munro, Spiller, arxiv:1008.2147 } formal definition of tagging
teleportation attacks on
previous schemes
- ▶ K (2010): AK, arxiv:1008.5380 } secure tagging for tags containing secret data
- ▶ LL (2010): Lau, Lo: arxiv:1009.2256
- ▶ BCFGGOS (2010): Buhrman,CFGGO,Schaffner, arxiv: 1009.2490 } beautiful
general no-go
theorem +
wider applications
- ▶ (Relies on Vaidman (2003): Phys. Rev. Lett 90 010402.)

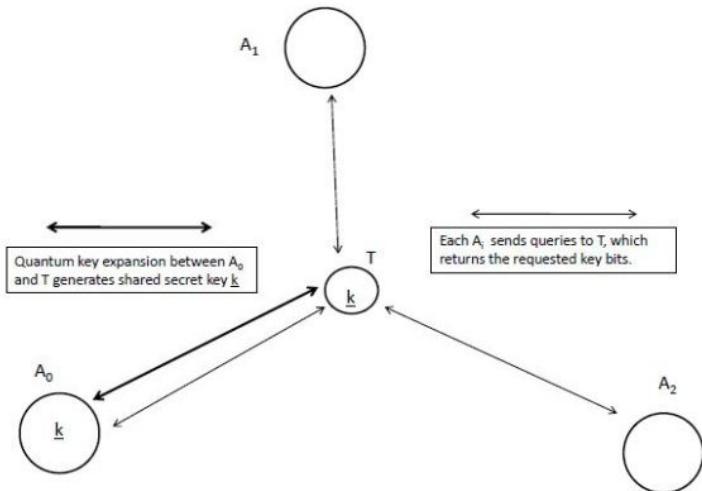


FIG. 1: One implementation of secure tagging in two dimensions. Here the key is generated by quantum key expansion between A_0 and T . A_0 shares the key with A_1 and A_2 either via secure communication based on quantum key expansion, or by transmitting relevant key bits after they have been queried.

Secure Quantum tagging (position authentication in Minkowski space) **is possible** for any tagged object that can store a classical key securely. The security follows from the security of QKD and the impossibility of superluminal signalling. (AK, Phys Rev A 84, 022335 (2010))

Returning to the original problem: we cannot verify that the state lies in the excluded region using (only) the remote query protocol we tried. 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.

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

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

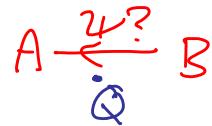
An example of a relativistic quantum impossibility: Summoning a quantum state

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

N.B.)

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.



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.

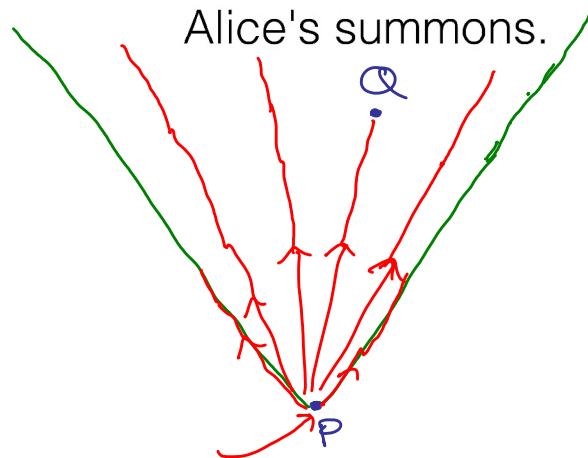
In principle, with arbitrarily short delay, Bob **can** comply if the underlying theory is quantum mechanics in Galilean space-time, or classical mechanics in Minkowski space-time.

However, as we will show, given an unknown quantum state in Minkowski space-time, he **cannot** comply.

