Title: Talk 120 - Security of position-based cryptography limits Hamiltonian simulation via holography

Speakers:

Collection: It from Qubit 2023

Date: August 01, 2023 - 4:00 PM

URL: https://pirsa.org/23080006

Abstract: We investigate the link between position-based quantum cryptography (PBQC) and holography established in [May19] using holographic quantum error correcting codes as toy models. If the "temporal" scaling of the AdS metric is inserted by hand into the toy model via the bulk Hamiltonian interaction strength we recover a toy model with consistent causality structure. This leads to an interesting implication between two topics in quantum information: if position-based cryptography is secure against attacks with small entanglement then there are new fundamental lower bounds for resources required for one Hamiltonian to simulate another.

UCL

Security of Position Based Cryptography and Hamiltonian Simulation via Holography

Harriet Apel

Joint work with Toby Cubitt (UCL), Patrick Hayden (Stanford)
Tamara Kohler (ICMAT, Madrid) & David Pérez-Garcia (ICMAT, Madrid)

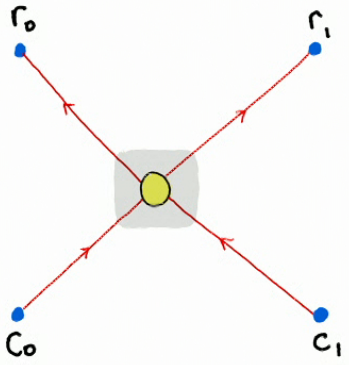
↳ thanks to insights from Kfir Dolev into PBQC.

UCL

POSITION BASED QUANTUM CRYPTOGRAPHY

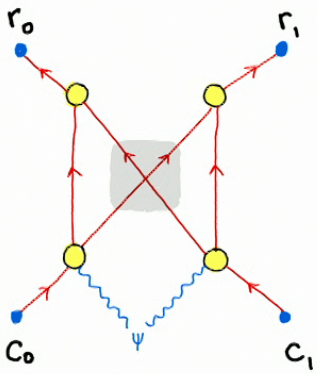
PBQC uses the prover's position in space time as its credential

LOCAL



HONEST PROTOCOL

↳ local unitary on n qubits



NON-LOCAL

NON-LOCAL ATTACK

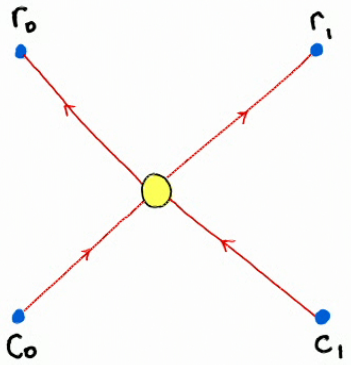
↳ uses shared entanglement and a round of communication

UCL

POSITION BASED QUANTUM CRYPTOGRAPHY

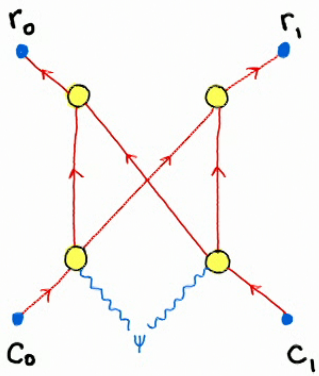
PBQC uses the prover's position in space time as its credential

LOCAL



HONEST PROTOCOL

↳ local unitary on n qubits



NON-LOCAL

NON-LOCAL ATTACK

↳ uses shared entanglement and a round of communication

Known bounds on security of PBQC for general local unitary

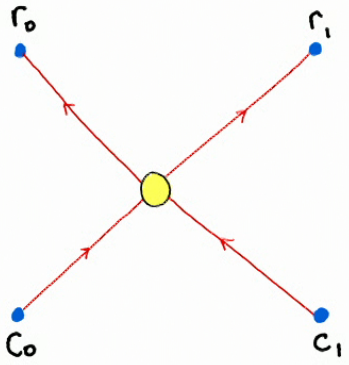
$O(n)$ < minimal amount of entanglement for successful attack < $O(\exp(n))$

UCL

POSITION BASED QUANTUM CRYPTOGRAPHY

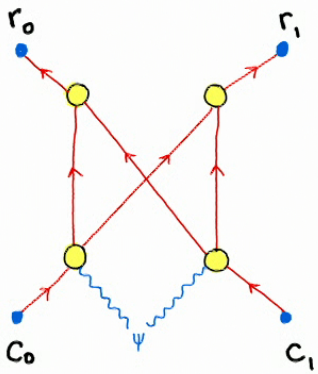
PBQC uses the prover's position in space time as its credential

