Localizing and excluding quantum information; or, how to share a quantum secret in spacetime

Patrick Hayden[1] and Alex May[2]

[1]Stanford University

[2]The University of British Columbia

October 15, 2019

When can quantum information be localized to each of a collection of spacetime regions, while also excluded from another collection of regions? We answer this question by defining and analyzing the localize-exclude task, in which a quantum system must be localized to a collection of authorized regions while also being excluded from a set of unauthorized regions. This task is a spacetime analogue of quantum secret sharing, with authorized and unauthorized regions replacing authorized and unauthorized sets of parties. Our analysis yields the first quantum secret sharing scheme for arbitrary access structures for which the number of qubits required scales polynomially with the number of authorized sets. We also study a second related task called state-assembly, in which shares of a quantum system are requested at sets of spacetime points. We fully characterize the conditions under which both the localize-exclude and state-assembly tasks can be achieved, and give explicit protocols. Finally, we propose a cryptographic application of these tasks which we call party-independent transfer.

Patrick Hayden: phayden@stanford.edu

Alex May: may@phas.ubc.ca

Contents

1 Introduction **2**

2 Localizing and excluding quantum information **4**
2.1 Localizing quantum information to many regions 4
2.2 Localizing and excluding quantum information 10

3 State-assembly **19**
3.1 State-assembly with authorized regions 19
3.2 State-assembly with authorized and unauthorized regions 23

4 An application: party-independent transfer **24**

5 Discussion **29**

6 Acknowledgements **31**

A Summoning, state-assembly and localization **31**

B Many-call single-return summoning **35**

1 Introduction

The study of the interplay between quantum theory and relativity has recently begun a new chapter with the consideration of quantum information tasks in a Minkowski space background [1, 2, 3]. For instance, the study of information causality [4] and of causal operators [5] has given further insight into ties between information processing and relativity. Along with other results in this area [6, 7, 8, 9], these can be placed into the general framework of quantum tasks in Minkowski space [10].

One task of particular interest is *summoning*, defined by Kent [11], where the associated no-summoning theorem is a statement of no-cloning appropriate to the spacetime setting. We have also argued that a generalization of the summoning task [6] provides an operational framework within which to study how quantum information can move through spacetime. The importance of having such a framework is highlighted by recent subtle questions concerning spacetime structure and the no-cloning principle in the context of black holes [12, 13]. Understanding how a quantum system may be delocalized in Minkowski space should be a useful step towards understanding such fundamental puzzles.

The study of quantum tasks in Minkowski space has been given a second motivation with the discovery of cryptographic protocols that exploit the properties of either or both of quantum mechanics and special relativity. Bit-commitment is a well-known example [14, 15]; other examples include coin flipping [16], key distribution (where signalling constraints enter into some security proofs [17, 18]), and two spacetime analogues

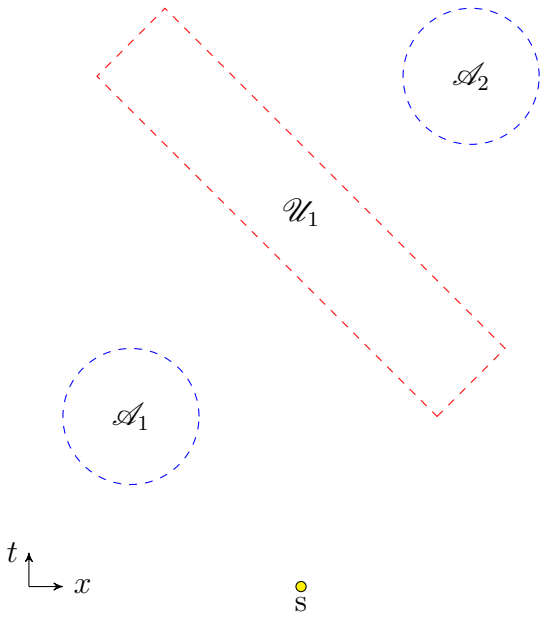

Figure 1: An example of a localize-exclude task. A single copy of an unknown quantum system is initially localized near the spacetime point s, and needs to be localized to within regions $\mathscr{A}_1$ and $\mathscr{A}_2$, while avoiding region $\mathscr{U}_1$. Theorem 8 shows that this is possible to do.

of oblivious transfer dubbed location-oblivious transfer [19] and spacetime-constrained oblivious transfer [20].

In quantum secret sharing, a central result of quantum cryptography, a quantum system is distributed among many parties such that only certain subsets of parties may collectively use their shares to reconstruct the system. Other subsets of parties are required to not be able to learn any information about the secret from their shares. In the context of quantum tasks in Minkowski space, where the movement of information in spacetime is central, and in the context of relativistic quantum cryptography, it is natural to consider a spacetime generalization of quantum secret sharing.

To do this we replace the notions of authorized and unauthorized sets of parties with authorized and unauthorized spacetime regions. We define the localize-exclude task, where the goal is to move a quantum system through spacetime in such a way that it is localized to each of the authorized regions and excluded from the unauthorized ones. Figure 1 gives a simple example. In theorem 8, we find necessary and sufficient conditions for completing the localize-exclude task. To argue that the localize-exclude task is a natural spacetime generalization of secret sharing, we show in the main text that there is a simple construction that embeds any quantum secret sharing scheme as a localize-exclude task, and that the conditions of this theorem reduce to those for quantum secret sharing in that case.

In the summoning task one party, Bob, puts in requests for the quantum system at certain spacetime points, asking that the system be returned at one of another set of points. The localize-exclude task removes this structure, but adds a notion of unautho-

rized region. It is interesting to also consider a task in the request-return setting, but which includes unauthorized regions. In this *state-assembly* task, we consider many parties Bob_i who may each request a share of the quantum system at an associated spacetime region D_i. Alice should respond to the collection of requests given by the Bobs in a careful way: she should hand over a collection of shares sufficient to construct a single copy of the system when the collection of requests is authorized, and she should not reveal any information about the system when that collection is unauthorized. The conditions for Alice to complete this task are the same as for localize-exclude in the case of causally separated regions, but differ when non-trivial causal structures are considered. In theorem 13 below we precisely characterize the conditions under which this task can be completed, and describe an explicit protocol for completing it when it is possible.

Together the state-assembly and localize-exclude tasks provide a rich set of scenarios to consider. We suggest *party-independent transfer* as a potential cryptographic application of this framework, a task where two other parties wish to receive information from Alice and want the information they receive to be both private and independent of their identity. We propose a protocol for completing this task which is built on the state-assembly task. Establishing the security of this protocol we leave to future work.

The layout of this paper is as follows. Section 2 gives the necessary definitions to study localization to arbitrary spacetime regions and proves theorem 8, which characterizes the localize-exclude task. We discuss the relation between localize-exclude and quantum secret sharing in the same section. In section 3 we discuss state-assembly and give its characterization. In section 4 we study the party-independent transfer task. Two appendices are included which clarify the relationship of this work to earlier work on summoning. The first shows that state-assembly is equivalent to a certain summoning task, and the second addresses the points raised by Adlam and Kent [7] against interpreting summoning tasks in terms of the localization of information.

2 Localizing and excluding quantum information

2.1 Localizing quantum information to many regions

As a first step towards characterizing the localize-exclude task we discuss the problem of localizing quantum information to a collection of spacetime regions, leaving excluded regions to the next section. To do this we consider the following setting. Alice holds the A subsystem of a pure state $|\Psi\rangle_{RA}$, with A recorded into a collection of classical and quantum systems held within secure laboratories not accessible to her adversary, Bob[1]. We would like to ask where system A is. For instance, Alice might have recorded A into an error-correcting code and distributed the shares of this code to various laboratories.

[1]Alice and Bob are both agencies, who have many agents that may be distributed to many different laboratories.

Further, she might be constantly rerouting these shares between labs, so that shares are held only at certain labs between specified times.

We can ask where the subsystem is in spacetime by temporarily relaxing the security of Alice's labs — we give Bob access to some collection of Alice's labs for certain time intervals. If by accessing these labs Bob is able to prepare the A system (potentially making use of later data processing), we say that system A was localized to the collection of labs and intervals of time Bob accessed. More generally, we can abstract away from the language of labs and time intervals and give a more general definition.

Definition 1 *Suppose one party, Alice, holds system A of a quantum state $|\Psi\rangle_{AR}$. Then we say the subsystem A is **localized** to a spacetime region Σ if a second party, Bob, for whom the state is initially unknown is able to prepare the A system by collecting quantum and classical systems from within Σ, and then applying later data processing.*

Conversely, if Bob is unable to learn anything about A we say the system is ***excluded*** from Σ. Note that the later data processing referred to in the definition may occur outside of the region Σ. Further, a system may be neither localized nor excluded from a region if partial information about the system is available there.

To be more precise we should specify how it is verified that Bob holds the A system after he has accessed Σ. One natural possibility is to introduce a third party, call him Charlie, who plays the role of a referee. We have Charlie hold both the purifying system R of $|\Psi\rangle_{AR}$ as well as a classical description $|\Psi\rangle_{AR}$. To verify Bob holds the system then, we have Bob pass the A system to Charlie, who performs a projective measurement of the AR system in a basis that includes $|\Psi\rangle_{AR}$. If Alice can pass Charlie's test with certainty, we declare that Alice localized the system to Σ. Of course, Alice will also pass this test with some probability so long as Charlie's final state has non-trivial overlap with $|\Psi\rangle_{AR}$[2].

It is interesting to compare this notion of localizing a quantum system to a spacetime region to a notion of spacetime localization based on the summoning task [6]. Perhaps the key distinction is that, in the definition given here, information processing may occur outside the spacetime region in order to prepare the system. This point carries with it certain subtleties that are taken up in appendix A and the discussion. The key advantage of definition 1 however is its applicability to regions of arbitrary shape.

One strategy for hiding a quantum system from Bob would be for Alice to send A into a region Σ, while also sending various decoys $A_{d1}, A_{d2}, ...$ so that Bob, though he may collect all of the systems $A, A_{d1}, A_{d2}, ...$ is left unsure as to which system to hand to Charlie. This reveals a finer point to definition 1: the system Bob is searching for may enter Σ, but if appropriate classical instructions do not also enter Σ (in this case

[2]In the context of the localize-exclude tasks we consider later, we may be interested in whether or not a quantum system can be localized to two or more regions with fixed relative positions, rather than if a system can be localized to one particular spacetime region. In this case, and when the spacetime is suitably translation invariant, one can consider repeating the task many times (sequentially or in parallel). In this scenario Charlie could determine with what probability Alice is able to complete the task.

a label denoting which system actually holds A), then definition 1 says the system is not localized there. To avoid confusion around this point we will always have Alice, at some early time, reveal the classical instructions that constitute her protocol to Bob. The only information Alice will not broadcast is a classical string k (as well as the quantum system itself). As we will see, protocols where Alice holds only a secret key k and reveals all other details to Bob are sufficient to complete any physically possible localize-exclude task, so this restriction on Alice amounts to a useful simplification of notation and language.

In the protocols we construct Alice will encode her quantum system into an error-correcting code that corrects erasure errors, and then apply a quantum one-time pad to each of the shares in the quantum code. Alice does not broadcast the classical strings used in the one-time pads; taken together these constitute her secret key k. However, she does reveal her procedure for putting A into an error-correcting code and applying the one-time pad, and reveals the spacetime trajectories of each share in the code. Within this context, Bob reconstructs A by accessing a region Σ whenever a correctable subset of shares in the error-correcting code along with their corresponding classical keys from the the one-time pad pass through Σ.

Definition 1 specifies what is meant by a quantum system being localized to a single spacetime region. To extend this to multiple regions, we define the localize task as follows.

Definition 2 *A **localize task** is a task involving two agencies, Alice and Bob, specified by a tuple $\{A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}\}$, consisting of:*

- *A quantum system A. In general A may be a subsystem of some overall pure state $|\Psi\rangle_{AR}$. The state on AR is unknown to both Alice and Bob.*
- *A start point s, at which Alice initially holds system A*
- *A collection of spacetime regions $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$, which we call the authorized regions*

Alice successfully completes the task if Bob is able to prepare system A after he accesses any one of the $\mathscr{A}_i$.

If Alice is able to successfully complete the localize task with regions $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ we say she has localized the system to each of those regions. The authorized regions may be of arbitrary shape and may overlap.

To analyze this task it is useful to introduce some language. We give the following definition which specifies a relation between pairs of spacetime regions.

Definition 3 *Two spacetime regions Σ_i and Σ_j are said to be **causally connected** if there is a point q_i in Σ_i and q_j in Σ_j such that there is a causal curve from q_i to q_j, or from q_j to q_i.*

We illustrate this definition in figure 2a. If two regions are not causally connected we say they are **causally disjoint**. In the context of the localize-exclude task discussed in the next section we will also need one further definition relating to spacetime geometry.

