

Title: QPV - A retrospective

Speakers: Adrian Kent

Collection: QPV 2023: Advances in quantum position verification

Date: September 18, 2023 - 9:30 AM

URL: <https://pirsa.org/23090011>

Abstract: Quantum position verification (QPV) was first introduced, under the name quantum tagging, in a patent filed in 2004. It was first discussed in the academic literature in 2009-10. The schemes proposed to that point were shown to be breakable by teleportation attacks in 2010, and a general no-go theorem showing all schemes in this class are breakable was subsequently proved. However, in an alternative standard cryptographic security scenario, in which the tag is assumed to be able to keep classical data secret, unconditionally secure schemes were presented in 2010.

The various terminologies and security scenarios highlight important points whose theoretical and practical implications still remain underexplored. In practice, one normally wants to verify the location of a person or valuable object, not of an easily replaceable tagging device, for at least two reasons: (i) the device itself is not so valuable, (ii) adversaries can easily construct a replacement device and thereby potentially spoof the scheme. This requires physical assumptions about the integrity of the tag and its attachment, and bounds on the speed with which the tag may be displaced or destroyed and replaced. QPV schemes that do not rely on such assumptions are breakable without teleportation or non-local computation attacks. In the other direction, when such significant physical assumptions are necessary, it may generally be reasonable to include tag security among them.

In this overview I review the early history of QPV and describe various security scenarios and their potential applications. I give versions of the secure 2010 scheme designed for efficient practical implementation and discuss the frequency, accuracy and security of position verification attainable for these schemes with present technology. I also discuss the implied constraints on what may be attainable for QPV schemes involving real-time quantum measurement and/or quantum information processing.

# Quantum Position Verification: A RetroProspective

Adrian Kent

Centre for Quantum Information and Foundations,  
DAMTP, University of Cambridge

*and*

Perimeter Institute for Theoretical Physics

talk at QPV2023, Perimeter Institute, 18.9.23



# Quantum Position Verification: A RetroProspective

Adrian Kent

Centre for Quantum Information and Foundations,  
DAMTP, University of Cambridge

*and*

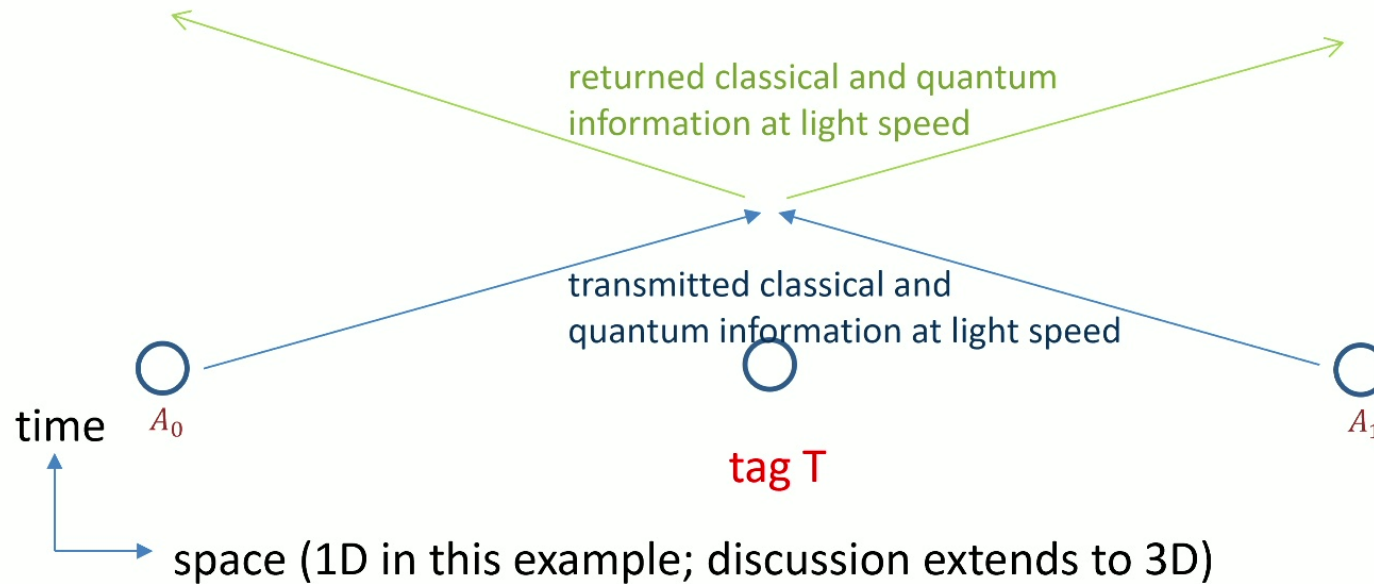
Perimeter Institute for Theoretical Physics

talk at QPV2023, Perimeter Institute, 18.9.23

Joint work with  
Damián Pitalúa-García and  
George Cowperthwaite



Quantum tagging (QPV): the key idea  
(AK-Beausoleil-Munro-Spiller 2002 patent (published 2006);  
independently Chandran et al., Malaney 2010)



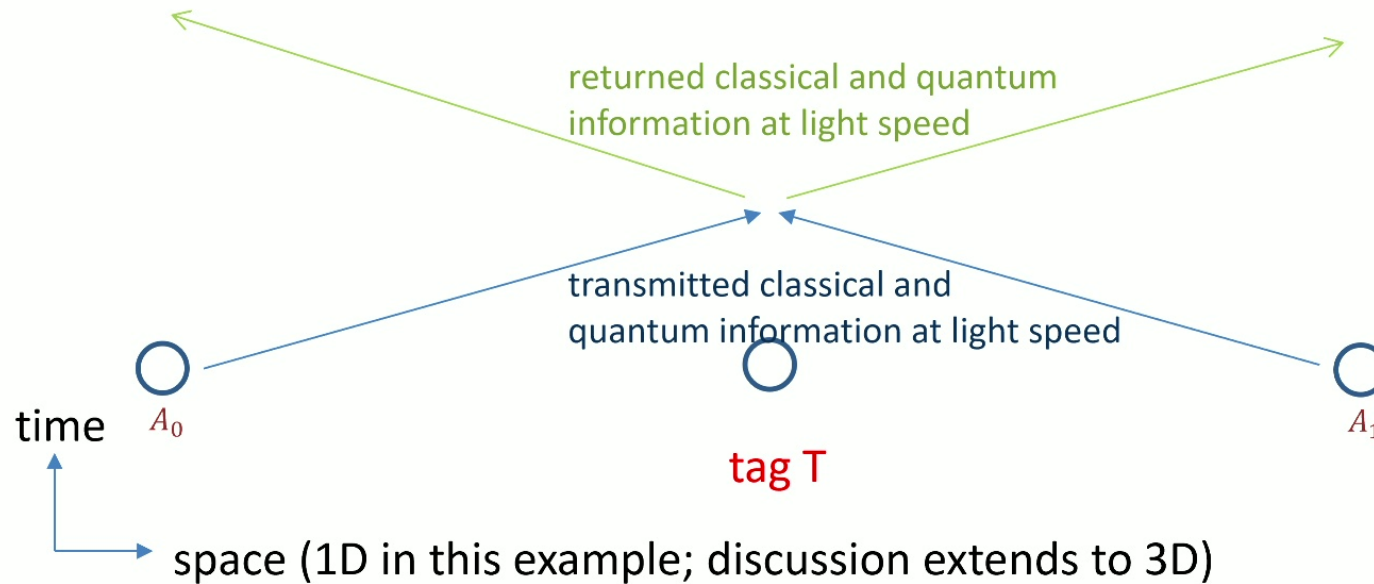
(19) **United States**

(12) **Patent Application Publication**  
Kent et al.

(10) **Pub. No.: US 2006/0022832 A1**

(43) **Pub. Date: Feb. 2, 2006**

Quantum tagging (QPV): the key idea  
 (AK-Beausoleil-Munro-Spiller 2002 patent (published 2006);  
 independently Chandran et al., Malaney 2010)



(54) **TAGGING SYSTEMS**

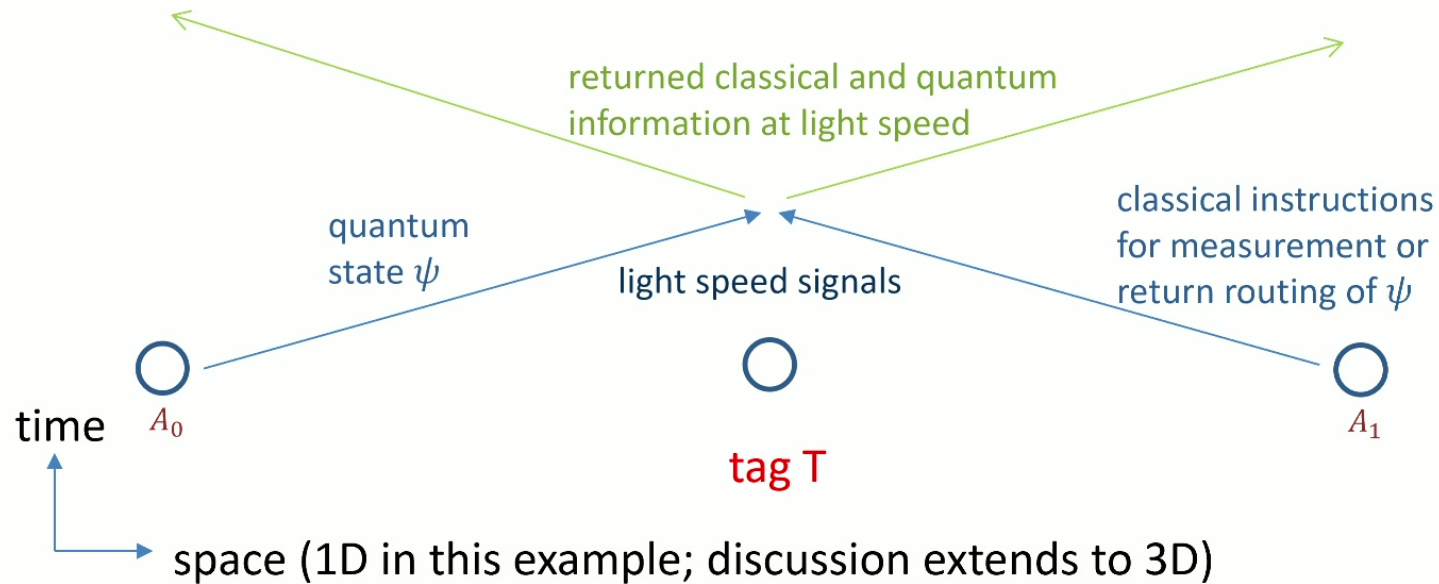
(76) Inventors: **Adrian P. Kent**, Cambridge (GB);  
**William J. Munro**, Bristol (GB);  
**Timothy P. Spiller**, North Somerset  
 (GB); **Raymond G. Beausoleil**,  
 Redmond, OR (US)

(57) **ABSTRACT**

A method of verifying the position of a tagging device is described. The method comprises: storing response information in a quantum state of a quantum entity, the quantum entity comprising an entangled pair; separating the entangled pair into first and second entangled particles; conveying the first and second entangled particles to first

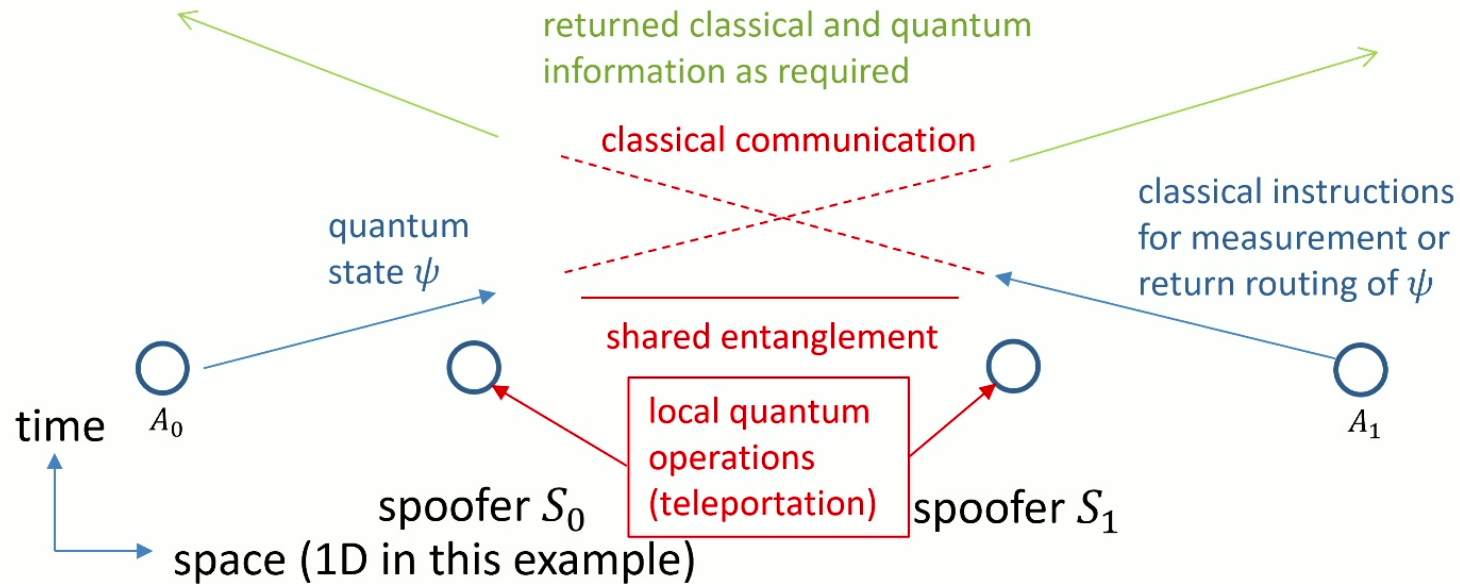
## QPV example

(AK-Beausoleil-Munro-Spiller 2002 patent (published 2006);  
independently Chandran et al., Malaney 2010)



In this example, the tag T is supposed to prove its position to verifiers  $A_0, A_1$  by acting on  $\psi$  as instructed and returning the required information at light speed. Since  $\psi$  cannot be copied and the timings allow no delay, this *seems* (and was claimed by Chandran et al. to be) secure.

