gives rise to secure bit co
a combination of quantu
Secure bit commitment i
chanics alone [9, 10].

Another simple examp
Figure 2. Even though t
each of the reveal points
the summoning task.
there is a causal curve pa
diamonds, then summon

SUMMONING INFORMATION IN SPACETIME

Where and when can a qubit be?

eral n can be b
$n = 2$. Encode
in an $((n-1, n)$
There are n subs

Patrick Hayden and Alex May

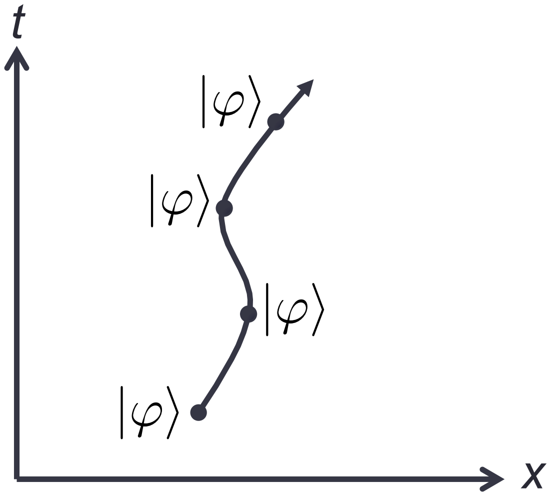
arXiv:1210.0913

Quantum information bedrock

Quantum information cannot be cloned.

Quantum information cannot be replicated in space.

And yet…

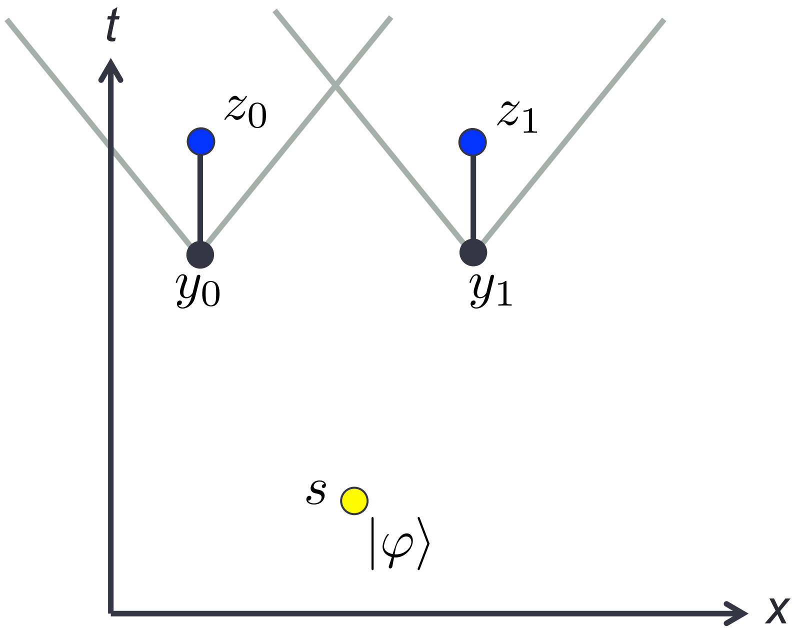


Quantum information **must** be widely replicated in space*time*.

This talk will precisely characterize which forms of replication are possible.

Goal: understand how quantum information can be delocalized in space and time

(No-)summoning



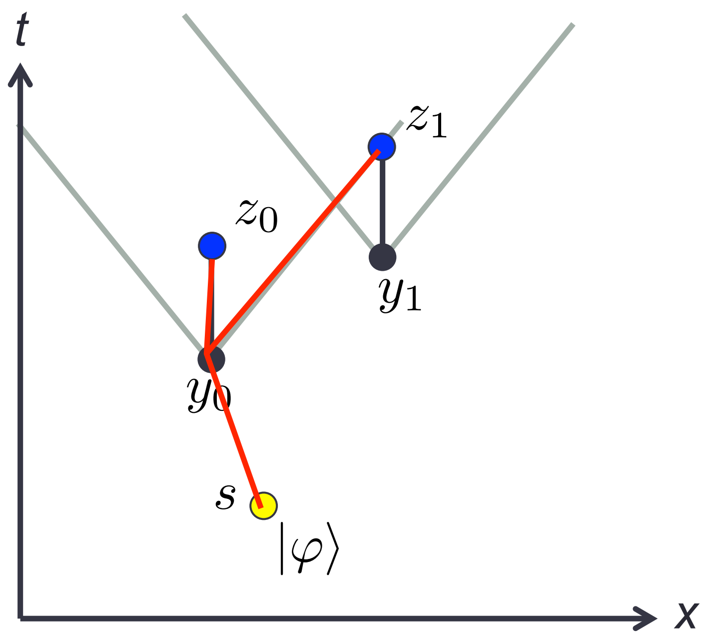
Unknown quantum state is originally localized at s.