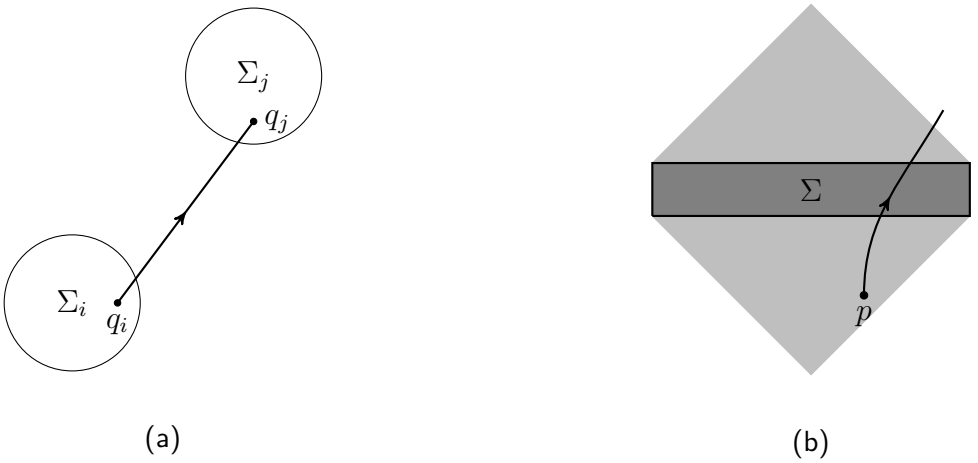

Figure 2: Two geometric notions used in the text. a) Two causally connected regions. Two spacetime regions Σ_i and Σ_j are said to be causally connected if there is a point q_i in Σ_i and q_j in Σ_j such that there is a causal curve from q_i to q_j, or from q_j to q_i. b) The domain of dependence (light grey) of a spacetime region Σ (dark grey). The domain of dependence is defined as the set of all points p in the spacetime such that all causal curves passing through p must also enter Σ.

Definition 4 *The **domain of dependence** of a spacetime region Σ, denoted $D(\Sigma)$, is the set of all points p such that every causal curve through p must also enter Σ.*

This definition is illustrated in figure 2b.

As a first step towards the more general scenario consider the localization of a quantum system to two authorized regions $\mathscr{A}_1$ and $\mathscr{A}_2$.

Theorem 5 *Given a quantum system initially localized near a spacetime point s, the system may be localized to both of the spacetime regions $\mathscr{A}_1$ and $\mathscr{A}_2$ if and only if the following two conditions hold.*

i. $\mathscr{A}_1$ and $\mathscr{A}_2$ both have a point in the future light cone of s.

ii. $\mathscr{A}_1$ and $\mathscr{A}_2$ are causally connected.

Proof. First, note that if an authorized region is entirely outside the future light cone of the start point then successfully localizing the system to that region would constitute superluminal communication. Thus, the first condition is necessary. To see necessity of the second condition suppose there exists a protocol for localizing a quantum system to two causally disjoint regions $\mathscr{A}_1$ and $\mathscr{A}_2$. Then by definition it is possible to construct the system by accessing the region $\mathscr{A}_1$, and by accessing $\mathscr{A}_2$. By causality however accessing region $\mathscr{A}_1$ cannot affect the system constructed from $\mathscr{A}_2$, and vice versa, so it would be possible to construct two copies of the quantum system. But this constitutes cloning, so no such protocol can exist.

To understand sufficiency we construct a task with the minimal properties specified by the two assumed conditions. Such a task is shown in figure 3. There, a point $p_1 \in \mathscr{A}_1$

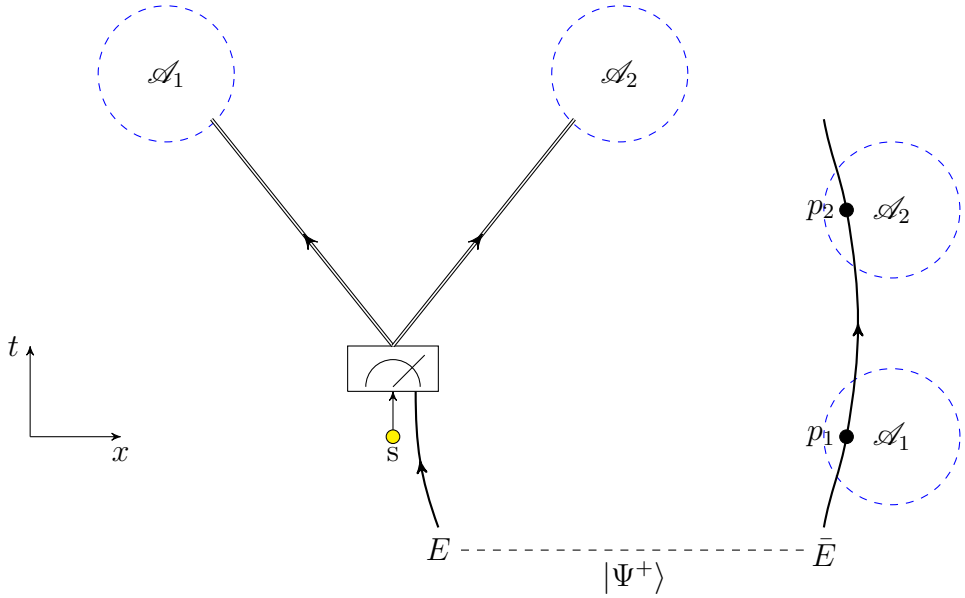

Figure 3: An arrangement of two authorized regions that has the minimal requirements to satisfy the conditions of theorem 5. By the first condition $\mathscr{A}_1$ and $\mathscr{A}_2$ are causally connected. This guarantees the existence of a point p_1 in $\mathscr{A}_1$ which is in the causal future of some point p_2 in $\mathscr{A}_2$ (up to relabelling). The second condition gives that each region have at least one point in the future light cone of s. However, the regions $\mathscr{A}_1$ and $\mathscr{A}_2$ may be disconnected (as shown here) and so satisfy this requirement while having the points p_1, p_2 be outside the future light cone of s. To localize a system A to both regions a maximally entangled state $|\Psi^+\rangle_{E\bar{E}}$ is shared between s and p_1. Near to s the A system is teleported using this entanglement, and the entangled system at p_1 is sent to p_2. Meanwhile, the classical measurement outcomes from the teleportation protocol are sent to the points in $\mathscr{A}_1$ and $\mathscr{A}_2$ which are in the causal future of s. Each region has both the classical measurement outcomes and the entangled particle pass through it, so the A system is localized to each.

is causally connected to $p_2 \in \mathscr{A}_2$, and each of $\mathscr{A}_1$ and $\mathscr{A}_2$ have a point in the future light cone of s. However, p_1 and p_2 sit outside the future light cone of s. Nonetheless it is straightforward to complete such a task. To do so a system E is maximally entangled with $\bar{E}$, then E is brought to s while $\bar{E}$ is brought to p_1. At s, E is used to teleport the A system onto the $\bar{E}$ system. The measurement outcome from the teleportation is sent to $\mathscr{A}_1$ and $\mathscr{A}_2$ from s. Meanwhile, $\bar{E}$ is sent from p_1 to p_2. Each authorized region contains the classical measurement outcome and the system $\bar{E}$, so accessing either region allows reconstruction of A. ■

We can now move on to understanding localize tasks with arbitrary numbers of authorized regions. We find in particular that it is only the structure of causal connections between pairs of regions and the start point that are needed to characterize a task as possible or impossible.

Theorem 6 *Given a quantum system A initially localized near a spacetime point s, the system may be localized to each spacetime region $\mathscr{A}_i$ in a collection $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ if and only if the following two conditions hold.*

i. Each region $\mathscr{A}_i$ has at least one point in the causal future of s

ii. Each pair of regions $(\mathscr{A}_i, \mathscr{A}_j)$ is causally connected.

Proof. Necessity of the two conditions follows from the same arguments as in the two region case given as theorem 5: localizing a system to a region outside of its future light cone violates no signaling, and localizing a system to two spacelike separated regions would allow two copies of the system to be produced.

To demonstrate sufficiency we construct an explicit protocol for completing any task satisfying the two conditions. To this end it is useful to introduce a directed graph G which describes the causal structure of the task: for each authorized region $\mathscr{A}_i$ introduce a vertex, also labelled $\mathscr{A}_i$, to the graph. For each pair of regions $(\mathscr{A}_i, \mathscr{A}_j)$ such that there is a point in $\mathscr{A}_j$ connected by a causal curve to a point in $\mathscr{A}_i$ introduce a directed edge $(\mathscr{A}_i \to \mathscr{A}_j)$. An example of a task and its associated graph is given as figure 4.

From the no-cloning theorem it follows that some quantum information must be shared between every pair of authorized regions. In our construction these quantum systems that move between pairs of authorized regions form the shares of an error-correcting code. In particular, for each edge in the graph G we associate one share. In theorem 5 and figure 3 we showed how to localize a quantum system to two authorized regions whenever they share a causal connection. We can execute this protocol on the shares of our error-correcting code to ensure the share associated to edge $\mathscr{A}_i \to \mathscr{A}_j$ is localized to both $\mathscr{A}_i$ and $\mathscr{A}_j$. To complete the task then, our error-correcting code should have the property that, given any vertex, the set of shares associated to the edges attached to that vertex are sufficient to construct the initial system A. We illustrate the requirement on this code in figure 5.

In fact, given that every pair of vertices in this graph share an edge, which is guaranteed by condition (ii), such error-correcting codes have already been constructed.

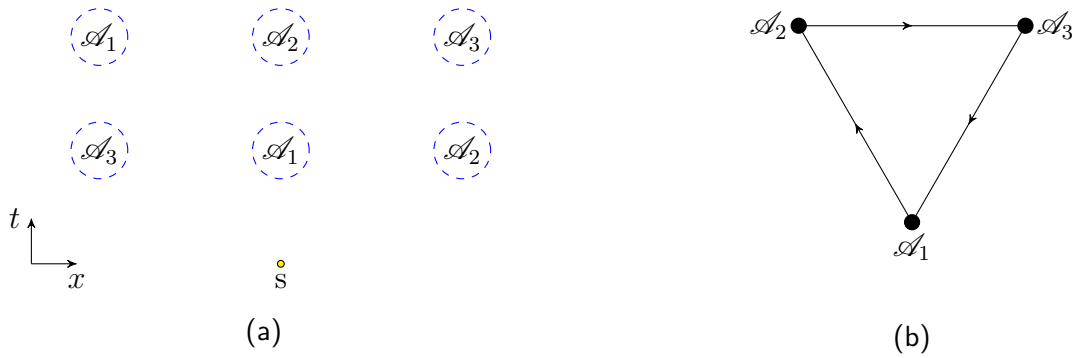

Figure 4: An example of a task with three authorized regions $\mathscr{A}_1, \mathscr{A}_2$ and $\mathscr{A}_3$. (a) The arrangement of the regions in spacetime, notice that each region consists of two disconnected ball-shaped regions. (b) The corresponding graph of causal connections, used in the proof of theorem 6 to construct the error-correcting code needed to complete the task.

To encode finite-dimensional quantum systems we constructed such codes using the codeword-stabilized formalism in the context of a similar summoning problem [6]. Constructions for continuous variable systems have also been given [8] and then adapted to the finite-dimensional case [21]. In the code-word stabilized construction a single logical qubit is recorded using 2 physical qubits for each edge in the graph, resulting in a total of $2\binom{n}{2}$ physical qubits for n the number of authorized regions. ■

This result is particularly simple and expected from earlier work on summoning. Indeed, the conditions for summoning to a collection of diamonds are the same as for localizing to a collection of authorized regions (see [6], or appendix A).

2.2 Localizing and excluding quantum information

Now that we have an understanding of when and how a quantum system can be localized to many spacetime regions, we can approach the localize-exclude task. This task includes a notion of unauthorized region, a region in spacetime from which the system must be excluded in the sense described in the last section. Further, we will require that accessing an unauthorized region reveals no information about the quantum system. We collect these ideas into the following definition.

Definition 7 *A **localize-exclude task** involves two agencies, Alice and Bob, and is specified by a tuple* $\{A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\}\}$*, consisting of:*

i. A quantum system A*. In general* A *may be a subsystem of some overall pure state* $|\Psi\rangle_{AR}$*. The state on* AR *is unknown to both Alice and Bob.*

ii. A start point s*, at which Alice initially holds system* A

iii. A collection of spacetime regions $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$*, which we call the authorized regions*

Figure 5: Illustration of the functioning of the error-correcting code used in theorem 6. a) A directed graph that describes the causal connections between the authorized regions of a localize task. In this case the task involves four authorized regions. b) To complete the task, we employ an error-correcting code that associates a share to each edge in the corresponding undirected graph. The encoded qubit can be reconstructed from the shares associated with the edges attached to any one vertex, corresponding to the sets of edges crossed by the purple arcs. For a single logical qubit, the shares on each edge consist of two qubits. A detailed construction of the code can be found in [6], and a more efficient version in [21]. For infinite dimensional versions see [8].

iv. A collection of spacetime regions $\{\mathscr{U}_1, ..., \mathscr{U}_m\}$*, which we call the unauthorized regions*

Bob will choose to access one of the $\mathscr{A}_i$ *or* $\mathscr{U}_i$*, and will attempt to construct the quantum system A from his access. Alice successfully completes the task if both (a) Bob is able to construct A when he accesses any one of the* $\mathscr{A}_i$ *and (b) Bob learns no information about A if he accesses any one of the* $\mathscr{U}_i$*.*

If Alice successfully completes the localize-exclude task, we say she has localized system A to the corresponding authorized regions while excluding it from the unauthorized regions.