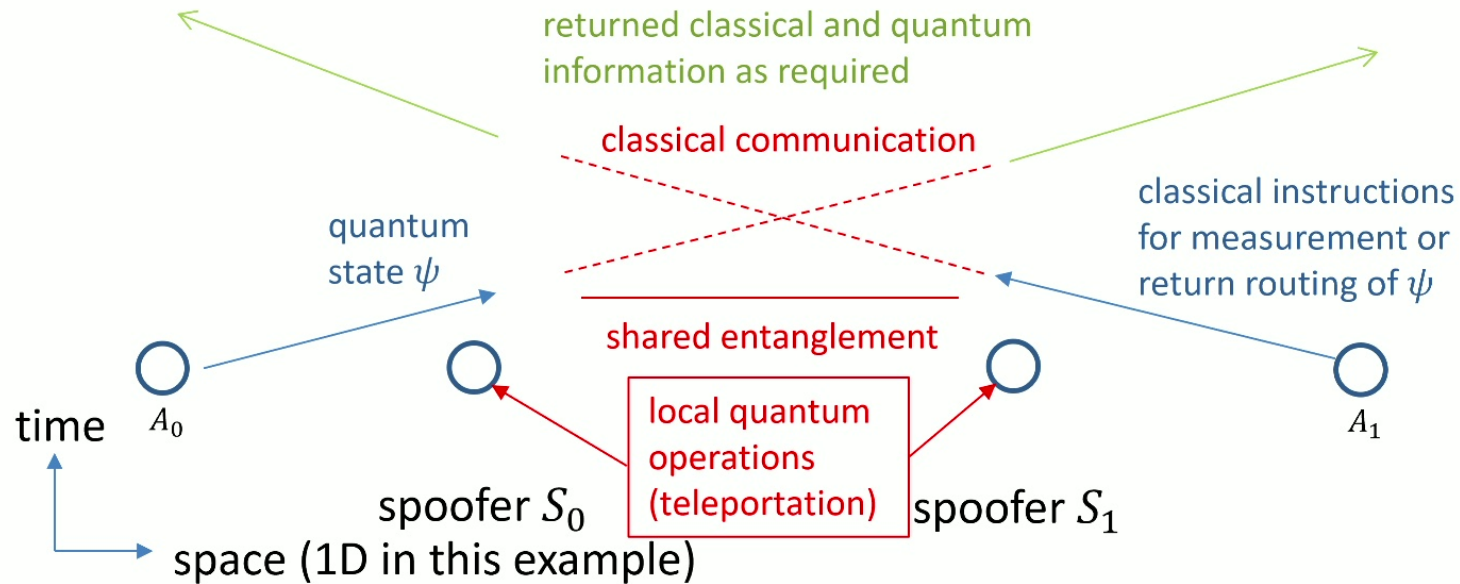
# Teleportation attacks on quantum tagging (AK-Munro-Spiller, 2010)



Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints

Adrian Kent, William J. Munro, and Timothy P. Spiller  
Phys. Rev. A **84**, 012326 – Published 21 July 2011

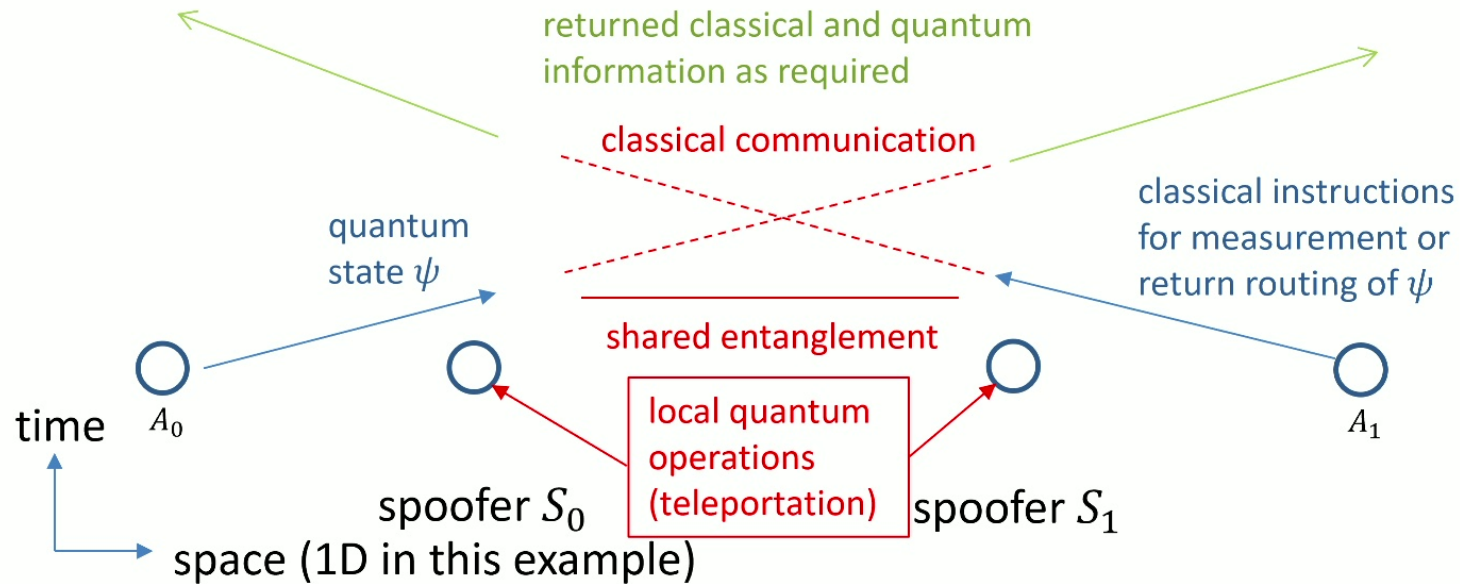
# Teleportation attacks on quantum tagging (AK-Munro-Spiller, 2010)



**But** (see KMS 2010) the proposed schemes are insecure: intervening spoofers can use teleportation attacks to simulate the tag's operations, even though the quantum information never reaches the tag's purported location.



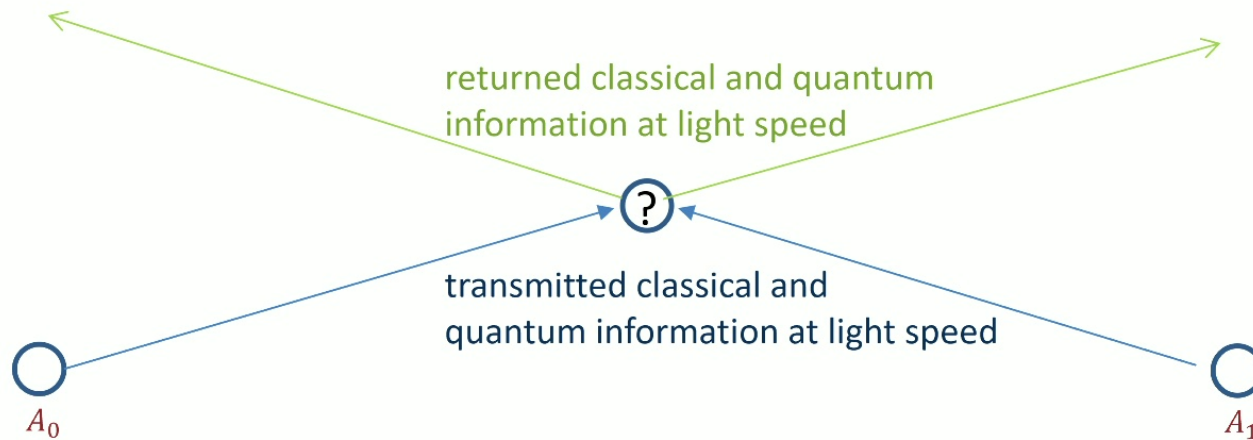
# Teleportation attacks on quantum tagging (AK-Munro-Spiller, 2010)



These attacks applied to specific published tagging protocols. They inspired a beautiful general no-go theorem by Buhrman et al. (2010) that applies to all QPV/tagging schemes **in the given security model**.

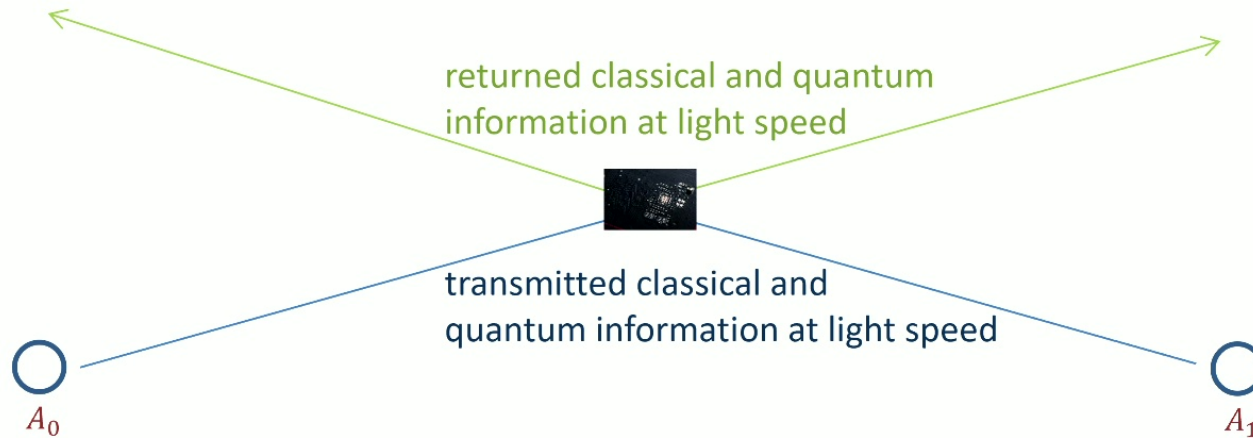
# QPV or Tagging security models

What should a QPV protocol aim to verify the position of ....?



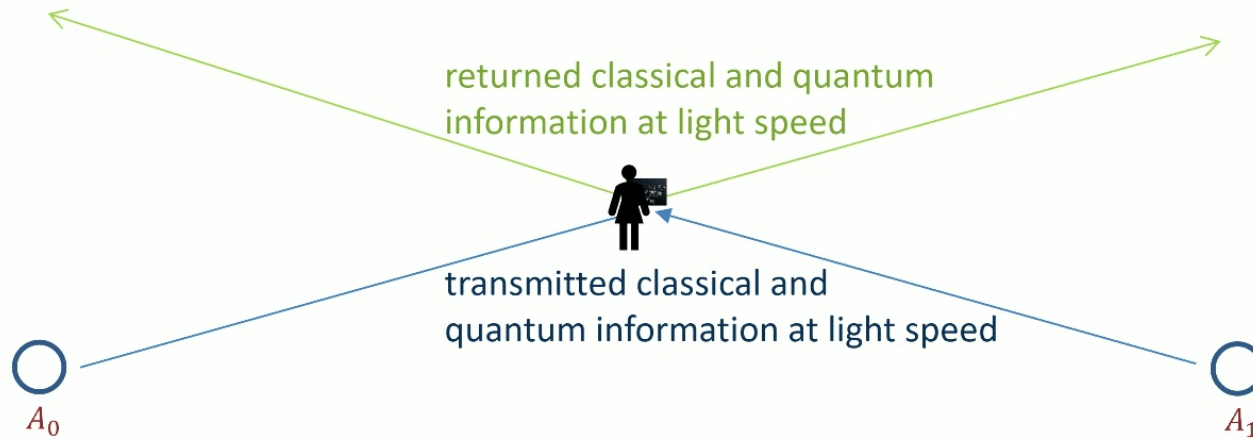
# QPV or Tagging security models

Should a QPV protocol aim to verify the position of a tagging device?