A request for the state will be made at either y_0 or y_1, at which point the state must be exhibited at z_0 or z_1, resp.

This is prohibited by the combination of no-cloning and relativistic causality if the line segments y_0z_0 and y_1z_1 are outside each others' lightcones.

Kent : arXiv:1101.4612

(No-)summoning



Unknown quantum state is originally localized at s.

A request for the state will be made at either y_0 or y_1, at which point the state must be exhibited at z_0 or z_1, resp.

This is possible if…?

Summoning is possible iff z_1 is in the future of y_0 or z_0 is in the future of y_1.

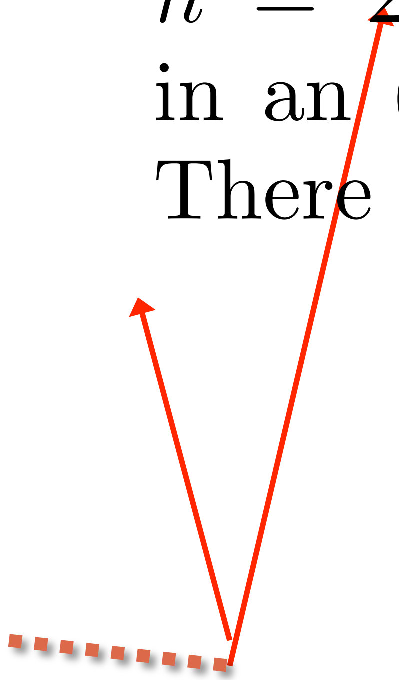
General solution: Exploiting teleportation

eral n can b

$n = 2.$ E

in an $((n$ -

There are n



Request arrives at y_0 or y_1

Causality prevents direct transmission of φ from s to the correct z_0 or z_1

Instead, a Bell pair is shared between s and y_0

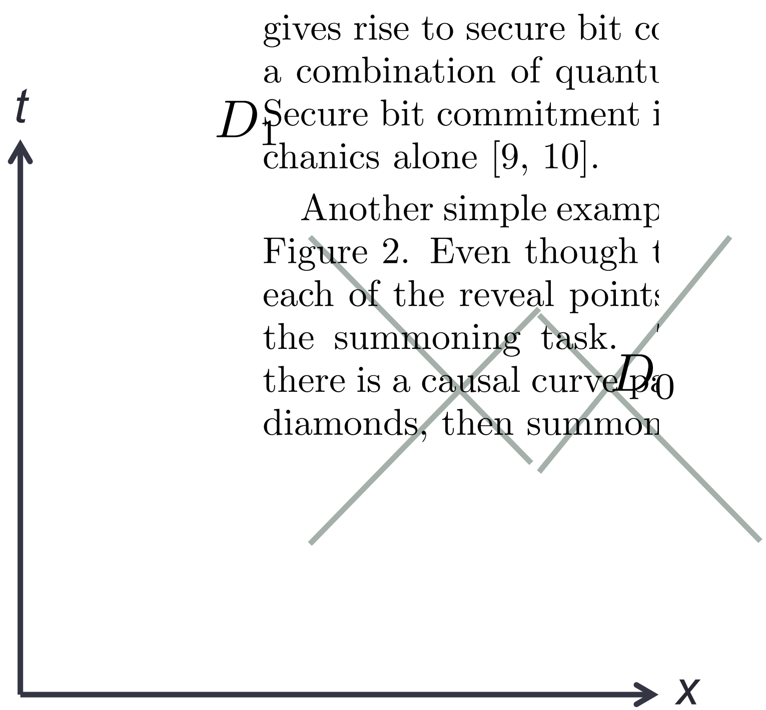
Teleportation performed at s, with measurement outcome forwarded to both z_0 and z_1