As an initial approach to understanding the localize-exclude task we can list off the most basic restrictions that we expect to apply. First, the two restrictions occurring in the context of the localize task are still relevant: the start point should have a point from each authorized region in its future light cone, and there should be no causally disjoint pairs of authorized regions. There are also additional restrictions relating to the unauthorized regions however. In particular, we can never have an authorized region $\mathscr{A}_i$ be contained in the domain of dependence of an unauthorized region $\mathscr{U}_j$, since then all information which enters $\mathscr{A}_i$ also enters $\mathscr{U}_j$. Finally, the start point too should not be contained in the domain of dependence of any unauthorized region. We illustrate each these conditions in figure 6. Remarkably, a localize-exclude task

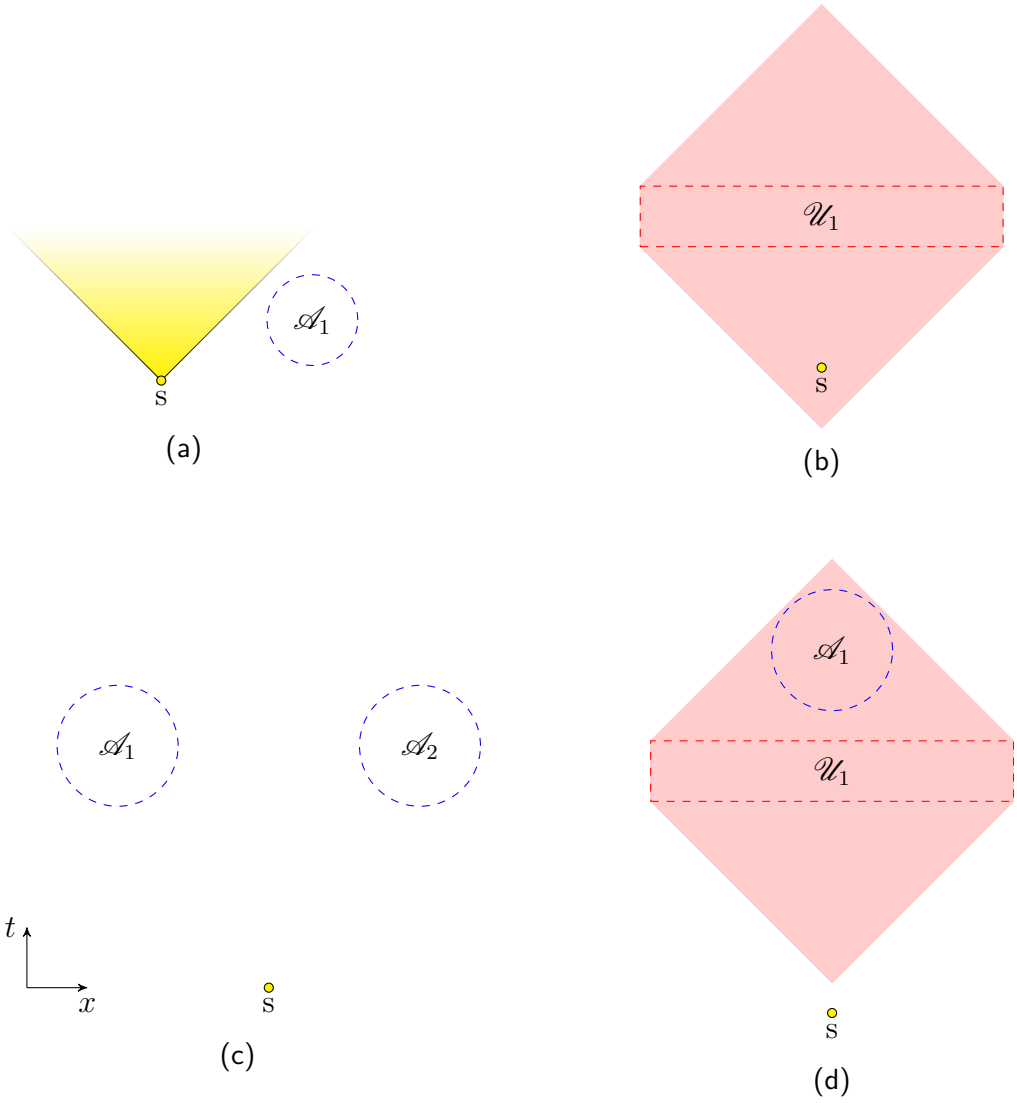

Figure 6: Four impossible localize-exclude tasks: (a) An authorized region is entirely outside the future light cone of s, so system A can't be localized there without violating the no-signalling principle. (b) The initial location of the quantum system is in the domain of dependence of an unauthorized region $\mathscr{U}_1$, so can be reconstructed from data in $\mathscr{U}_1$. (c) A quantum system cannot be localized to both the spacetime regions $\mathscr{A}_1$ and $\mathscr{A}_2$, due to the no-cloning theorem. (d) A quantum system cannot be localized to $\mathscr{A}_1$ without passing through the region $\mathscr{U}_1$, since there is no causal curve which passes through $\mathscr{A}_1$ and not $\mathscr{U}_1$. The red shaded region indicates the domain of dependence of the unauthorized region $\mathscr{U}_1$. The yellow shading indicates the future light cone of the start point.

$\{A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\}\}$ will turn out to be possible to complete so long as none of the four situations in figure 6 occur.

As a warm-up to the general case, consider the example given in the introduction as figure 1. There, a single unauthorized region blocks the path between two authorized ones. As we illustrate in figure 7, it is nonetheless possible to complete the task using the quantum one-time pad [22]. Near the start point, a unitary $\mathcal{U}_k$ is applied to A with k chosen at random. The overall pure state is then $\mathcal{U}_k \otimes \mathcal{I}|\Psi\rangle_{AR}$. To an observer who is unaware of the key k, the density matrix of the state is $\rho_{AR} = \sum_k \frac{1}{|k|}(\mathcal{U}_k \otimes \mathcal{I})|\Psi\rangle\langle\Psi|(\mathcal{U}_k^\dagger \otimes \mathcal{I})$. By carefully choosing the set of possible unitaries $\mathcal{U}_k$, one can arrange that $\rho_{AR} = \mathcal{I}_A/d_A \otimes \rho_R$, so that Bob has learned nothing about the A system whenever he does not learn k. This is possible when A consists of n qubits and k consists of $4n$ bits [22]. Once encoded using the one-time pad, the A system is sent through both authorized regions by allowing it to pass through the unauthorized region. An access to the unauthorized region then only sees the maximally mixed state. The classical key k is also sent to both authorized regions, but along trajectories that avoid the unauthorized one.

A similar technique can be applied to the general case of many authorized and many unauthorized regions. As we show in the proof of theorem 8 given below, the strategy is to first encode the A system into an error-correcting code so that it can be localized to each authorized region. Then each share in that error-correcting code is encoded using a classical string and the quantum one-time pad. We then leverage classical secret sharing to allow us to get the encoding string to the needed authorized regions while avoiding all the unauthorized regions.

We are now ready to state theorem 8 and give the proof. The proof of sufficiency is somewhat lengthy, so we have provided figure 8 which summarizes the key steps taken.

Theorem 8 *Given a collection of authorized regions $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$, unauthorized regions $\{\mathscr{U}_1, ..., \mathscr{U}_m\}$, and start point s, a localize-exclude task is possible if and only if the following three conditions are satisfied.*

i. The starting location of the system A (a) has at least one point from each authorized region in its causal future, and (b) is not in the domain of dependence of any unauthorized region.
ii. Every pair of authorized regions $(\mathscr{A}_i, \mathscr{A}_j)$ are causally connected.
iii. For every pair $(\mathscr{A}_i, \mathscr{U}_j)$ of authorized and unauthorized regions, $\mathscr{A}_i$ is not contained in the domain of dependence of $\mathscr{U}_j$.

Proof. The necessity of conditions $(i)(a)$ and (ii) follow from the same arguments as in theorem 6. To argue the necessity of condition (iii), notice that if $\mathscr{A}_i$ is contained in the domain of dependence of $\mathscr{U}_j$, then the state of the quantum fields within $\mathscr{A}_j$ is determined by unitary evolution from the fields within $\mathscr{U}_i$. Then whenever the A system can be determined from $\mathscr{A}_i$ it is also possible to recover it from $\mathscr{U}_j$. Condition $(i)(b)$ is necessary for the same reason.

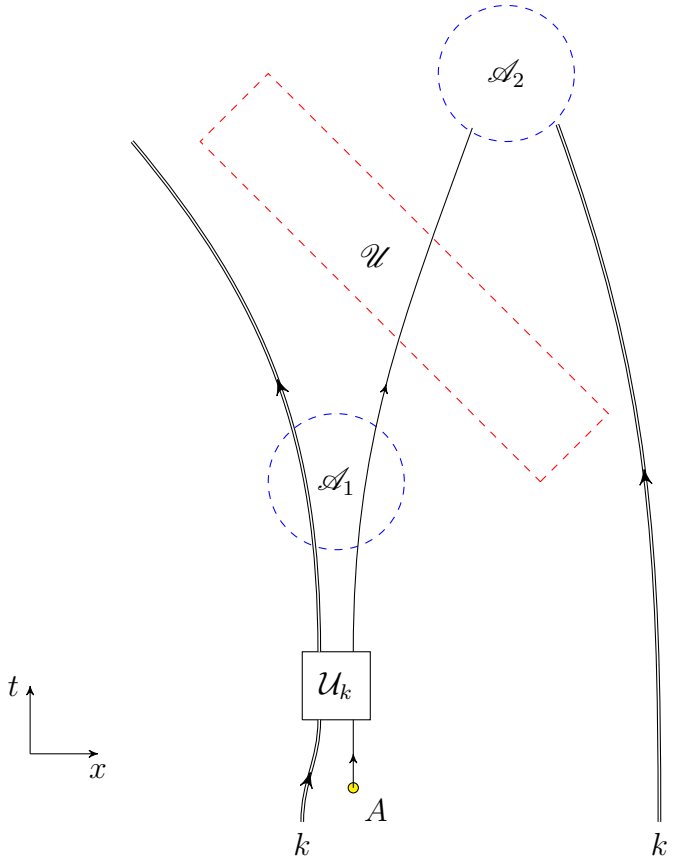

Figure 7: Illustration of the protocol for completing a localize-exclude task with two authorized regions and one unauthorized region that satisfy the conditions of theorem 8. In the distant past, Alice prepares copies of the classical string k. She brings one copy of k to each of $\mathscr{A}_1$ and $\mathscr{A}_2$ along a path which does not cross $\mathscr{U}$ — this is always possible by condition (iii). She must also bring the classical string to the start point s, and encode the A system using the quantum one-time pad [22]. The overall state on A and its purifying system R is then of the form $(\mathcal{U}_k \otimes \mathcal{I})|\Psi\rangle_{AR}$. The encoded system A is sent through both authorized regions. By following this protocol both authorized regions contain k and the encoded A system, while the unauthorized region contains the encoded system only.

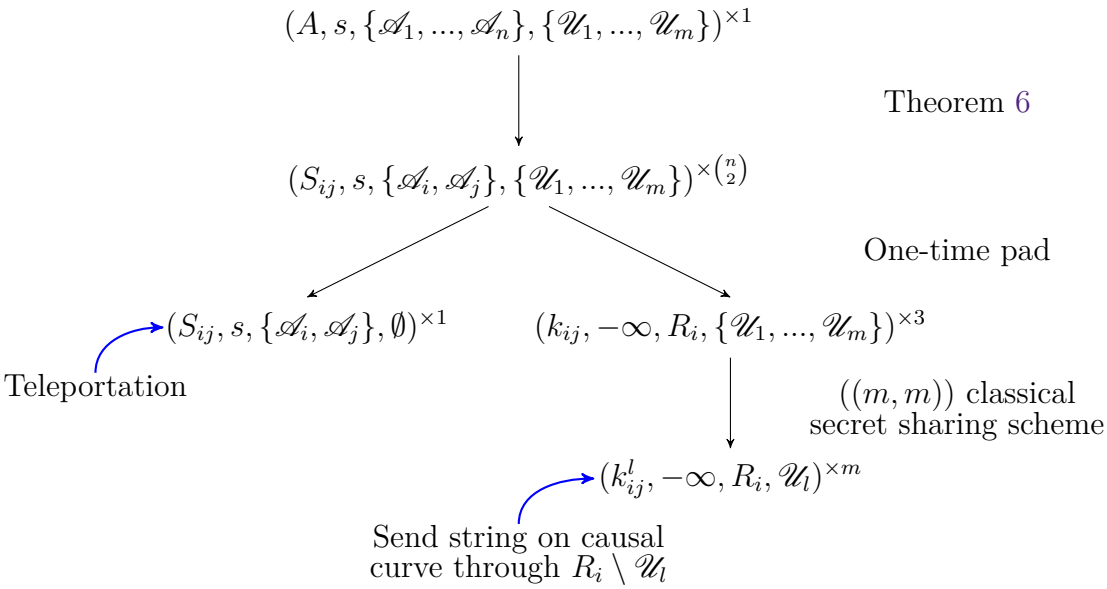

Figure 8: Diagram of the sufficiency proof of theorem 8. In three steps, the proof reduces completing the localization task on the system A with n authorized sets and m unauthorized sets, denoted by $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, to completing $\binom{n}{2}$ instances of $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ on quantum shares, and $3m\binom{n}{2}$ instances of $(k^l_{ij}, -\infty, R_i, \mathscr{U}_l)$ on classical shares, where the region R_i may be either the start point or an authorized region. The notation $-\infty$ indicates the share is available at early times. The first step in the protocol is to recycle the error-correcting code from theorem 6 to encode the A system into shares S_{ij}. At the second step, the one-time pad is applied to each of the S_{ij}. This allows the unauthorized regions to be avoided by introducing additional classical shares, but without the need for further uses of quantum error-correcting codes.