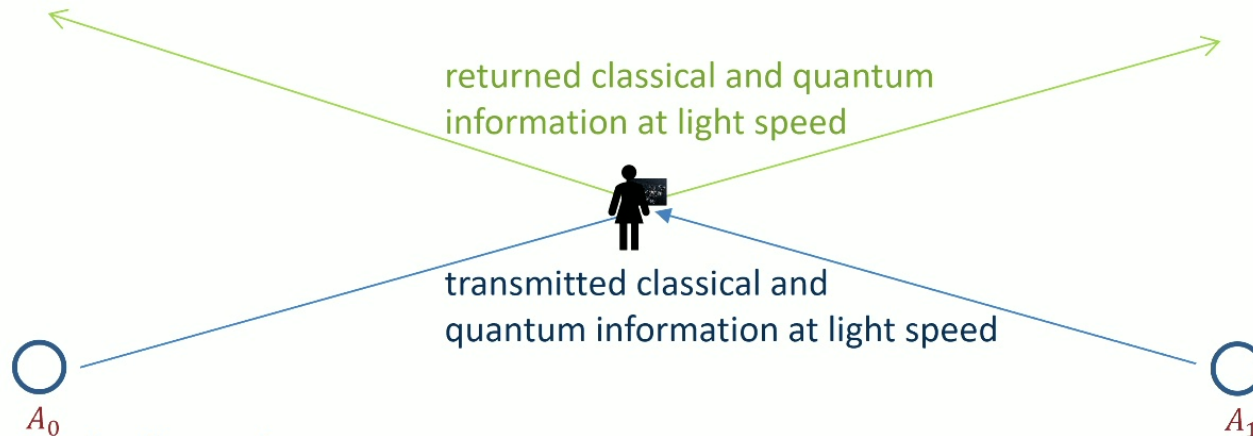
# QPV or Tagging security models

Should a QPV protocol aim to verify the position of a tagging device?  
or of a tagged person or object?



# QPV or Tagging security models

Should a QPV protocol aim to verify the position of a tagging device?  
or of a tagged person or object?

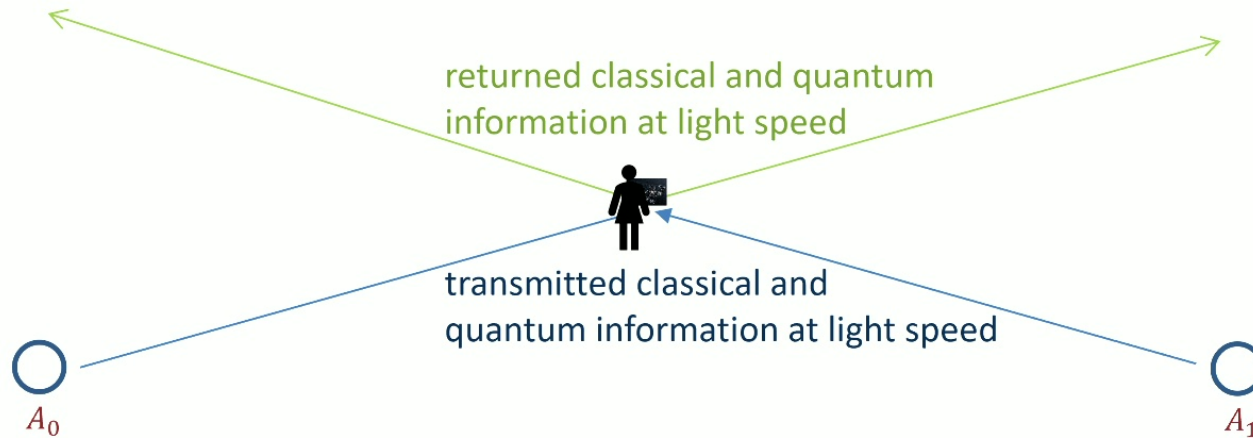


**Surely the latter!**

**The point of QPV technology is to locate and protect valuable people or objects, not to create a class of locatable devices that have no other value.**

# QPV or Tagging security models

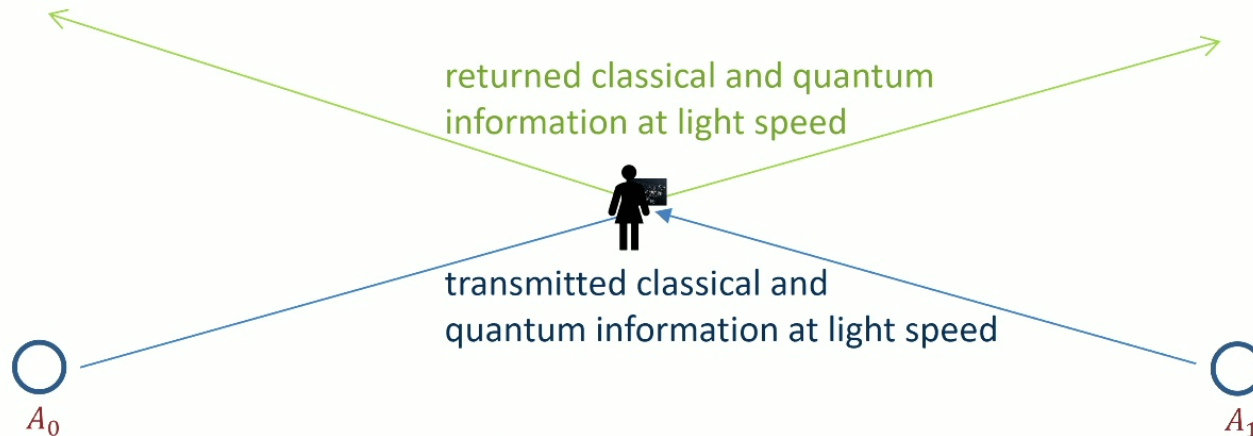
A QPV protocol should aim to verify the position of a tagged person or object



Which means it's potentially vulnerable to *separation attacks*.

# QPV or Tagging security models

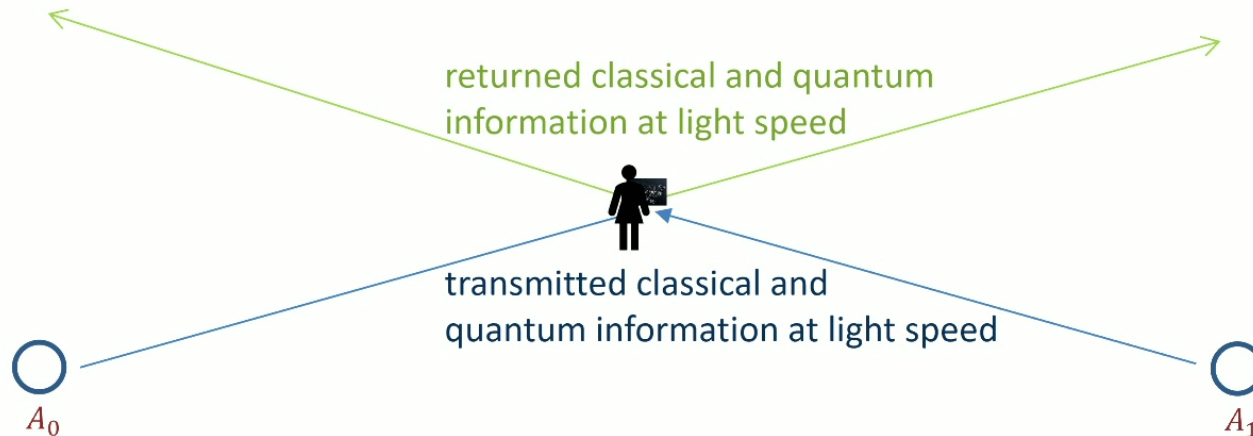
A QPV protocol should aim to verify the position of a tagged person or object



In the original QPV models of AK-Beausoleil-Munro-Spiller, Chandran et al., Buhrman et al., followed by most subsequent authors, **the device follows a public algorithm** – that's crucial for the spoofing attacks.

# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object



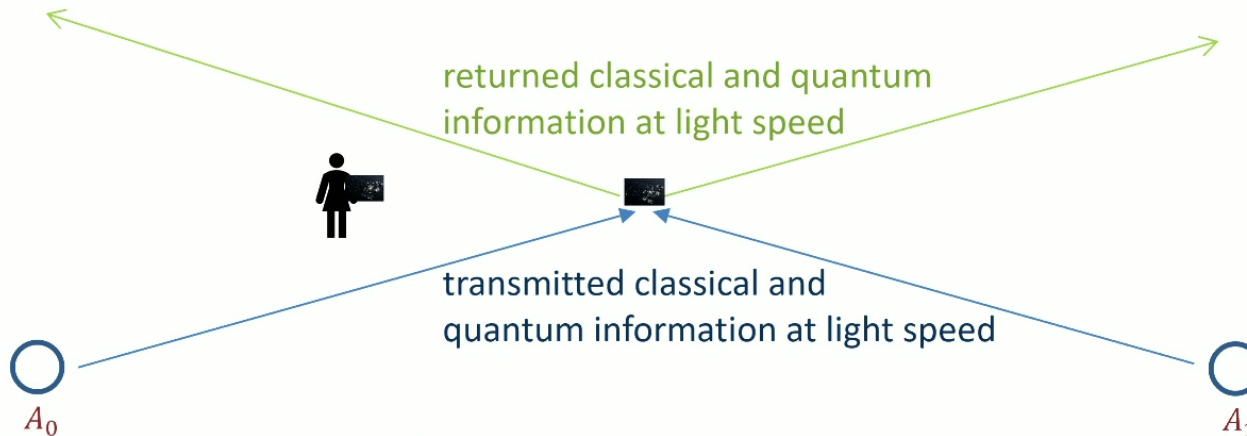
In the original QPV models of AK-Beausoleil-Munro-Spiller, Chandran et al., Buhrman et al., followed by most subsequent authors, the device follows a public algorithm – that's crucial for the spoofing attacks.

**So the device is replicable by spoofers.**



# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object



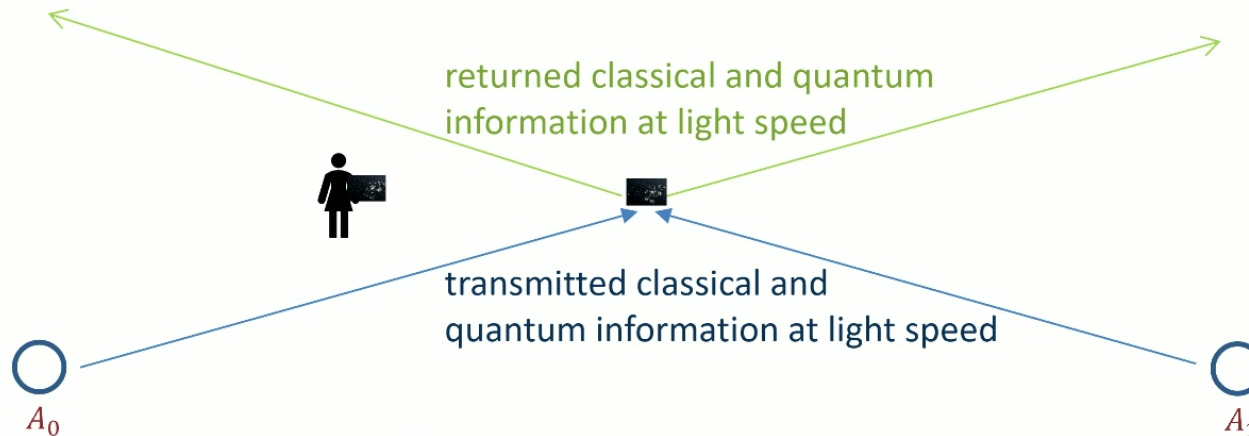
So it's replicable by spoofers.

So the schemes are also vulnerable to **dislocation and replacement attacks**.

They may guarantee\* that **a** device is at the given location, but not necessarily **the** original device. (\*given technological bounds on spoofers)

# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object



So it's replicable by spoofers.

So the schemes are also vulnerable to **dislocation and replacement attacks**.

They may guarantee that **a** device is at the given location, but not necessarily **the** original device.

# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object

It needs to defend against *separation attacks*

and *dislocation and replacement attacks*.



The term “prover” is potentially misleading here. In mathematical analyses it applies to a device. But the name suggests an agent carrying the device.

# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object

It needs to defend against *separation attacks*

and *dislocation and replacement attacks*.