Half of Bell pair at y_0 sent to either z_0 or z_1 depending on request

Classical data: unconstrained by no-cloning
Entanglement: unconstrained by causality

Kent : arXiv:1204.4022

Summoning as replication



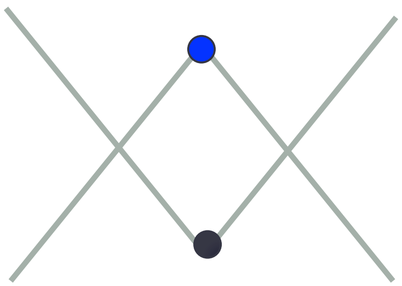
Summoning is possible iff z_1 is in the future of y_0 or z_0 is in the future of y_1.

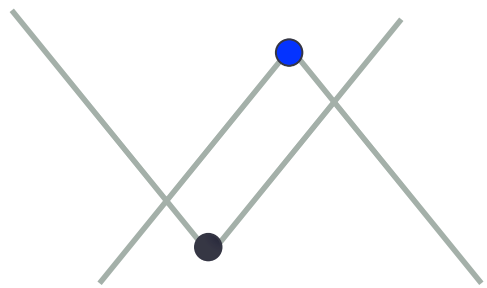
Define causal diamond D_j to be the intersection of the future of y_j and the past of z_j -- the points that can both be affected by the request at y_j and can affect the outcome at z_j.

Summoning is possible iff the *causal diamonds* D_0 and D_1 are causally related: there exists a causal curve from D_0 to D_1 or vice-versa.

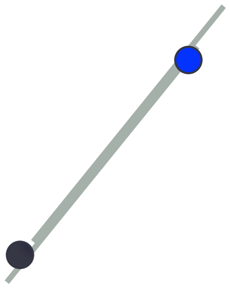
Summoning provides an operational definition of what it means for quantum information to be localized in the diamond D_j.

Causal diamond geometry





Diamond becomes a line segment when top and bottom are lightlike separated:



Exploiting quantum error correction

a combination of quantum
Secure bit commitment is in
chanics alone [9, 10].

Another simple example i
Figure 2. Even though ther
each of the reveal points, it
the summoning task. The
there is a causal curve passi
diamonds, then summoning

A ((2,3)) threshold quantum secret sharing scheme is prepared at s

One share sent to each of y_j

Each share is then sent at the speed of light along a red line

2 shares pass through each causal diamond $y_j z_j$

The same quantum information is replicated in each causal diamond

Summoning language: if a request is made at y_j then the share at y_j is sent to z_j instead of to z_{j-1}

A more complicated scenario:

so each vertex is incid
number of edges is (
must be recoverable f
total number of shares

eral n can be b
$n = 2$. Encode
in an $((n-1, n))$
There are n subs

?:
All diamonds are causally related

Each and every diamond can contain the same quantum information iff every pair is causally related

Equivalently: iff there is no *obvious* violation of causality or no-cloning

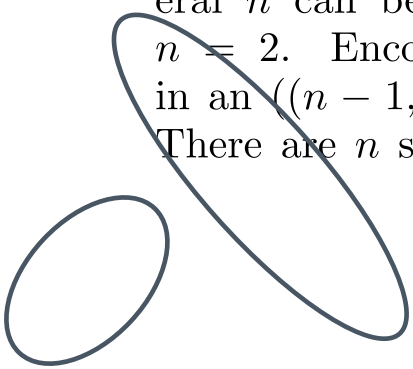
Information replication: the general case

Each and every causal diamond can contain the same quantum information if and only if every pair is causally related.

