# How to share a quantum secret in spacetime


Alex May, with Patrick Hayden

arXiv:1902.06845

THE UNIVERSITY OF BRITISH COLUMBIA

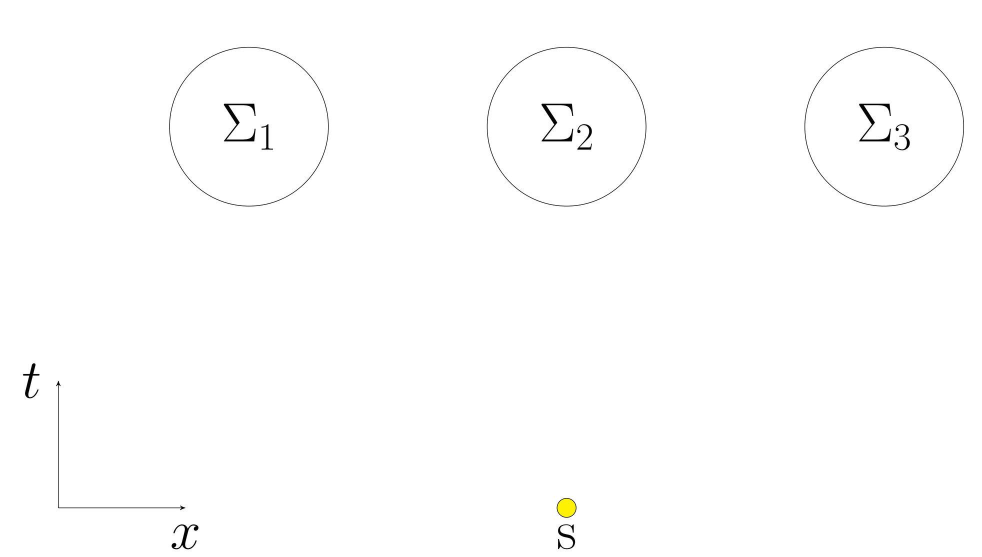

## Outline

- We define the **localize-exclude** task, wherein a quantum state should be localized to a collection of authorized spacetime regions and excluded from a collection of unauthorized regions.
- The authorized and unauthorized spacetime regions generalize the authorized and unauthorized sets of quantum secret sharing.
- Our results build on earlier work on "summoning".

## Quantum secret sharing

In quantum secret sharing, a quantum state $\rho$ is encoded into many shares $S_1, ..., S_n$ and shared among many parties Bob$_1$, Bob$_2$, ... Bob$_n$, such that specific subsets of the Bob's deemed authorized may reconstruct the state, and other subsets deemed unauthorized may not. Quantum secret sharing finds various applications in cryptography.

We may consider quantum secret sharing as a task that occurs in spacetime. Assign each Bob$_i$ a spacetime region $\Sigma_i$. Split the state $\rho$ into shares $S_i$ sent to each $\Sigma_i$ (see figure below). Collections of $\Sigma_i$ become authorized spacetime regions, other collections become unauthorized spacetime regions.




Embedding of a quantum secret sharing task into a spacetime setting. Three different parties, Bob$_1$, Bob$_2$, and Bob$_3$ control the three regions $\Sigma_1$, $\Sigma_2$, and $\Sigma_3$. Alice, who initially holds the state $\rho$ near $s$, must de-localize the state such that only certain combinations of the $\Sigma_i$ contain sufficient information to reconstruct the state.