The term “tag” may also be potentially misleading. It could be an integral part of a satellite or plane – separable in principle but with great difficulty.

# QPV or Tagging security models

A QPV protocol should aim to verify the position of a tagged person or object

It needs to defend against *separation attacks*

and *dislocation and replacement attacks*.



There are **no unconditionally secure defences** against these attacks.

**Security can only be based on physical assumptions:**

- the tag is hard to detach
- the tag (and/or taggee) is hard to move quickly
- detaching or moving sets off an alarm that's hard to prevent

....

# QPV or Tagging security models

There are no unconditionally secure defences against these attacks.

**Security can only be based on physical assumptions:**

- the tag is hard to detach
- the tag (and/or taggee) is hard to move quickly
- detaching or moving sets off an alarm that's hard to prevent
  
- ... and maybe that the tag is hard to replicate?

**Now, in the original security model, we can't assume the tag is hard to replicate. Its functionality is public.**

# QPV or Tagging security models

There are no unconditionally secure defences against these attacks.

**Security can only be based on physical assumptions:**

- the tag is hard to detach
- the tag (and/or taggee) is hard to move quickly
- the tag is hard to replicate?

**Now, in the original security model, we can't assume the tag is hard to replicate. Its functionality is public.**

But given that we need physical assumptions anyway, in many scenarios it's reasonable to add a standard cryptographic assumption – that the tag can keep data secure (i.e. known to verifiers, not to adversaries).

Then we can make it impossible to replicate, except with small probability.

# QPV or Tagging security models

But given that we need physical assumptions anyway, in many scenarios it's reasonable to add a standard cryptographic assumption – that the tag can keep data secure (i.e., known to verifiers, not to adversaries).

Then we can make it impossible to replicate, except with small probability.



(To be precise, there's a small probability of making an **identifiable** replica. A spoofer can make tags with all possible keys, but this isn't so helpful.)



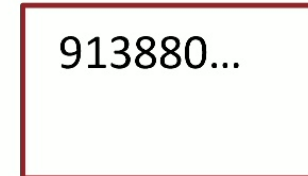
# QPV or Tagging security models

**Security can only be based on physical assumptions:**

**Security model 1:** In the original security model, we can't assume the tag is hard to replicate. Its functionality is public.



**Security model 2:** The tag can keep data secure (known to verifiers, not to adversaries).



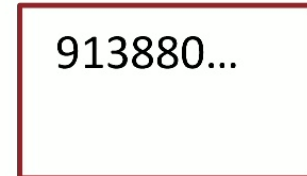
# QPV or Tagging security models

**Security can only be based on physical assumptions:**

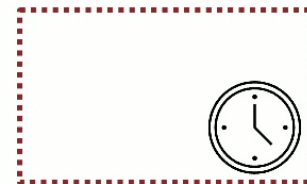
**Security model 1:** In the original security model, we can't assume the tag is hard to replicate. Its functionality is public.



**Security model 2:** The tag can keep data secure (known to verifiers, not to adversaries).



**(Security model 1C:** SM1, but the tag can contain a reliable clock, previously synchronized with verifiers' clocks.)



# QPV with tags that can keep secure data

Quantum tagging for tags containing secret classical data

Adrian Kent

Phys. Rev. A **84**, 022335 – Published 25 August 2011

**Security model 2:** The tag can keep data secure (known to verifiers, not to adversaries).

913880...

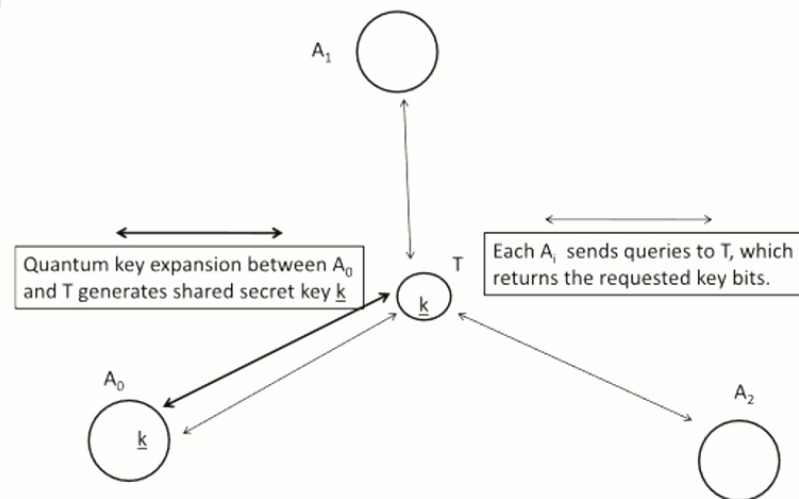


FIG. 1. One implementation of secure tagging in two dimensions. Here the key is generated by quantum key expansion between  $A_0$  and  $T$ .  $A_0$  shares the key with  $A_1$  and  $A_2$  either via secure communication based on quantum key expansion, or by transmitting relevant key bits after they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

# QPV with tags that can keep secure data

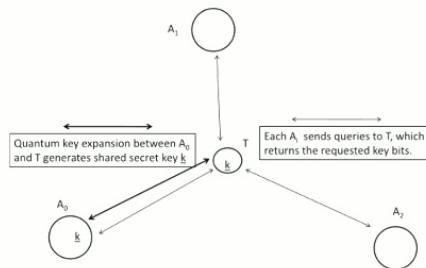


FIG. 1. One implementation of secure tagging in two dimensions. Here the key is generated by quantum key expansion between  $A_0$  and  $T$ .  $A_0$  shares the key with  $A_1$  and  $A_2$  either via secure communication based on quantum key expansion, or by transmitting relevant key bits after they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

## Before protocol:

$A_i$  shares key  $k_i = \{k_{i1}, \dots, k_{iN}\}$  with  $T$

$$k_{ij} = (q_{ij}, r_{ij}) = (\text{query}_{ij}, \text{response}_{ij})$$

## Protocol: round $j$

$A_i$  sends  $q_{ij}$  to arrive at time  $T_j$  at  $T$ 's presumed location  $L$ .

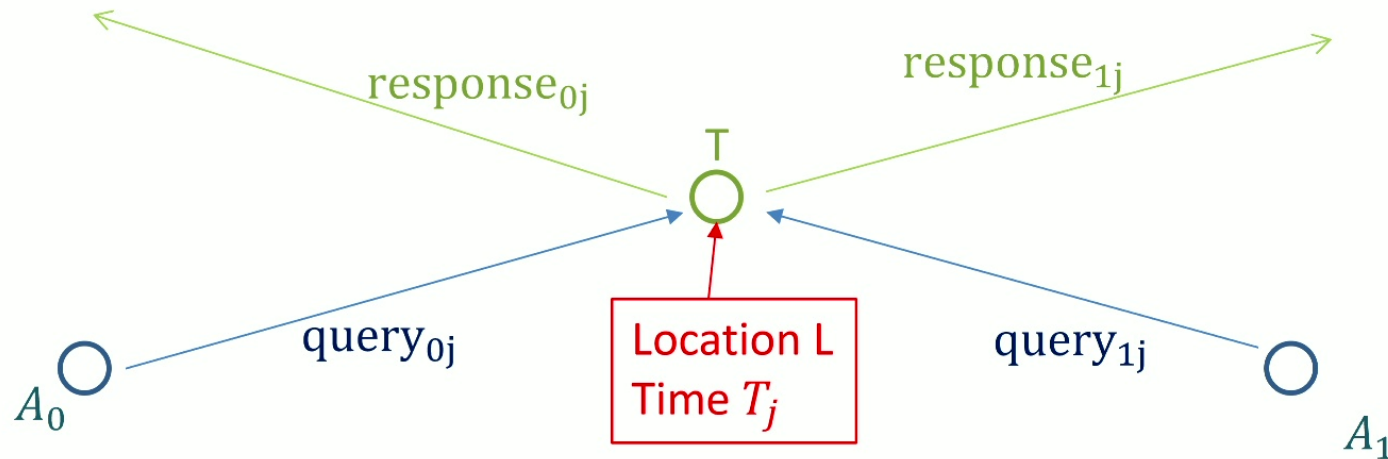
$T$  verifies  $q_{ij}$  and (iff ok) responds with  $r_{ij}$

$A_i$  verifies  $r_{ij}$

If all  $A_i$  verify, then accept  $T$  was within  $\delta$  of  $L$  at time  $T_j$ .

(This variation of AK2011 scheme and discussion from G. Cowperthwaite, AK, D. Pitalúa-Garcia, arxiv/tomorrow)

# QPV with tags that can keep secure data



## Before protocol:

$A_i$  shares key  $k_i = \{k_{i1}, \dots, k_{iN}\}$  with  $T$

$$k_{ij} = (q_{ij}, r_{ij}) = (\text{query}_{ij}, \text{response}_{ij})$$

## Protocol: round $j$

$A_i$  sends  $q_{ij}$  to arrive at time  $T_j$  at  $T$ 's presumed location  $L$ .

$T$  returns  $r_{ij}$  if  $q_{ij}$  is correct. (Or may broadcast  $r_{ij}$  if  $q_{ij}$  is correct.)

# QPV with tags that can keep secure data

**N.B. keys can be replenished if T is equipped for QKD**

**N.B. there are always timing delays and uncertainties. So  $\delta > 0$  and minimizing  $\delta$  is crucial.**

**Before protocol:**

$A_i$  shares key  $k_i = \{k_{i1}, \dots, k_{iN}\}$  with T

$$k_{ij} = (q_{ij}, r_{ij}) = (\text{query}_{ij}, \text{response}_{ij})$$

**Protocol: round j**

$A_i$  sends  $q_{ij}$  to arrive at time  $T_j$  at T's presumed location L.

T verifies  $q_{ij}$  and (iff ok) responds with  $r_{ij}$

$A_i$  verifies  $r_{ij}$

If all  $A_i$  verify, then accept T was within  $\delta$  of L at time  $T_j$ .

## QPV with tags that can keep secure data: back of envelope estimates

**All position verification comms are classical.**  
**Assume no classical errors (small error rate makes little difference).**  
**Assume comms direct free space at precisely  $c$  (best case).**

## QPV with tags that can keep secure data: back of envelope estimates

**All position verification comms are classical.**

**Assume no classical errors.**

**Assume comms direct free space at precisely  $c$  (best case).**

**Take query and response key substrings of  $\sim 30$  bits.**

**Probability of successful spoofing on each round  $\sim 10^{-9}$**

**Using state-of-the-art FPGAs, tag processing and response time  $\sim 10$ ns.**

**This gives a lower bound  $\delta \geq 3$ m for the uncertainty in tag location.**

**Suppose a verification round every  $\mu$ s.**

**Then tag can move by no more than 300m between responses  
(light speed bound).**

**For 4 verifiers, consumes  $\sim 4 \times 60 \times 10^6 \sim 2 \times 10^8$  key bits per second.**



## QPV with tags that can keep secure data: back of envelope estimates

**All position verification comms are classical.**

**Assume no classical errors.**

**Assume comms direct free space at precisely  $c$  (best case).**

**Take query and response key substrings of  $\sim 30$  bits.**

**Probability of successful spoofing on each round  $\sim 10^{-9}$**

**Using state-of-the-art FPGAs, tag processing and response time  $\sim 10$ ns.**

**This gives a lower bound  $\delta \geq 3$ m for the uncertainty in tag location.**

**Suppose a verification round every  $\mu$ s.**

**Then tag can move by no more than  $\sim 3 \times 10^{-4}$  m between responses (sound speed bound).**

**For 4 verifiers, consumes  $\sim 4 \times 60 \times 10^6 \sim 2 \times 10^8$  key bits per second.**

## QPV with tags that can keep secure data: back of envelope estimates

Take query and response key substrings of  $\sim 30$  bits.  
Probability of successful spoofing on each round  $\sim 10^{-9}$   
Using state-of-the-art FPGAs, tag processing and response time  $\sim 10$ ns.

This gives a lower bound  $\delta \geq 3$ m for the uncertainty in tag location.

Suppose a verification round every  $\mu$ s.  
Then tag can move by no more than  $\sim 300$  m between responses  
(light speed bound).

**Note that these are also (maybe even more?) challenging numbers for QPV involving QIP in the standard security model.**  
Measurement and response times  $\sim 10$ ns still give  $\delta \geq 3$ m.  
How fast can (e.g.) a photon polarization measurement be made?

## QPV with tags that can keep secure data: back of envelope estimates

Take query and response key substrings of  $\sim 30$  bits.  
Probability of successful spoofing on each round  $\sim 10^{-9}$   
Using state-of-the-art FPGAs, tag processing and response time  $\sim 10$ ns.

This gives a lower bound  $\delta \geq 3$ m for the uncertainty in tag location.