Summoning in classical theories

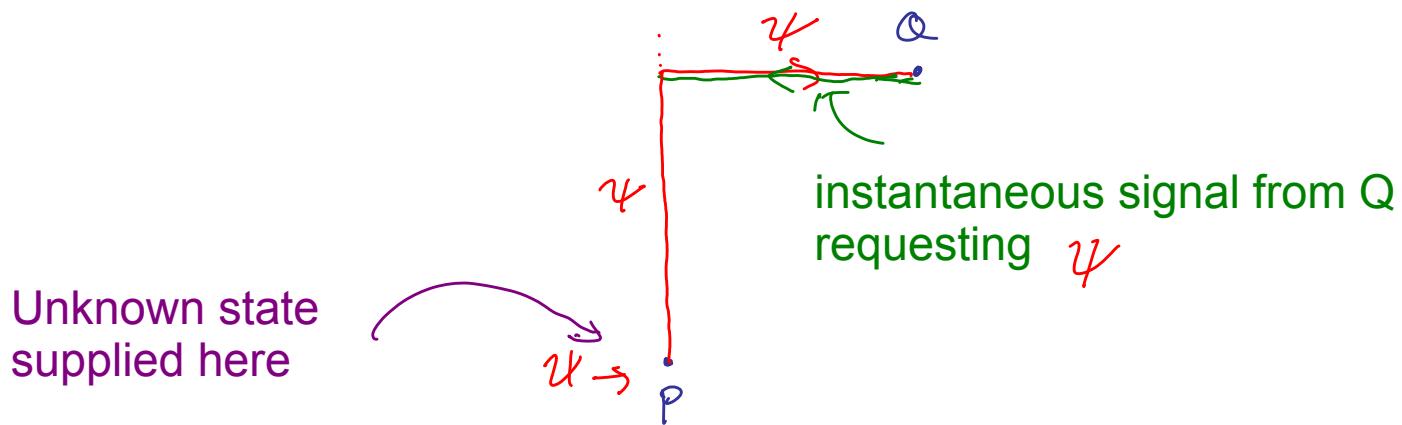
Given an unknown classical state at point P in Minkowski space, Bob can (in principle) measure it precisely, broadcast the information in all directions, and reconstruct the state at any point Q in the causal future of P -- and so comply with

Alice's summons.



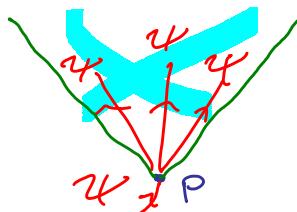
Summoning in non-relativistic quantum mechanics

Given an unknown quantum state ψ 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.