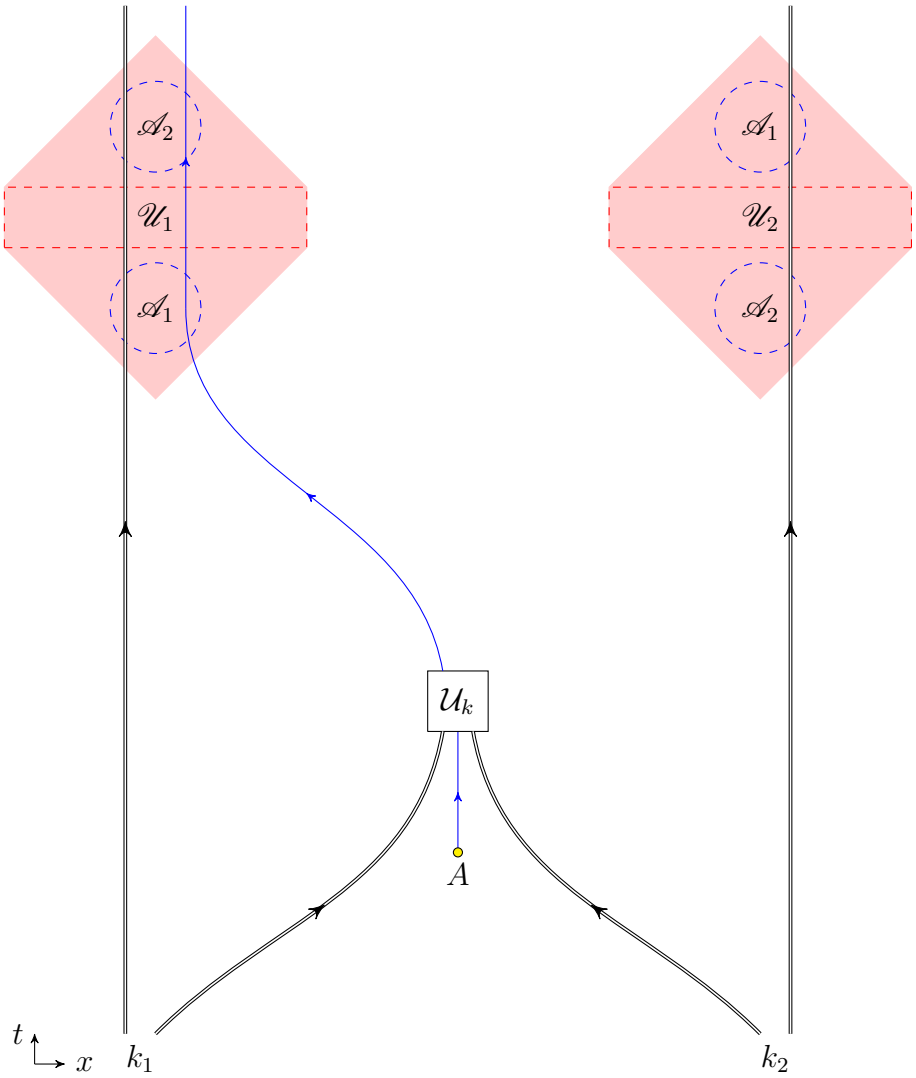

Figure 9: An example of a localize-exclude task and illustration of the protocol provided by theorem 8 for its completion. Near the start point the system A is encoded using the quantum one-time pad and sent (along the blue curve) through both authorized regions. The string k satisfies $k = k_1 \oplus k_2$, so that k_1, k_2 form the two shares of a $((2,2))$ secret sharing scheme. k_1 is sent through $\mathscr{A}_1$ and $\mathscr{A}_2$ while avoiding $\mathscr{U}_1$, while k_2 is sent through $\mathscr{A}_1$ and $\mathscr{A}_2$ while avoiding $\mathscr{U}_2$. Consequently, each $\mathscr{A}_i$ contains all of the classical shares k_i along with the encoded A system, while each $\mathscr{U}_i$ is missing one k_i.

To demonstrate sufficiency we construct an explicit protocol to complete the task in the case where all three conditions are true. It is useful to recall the notation $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, which describes a localize-exclude task by specifying the system on which we must complete the task, the start point, authorized regions, and unauthorized regions. As a first step in constructing our protocol, we encode the system A into the error-correcting code used in theorem 6. Using this code and localizing each share in the code to its two associated authorized regions would localize the system to each authorized region. However, here we also need to exclude the system from all of the unauthorized regions. To do this, we will localize each share S_{ij} to $\mathscr{A}_i$ and $\mathscr{A}_j$ while also avoiding every unauthorized region. In other words, encoding A into the codeword stabilized code reduces completing the original task to completing the tasks $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ for every share S_{ij}.

By using the quantum one-time pad and classical secret sharing it is possible to further reduce completing the $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ task. In particular, at s use the quantum one-time pad to encode the share S_{ij} using some classical string k_{ij}. We may freely send the encoded share through $\mathscr{A}_i$ and $\mathscr{A}_j$ so long as the classical string k_{ij} is kept out of all of the unauthorized regions, and is made available at $s, \mathscr{A}_i$, and $\mathscr{A}_j$. Thus, the task $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ is equivalent to completing $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ along with $(k_{ij}, -\infty, \{s, \mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$[3].

To finish the protocol, we first notice that theorem 6 shows that we can complete any task of the form $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ given that conditions $(i)(a)$ and (ii) hold. The task $(k_{ij}, -\infty, \{s, \mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ is also easily handled. Note that since the task is to be completed on a classical string, we can produce three copies of k_{ij} and worry separately about sending the string to s and each of $\mathscr{A}_i$ and $\mathscr{A}_j$, so we have to complete three instances of $(k_{ij}, -\infty, R, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, where R can be $s, \mathscr{A}_i$ or $\mathscr{A}_j$. To complete these, encode k_{ij} into an $((m, m))$ secret sharing scheme[4] with shares k^l_{ij}. Then complete the tasks $(k^l_{ij}, -\infty, R, \mathscr{U}_l)$. This completes the task with all m unauthorized regions since the classical string is kept out of $\mathscr{U}_l$ so long as at least one of the shares in the $((m, m))$ scheme is.

It remains to complete the tasks of the form $(k^l_{ij}, -\infty, R, \mathscr{U}_l)$. When R is one of the authorized sets, condition (iii) guarantees that R is not in the domain of dependence of $\mathscr{U}_l$, which means there is a causal curve passing through R which does not enter $\mathscr{U}_l$. To complete the task, simply send k^l_{ij} along this curve. When R is the start point s, condition $(i)(b)$ guarantees there is a causal curve passing through s and not $\mathscr{U}_l$, so again we can complete this task. ■

An example of the protocol used in this proof is given as figure 9.

[3]We've introduced the notation $-\infty$ to indicate the start point is located in the distant past. This is the appropriate task to consider completing on the classical system k_{ij} as Alice may prepare these strings at some early time.

[4]A $((k, n))$ secret sharing scheme is one where any k of the n total shares can be used to reconstruct the secret while any $k-1$ shares reveal nothing about the secret. A $((m, m))$ scheme is the appropriate one here because we want every share to be needed to reconstruct k_{ij}.

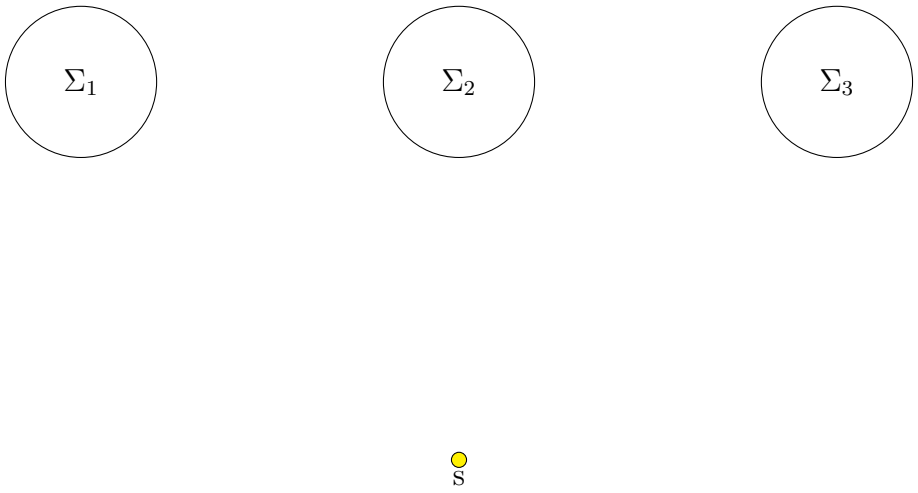

Figure 10: Example of the embedding of a secret sharing scheme with arbitrary access structure into a localize-exclude task. We consider a secret sharing scheme that involves three parties, and has authorized sets $S_1 = \{1, 2\}$, $S_2 = \{2, 3\}$ and $S_3 = \{1, 2, 3\}$, with all other subsets of parties deemed unauthorized. In the corresponding localize-exclude task, the three parties become three causally disjoint spacetime regions Σ_1, Σ_2 and Σ_3. Further, this localize-exclude task has authorized regions $\mathscr{A}_1 = \Sigma_1 \cup \Sigma_2$, $\mathscr{A}_2 = \Sigma_2 \cup \Sigma_3$ and $\mathscr{A}_3 = \Sigma_1 \cup \Sigma_2 \cup \Sigma_3$. The start point s has been placed at an early enough time that all the Σ_i are in its future light cone.

Earlier we mentioned the similarity of conditions (ii) and (iii) to corresponding conditions for quantum secret sharing. A quantum secret sharing scheme [23] is specified by an access structure, with the access structure consisting of subsets of parties deemed authorized and subsets deemed unauthorized. A quantum secret sharing scheme can be constructed under two conditions [23]: (a) (no-cloning) no two authorized sets can be disjoint and (b) (monotonicity) no authorized set can be contained within an unauthorized set. Conditions (ii) and (iii) of the localize-exclude theorem are exactly these conditions rephrased in a context appropriate to spacetime.

Beyond this similarity, we can embed any secret sharing scheme into a localize-exclude task. Consider n parties, Bob_1,...,Bob_n, who each can potentially access an associated spacetime region Σ_i. Take the authorized and unauthorized regions to consist of unions of Σ_i's so that a full authorized region $\mathscr{A}_i$ can be accessed only if some collection of Bobs agree to cooperate. Choose the regions Σ_i to be all causally disjoint. In this setting two authorized regions being causally connected occurs if and only if they share a Σ_i. Then condition (ii) of theorem 8, which requires causal connections between authorized regions, reduces to the requirement that every pair of authorized regions share at least one Σ_i. This is exactly the no-cloning requirement on secret sharing. Further, condition (iii) reduces to no $\mathscr{U}_i = \Sigma_{i1} \cup ... \cup \Sigma_{in}$ containing as a subset some $\mathscr{A}_j = \Sigma_{j1} \cup ... \cup \Sigma_{j2}$ under the same restriction of having causally disjoint Σ_i. This is just the monotonicity condition on quantum secret sharing schemes. Finally, to embed our quantum secret sharing task into a localize-exclude task we should ensure

that condition (i) becomes trivial, which we can do by sending the start point s to an early time. We illustrate the embedding of a secret sharing task into a localize-exclude task in figure 10.

Theorem 8 shows that completing a localize-exclude task with unauthorized regions requires only the same quantum error-correcting code as used in the case with no unauthorized regions. Hiding the system from the unauthorized regions can be accomplished using only the quantum one-time pad and classical secret sharing. This is similar to the approach taken in [24], where quantum error-correcting codes are combined with the quantum one-time pad to yield quantum secret sharing schemes. By using the efficient error-correcting code underlying our protocol however, we arrive at a particularly efficient construction of quantum secret sharing schemes. In particular we find that there is a universal quantum error-correcting code with $2\binom{n}{2}$ shares for n the number of authorized sets which, along with uses of the one-time pad and classical secret sharing, constructs quantum secret sharing schemes with arbitrary access structures. Using Shamir's method [25] to construct the classical secret sharing schemes, the $3m\binom{n}{2}$ instances of the $((m, m))$ classical scheme will each require $O(m \log m)$ bits, where m was the number of unauthorized sets. In total, $O(n^2)$ qubits and $O(m^2 n^2 \log m)$ classical bits are used in the localize-exclude construction. This provides the first construction of quantum secret sharing schemes using a number of qubits polynomial in the number of authorized sets. Previously, efficient constructions were known for threshold schemes and certain other special access structures. (See, *e.g.* [26, 27, 24].) Since the number of unauthorized sets can grow exponentially with n, the classical bits used can be exponentially large. This is to be expected since it is conjectured to be impossible to construct classical secret sharing schemes for arbitrary access structures without consuming exponential resources [28].