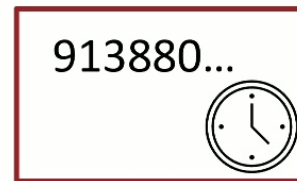
Suppose a verification round every  $\mu$ s.  
Then tag can move by no more than  $\sim 300$  m between responses  
(light speed bound).

**Note that these are also (maybe even more?) challenging numbers for QPV involving QIP in the standard security model.**  
Verification every  $\mu$ s still leaves movement of  $\sim 300$ m and replacement possible between rounds.

# QPV with tags that can keep secure data and a secure clock synchronized with verifiers' clocks

(G. Cowperthwaite, AK, D. Pitalúa-Garcia, arxiv/forthcoming)

**Security model 2C:** SM2, and the tag can contain a reliable clock, previously synchronized with verifiers' clocks.



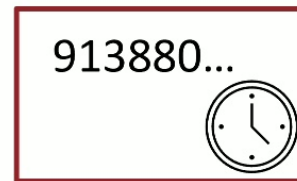
Tag releases responses to authenticated queries at pre-agreed times.

**Advantages:** • Avoids delay due to processing.

# QPV with tags that can keep secure data and a secure clock synchronized with verifiers' clocks

(G. Cowperthwaite, AK, D. Pitalúa-Garcia, arxiv/forthcoming)

**Security model 2C:** SM2, and the tag can contain a reliable clock, previously synchronized with verifiers' clocks.



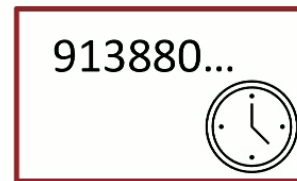
Tag releases responses to authenticated queries at pre-agreed secret times.

- Advantages:**
- Avoids delay due to processing.
  - Replaces (tag signalling time) with (uncertainty in signalling time)

# QPV with tags that can keep secure data and a secure clock synchronized with verifiers' clocks

(G. Cowperthwaite, AK, D. Pitalúa-Garcia, arxiv/forthcoming)

**Security model 2C:** SM2, and the tag can contain a reliable clock, previously synchronized with verifiers' clocks.



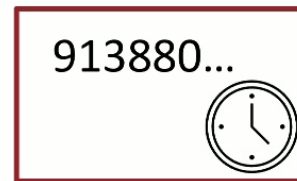
Tag releases responses to authenticated queries at pre-agreed secret times.

- Advantages:**
- Avoids delay due to processing.
  - Replaces (tag signalling time) with (uncertainty in signalling time)
  - Improves on position uncertainty  $\delta \sim 3\text{m}$ , perhaps by one or more orders of magnitude.

# QPV with tags that can keep secure data and a secure clock synchronized with verifiers' clocks

(G. Cowperthwaite, AK, D. Pitalúa-Garcia, arxiv/forthcoming)

**Security model 2C:** SM2, and the tag can contain a reliable clock, previously synchronized with verifiers' clocks.



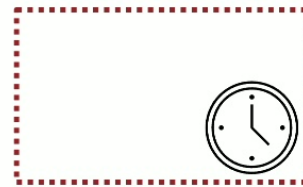
Tag releases responses to authenticated queries at pre-agreed secret times.

- Advantages:**
- Avoids delay due to processing.
  - Replaces (tag signalling time) with (uncertainty in signalling time)
  - Improves on position uncertainty  $\delta \sim 3\text{m}$ , perhaps by one or more orders of magnitude.

- Disadvantages:**
- more technological demands on tag
  - potential issues with clock desynchronization

What about tags that cannot keep secure data but have a secure clock synchronized with verifiers' clocks?

**Security model 1C:** SM1, so no secret info, but the tag can contain a reliable clock, previously synchronized with verifiers' clocks.



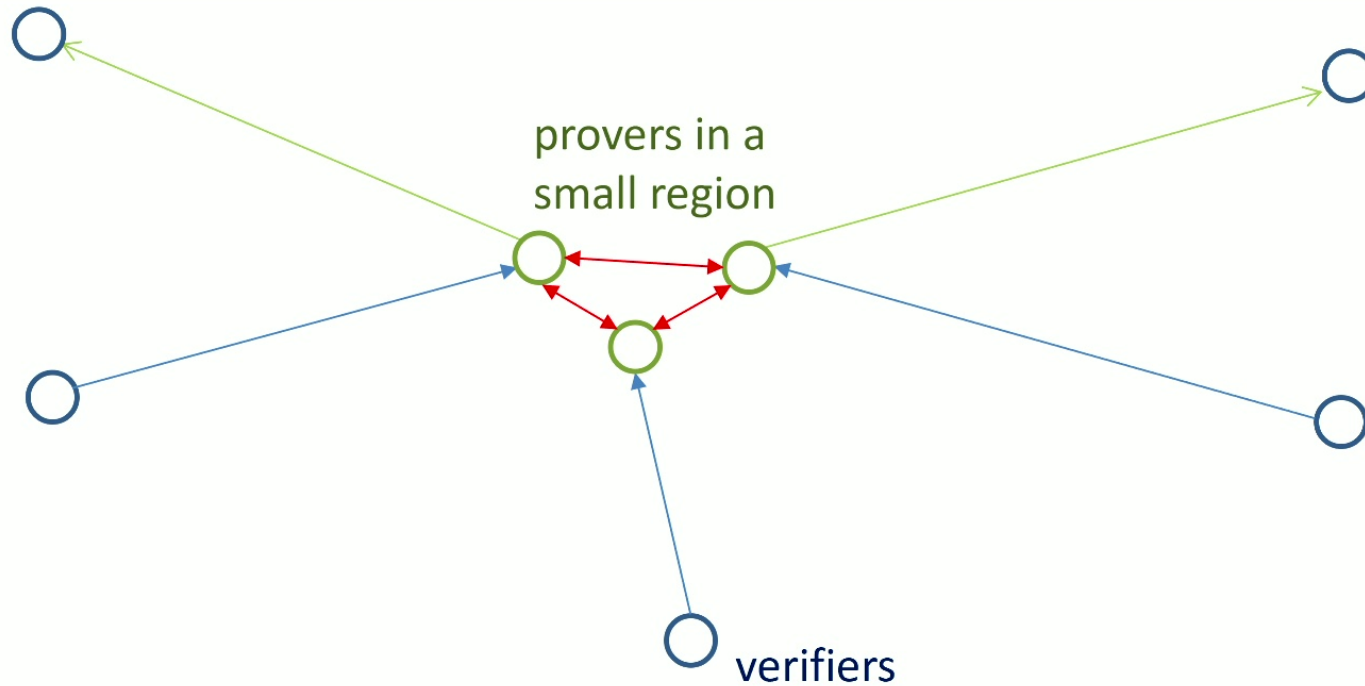
Not clear this is a useful model! If the tag can't keep data secure, then storing it to respond at later times is insecure.

This comment also applies to storing generated quantum info – so not clear there is a useful advantage in adding clocks in the standard security model.

Unless stored quantum info can be kept secure but stored classical info can't.



Consider QPV with a network of provers: i.e. a tag with internal structure and comms. Can *this* be spoofed?



# Which quantum tasks in space-time are (im)possible?

## Quantum tasks in Minkowski space

Adrian Kent<sup>1,2</sup>

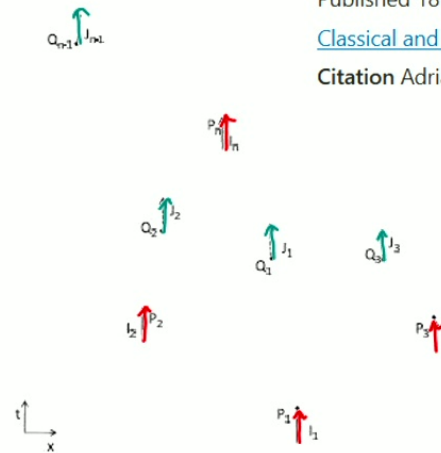
Published 18 October 2012 • © 2012 IOP Publishing Ltd

[Classical and Quantum Gravity](#), Volume 29, Number 22

Citation Adrian Kent 2012 *Class. Quantum Grav.* 29 224013

Classical and/or quantum inputs arrive at the  $P_i$

Classical and/or quantum outputs are required at the  $Q_j$   
Both the outputs and the points  $Q_j$  may depend on the inputs and the  $P_i$ .



The task is given to “Alice”, a dense network of agents in spacetime, all working together. They know the task well in advance but not the inputs.

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. from: AK, op. cit. )

**Impossible tasks:** imply restriction on information flow – cryptographically useful.

**(Surprisingly) possible tasks:** computationally useful, cryptographically threatening.

# Networks of provers *can* be spoofed: another step towards a taxonomy of possible quantum tasks in space-time

## Constraining the doability of relativistic quantum tasks

Kfir Dolev<sup>1</sup>, 

<sup>1</sup>*Stanford Institute for Theoretical Physics, Stanford University, Palo Alto, California 94305, USA*

We show within the framework of relativistic quantum tasks that the doability of any task is fully determined by what we call its “coarse causal structure”, that is the causal relation between each input point and each output point. We do this by introducing a new structure we call a spacetime circuit, with which we make rigorous the notion of a protocol. Using spacetime circuits we show that any protocol that can accomplish a given task can be modified to accomplish all tasks differing from the original by the location of input and output points, which may be changed in any way so long as the coarse causal structure of the task is maintained. Our results strengthen the no-go theorem for position based quantum cryptography to include arbitrary sending and receiving of signals by verifier agents outside the authentication region. Our results also serve as a consistency check for the holographic principle by showing that discrepancies between bulk and boundary causal structure can not cause a task to be doable in one but not the other.

arXiv:1909.05403, building on earlier work by Munro-Spiller-AK, Buhrman et al., Hayden-May, AK,....

## II. SPACETIME CIRCUITS

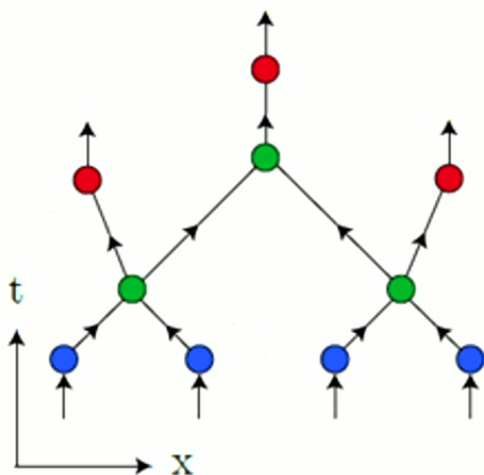


FIG. 1. A spacetime circuit. Blue, green, and red points represent input, gate, and output points respectively. The directed edges connecting the points represent the trajectory of physical systems. Dashed grey lines represent the relevant light cones of the points.

(Figure from Dolev, op. cit.)

A spacetime circuit gives a concrete way of implementing a task that takes **quantum inputs** to **quantum outputs**.

A circuit, by definition, shows the task is possible.

**Result 1.** *The possibility of the task depends only on its coarse causal structure, i.e. the causal relations between the **input** and **output** points (not also on their locations).*

**Result 2.** *If a task is possible, it's possible with no **gates**, using just predistributed entanglement and communication between **input** and **output** points.*

## II. SPACETIME CIRCUITS

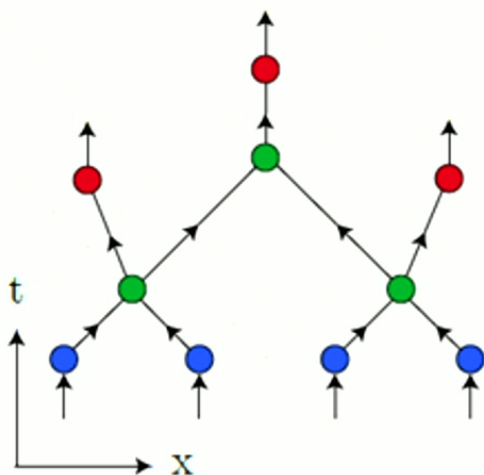


FIG. 1. A spacetime circuit. Blue, green, and red points represent input, gate, and output points respectively. The directed edges connecting the points represent the trajectory of physical systems. Dashed grey lines represent the relevant light cones of the points.

(Figure from Dolev, op. cit.)

A spacetime circuit gives a concrete way of implementing a task that takes **quantum inputs** to **quantum outputs**.

A circuit, by definition, shows the task is possible.