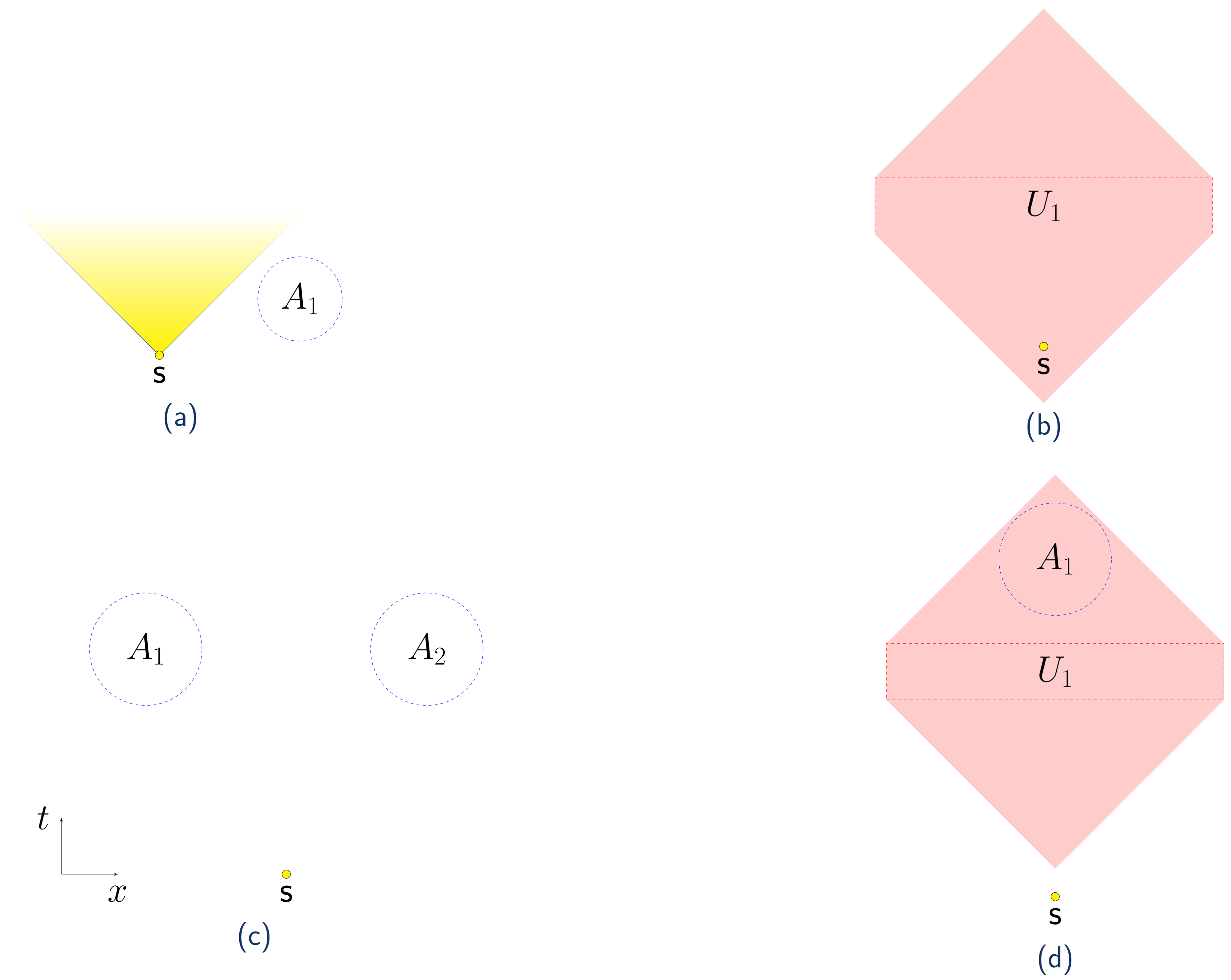



Figure: Four impossible localize-exclude tasks: (a) An authorized region is entirely outside the future light cone of $s$, so can't be localized there without violating the no-signalling principle. (b) The initial location of the quantum state is in the domain of dependence of an unauthorized region $U_1$, so can be reconstructed from data in $U_1$. (c) A quantum state cannot be localized to both the spacetime regions $A_1$ and $A_2$, due to the no-cloning theorem. (d) A quantum state cannot be localized to $A_1$ without passing through the region $U_1$, since there is no causal curve which passes through $A_1$ and not $U_1$. The red shaded region indicates the domain of dependence of the unauthorized region $U_1$. The yellow shading indicates the future light cone of the start point. Our theorem shows the localize-exclude task is possible whenever none of these scenarios occurs.

## The localize-exclude task

A state is **localized** to a region $A_i$ if it is possible to construct the state by collecting information from $A_i$ and doing later data processing. If a state is not localized somewhere, it is **excluded**.

In a localize-exclude task, Alice begins with a quantum state at a point $s$. She then must localize the state to a set of regions $\{A_i\}$ while excluding it from a second set of regions $\{U_i\}$.

The regions $A_i, U_i$ may share causal connections, overlap, and have arbitrary shape. Taking the $A_i$ and $U_i$ to be built from unions of a set of causally separated regions $\Sigma_i$ recovers quantum secret sharing.

## The localize-exclude theorem

We prove a theorem that gives if and only if conditions for a localize-exclude task to be possible for Alice to complete.

### Localize-exclude theorem

It is possible to localize a quantum state to a collection of spacetime regions $A_i$ and exclude it from another collection $U_i$ if and only if the authorized regions, unauthorized regions, and starting location of the state are such that no subset of regions has any of the four scenarios shown above occur.