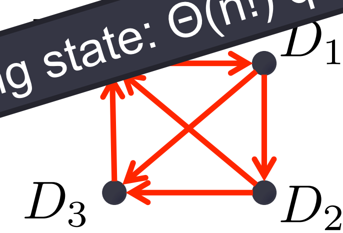
Proof: For n=2, the teleportation strategy works for any pair of diamonds

Assume the existence of a protocol for sets of n-1 diam

eral n can be b
$n = 2$. Encode
in an $((n-1, n))$
There are n subs

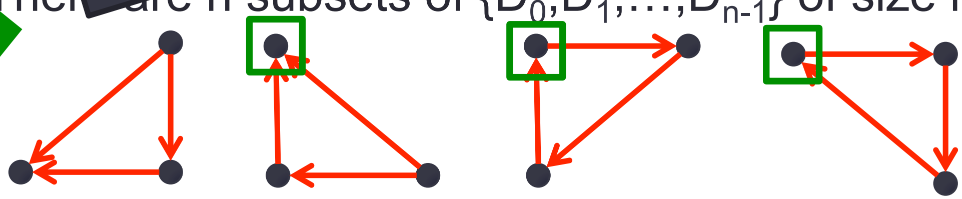


Graph of causal relation



BAD: Size of secret sharing state: Θ(n!) qubits

There are n subsets of $\{D_0, D_1, \ldots, D_{n-1}\}$ of size n-1.



Request at y_0

z_0 receives n-1 shares

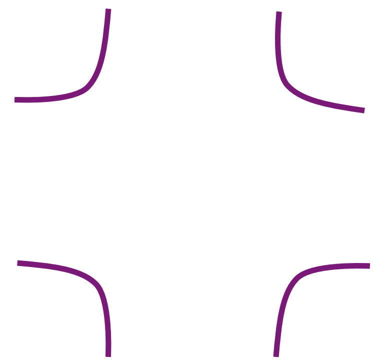
Encode φ into an ((n-1,n)) threshold secret sharing scheme.

Associate one share to each such subset and for each subset execute the protocol recursively with one diamond removed.

Efficient protocol

$n = 2$. Enc
in an $((n - 1$
There are n

G = (V,E) graph of
causal relationships:



Encode φ into a quantum error correcting code with one share for each edge.

Code property: φ can be recovered provided all the shares associated to any D_j

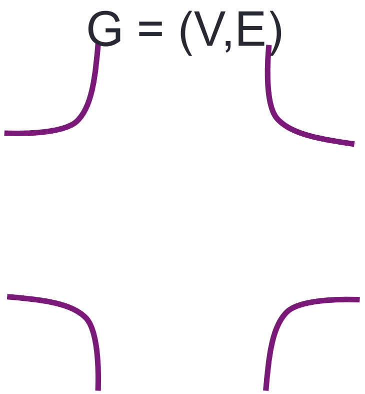
Execute the n=2 teleportation protocol for each edge.

If request made at y_j, then z_j receives all shares associated to D_j and can recover φ.

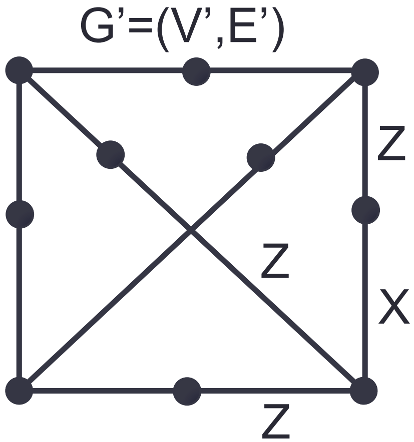
Unusual QEC: ~n^2 shares but recovery using n-1. Vanishing fraction O(1/n).

The quantum error correcting code

Designed using the codeword-stabilized (CWS) quantum code formalism [CSSZ'08]



Subdivide every edge:



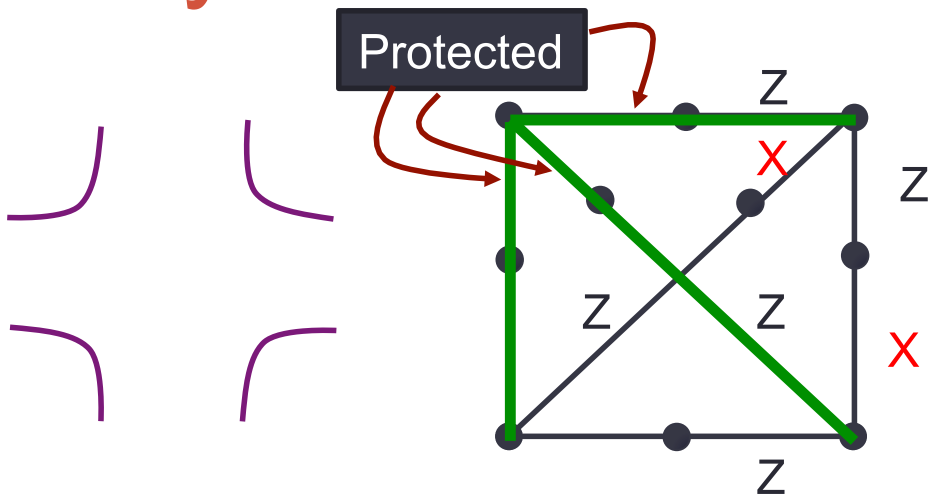
One qubit for each edge of G': |E'| = n(n-1)