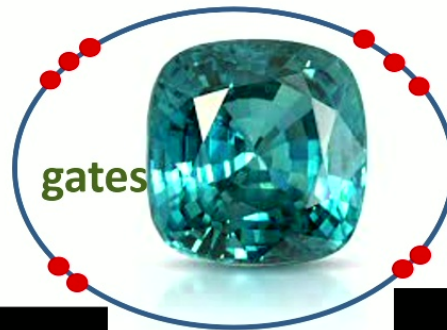
**Result 1.** *The possibility of the task depends only on its coarse causal structure, i.e. the causal relations between the **input** and **output** points (not also on their locations).*

**Result 2.** *If a task is possible, it's possible with no **gates**, using just pre-distributed entanglement and communication between **input** and **output** points.*

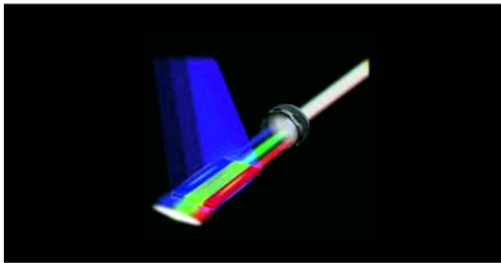
**A version of the holographic principle. Every physical system is perfectly simulable by devices on a distant enclosing surface.**



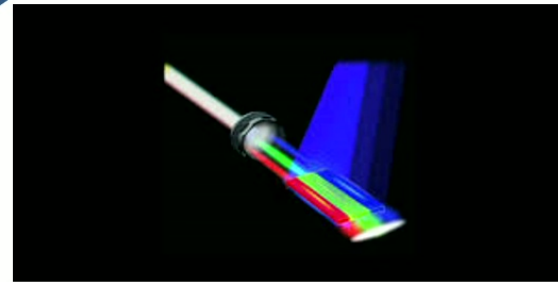
outputs



spoofing devices on boundary can simulate the crystal's responses to any probes



inputs



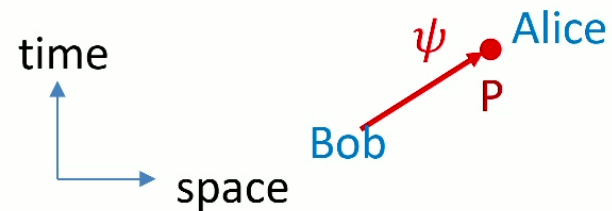
**Every physical system is perfectly simulable by devices on an enclosing surface.**

## Summoning a quantum state: another key relativistic quantum task (AK, Quantum Info. Proc. 12 1023-1032 (2013))

### A no-summoning theorem in relativistic quantum theory

[Adrian Kent](#) 

[Quantum Information Processing](#) 12, 1023–1032 (2013) | [Cite this article](#)



## Summoning a quantum state: another key relativistic quantum task (AK, Quantum Info. Proc. 12 1023-1032 (2013))

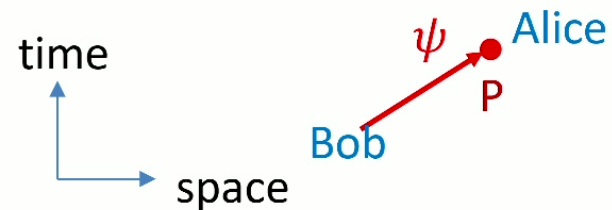
Consider two **agencies**, Alice and Bob, each with dense networks of agents in spacetime. All Alice's agents work together, so we identify them all as "Alice". Similarly "Bob".

Bob prepares a pure quantum state  $\psi \in H$   
He knows  $\psi$ ; for Alice it is a random state in  $H$ .  
He gives it to Alice at point P.



At some point Q in the causal future of P,  
he **summons** the state, i.e. asks Alice to return it.

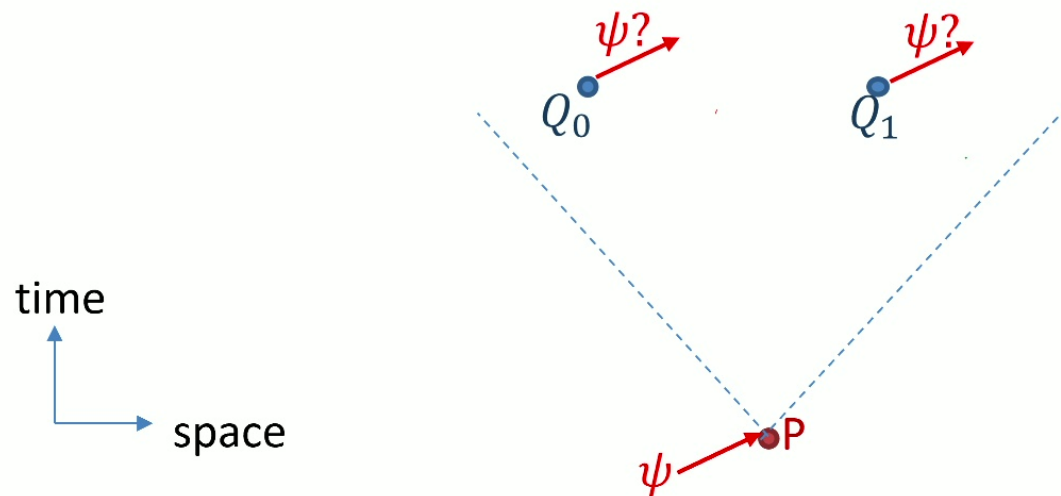
Since he knows  $\psi$ , he can (probabilistically)  
verify whether it was returned.





## The “no-summoning theorem” in relativistic quantum theory (AK, Quantum Info. Proc. 12 1023-1032(2013))

Whatever strategy Alice uses, her agent’s ability to return the state at  $Q_0$  is independent of whether or not the state is (also) requested at  $Q_1$ , and vice versa. The no-cloning theorem and no superluminal signalling principle thus imply “**no-summoning**”: she **cannot** generally comply with summonses that might arrive at one of two or more spacelike separated points.



# Summoning with separated Call and Return Points

IOP Publishing

Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. 49 (2016) 175304 (10pp)

doi:10.1088/1751-8113/49/17/175304

## Summoning information in spacetime, or where and when can a qubit be?

Patrick Hayden<sup>1,2</sup> and Alex May<sup>3</sup>

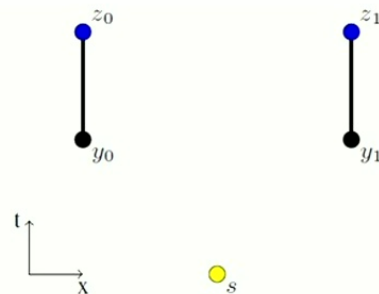
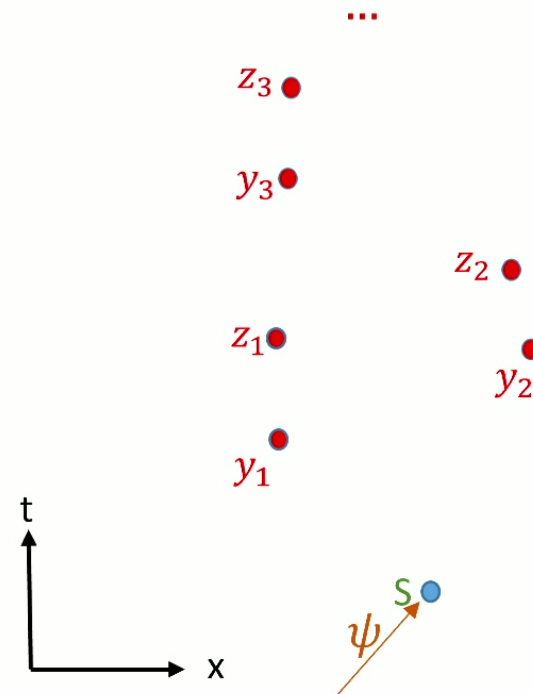


FIG. 1: Spacetime diagram of a summoning task with call and reveal points separated. The state is initially localized at  $s$  and will be called at one of  $y_0$  or  $y_1$ , in which case the state must be revealed at  $z_0$  or  $z_1$ , respectively.

Figure from  
Hayden-May  
(op. cit.)

# Hayden-May summoning tasks

- The state  $\psi$  is supplied at a source point  $s$  on the network by Bob to Alice. Bob knows  $\psi$  but Alice doesn't, so she can't copy it.
- Both parties have agents throughout the network.
- Both parties know well in advance the list of call-return point pairs  $(y_i, z_i)_{i=1}^n$ .
- At any pre-agreed call point  $y_i$  in space-time an agent of Bob's may **summon** the state – requiring Alice to return it at the return point  $z_i$ .



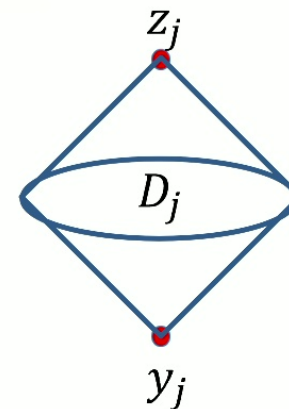
## Iterating Teleportation and Secret Sharing gives a beautiful theorem

**Theorem 1** *Summoning is possible if and only if the following conditions hold:*

1. *Every reveal point is in the future light cone of the starting point  $s$ .*
2. *For each pair  $(i, j)$ , the diamonds  $D_i$  and  $D_j$  are causally related, meaning that there exists a causal curve from  $D_i$  to  $D_j$  or vice versa.*

from Hayden-May, *op. cit.*

Define the causal diamond  $D_j$  to be the intersection of the causal future of  $y_j$  and the causal past of  $z_j$ .



## Iterating Teleportation and Secret Sharing gives a beautiful theorem

**Theorem 1** *Summoning is possible if and only if the following conditions hold:*

1. *Every reveal point is in the future light cone of the starting point  $s$ .*
2. *For each pair  $(i, j)$ , the diamonds  $D_i$  and  $D_j$  are causally related, meaning that there exists a causal curve from  $D_i$  to  $D_j$  or vice versa.*

from Hayden-May, *op. cit.*

⇐ is not at all obvious!

These are surprisingly weak conditions. They can be satisfied **even if there is no causal path** running from  $s$  through all the causal diamonds. This form of summoning is possible unless it's obviously impossible!

# A “quantum paradox of choice”

Another natural summoning problem allows **multiple calls** at  $\{y_i\}_{i \in I}$ , requiring  $\psi$  returned at **any one** corresponding  $z_i, i \in I$ . Naively, this might seem an easier task. In fact, it is strictly harder!

**Theorem (Adlam-AK):** Summoning with multiple calls is possible  $\Leftrightarrow$  the Hayden-May conditions hold **and there is a causal total ordering of the causal diamonds.**

Quantum paradox of choice: More freedom makes summoning a quantum state harder

Emily Adlam and Adrian Kent  
Phys. Rev. A **93**, 062327 – Published 21 June 2016



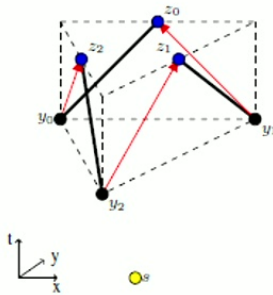
# A “quantum paradox of choice”

Another natural summoning problem allows **multiple calls** at  $\{y_i\}_{i \in I}$ , requiring  $\psi$  returned at **any one** corresponding  $z_i, i \in I$ . Naively, this might seem an easier task. In fact, it is strictly harder!

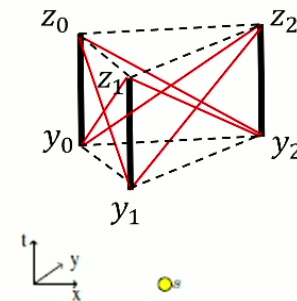
**Theorem (Adlam-AK):** Summoning with multiple calls is possible  $\Leftrightarrow$  the Hayden-May conditions hold **and there is a causal total ordering of the causal diamonds**.

This is **stronger** than the HM conditions but still **weaker** than requiring a causal path through all diamonds.

**So multi-call summoning is impossible in the previous triangular example:** causal diamonds (black lines) are pairwise causally related but there is no total causal ordering among all three.



**But multi-call summoning is possible in the example below,** although again there is no causal path through all three causal diamonds (black lines).



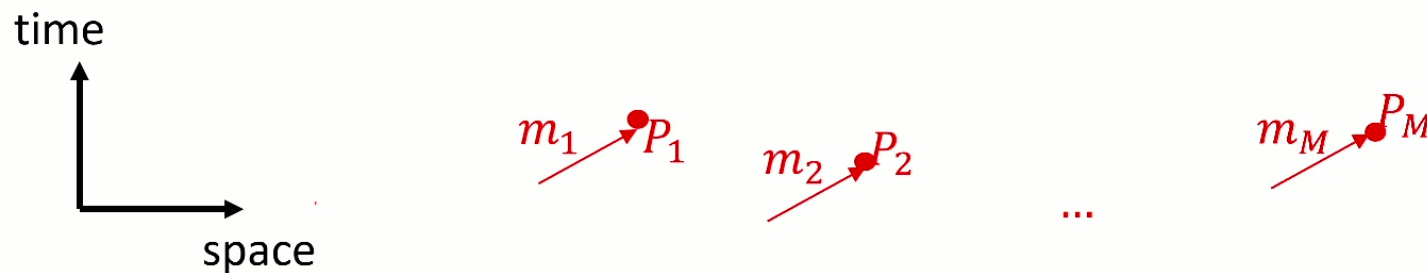
## Unconstrained summoning tasks (AK PRA 98, 062332 (2018))

Alice – represented by agents at various locations – may wish to send a quantum state to an output point depending on incoming classical data, e.g.  $m_i$  in the range  $0 \leq m_i \leq n_i$ , arriving at various spacetime points  $P_i$ .