3 State-assembly

3.1 State-assembly with authorized regions

In the localize-exclude task Bob can access any one of a set of spacetime regions. Alice, who holds various quantum systems within those regions, is helpless to prevent Bob's access. In an alternative scenario we can have Bob request information from Alice. Alice is free to comply with the request or to reject it, and hand over no information. Certain sets of requests are deemed authorized, others unauthorized. Sets of requests corresponding to authorized sets should result in Alice handing over sufficient information for the system to be reconstructed; requests to unauthorized sets should reveal no information about the system. Considering such scenario's leads us to construct the *state-assembly task*.

Before giving a precise definition of the task we introduce a few constructions. To specify locations where Bob may request the system we designate certain spacetime points as call points c_i. At each call point a bit $b_i \in \{0, 1\}$ is revealed to Alice. To

each call point there corresponds a return point r_i. Together, a call point and the corresponding reveal point define a causal diamond.

Definition 9 *The **causal diamond** D_i is defined as the intersection of the points in the past light cone of r_i with those in the future light cone of c_i.*

If $b_i = 1$ we say the diamond D_i has been called to. The causal diamond represents the spacetime region in which it is possible to both know that a call was received, and to use this information to influence what is handed over at the corresponding return point.

We can now define the state-assembly task.

Definition 10 *A **state-assembly** task involves two agencies, Alice and Bob, and is specified by a tuple $\{A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\}\}$, consisting of*

i. A quantum system A. In general A may be a subsystem of some overall pure state $|\Psi\rangle_{AR}$. The state on AR is known to Alice and unknown to Bob.

ii. A start point s at which Alice initially holds A.

iii. A collection of authorized sets of diamonds $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$. Each authorized set consists of a collection of diamonds, $\mathscr{A}_i = \{D_{1i}, ..., D_{ki}\}$.

iv. A collection of unauthorized sets of diamonds $\{\mathscr{U}_1, ..., \mathscr{U}_m\}$. Each authorized set consists of a collection of diamonds, $\mathscr{U}_i = \{D_{1i}, ..., D_{ki}\}$.

Alice will receive calls at a subset of the D_i. If the set of called to diamonds corresponds to an authorized set, Alice should return quantum systems and classical instructions sufficient to reconstruct A at the associated reveal points r_i. If the set of calls corresponds to an unauthorized set, the systems she hands over should reveal no information about A. Further, no set of calls should result in Alice returning systems sufficient to construct two copies of the system.

There are a few points to clarify regarding this definition. First, Alice need not hand the system over at any one of the called to diamonds. Instead the systems she hands over at the called to diamonds should together be sufficient to recover the A system. Second, calls to sets of diamonds not specified as authorized or unauthorized may result in the system being handed over — Alice still completes the task successfully so long as she does not hand over two copies of the system.

In state-assembly Alice knows the state $|\Psi\rangle_{AR}$ and can potentially prepare many copies of the A system. This differs from the localize-exclude task and earlier work on summoning. However, we have also required that she never hand over more than one copy of A. As discussed in more detail in appendix A, this is actually leads to conditions on state-assembly that are equivalent to having Alice hold an unknown state. We have chosen to discuss this task from the perspective of a known quantum state however as it is more natural in the context of the application given in section 4.

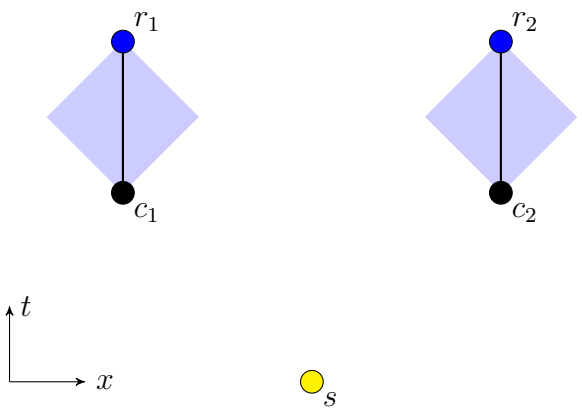

Figure 11: A state-assembly task with two call-return pairs. A call to c_1 is required to result in the system returned at r_1, and likewise for c_2 and r_2 (indicated by the black lines), while a call to both shouldn't result in more than one copy of the system being turned over. This task is impossible as shown by theorem 11, because r_2 is outside the future light cone of c_1 and r_1 is outside the future light cone of c_2. In the language of definitions 9 and 10, c_1 and r_1 form a causal diamond D_1 (shown in blue), and the authorized set $\mathscr{A}_1$ consists of the single diamond D_1 (similarly for c_2 and r_2).

Before discussing more general constructions we begin with the simplest state-assembly task, illustrated in figure 11, and prove a no-assembly theorem. In this scenario there are just two authorized sets $\mathscr{A}_1$ and $\mathscr{A}_2$.

Theorem 11 *Consider a state-assembly task with authorized sets $\mathscr{A}_1$ and $\mathscr{A}_2$ which are causally disconnected. Then this assembly task is impossible to complete with a perfect success rate.*

Proof. For Alice to successfully complete the assembly task, she must have a protocol which

i. Returns sufficient information to construct the system when $\mathscr{A}_1$ or $\mathscr{A}_2$ receive calls.
ii. Hand over information sufficient to construct at most one copy of the system for any set of calls.

We can straightforwardly show that any protocol which satisfies the first requirement cannot satisfy the second, and consequently there is no such successful protocol. Indeed, suppose both $\mathscr{A}_1$ and $\mathscr{A}_2$ receive calls. Then since $\mathscr{A}_1$ and $\mathscr{A}_2$ are causally disjoint Alice's agents at the diamonds in $\mathscr{A}_1$ cannot distinguish this situation from one where only $\mathscr{A}_1$ has been called to. By (i) then they hand in sufficient information to construct the system. Similarly, Alice's agents at $\mathscr{A}_2$ will also hand in sufficient information to construct the system. Since Bob may now construct two copies of A, (ii) is violated. ■

We see that completing the assembly task to causally separated regions is impossible. Notice that it is essential that the Bobs may give calls to both diamonds: the possibility

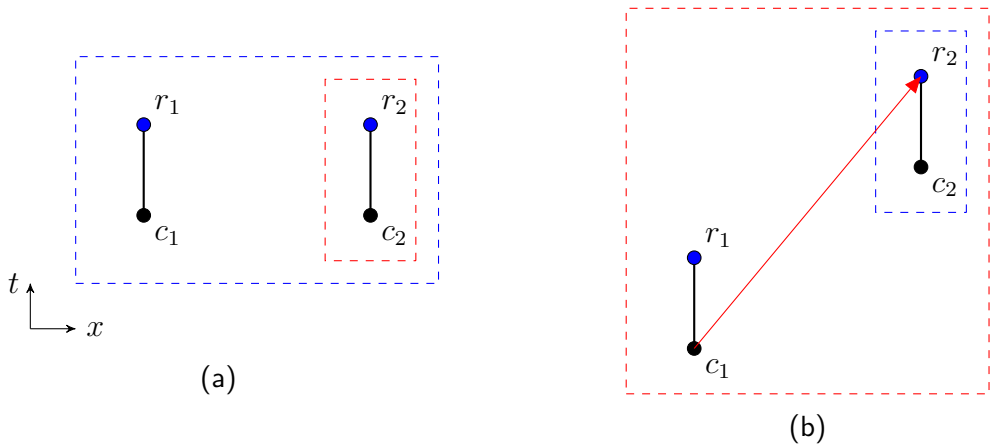

Figure 12: Illustration of condition (iii) in theorem 13. Dashed red boxes enclose unauthorized sets while dashed blue boxes enclose authorized sets. The condition states that every pairing $(\mathscr{A}_a, \mathscr{U}_i)$ of authorized with unauthorized set must have either (a) $\mathscr{A}_a \setminus \mathscr{U}_i \neq \emptyset$ or (b) $\mathscr{U}_i \setminus \mathscr{A}_a$ is causally connected to $\mathscr{A}_a$.

of a call to $\mathscr{A}_1 \cup \mathscr{A}_2$ along with the requirement that Alice allow assembly of not more than one copy of the system leads to Alice being unable to complete the task successfully.

Next, we look at a wider class of assembly tasks involving an arbitrary number of authorized sets $\{\mathscr{A}_i\}$.

Theorem 12 *An assembly task with authorized sets $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ and start point s can be completed with a perfect success rate if and only if the following conditions hold.*

i. The return point of at least one diamond from each authorized set is in the causal future of the start point.

ii. Every pair of authorized sets $(\mathscr{A}_i, \mathscr{A}_j)$ are causally connected.

Proof. The first condition is necessary by no-signalling. The necessity of the second condition follows from the same argument as given in theorem 11.

We can use theorem 8 to show sufficiency of these conditions. There, we constructed an explicit protocol that localizes the system to each authorized region. In particular, the system is recorded as classical teleportation data and shares in a quantum error-correcting code. To complete the assembly task then, Alice should execute the localization protocol from theorem 8, with the authorized sets of diamonds considered as authorized regions. Then to complete the assembly task Alice need only hand over the classical and quantum data in $\mathscr{A}_i$ when she receives calls there.

Notice that this protocol automatically ensures Bob cannot give calls to receive two copies of the system, since Alice only uses one copy of A. ■

3.2 State-assembly with authorized and unauthorized regions

We can now proceed to characterize the state-assembly tasks with both authorized and unauthorized sets that can be completed by Alice. The difficulty here for Alice is different than in the case of localize-exclude. In localize-exclude, she had to keep the system out of a region $\mathscr{U}_i$ from an attacker who might gain full access to $\mathscr{U}_i$. Now, Alice's labs are secure. However the sets of spacetime points corresponding to an authorized call can be overlapping with those corresponding to an unauthorized call. This means that locally she may not be able to tell an authorized and unauthorized call apart.

To understand under what conditions Alice can avoid an accidental reveal of the system to an unauthorized set of diamonds, we can first consider a task of the form $(A, s, \mathscr{A}, \mathscr{U})$ having one authorized and one unauthorized set of diamonds. In this case, Alice can be successful if either (a) there is a diamond in $\mathscr{A}$ which is not in $\mathscr{U}$, since then she can turn over the system at that diamond only when there is a call there or (b) there is a diamond D_* in $\mathscr{A}$ which, although it is in $\mathscr{U}$, is positioned such that Alice can tell at D_* whether the global set of calls is authorized or unauthorized. In particular, this occurs exactly when there is a diamond in $\mathscr{U} \setminus \mathscr{A}$ which is causally connected to $\mathscr{A}$. Figure 12 illustrates these two possibilities.

We now state and prove the theorem characterizing the state-assembly tasks with authorized and unauthorized sets of diamonds.

Theorem 13 *A state-assembly task with authorized sets $\{\mathscr{A}_a\}$ and unauthorized sets $\{\mathscr{U}_i\}$ and start point s can be completed if and only if the following three conditions hold:*

i. The return point of at least one diamond from each authorized set is in the causal future of the start point.

ii. Each pair of authorized sets $(\mathscr{A}_a, \mathscr{A}_b)$ is causally connected.

iii. Each pair $(\mathscr{A}_a, \mathscr{U}_i)$ of authorized with unauthorized sets has the property that either $\mathscr{A}_a \setminus \mathscr{U}_i \neq \emptyset$ or $\mathscr{U}_i \setminus \mathscr{A}_a$ is causally connected to $\mathscr{A}_a$.

Proof. The necessity of conditions (i) and (ii) follow from the same arguments as in theorem 12. To see the necessity of condition (iii), consider that its negation is that both $\mathscr{A}_a \subset \mathscr{U}_i$ and $\mathscr{U}_i \setminus \mathscr{A}_a$ is not causally connected to $\mathscr{A}_a$. Then Alice's agents in the diamonds of $\mathscr{A}_a$, should they receive calls, cannot distinguish a call to $\mathscr{A}_a$ from a call to $\mathscr{U}_i$ since they are causally disconnected from diamonds in $\mathscr{U}_i \setminus \mathscr{A}_a$. In order to complete the task, Alice must always hand the system over to $\mathscr{A}_a$ when she receives a call there. She will then also always hand over the system when the call is to $\mathscr{U}_i$, leading to her failing the task.

To demonstrate sufficiency we construct an explicit protocol to complete the task in the case where all three conditions are true. Using the error-correcting code constructed from the graph of causal connections (also used in theorems 6, 8, and 12) we can reduce the initial $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ task to many tasks of the form

$(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, where the S_{ij} are the shares of the error-correcting code associated to the $i-j$ pair of regions.

To complete the $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ tasks, we encode the share S_{ij} using the quantum one-time pad with some classical randomness k_{ij}. Now notice that we can complete the $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ task by completing $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ on the quantum share S_{ij} and $(k_{ij}, s, \mathscr{A}_i, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ and
$(k_{ij}, s, \mathscr{A}_j, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ on the classical string. Stated another way, the use of the one-time pad lets us ignore avoiding the unauthorized sets when considering the quantum data, and only worry about not handing the classical string over at the unauthorized sets.