## Key conclusions

- We are able to characterize all localize-exclude tasks into possible and impossible.
- Localize-exclude tasks contain secret sharing with arbitrary access structures as a special case.
- The localize-exclude theorem characterizes how quantum information can move through spacetime.
- We give variations of this task and suggest a cryptographic application in the paper version.

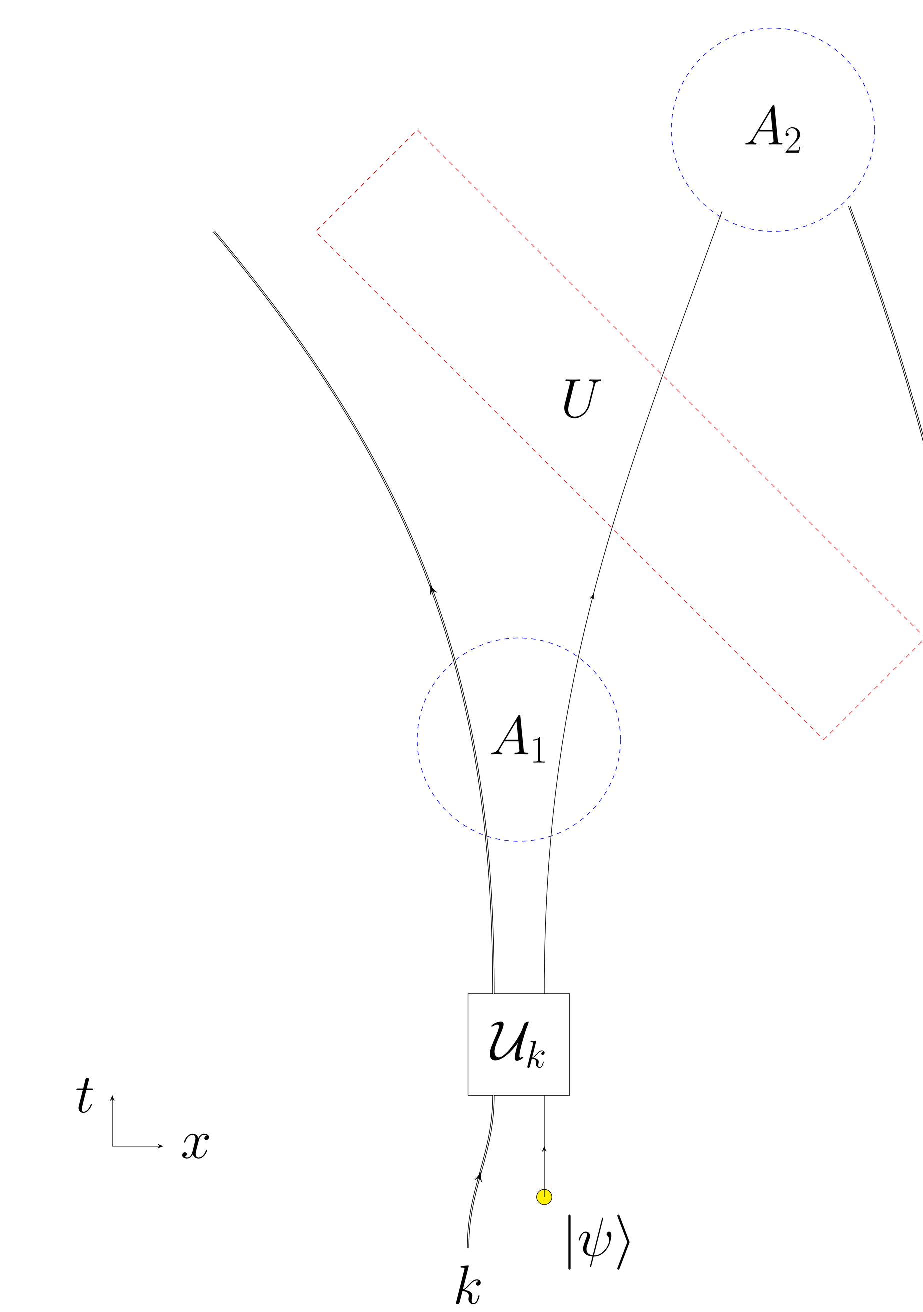



Figure: The general strategy for completing localize-exclude tasks given makes extensive use of the quantum one-time pad. Here we illustrate its use to complete a simple task with a single authorized region and two authorized regions.

## Acknowledgements


Many thanks to Adrian Kent, Daniel Gottesman, Eric Hanson, Fang Xi Lin, David Stephen, Sepehr Nezami, Geoff Penington, Grant Salton and Leonard Susskind for helpful discussions.