LOCAL



HONEST PROTOCOL

↳ local unitary on n qubits



NON-LOCAL

NON-LOCAL ATTACK

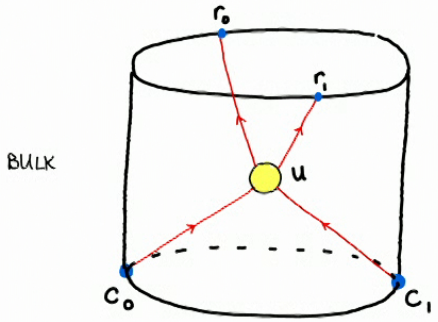
↳ uses shared entanglement and a round of communication

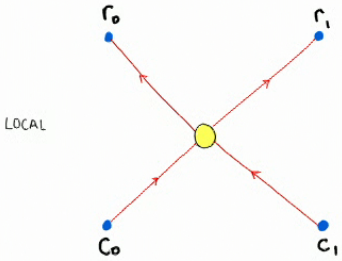
Known bounds on security of PBQC for general local unitary

$O(n)$ < minimal amount of entanglement for successful attack < $O(\exp(n))$

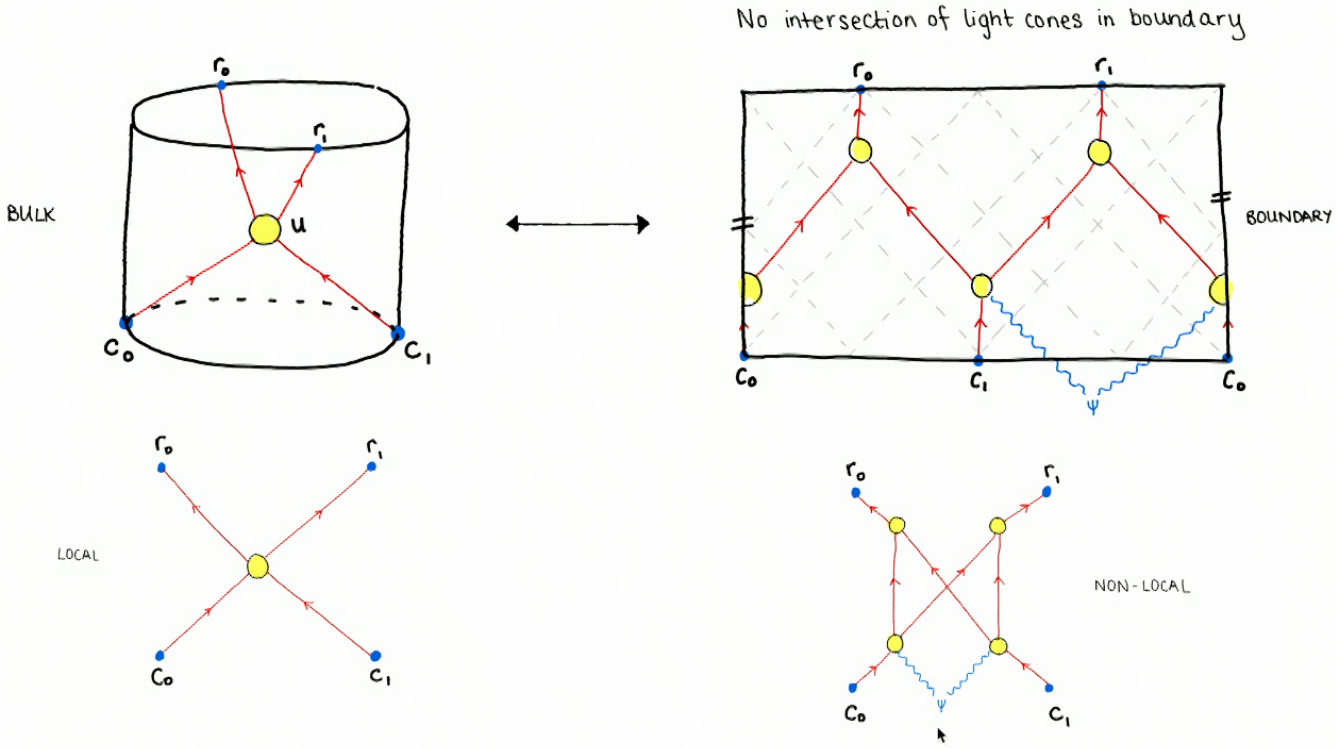
* $O(\exp(n))$ <

AN ATTACK FROM HOLOGRAPHY [May 19]