The task is **unconstrained on the  $m_i$** : all  $\{m_1, \dots, m_n\}$  in the given ranges are possible.

She knows the form and range of the function  $Q(m_1, \dots, m_M) \in \{Q_1, \dots, Q_N\}$ .

But she does not know the  $m_i$  until they arrive at the points  $P_i$ .

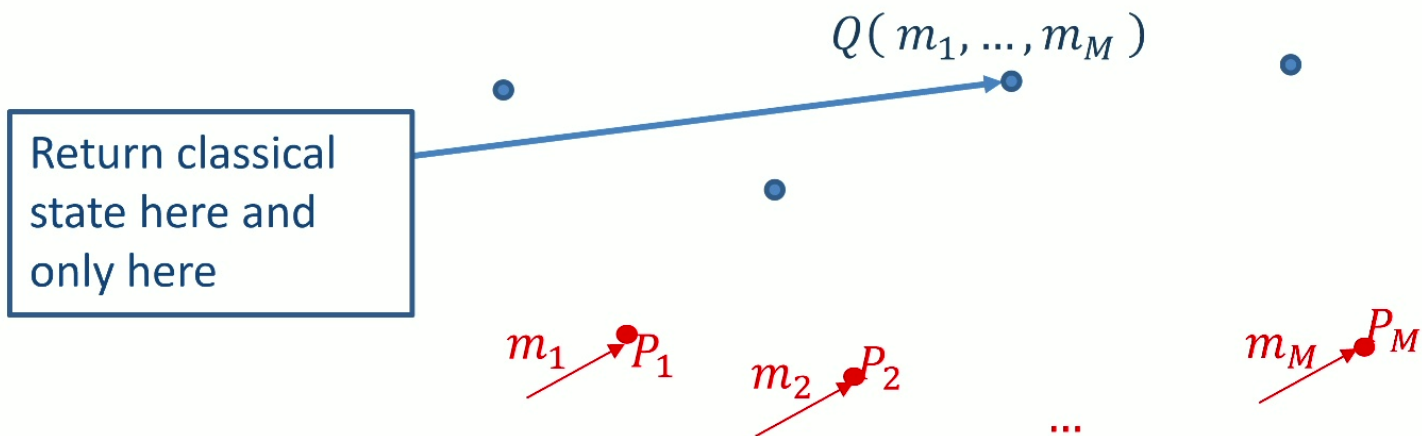




# Classical unconstrained summoning tasks

Define a classical version of a summoning task as follows: Alice is given a classical state at the start point, and can copy it and broadcast copies at up to light speed.

The task is **classically possible** if there is an algorithm that guarantees she will **return a copy at precisely one valid return point** (if there is one) and at no other point.

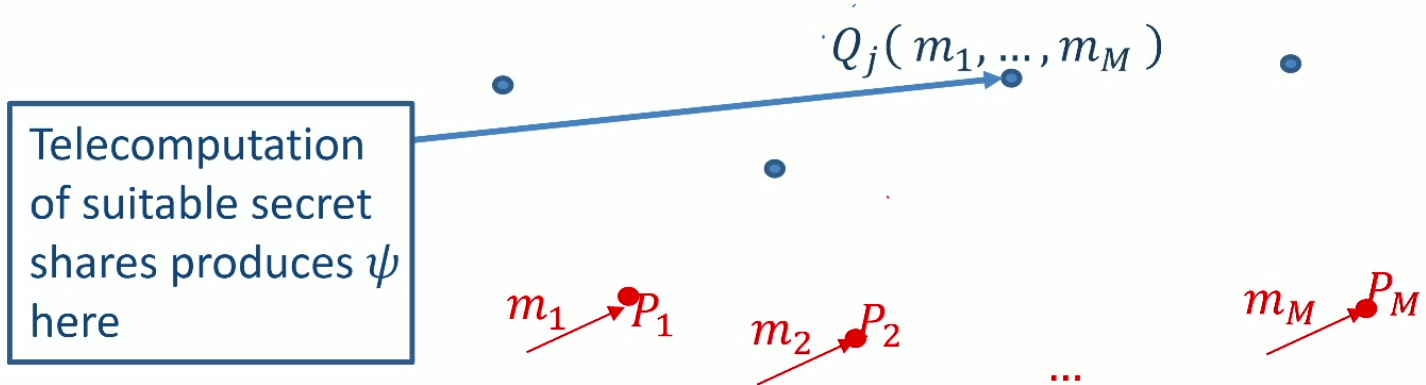


## An unconstrained summoning theorem (AK PRA 98 (2018))

**Theorem:** An unconstrained summoning task is *classically possible* if and only if it is *quantumly possible*.

**Proof:**  $\Rightarrow$  by constructive algorithm. This uses quantum secret sharing and distributed telecomputation.

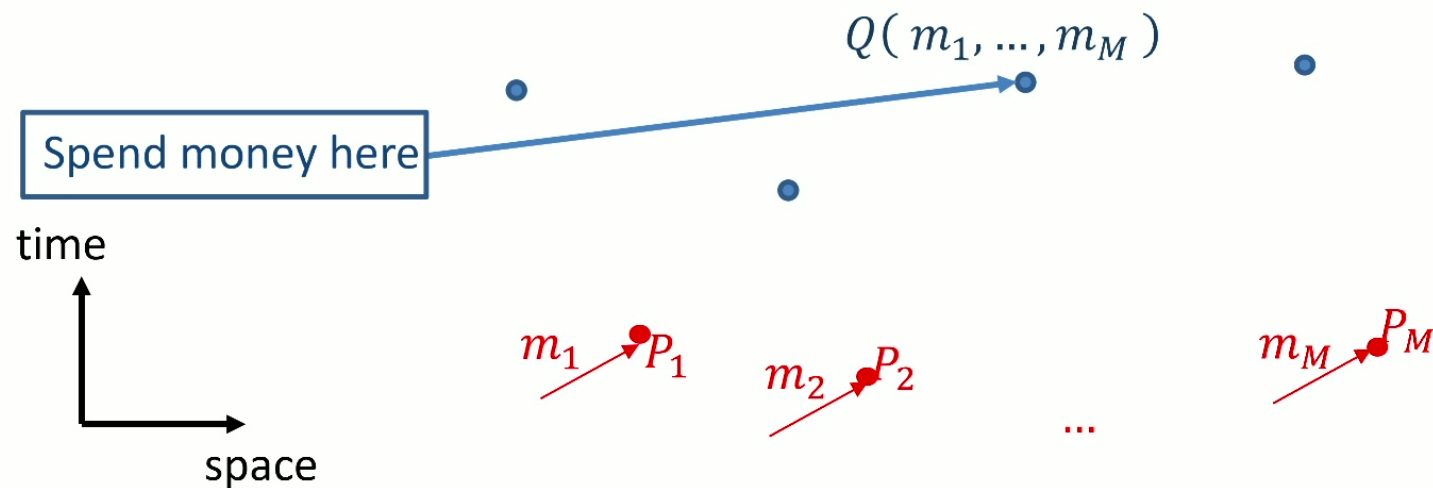
$\Leftarrow$  by an emulation argument.



## In a relativistic context: *money should be summonable*

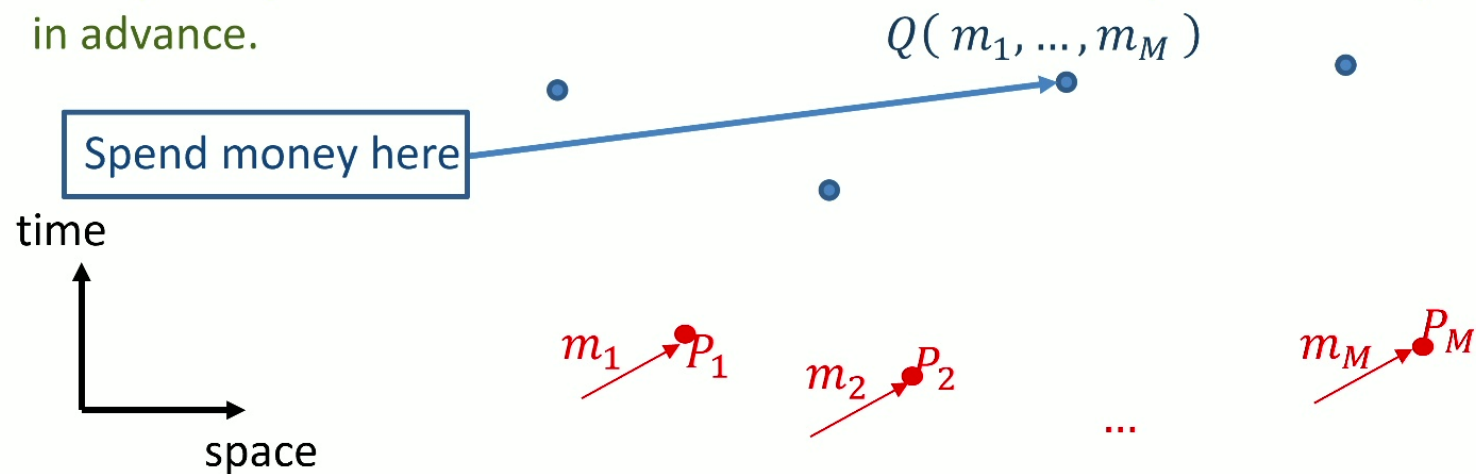
Generalized summoning tasks also define trading strategies for users with agents at nodes on a distributed network who collect incoming data across the network in order to decide when and where to make optimal trades.

Example: agencies trading on the global financial network.



## Desirable features of money on a distributed network with relativistic signalling constraints

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- **Instant verifiability:** The issuer can validate the money at the presentation point, without delays from cross-checking across the network
- **No double spending:** the issuer should be guaranteed that the money can only be validly presented at one point.
- **User privacy:** the issuer should not have info about the presentation point in advance.



## Desirable features of money on a distributed network with relativistic signalling constraints

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- **Instant verifiability:** The issuer can validate the money at the presentation point, without delays from cross-checking across the network
- **No double spending:** the issuer should be guaranteed that the money can only be validly be presented at one point.
- **User privacy:** the issuer should not have info about the presentation point in advance.

KEY POINT: RELATIVITY MOTIVATES A RECONCEPTUALISATION OF MONEY. WE REFRAME MONEY AS ANY COMBINATION OF HARDWARE AND SOFTWARE THAT GUARANTEES ALL THESE FEATURES.

MONEY THUS DEFINED IS **NOT** GENERALLY ASSOCIATED WITH ANY DEFINITE PATH THROUGH SPACE-TIME (cf. quantum state propagation).

## Desirable features of money on a distributed network with relativistic signalling constraints

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- **Instant verifiability:** The issuer can validate the money at the presentation point, without delays from cross-checking across the network
- **No double spending:** the issuer should be guaranteed that the money can only be validly be presented at one point.
- **User privacy:** the issuer should not have info about the presentation point in advance.

KEY POINT: RELATIVITY MOTIVATES A RECONCEPTUALISATION OF MONEY. WE REFRAME MONEY AS ANY COMBINATION OF HARDWARE AND SOFTWARE THAT GUARANTEES ALL THESE FEATURES.

Note that the first three features either make no sense or are trivial to ensure in a non-relativistic setting.

Wiesner's quantum money has these desiderata: *arguably its major (long unappreciated!) advantages are in relativistic contexts*

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- ✓ **Can respond to any possible quantum summoning task**
- **Instant verifiability:** The issuer should be able to validate the money at the presentation point, without delays from cross-checking.
- ✓ **Guaranteed if issuer agents pre-share the quantum money data**
- **No double spending:** the issuer should be guaranteed that the money can only be validly be presented at one point.
- ✓ **Guaranteed by no-cloning and unforgeability of quantum money**
- **User privacy:** issuer cannot tell where the user will spend the money
- ✓ **Guaranteed by secure classical and quantum communication.**



Wiesner banknote with public serial number and private quantum states (known only to bank)

Wiesner's quantum money (1983) has these desiderata: arguably its major (long unappreciated!) advantages are in relativistic contexts

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- ✓ Can respond to any possible quantum summoning task
- **Instant verifiability:** The issuer should be able to validate the money at the presentation point, without delays from cross-checking.
- ✓ Guaranteed if issuer agents pre-share the quantum money data
- **No double spending:** the issuer should be guaranteed that the money can only be validly be presented at one point.
- ✓ Guaranteed by no-cloning and unforgeability of quantum money
- **User privacy:** issuer cannot tell where the user will spend the money
- ✓ Guaranteed by secure classical and quantum communication.