To complete the tasks of the form $(k_{ij}, s, \mathscr{A}_i, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, we encode k_{ij} into a $((m, m))$ classical secret sharing scheme with shares labelled k^l_{ij}. Then completing the tasks $(k^l_{ij}, s, \mathscr{A}_i, \mathscr{U}_l)$ ensures each share k^l_{ij} ends up at $\mathscr{A}_i$, so the string k_{ij} can be constructed there along with the quantum share S_{ij}. At the same time, completing the tasks $(k^l_{ij}, s, \mathscr{A}_i, \mathscr{U}_l)$ ensures the share k^l_{ij} is missing from $\mathscr{U}_l$, and since every share k^l_{ij} is needed to recover S_{ij}, S_{ij} cannot be decoded there.

To complete these $(k, s, \mathscr{A}_i, \mathscr{U}_j)$ tasks, recall that by condition (iii) either $\mathscr{A}_i \setminus \mathscr{U}_j$ is not empty or $\mathscr{U}_i \setminus \mathscr{A}_i$ is causally connected to $\mathscr{A}_i$. If $\mathscr{A}_i \setminus \mathscr{U}_i$ is not empty, then send k to a diamond D_* in $\mathscr{A}_i \setminus \mathscr{U}_i$. Then hand over k at D_* if there is a call there. If $\mathscr{U}_i \setminus \mathscr{A}_i$ is causally connected to $\mathscr{A}_i$ then send k to any diamond D_* in $\mathscr{A}_i$ which has at least one call point of $\mathscr{U}_i \setminus \mathscr{A}_i$ in its causal past. Then hand over k at D_* if there is a call there and no call at the diamonds in $\mathscr{U}_j \setminus \mathscr{A}_i$. ■

We give a task on four diamonds in figure 13 and demonstrate how to complete it using the protocol constructed in this proof.

The state-assembly task seems a less natural extension of quantum secret sharing to spacetime, since condition (iii) differs notably from the corresponding condition in secret sharing. In particular, some allowed state-assembly tasks have unauthorized sets which contain authorized ones, violating the monotonicity requirement of quantum secret sharing [23]. In contrast, the localize-exclude task mimics the monotonicity requirement closely, since the condition there is that (the domain of dependence of) the unauthorized region not contain the authorized region. However, this distinction from secret sharing opens up interesting new possibilities; in the next section we propose a cryptographic task and protocol which exploits the failure of monotonicity in the state-assembly task.

4 An application: party-independent transfer

As discussed in the introduction, relativistic tasks in Minkowski space have provided an interesting set of tools for the cryptographer. In part, our motivation for considering the state-assembly task with authorized and unauthorized regions is in the hope it will find such application. The state-assembly task includes scenarios with many parties, and allows for a rich array of possible causal structures. Each causal structure translates to

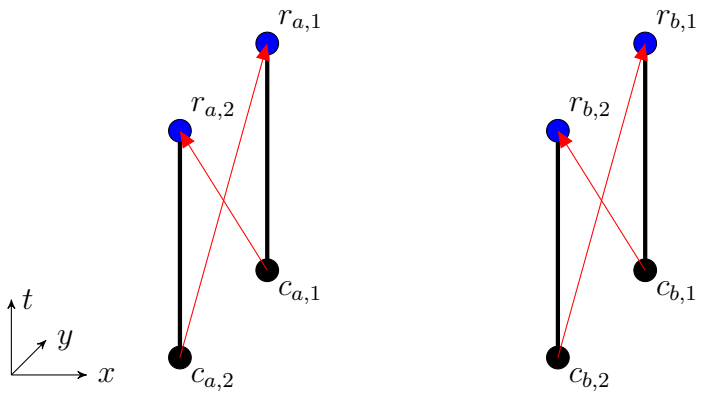

Figure 13: An arrangement of causal diamonds on which we can define an assembly task. Define authorized sets $\mathscr{A}_1 = \{D_{a,1}, D_{b,1}\}$ and $\mathscr{A}_2 = \{D_{a,2}, D_{b,2}\}$ while any set of three or four diamonds is deemed unauthorized. One can check that every unauthorized set has $\mathscr{U}_i \setminus \mathscr{A}_j$ causally connected to $\mathscr{A}_j$, so theorem 13 gives that this task can be completed. To do so, the initial system A is encoded using the quantum one-time pad and sent towards the pair of diamonds labelled 'a', D_{a1} and D_{a2}. It should be handed over at whichever diamond receives a call. The key k from the one-time pad is stored in a $((2,2))$ secret sharing scheme as $k = k_a \oplus k_b$ and k_a and k_b are sent towards the 'a' and 'b' pairs of diamonds respectively. At the 'a' pair of diamonds, k_a is returned to D_{a1} if there is a call there and no call at D_{a2}, or at D_{a2} if there is a call there and no call at D_{a1}. The k_b string is returned to D_{b1} or D_{b2} using the same logic. If three or four diamonds receive calls, then at least one of the 'a' or 'b' pairs of diamonds will not receive a share of the $((2,2))$ scheme, so Bob will not receive the A system. Notice that the task is possible even though $\mathscr{A}_1, \mathscr{A}_2$ are subsets of the unauthorized sets, violating the monotonicity requirement of quantum secret sharing.

a set of restrictions on which parties can know what, and when, and it seems plausible that these restrictions can be exploited to perform some interesting multiparty task or computation securely.

We suspect there are many possible directions to consider, and make a small start at this by suggesting below one particular task. We do not offer complete security arguments for our proposal or careful discussion of the practicality of this task. Our aim is simply to suggest the applicability of the state-assembly task to cryptography.

To motivate the task consider the following scenario. Alice is an employer who wishes to hire either Bob_1 or Bob_2. Alice is known to be inclined to prejudice, and the Bobs wish to ensure they are paid based on the work done alone, without regard to their identity. An easy solution would be to announce publicly the position's salary, but unfortunately the Bobs are private people. They wish to keep their salaries secret while also having a guarantee of fairness. We define the *party-independent transfer* task in order to satisfy these two competing needs.

In the party-independent transfer task, we specify that each Bob will give an input X_i to Alice. Alice will then output quantum systems $S(X_1, X_2, a)$ and $T(X_1, X_2, a)$, with one system handed to each of the Bobs, where a is a variable fixed by Alice. The task occurs in a spacetime setting, so in general the X_i may be stored as several bits handed over from Bob's agents to Alice's agents at distributed spacetime points. The X_i should be distinct. If not, then the protocol aborts.

To meet the needs of our jealousy-prone but private Bobs, and guard against the prejudiced Alice, we need the transfer to have the following properties:

i. *Party independence:* The output systems S and T produced by Alice have the property that

$$S(X_1, X_2, a) = T(X_2, X_1, a) \quad \textit{and} \quad S(X_2, X_1, a) = T(X_1, X_2, a). \tag{1}$$

In words, we require that the output given to Bob_1 would have been given to Bob_2 had the Bobs reversed their inputs.

ii. *Fixed:* As a set, $\{S(X_1, X_2, a), T(X_1, X_2, a)\}$ is determined by the variable a only. In words, the Bobs' input influences who receives which system only, not which two systems are handed over.

iii. *Secret:* Each Bob does not learn Alice's output to the other Bob. In particular, this requires that Alice not satisfy condition 1 trivially by having $S(X_1, X_2, a) = T(X_1, X_2, a)$ always.

To assure ourselves completing this task is not trivial consider various naive approaches. We might have Alice share two entangled sets of degrees of freedom, E_1 given to Bob_1 and E_2 given to Bob_2, onto which she will later teleport T and S, respectively. The Bobs could then exchange degrees of freedom if they decide to reverse the arrangement of who receives which system. This is certainly party-independent, since Alice performs the teleportation without knowing who holds which degrees of freedom. However, the fixed property is violated, as either Bob can act on their degrees of freedom before exchanging it.

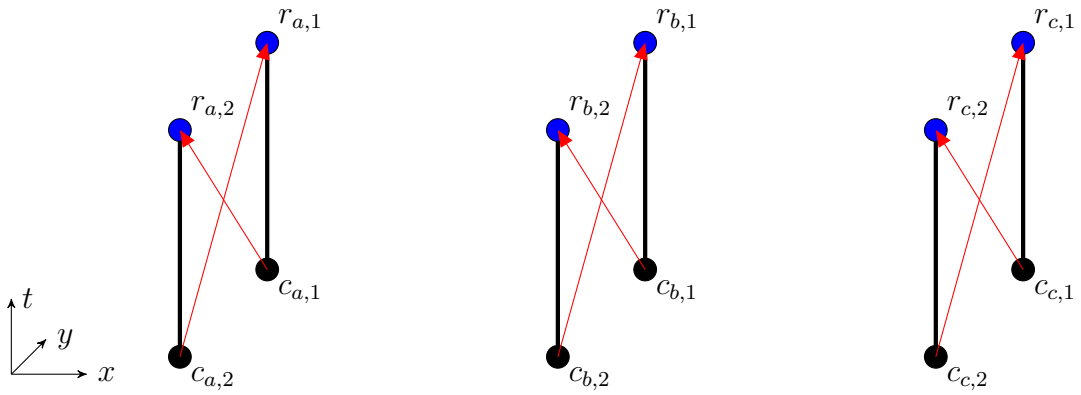

Figure 14: Arrangement of call-reveal pairs used in the proposed party-independent transfer protocol. Bob_1 controls the diamonds $D_{a,1}, D_{b,1}, D_{c,1}$ while Bob_2 controls $D_{a,2}, D_{b,2}, D_{c,2}$.

Another strategy would be to have Alice publicly announce a protocol for preparing each of S and T. Clearly this is fixed and party-independent, but fails to be secret. Finally, Alice could separately hand S to Bob_1 and T to Bob_2 (or vice versa). This would be fixed and secret but not party-independent.

Although the obvious strategies fail, the state-assembly task seems to be well-suited to achieving party-independent transfer. As intuition, we can note that in a state-assembly task Alice's agents, who only have access to local information and not the global set of calls made by the Bobs, may not be aware of who has received the system until a late time when she has been able to collect and compare all of the call data. Further, we have already introduced the notion of an unauthorized set of calls and can hope to exploit this to achieve the secrecy property of party-independent transfer.

Indeed, we can put forward a candidate protocol built on a state-assembly task that seems to achieve all three security requirements of party-independent transfer. Before explaining the protocol however, we need to highlight one feature of the $((2,3))$ secret sharing scheme which will be used. We will use an error-correcting code on three physical qutrits which stores one logical qutrit. The logical states are given by

$$\begin{aligned}
|0_L\rangle &= \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle), \\
|1_L\rangle &= \frac{1}{\sqrt{3}}(|012\rangle + |201\rangle + |120\rangle), \\
|2_L\rangle &= \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle).
\end{aligned} \tag{2}$$

One may check explicitly that there exists a decoding operation $U_{12}^\dagger$ supported on the first two qutrits such that

$$\mathcal{U}_{12}^\dagger |i_L\rangle = |i\rangle_1 |\chi\rangle_{23}, \tag{3}$$

where

$$|\chi\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle + |11\rangle + |22\rangle\right). \tag{4}$$

By the symmetry in the code, a similar decoding operation exists for any subsystems of two qutrits. We wish to highlight that after the decoding operation is applied, two of the qutrits are left in a maximally entangled state.

To construct the protocol, we will use the arrangement of diamonds shown in figure 14. Bob_1 controls the diamonds $D_{a,1}, D_{b,1}, D_{c,1}$ while Bob_2 controls $D_{a,2}, D_{b,2}, D_{c,2}$. We consider a scenario where the Bobs choose at random which of them receives which system, although modifications to this are easy. We divide the protocol into a preparation phase, transfer phase, and checking phase for clarity in presentation.

Protocol 14 ***Compensation protocol***

i. **Preparation phase**

   (a) Alice prepares a quantum state $|\Psi\rangle_{SR}$, and encodes the S system into the $((2,3))$ secret sharing scheme using the encoding given in equation 2.

   (b) Bob_1 and Bob_2 execute a coin flipping protocol. The outcome is not revealed to Alice. Without loss of generality, suppose that Bob_1 wins the coin toss, which determines that he should receive S.

   (c) Bob_1 chooses at random two of the three diamonds he controls and sends calls to each of them. Without loss of generality, we call these diamonds $D_{a,1}$ and $D_{b,1}$. Bob_2 then sends a call to the diamond he controls which is not causally connected to $D_{a,1}$ or $D_{b,1}$, which in this case is $D_{c,2}$.

ii. **Transfer phase**

   (a) Alice routes one share of her secret sharing scheme towards each of the diamond pairs labelled by a, b and c.

   (b) Alice responds to the summons at each of the call points by comparing the calls from $D_{x,1}$ and $D_{x,2}$. If both have $b = 1$ or both have $b = 0$, Alice does not hand over the share to either diamond. If exactly one of the two diamonds has $b = 1$, Alice hands the share over at the corresponding return point.

iii. **Checking phase**

   (a) Bob_1 applies the decoding map to his two shares, producing $|\Psi\rangle_{SR} \otimes |\chi\rangle$ where $|\chi\rangle$ is the maximally entangled state given in equation 4.

   (b) Bob_2 sends his share of the maximally entangled state to Bob_1, who then measures the pair jointly to ensure he holds $|\chi\rangle$.

