Abstract: 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. 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.
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)
Given inputs in the form of quantum states $\psi_i$ 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 and classical data at locations, where the output data and locations generally depend on the input data and locations.

Given inputs in the form of quantum states and classical data at locations, 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 and classical data at locations, where the output data and locations generally depend on the input data and locations.

Given inputs in the form of quantum states and classical data at locations, where neither the locations nor the classical or quantum data are generally known in advance.
requires output of $\psi$ at $(-L, t+2L)$

possible input at $(L, \tau)$ requesting return of $(\text{for any } t)$

light cone

input $\psi$ at $(0, 0)$
Simple solution to this task

- Relay request and fetch \( |r\rangle \) to left
- Hold \( |n\rangle \) at \((0,1)\)
- Relay request and fetch \( |n\rangle \) to right
- Input \( |y\rangle \) at \((0,0)\)
But what if the taste forbids access to a region around $(0, t)$ for $t > \delta$?

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

And holding $|\psi\rangle$ on either the left or right of the excluded region doesn't work either: the output on the opposite side would arrive too late.
But what if the taste forbids access to a region around \((0, t)\) for \(t > \delta\)?

*EXCLUDED*

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

And holding \(|\psi\rangle\) on either the left or right of the excluded region doesn't work either: the output on the opposite side would arrive too late.

Input \(|\psi\rangle\) at \((0, 0)\)
But what if the taste forbids access to a region around $(0, t)$ for $t > S$?

There is nonetheless a simple solution:

1) send $\psi$ to (say) the point $(-L,L)$.
But what if the taste forbids access to a region around \((0, t)\) for \(t > \delta\)?

There is nonetheless a simple solution:

1) send \(\psi\) to (say) the point \((-L, L)\).

2) repeatedly "teleport" the quantum state \(\psi\) 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 \(\psi\).
But what if the taste forbids access to a region around (0, t) for t > ε?

|ψ⟩ is effectively delocalized by the repeated teleportations.

The task can be completed as though |ψ⟩ 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? 

\[ \lvert u \rangle \text{ is effectively delocalized by the repeated teleportations.} \]

The task can be completed as though \( \lvert u \rangle \) 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 $t > \delta$?

$\lvert u \rangle$ is effectively delocalized by the repeated teleportations.

The task can be completed as though $\lvert u \rangle$ 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


- 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 Jennewey'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


• Various tagging schemes proposed: CFGGGO 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 Jenneweg'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.
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)
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)
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.
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.
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.
To decrypt 0, Alice returns $\psi$ somewhere on this ray

To decrypt 1, Alice returns $\psi$ somewhere on this ray

To commit 0, Alice sends $\psi$ at light speed securely along this ray

To commit 1, Alice sends $\psi$ at light speed securely along this ray

*secure channel, teleportation, ...

Bob gives Alice state $\psi$ 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 $\psi$ 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 $P$.

Alice chooses some action at $P$.

$U$ supplied at $P$.

\[
P(\text{Bob accepts unveiling at } Q_0) + P(\text{Bob accepts unveiling at } Q_1) = |\langle u | X | q_0 \rangle| + |\langle u | X | q_1 \rangle| \\
\leq 1 + \frac{2}{d+1}
\]

Alice's "wiggle room" decays exponentially in the number of 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 $P$

Alice chooses some action at $P$.

$U$ supplied at $P$;

\[
P(\text{Bob accepts unveiling at } Q_0) + P(\text{Bob accepts unveiling at } Q_1) \\
= \langle u | p_0 | u \rangle + \langle u | p_1 | u \rangle \\
\leq 1 + \frac{2}{d+1}
\]

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

**Diagram:**
- **A** sends a quantum state to **B**.
- Alice reveals outcomes.
- Outcomes are transmitted securely.
- Alice measures in 0 or 1 basis, ([0], [1]) or ([+], [-]).
- B receives sequence of BB84 states supplied here.
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.

Alice reveals outcomes

outcomes are transmitted securely

sequence of BB84 states supplied here

Alice measures in O or 1 basis, (|0⟩, |1⟩) or (|+⟩, |--⟩)

Alice reveals outcomes
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.
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.
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.
b is unveiled at Q1 and Q2 - but Alice neither knew it nor was committed at P1.

the bit b is obtained only at two sites in the future light cone of P (perhaps after computations or from natural events)

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.

(All Quantum Tasks in Minkowski Space, arXiv:1204.4022
see also Kaniewski et al. arXiv:1206.1740)
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 $P$. 
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 $I_1, \ldots, I_m$ at points $P_1, \ldots, P_m$. Following a prearranged protocol, she is required to calculate output points $Q_1, \ldots, Q_n$ and produce the output data $J_1, \ldots, J_n$ there.
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 $I_1, \ldots, I_m$ at points $P_1, \ldots, P_m$. Following a prearranged protocol, she is required to calculate output points $Q_1, \ldots, Q_n$ and produce the output data $J_1, \ldots, J_n$ there.
FIG. 11: The principle of information causality [11] represented in our framework. Alice receives input $I_1$, which takes the form of a string of $M$ bits, at point $P_1$, and input $I_2$, which takes the form of a query for $N+1 \leq M$ of the $M$ bits, at point $P_2$. She is required to produce the $N+1$ requested bits at the point $Q_1$. Her agents may be located anywhere in space-time except for the darkened region. The darkened region is only penetrable to a limited extent: she may transmit no more than a total of $N$ bits through it. She cannot generally complete the task.
FIG. 11: The principle of information causality [11] represented in our framework. Alice receives input $I_1$, which takes the form of a string of $M$ bits, at point $P_1$, and input $I_2$, which takes the form of a query for $N + 1 \leq M$ of the $M$ bits, at point $P_2$. She is required to produce the $N + 1$ requested bits at the point $Q_1$. Her agents may be located anywhere in space-time except for the darkened region. The darkened region is only penetrable to a limited extent: she may transmit no more than a total of $N$ bits through it. She cannot generally complete the task.
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-obliviuous 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.