**BUT** Wiesner-type quantum money requires **long term quantum state storage:** beyond current technology, likely expensive even when possible.




## “S-money” token schemes for relativistic networks

(AK: Proc. Roy. Soc. A 475 20190170 (2019))

- Schemes are defined by some pre-agreed rules that determine the valid presentation point in terms of previous local communications
- The rules may take any form, but must ensure the user *commits to data that imply only one valid presentation point*, verifiable instantly by both issuer and user
- **Short range quantum communications** allow the user privacy – the bank cannot know in advance where the token will be valid. **Privacy is guaranteed by suitable relativistic bit commitment\* protocols.**
- Schemes are practical with current technology, needing only short range QKD links and fast classical communication and computation.

S-money: virtual tokens for a relativistic economy

Adrian Kent 

Published: 08 May 2019 <https://doi.org/10.1098/rspa.2019.0170>

PROCEEDINGS OF THE ROYAL  
SOCIETY A

MATHEMATICAL, PHYSICAL AND ENGINEERING SCIENCES

Flexible quantum tokens in spacetime

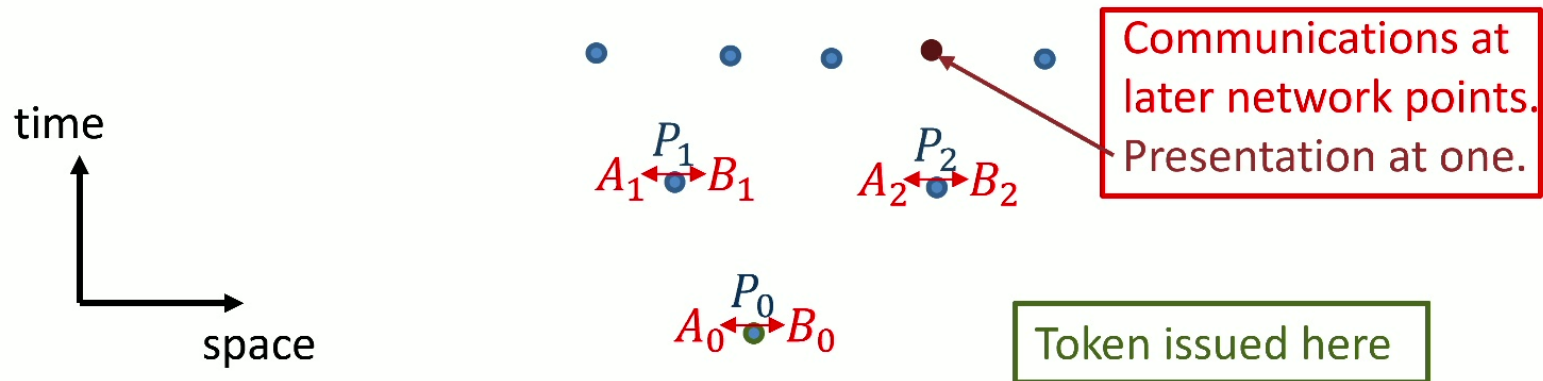
Adrian Kent and Damián Pitalúa-García

Phys. Rev. A **101**, 022309 – Published 10 February 2020

## “S-money” token schemes for relativistic networks

(AK: Proc. Roy. Soc. A 475 20190170 (2019))

- Schemes are defined by some pre-agreed rules that determine the valid presentation point in terms of previous local communications
- The rules may take any form, but must ensure the user *commits to data that imply only one valid presentation point*, verifiable instantly by both issuer and user
- **Short range quantum communications** allow the user privacy – the bank cannot know in advance where the token will be valid. **Privacy is guaranteed by suitable relativistic bit commitment\* protocols.**
- Schemes are practical with current technology, needing only short range QKD links and fast classical communication and computation.



## Every summoning task solvable by quantum money is also solvable by S-money

Recall from earlier slides:

- We define a classical version of a summoning task as follows: Alice is given a classical state at the start point, and can copy it and broadcast copies at up to light speed.
- The task is **classically possible** if there is an algorithm that guarantees she will **return a copy at precisely one valid return point** (if there is one) and at no other point.
- Unconstrained summoning theorem: an unconstrained summoning task is classically possible if and only if it is quantumly possible.
- **So, the summonability of quantum money can be emulated by classical schemes, and in particular by S-money.**

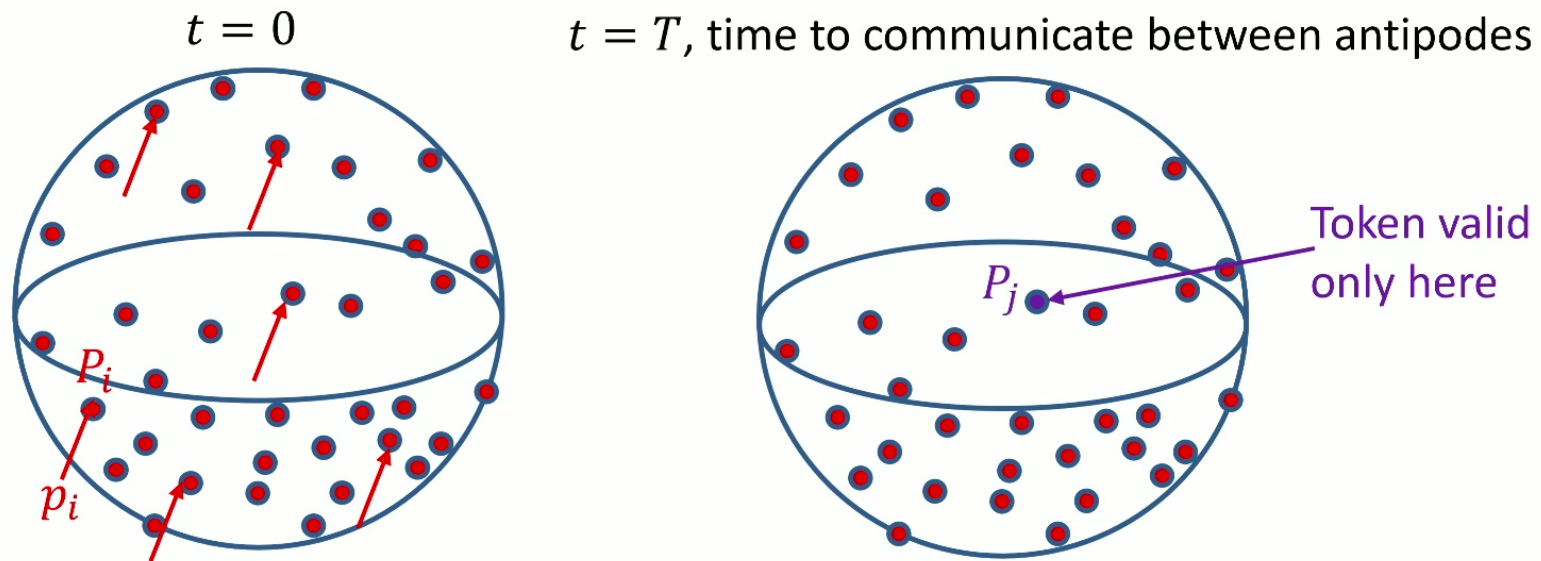
**S-money also has all the desiderata, is designed for relativistic contexts, and is practical with current technology\*.**

- **Summonability:** The user can respond as flexibly as possible to incoming data, presenting the money at the optimal space-time point
- ✓ **Can emulate quantum money and respond to any summoning task.**
- **Instant verifiability:** The issuer should be able to validate the money at the presentation point, without delays from cross-checking.
- ✓ **Guaranteed as the user's S-money token is initially generated by measurements on quantum states sent by the issuer.**
- **No double spending:** the issuer should be guaranteed that the money can only be validly be presented at one point.
- ✓ **Guaranteed by relativistic quantum bit commitments\*.**
- **User privacy:** issuer cannot tell where the user will spend the money
- ✓ **Guaranteed by relativistic quantum bit commitments\*.**

**\*No long term quantum memory required.**

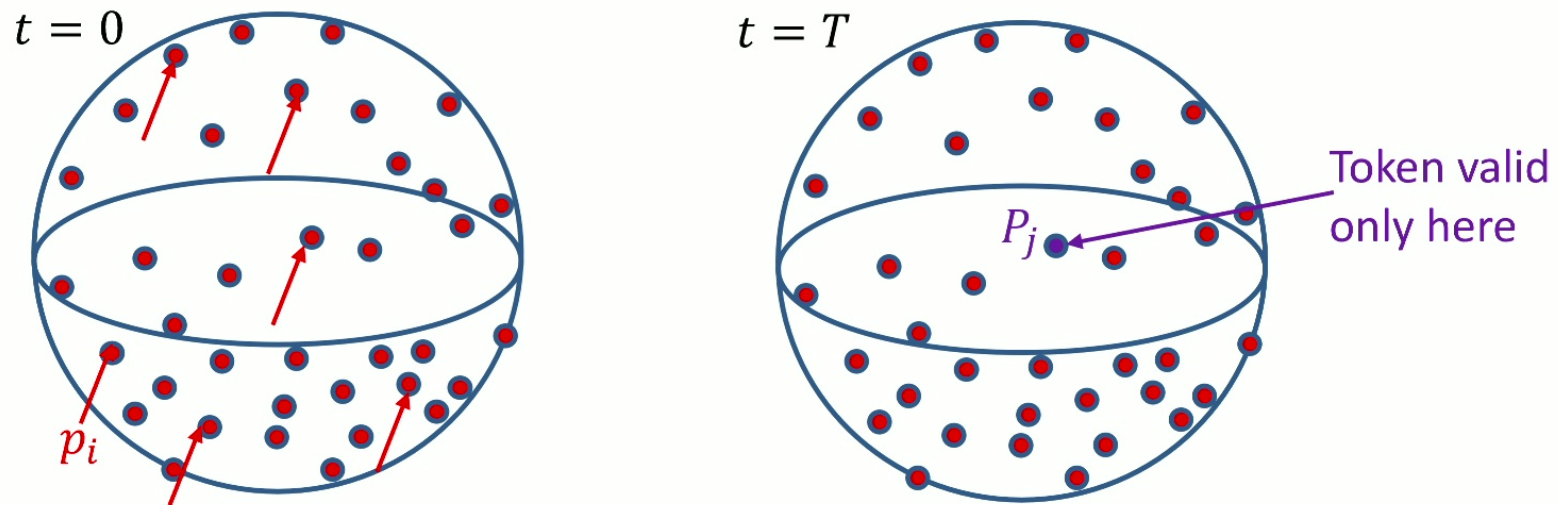
\*To be precise, the protocols are for a closely related and intrinsically relativistic task: *secure relativistic bit coordination*.

Example of a simple money summoning task: token valid at a unique maximum point. S-money solution.



A's agents  $A_i$  send **bit commitments\*** to inputs  $p_i$  (some measure of optimality for trading, private to A at this point) to B's agents  $B_i$  at each point  $P_i$  at time  $t = 0$ . Each  $A_i$  sends their **commitment data** to all  $A_j$ ; each  $B_i$  sends the **committed data** they received to all  $B_j$ . At  $t = T$ , the token is valid (only) at the point  $P_j$ , where  $p_j = \max(p_i)$ .  $A_j$  proves this to  $B_j$  by unveiling all the commitments.

Solving this task with quantum money: best known solution requires large amounts of pre-distributed entanglement



Quantum money can *in principle* also be propagated to the maximum point  $P_j$  ( $p_j = \max_i (p_i)$ ) given the  $p_i$  as input data.

There is a general algorithm using nonlocal telecomputation – but this requires **huge** quantum resources:  $O((\text{\#values of } p_i)^{\text{\#nodes in network}})$  entanglement pre-shared between network points  $P_i$ . **Open question: what is the most efficient algorithm?**

## Summary

- Practical QPV/tagging requires a security model that addresses detachment and dislocation/replacement attacks.
- A natural model includes cryptographically secure tags. This prevents replacement attacks and allows purely classical QPV protocols.
- Practical QPV/tagging with good precision is very challenging, even for protocols with purely classical query/response – but should be possible.

## Summary

- Practical QPV/tagging requires a security model that addresses detachment and dislocation/replacement attacks.
- A natural model includes cryptographically secure tags. This prevents replacement attacks and allows purely classical QPV protocols.
- Practical QPV/tagging with good precision is very challenging, even for protocols with purely classical query/response – but should be possible.
- Simulation results (KMS, Buhrman et al., Dolev) imply that QPV without cryptographically secure tags is theoretically breakable, but spoofers may (or may not?) need implausible amounts of entanglement. See later talks!
- Many other interesting questions in relativistic quantum crypto and computing -- e.g. the summonability of quantum money – turn on the resources required for quantum tasks in Minkowski space. Much to learn!