In the notation of our security definition, the inputs X_i by the Bobs consist of their three output bits $X_i = \{b_{i,a}, b_{i,b}, b_{i,c}\}$. Before the checking phase, the state is $|\Psi\rangle_{SR} \otimes |\chi\rangle$, with the receiving Bob holding S and half the maximally entangled state $|\chi\rangle$, and the

non-receiving Bob holding the other half of $|\chi\rangle$. After the checking phase however one Bob holds only S and the $|\chi\rangle$ state has been measured. We should then identify the T system of the definition as $T = \emptyset$. If we would like both Bobs to receive some quantum system we can run the protocol twice.

We can argue for the secret and fixed properties of this protocol. Fixed is clear, since the receiving Bob can reconstruct the system from degrees of freedom that have never been held by the non-receiving Bob. Regarding secrecy, we note that the non-receiving Bob receives only one share of the secret sharing scheme, so learns no information about S. The non-receiving Bob may try to receive additional shares by sending additional calls, but in this case Alice will notice that calls have been made at two causally related diamonds and not hand over any shares to those diamonds.

To argue for party-independence, note that Alice is already limited in her knowledge of who is receiving the system. Although at each pair of diamonds she knows whether she is handing a single share over to Bob_1 or Bob_2, none of Alice's agents have the global information of which Bob is receiving two shares, and thus the system S. Later on she will be able to collect information from all the call points and determine this, but at the spacetime points of transfer this is not known. Alice might try to have one set of shares which she hands to Bob_1 and a separate set to Bob_2, but using two unentangled sets of shares for Bob_1 and Bob_2 will lead to a failure in the checking phase. We leave proving or disproving the security of this protocol, which we regard as plausible but not obvious, to future work.

It is perhaps useful to note a connection of classical bit commitment with the party-independent transfer task. Given a bit commitment scheme which consists of 1) Alice handing a commitment to Bob, then 2) Alice later handing a reveal to Bob, which he uses to access Alice's committed bit, it is possible to construct a party-independent transfer protocol.[5] In particular, Alice publicly announces her commitment to both Bob_1 and Bob_2, then hands the reveal to only one of the Bobs. However, it is known that there are no unconditionally secure bit commitment schemes of this form [30, 31].

5 Discussion

In our first article on summoning [6], we argued that the summoning task gives an operational setting in which to understand how quantum information can and cannot move through spacetime. That setting was restricted however to asking if a quantum system could be localized to collections of causal diamonds.

In this article we have generalized in a way that allows us to ask if a quantum system is localized to a collection of arbitrary spacetime regions. We have defined the notion of localized by allowing some party with no prior knowledge of the system unrestricted access to the spacetime region. If they can later construct the system then we say it was localized there; if they learn nothing about the system we say it is excluded.

[5] This was pointed out to the authors on the cryptography stack exchange [29].

This is consistent with our previous definition of localization to a diamond, in that completing the summoning task means in particular that the system was localized to each diamond. However, the notion of localization implied by summoning is stronger than the notion used in this article, since in summoning Alice must perform the data processing needed to construct the system while within the diamond. In the localize task this data processing can occur outside the region.

In the absence of gravity, where there are no known limits on the rate of computation, the strong and weak notions of localization coincide, at least for diamond-shaped regions. In the presence of gravity Lloyd argued there is a limit on computational speed [32] but there are counterexamples to his proposed bound [33]. It is nonetheless plausible that computational speed is limited by quantum gravity, so one can imagine a scenario where a quantum system is localized to a region in the weaker sense (in that it is possible to construct it from systems that pass through that region) but not in the strong sense (in that it is impossible to do so within the spatial-temporal extent of that region due to gravitational constraints on computation). Thus, in the presence of gravity these notions of localization plausibly become distinct. Attempts to resolve fundamental puzzles like the black hole information paradox [34, 12, 35] have also hinted at this distinction, and indicate that it may be the stronger notion of localization for which the no-cloning theorem applies.

Also in the context of gravity the holographic bound [36] makes tasks with sufficiently small regions or sufficiently large numbers of regions impossible to complete, since it places a limit on how many qubits may be localized to a region of a given area without producing a black hole. Thus, we should understand the theorems given in this work as applying only in the absence of gravity. It would be interesting to perform a detailed study of exceptions to our theorems arising from gravitational physics.

By adding excluded regions to the localize task we have found a natural extension of quantum secret sharing to a spacetime setting. Indeed, the conditions for completing the localize-exclude task have close analogues in the conditions for constructing quantum secret sharing schemes, and we can embed any quantum secret sharing scheme as a carefully chosen localize-exclude task. The conditions on the start point in the localize-exclude task are somewhat awkward from this perspective, but can be seen as corresponding to certain trivial requirements in the secret sharing language.

Since the localize-exclude task corresponds so closely to quantum secret sharing, we might expect that it doesn't provide any new tools for the construction of cryptographic protocols. From this perspective the state-assembly task is more interesting, since there we can have an unauthorized set contain an authorized one. This violates the monotonicity requirement that occurs in both localize-exclude and quantum secret sharing.

We have given one proposed application that exploits this violation of monotonicity: party-independent transfer. This proposal is in need of a more complete study. We have not proven our proposed protocol is secure, nor considered what more practical goals within cryptography this primitive may be used to achieve. It would also be interesting to understand the relation of the proposed party-independent transfer task

to established cryptographic primitives. We have already pointed out a connection to bit commitment, but there may also be interesting relations to (for instance) the spacetime analogues of oblivious transfer mentioned in the introduction.

6 Acknowledgements

This work was started while the authors were at McGill University, and restarted while attending the first It from Qubit summer school at the Perimeter Institute for Theoretical Physics. This work also benefited from the Quantum Physics of Information program held at the Kavli Institute for Theoretical Physics in Santa Barbara, and from a visit by AM to the Stanford Institute for Theoretical Physics.

AM wishes to acknowledge the UBC REX program and his mentees Andrew Chun and Liam Vanderpoel, discussions with whom motivated some of the results given here. The authors would also like to thank Adrian Kent for many helpful discussions. Daniel Gottesman pointed out to us the use for the quantum one-time pad given here as figure 7. We are also grateful for discussions with Eric Hanson, Fang Xi Lin, David Stephen, Sepehr Nezami, Geoff Penington, Grant Salton and Leonard Susskind. Kevin Milner, David Wakeham, and Jason Pollack provided useful feedback on this manuscript.

Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Economic Development & Innovation. This research was supported in part by the National Science Foundation under Grant No. NSF PHY17-48958. AM was supported by a NSERC C-GSM award, later a NSERC C-GSD award, and by the It from Qubit collaboration sponsored by the Simons Foundation. PH was supported by AFOSR (FA9550-16-1-0082), CIFAR, and the Simons Foundation.

A Summoning, state-assembly and localization

In the main article we have discussed two related tasks: state-assembly and localize-exclude. A third task, summoning, has also been considered in earlier work [6]. All these tasks relate to how quantum information can move through spacetime; in this appendix we clarify the relationships among these three tasks.

The summoning task was introduced by Kent [11] and expanded on later in [6]. There are various variations on its definitions, as we discuss below. We give the definition from [6] first.

Definition 15 *A **single-call single-return summoning task** is a task involving two interacting agencies, Alice and Bob. The task is defined by*

i. A quantum system A, where Bob knows the state of the purification $|\Psi\rangle_{AR}$ and holds the R system.

ii. A start point s at which Bob gives Alice A

iii. A collection of causal diamonds D_i, each of which is defined by a call point c_i and return point r_i

At each call point c_i Alice receives a classical bit b_i. Alice is guaranteed that exactly one bit will be 1, say $b_{i^*} = 1$, and the remainder will have $b_j = 0$, but does not know the value of i^* in advance. To successfully complete the task, Alice should return the system A to the point r_{i^*} such that $b_{i^*} = 1$.

To complete the summoning task Alice must send systems sufficient to reconstruct the system through each diamond. Consequently, completing a summoning task with diamonds $\{D_i\}$ also completes an associated localize task with authorized regions $\mathscr{A}_i = D_i$. However, the reverse is not true: completing the localize task implies some collection of systems inside each authorized region can be used to construct the system, but doesn't require that this reconstruction can take place within the region. For instance, exhibiting the system could require the application of a high complexity circuit, perhaps requiring so many gates that gravitational speed limits would prevent their completion in the required time. Further, localize tasks deal with regions of arbitrary shape, whereas in a summoning task only causal diamond shaped regions are discussed.

The basic restriction on when a summoning task may be completed is the no-summoning theorem [11].

Theorem 16 *A single-call single-return summoning task with two diamonds D_1, D_2 is impossible whenever D_1 and D_2 are causally disjoint.*

Proof. Suppose there exists a protocol that returns the system to r_1 when there is a call to c_1 and returns the system to r_2 when there is a call to c_2. Then we can argue such a protocol can be used to clone a quantum system, and consequently no such protocol can exist. To see this, suppose there is a call to both c_1 and c_2. Then since D_1 and D_2 are causally disjoint, Alice's agent at D_1 cannot distinguish this case from the case where c_1 receives a call and c_2 does not. By assumption then she returns the system to r_1. Similarly, Alice's agent at D_2 returns the system at r_2. Alice has then handed over two copies of the quantum system. ■

The proof of the no-summoning theorem is similar to the proof of the no-assembly theorem we gave in the main text, see theorem 11.

Similar to the localize task, summoning is possible whenever each pair of diamonds are causally connected and every diamond has a point in the future light cone of the start point.

Theorem 17 *The single-call single-return summoning task is possible if and only if:*

i. The return point of each diamond is in the causal future of the start point.
ii. Every pair of diamonds (D_i, D_j) is causally connected.

We omit the proof of this theorem as it proceeds along now familiar lines: the many diamond case is reduced to a two diamond case by use of an error-correcting code, which

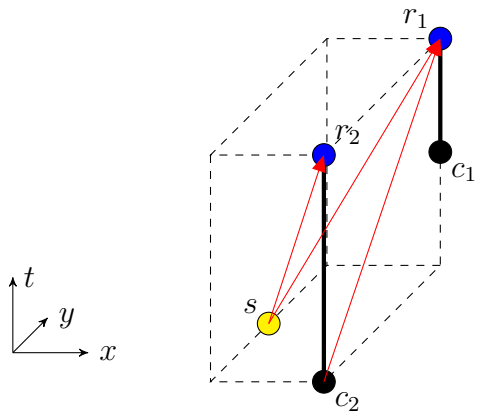

Figure 15: A summoning task on two diamonds in $2+1$ dimensions. In this task r_1 is in the future light cone of c_2, but r_2 is not in the future of c_1. (In all figures, red arrows indicate causal curves.) Additionally, r_1 and r_2 are in the future light cone of s. To complete this summoning task, Alice pre-shares entanglement between s and c_1. At s, Alice teleports the A system using the shared entanglement and then sends the classical teleportation data to both r_1 and r_2. At c_1, Alice routes the entangled particle she holds to r_1 if she receives $b_1 = 1$, and routes the particle to r_2 otherwise. This example is due to Kent [10].

can be constructed from the graph of causal connections among the regions. In the case of two diamonds we complete the task using the teleportation protocol illustrated in figure 15.

The summoning task as given above is "single-call" in that exactly one of the $b_i = 1$, and "single-return" in that the system should be returned in full at the called-to diamond. We can generalize this to allow for Alice to receive many calls (many $b_i = 1$) in two possible ways. First, we might specify that Alice return a subsystem at each called-to diamond such that taken together these subsystems can be used to reproduce the A system. In this case we have weakened the requirement on Alice — she need not hand over the quantum system itself, just quantum information and classical instructions sufficient for Bob to later construct the system. We will refer to this as many-call many-return summoning. Alternatively, we can specify that Alice hand over the system itself at one (but any one) of the called-to diamonds. We call this many-call single-return summoning. This second case is treated by Adlam and Kent [7] and discussed further in appendix B. The first case is closely related to the state-assembly task. We elaborate on this relation in the remainder of this section.

We can collect the discussion in the last paragraph into a definition of the many-call many-return summoning task.

Definition 18 *A **many-call many-return summoning task** is a task involving two interacting agencies, Alice and Bob. A task is defined by*

i. A quantum system A, where Bob knows the state of the purification $|\Psi\rangle_{AR}$ and holds the R system

ii. A start point s at which Bob gives Alice A

iii. A collection of authorized sets $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ each consisting of one or more causal diamonds, $\mathscr{A}_i = \{D_{i1}, ..., D_{ik_i}\}$

At the call point associated with each diamond Alice receives a bit b_i from Bob. Alice has a guarantee that the calls will be to one of the authorized sets of diamonds. Alice is required to return a collection of classical and quantum systems at the associated r_i which is sufficient to reconstruct A.

We characterize the many-call many-return summoning tasks which are possible and those which are impossible in the following theorem.

Theorem 19 *The many-call many-return summoning task is possible if and only if:*

i. The return point of at least one diamond from each authorized set is in the causal future of the start point.

ii. Every pair of authorized sets $(\mathscr{A}_i, \mathscr{A}_j)$ is causally connected.

Again we omit the proof, which follows the pattern of using the error-correcting code constructed from the graph of causal connections to reduce the many authorized set case to the two authorized set case. In the case of two authorized sets we use that the sets are causally connected, so in particular there exists a pair of causal diamonds chosen across the sets which are causally connected. We then complete the summoning task on these two diamonds using the teleportation protocol illustrated in figure 15.