Define commuting operators $S_e = X_e \prod_{f \in N_e} Z_f$

Code subspace is the span of the simultaneous +1 and -1 eigenspaces of all S_e.

Each share consists of the 2 qubits associated with each original edge of G.

Analysis of the code



CWS code property:
All errors converted to Z errors

For Pauli error P:
Err(P) = induced Z error

Condition 1: $\mathrm{Err}(P) \neq \prod_e Z_e$

Condition 2: If $\mathrm{Err}(P) = I$ then $[\prod_e Z_e, P] = 0.$

- Every possible X error induces exactly one Z error on a green edge
- To achieve Err(P) = I, need an *even* number of X errors.
- XZ=-ZX implies that if P contains an even number of X errors, then $[\Pi_e Z_e, P]=0$

Conclusions

- Quantum information can be replicated in a surprising variety of ways in spacetime
- The only constraints on replication are the simplest ones: there can be no obvious violations of no-cloning or causality
- Using the same code, the result can be extended to non-convex regions, giving an alternate proof of quantum secret sharing using general access structures
- Future directions:
  - Applications to cryptography in Minkowski (and more general) spacetime
  - Cloning paradoxes in black hole evaporation, complementarity, firewalls, etc.

Recruitment opportunity of the year:

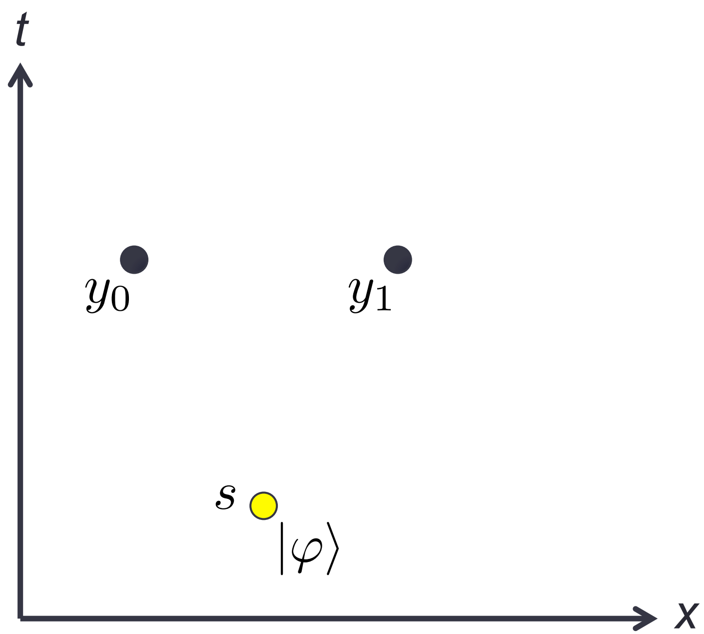
- Alex May: extraordinary undergraduate student

Lessons for complementarity?

eral n can be b
$n = 2$. Encode
in an $((n-1, n))$
There are n subs

- Surprising replication of quantum information is possible if time is considered
- The actions required to localize the information to specific points z_j will generally destroy the replication
- Firewalls:
  - Staying outside BH or falling in constitutes a choice analogous to localizing the information at a particular z_j
  - Simulating N_b measurement on early radiation could destroy replication

(No-)summoning



Unknown quantum state is originally localized at s.

A request for the state will be made at either y_0 or y_1, at which point the state must be exhibited there.

This is prohibited by the combination of no-cloning and relativistic causality.

Kent uses no-summoning as the basis for a quantum relativistically secure bit commitment protocol.

Kent : arXiv:1101.4612