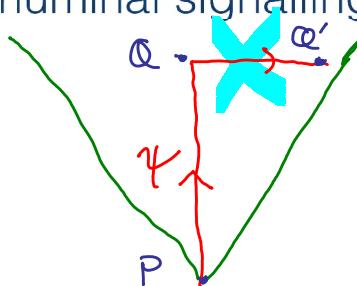


No summoning in relativistic quantum theory

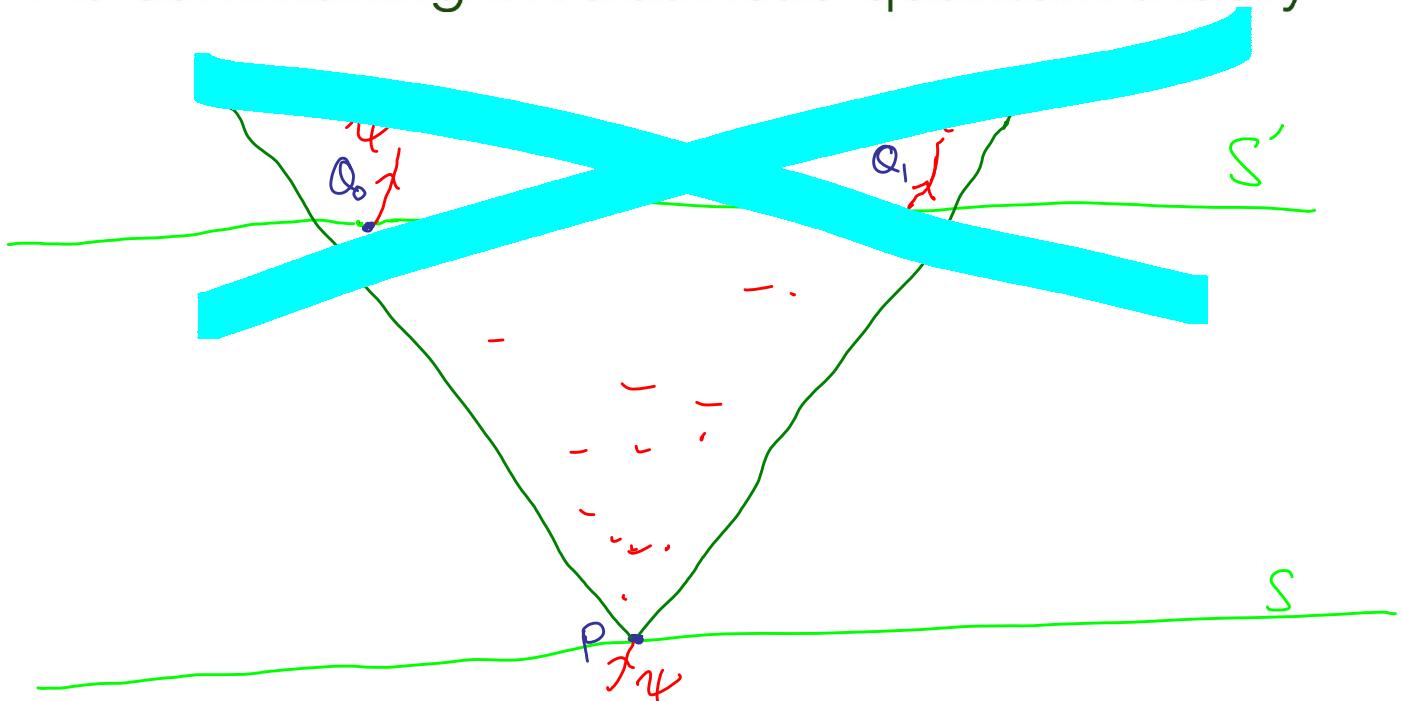
Given an unknown quantum state ψ at point P in Minkowski space-time, Bob cannot precisely identify it or copy it (because of the no-cloning theorem).



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 summoning in relativistic quantum theory



More generally, we can use no-cloning and no-signalling to prove that whatever strategy he follows, Bob cannot generally comply with a summons.

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 foundations

- The no-summoning theorem follows from the no-cloning theorem and the no-signalling principle, but not from either alone.
- Like the no-cloning theorem, it is mathematically elementary.
- But it says something new about the relationship between quantum theory and relativity: the first (?) example of a simple information-related task that distinguishes relativistic quantum theory from non-relativistic qm and relativistic classical physics.
- Whereas Bell's theorem, no-cloning, no-broadcasting, no-signalling, information causality, ... all apply to non-relativistic qm as well as to relativistic quantum theory.
- And, on the other hand, the impossibility of instantaneous measurement of non-localised states holds in classical relativistic theories as well as in relativistic quantum theory.

Summary

Relativistic quantum cryptography, perhaps once seen as esoteric, is developing into a major field in its own right.

There are direct applications to bit commitment, quantum tagging (position authentication), position-based quantum cryptography, location-oblivious quantum data transfer, as well as secure coin tossing with fixed and user-variable biases.

There are also direct applications of relativistic cryptographic protocols to device-independent quantum cryptography. Perhaps the prime example is the possibility of secure key distribution based on the no-signalling principle, whose realization began the ongoing research programme ultimately aiming at efficient secure device-independent quantum key distribution.

Future technologies will, I believe, be built using many of these ideas and others awaiting discovery.

New cryptographic ideas are out there waiting to be discovered, along with new perspectives