From theorems 12 and 19 we find that state-assembly and summoning are possible for exactly the same arrangements of authorized sets. This is interesting, as although the tasks are similar they have one key distinction. In summoning Alice holds the A system of an unknown quantum state $|\Psi\rangle_{AR}$, so can't produce copies of the A system due to the linearity of quantum mechanics; in state-assembly Alice holds a known quantum state, but has the additional requirement that she hand over the A system at most once. Thus, in the assembly task the requirement that Alice hand the system over at most once replaces the no-cloning restriction. The system Alice holds is essentially classical, since it is known to her and she may produce an arbitrary number of copies, but this gives her no additional power. In this sense we can view the state-assembly task as a classical analogue of the summoning task[6].

In the main article we discussed the state-assembly task with unauthorized regions. One could also consider a generalization of the summoning task with unauthorized regions, but this generalization is less well motivated. In particular, in the summoning task Bob both gives the system to Alice and requests it from her. It is unclear in what circumstance Alice would want to hide the system Bob gave to her from Bob when certain sets of calls are made. In the assembly setting this is more natural, since Alice has herself prepared the system and may want to hide it from certain subsets of other parties.

[6]Shortly before the publication of this manuscript reference [9] appeared, which also discusses a classical version of the summoning task and its relation to the quantum one.

B Many-call single-return summoning

In appendix A we discussed the many-call many-return summoning task, which we found is closely related to the state-assembly task discussed in the main article. Many-call many-return summoning is also interesting from the viewpoint of spacetime localization. In particular, completing the many-call many-return summoning task also completes the localize task. However, a second generalization of summoning to include many-calls is possible: we can consider a task with many calls but a single return, where Alice receives several calls from Bob and must return the system in full at exactly one (but any one) of the called-to diamonds.

We give a definition of the many-call single-return summoning task below.

Definition 20 *A **many-call single-return summoning task** is a task involving two interacting agencies, Alice and Bob, defined by:*

i. A quantum system A, where Bob knows the state of the purification $|\Psi\rangle_{AR}$ and holds the R system

ii. A start point s at which Bob gives Alice system A

iii. A collection of authorized sets $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ each consisting of one or more causal diamonds, $\mathscr{A}_i = \{D_{i1}, ..., D_{ik_i}\}$

At the call point associated with each diamond Alice receives a bit b_i from Bob. Alice has a guarantee that calls will be to one of the authorized sets. To successfully complete the task, Alice must return the A system at exactly one of the called to diamonds.

As defined here, the many-call single-return summoning task is somewhat more general than the task considered by Adlam and Kent. They considered in particular the case where the set of authorized sets $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ corresponds to every possible subset of the diamonds. We refer to this as **unrestricted-call single-return** summoning.

Adlam and Kent characterized the full set of possible arrangements of diamonds for this unrestricted-call single-return summoning task [7]. We recall their theorem here.

Theorem 21 ***(Adlam and Kent 15')*** *Summoning with unrestricted calls with the requirement that Alice return the system at exactly one diamond is possible if and only if the following two conditions are true:*

i. Every return point r_i is in the future light cone of the start point s.

ii. For any subset $\{D_{i_1}, D_{i_2}, ..., D_{i_n}\}$ of diamonds, there is at least one diamond D_{i_*} in the subset for which r_{i_*} is in the future light cone of all the c_i in the subset.

Interestingly, condition (ii) above is stronger than the corresponding condition for summoning with a single call. Adlam and Kent used this fact to argue against our interpretation of summoning in terms of localization of quantum information [7]; they argue that completing the summoning task depends on some resource provided to Alice by

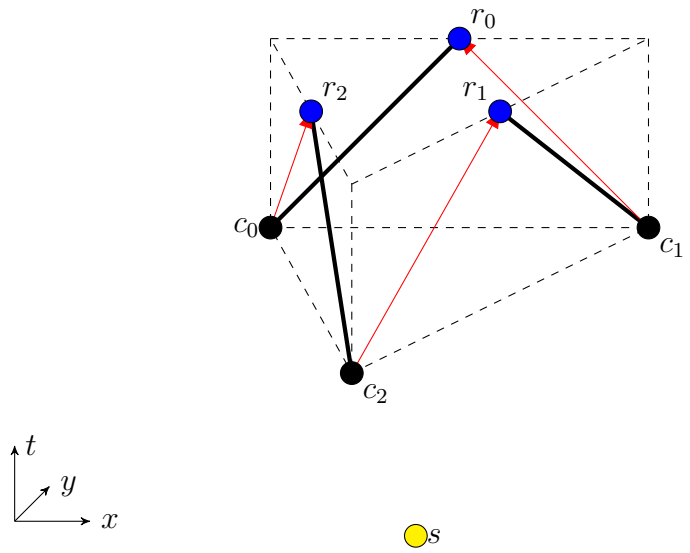

Figure 16: The three diamond task described in text. The known protocol for completing this task makes use of quantum error-correction: The system is encoded into a $((2,3))$ secret sharing scheme with one share sent to each of the call points c_i. The shares are then routed to $r_{i+1 \bmod 3}$ if $b_i = 0$, and to r_i if $b_i = 1$. This task is the simplest example of a summoning task which Alice can complete if there is a guarantee Bob will make only one call, but not if Bob may make an arbitrary number of calls.

Bob — a bit string of the form 000...010...000 — and thus that Alice is not localizing the system to each diamond. Instead, she is only successfully responding to the summons $b_i = 1$ by exploiting her knowledge that certain other calls are $b_j = 0$.

The simplest case where the conditions of many-call single-return summoning and those for many-call many-return summoning differ is the three diamond task shown in figure 16. Consider the arrangement of diamonds shown there, and take any set of diamonds to be authorized. Then to complete the many-call many-return task Alice encodes the system A into a $((2,3))$ secret sharing scheme and sends one share to each of the call points c_i. She then routes each share according to the bits b_i she receives at each point; if $b_i = 0$ she forwards the share to the next return point r_{i+1}, while if $b_i = 1$ she sends the share to the return point r_i. One can readily check that if one or two calls are sent two shares will end up at a single return point, and the system is handed over at a single diamond.

However, if a call is sent to all three diamonds, only one share ends up at each diamond. Indeed, Adlam and Kent showed that the unrestricted-call single-return task is impossible on this three diamond arrangement. This is interesting, but we argue it does not indicate that the system cannot be localized to each diamond, at least using the notion of localized we employ in this article. In the protocol using the $((2,3))$ secret sharing scheme, two shares pass through each diamond when Bob sends no calls. Someone with full access to the region enclosed by any one diamond can gather both

these shares from the secret sharing scheme and later use them to construct the system. Thus, in this sense the system is localized to all three diamonds.

When Bob sends a call, however, he may prevent the system from being reproduced in certain diamonds. This is obvious in a more prosaic example: Suppose we have two diamonds, with a diamond D_2 far in the causal future of the diamond D_1. Then Bob giving a call to D_1 results in Alice handing the system over to Bob there, and so she does not produce the system in diamond D_2. One thing that is interesting about the three diamond task, as revealed by Adlam and Kent, is that in some cases Bob's calls can prevent the system from being reproduced in any diamond. In particular this can happen in cases with cyclic connections among diamonds, as in the three diamond task.

References

[1] Ivette Fuentes-Schuller and Robert B Mann. Alice falls into a black hole: entanglement in noninertial frames. *Physical Review Letters*, 95(12):120404, 2005. URL https://doi.org/10.1103/PhysRevLett.95.120404.

[2] David Rideout, Thomas Jennewein, Giovanni Amelino-Camelia, Tommaso F Demarie, Brendon L Higgins, Achim Kempf, Adrian Kent, Raymond Laflamme, Xian Ma, Robert B Mann, et al. Fundamental quantum optics experiments conceivable with satellites reaching relativistic distances and velocities. *Classical and Quantum Gravity*, 29(22):224011, 2012. URL https://doi.org/10.1088/0264-9381/29/22/224011.

[3] Eduardo Martin-Martinez, David Aasen, and Achim Kempf. Processing quantum information with relativistic motion of atoms. *Physical Review Letters*, 110(16): 160501, 2013. URL https://doi.org/10.1103/PhysRevLett.110.160501.

[4] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. Information causality as a physical principle. *Nature*, 461(7267):1101–1104, 2009. doi:https://doi.org/10.1038/nature08400.

[5] David Beckman, Daniel Gottesman, MA Nielsen, and John Preskill. Causal and localizable quantum operations. *Physical Review A*, 64(5):052309, 2001. doi:https://doi.org/10.1103/PhysRevA.64.052309.

[6] Patrick Hayden and Alex May. Summoning information in spacetime, or where and when can a qubit be? *Journal of Physics A: Mathematical and Theoretical*, 49(17):175304, 2016. doi:https://doi.org/10.1088/1751-8113/49/17/175304.

[7] Emily Adlam and Adrian Kent. Quantum paradox of choice: More freedom makes summoning a quantum state harder. *Physical Review A*, 93(6):062327, 2016. doi:https://doi.org/10.1103/PhysRevA.93.062327.

[8] Patrick Hayden, Sepehr Nezami, Grant Salton, and Barry C Sanders. Spacetime replication of continuous variable quantum information. *New Journal of Physics*, 18(8):083043, 2016. doi:https://doi.org/10.1088/1367-2630/18/8/083043.

[9] Adrian Kent. Unconstrained summoning for relativistic quantum

information processing. *Physical Review A*, 98(6):062332, 2018. doi:https://doi.org/10.1103/PhysRevA.98.062332.

[10] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012. doi:https://doi.org/10.1088/0264-9381/29/22/224013.

[11] Adrian Kent. A no-summoning theorem in relativistic quantum theory. *Quantum information processing*, 12(2):1023–1032, 2013. doi:https://doi.org/10.1007/s11128-012-0431-6.

[12] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, 2007. doi:https://doi.org/10.1088/1126-6708/2007/09/120.

[13] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. Black holes: complementarity or firewalls? *Journal of High Energy Physics*, 2013(2):62, 2013. doi:https://doi.org/10.1007/JHEP02(2013)062.

[14] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Physical Review Letters*, 109:130501, Sep 2012. doi:https://doi.org/10.1103/PhysRevLett.109.130501.

[15] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011. doi:https://doi.org/10.1088/1367-2630/13/11/113015.

[16] Adrian Kent. Coin tossing is strictly weaker than bit commitment. *Physical Review Letters*, 83:5382–5384, Dec 1999. doi:https://doi.org/10.1103/PhysRevLett.83.5382.

[17] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95:010503, Jun 2005. doi:https://doi.org/10.1103/PhysRevLett.95.010503.

[18] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Physical Review A*, 86:062326, Dec 2012. doi:https://doi.org/10.1103/PhysRevA.86.062326.

[19] Adrian Kent. Location-oblivious data transfer with flying entangled qudits. *Physical Review A*, 84:012328, Jul 2011. doi:https://doi.org/10.1103/PhysRevA.84.012328.

[20] Damián Pitalúa-García. Spacetime-constrained oblivious transfer. *Physical Review A*, 93(6):062346, 2016. doi:https://doi.org/10.1103/PhysRevA.93.062346.

[21] Ya-Dong Wu, Abdullah Khalid, and Barry C Sanders. Efficient code for relativistic quantum summoning. *New Journal of Physics*, 20(6):063052, 2018. doi:https://doi.org/10.1088/1367-2630/aaccae.

[22] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald De Wolf. Private quantum channels. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 547–553. IEEE, 2000. doi:https://doi.org/10.1109/SFCS.2000.892142.

[23] Daniel Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61(4): 042311, 2000. doi:https://doi.org/10.1103/PhysRevA.61.042311.

[24] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 1–12. Springer, 2012. doi:https://doi.org/10.1007/978-3-642-35656-8_1.

[25] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. doi:https://doi.org/10.1145/359168.359176.

[26] Damian Markham and Barry C Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78(4):042309, 2008. doi:https://doi.org/10.1103/PhysRevA.78.042309.

[27] Pradeep Sarvepalli and Robert Raussendorf. Matroids and quantum-secret-sharing schemes. *Physical Review A*, 81(5):052333, 2010. doi:https://doi.org/10.1103/PhysRevA.81.052333.

[28] Amos Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011. doi:https://doi.org/10.1007/978-3-642-20901-7_2.

[29] Is there a studied notion of party independent transfer? https://crypto.stackexchange.com/questions/44256/is-there-a-studied-notion-of-party-independent-transfer. [Online; accessed 1-October-2017].

[30] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997. doi:https://doi.org/10.1103/PhysRevLett.78.3410.

[31] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414, 1997. doi:https://doi.org/10.1103/PhysRevLett.78.3414.

[32] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000. doi:https://doi.org/10.1038/35023282.

[33] Stephen P Jordan. Fast quantum computation at arbitrarily low energy. *Physical Review A*, 95(3):032305, 2017. doi:https://doi.org/10.1103/PhysRevA.95.032305.

[34] Leonard Susskind, Larus Thorlacius, and John Uglum. The stretched horizon and black hole complementarity. *Physical Review D*, 48(8):3743, 1993. doi:https://doi.org/10.1103/PhysRevD.48.3743.

[35] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6):85, 2013. doi:https://doi.org/10.1007/JHEP06(2013)085.

[36] Raphael Bousso. The holographic principle. *Reviews of Modern Physics*, 74(3): 825, 2002. doi:https://doi.org/10.1103/RevModPhys.74.825.