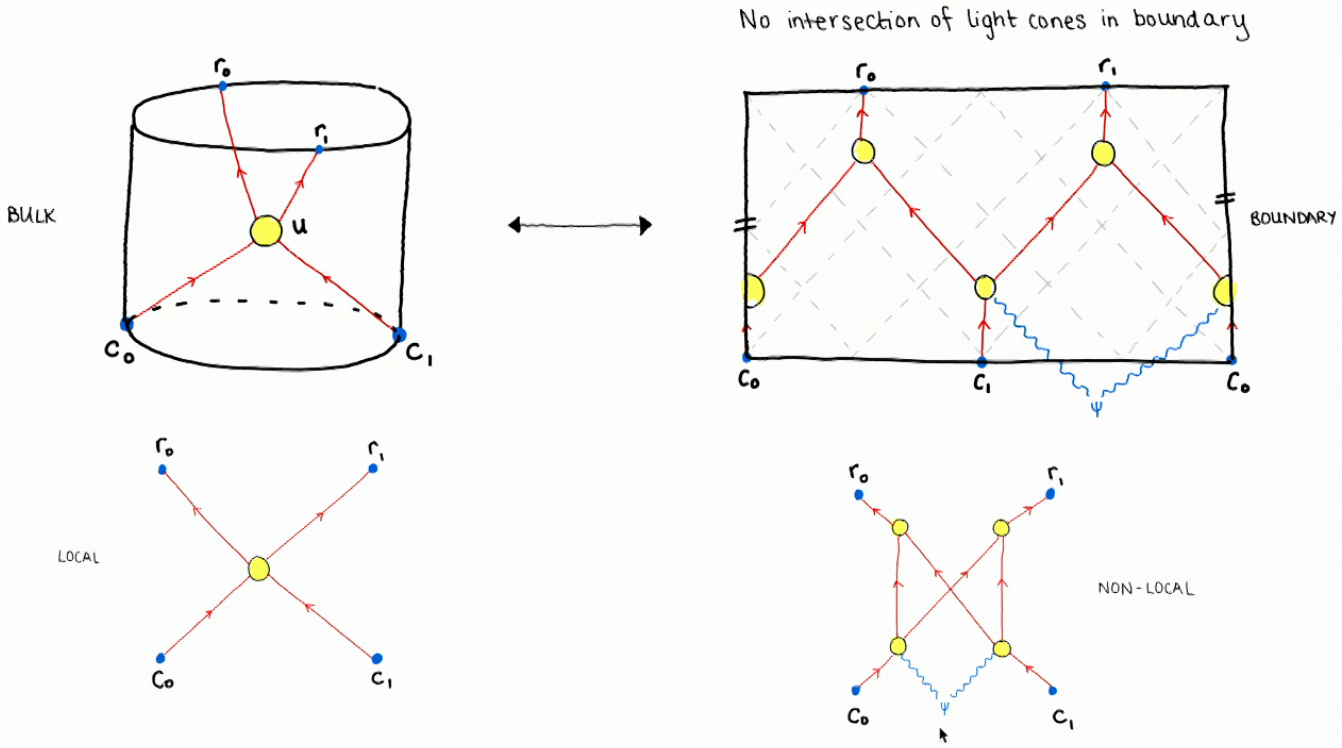




AN ATTACK FROM HOLOGRAPHY [May 19]



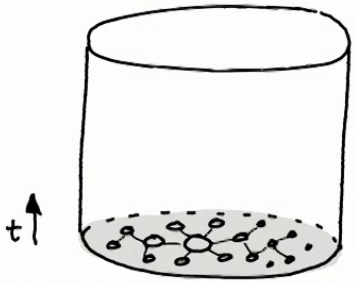
AN ATTACK FROM HOLOGRAPHY [May 19]



If unrestricted local unitary, would be a new PBQC attack using linear entanglement => NOT SECURE

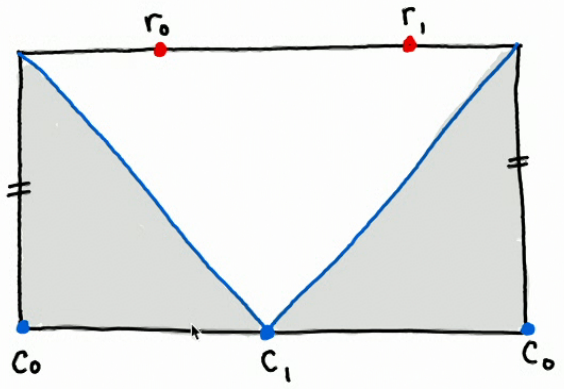
Using entanglement structure of AdS/CFT argued. O(n) entanglement between boundary regions

ATTACK IN TENSOR NETWORKS ?

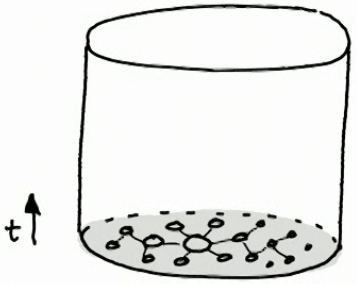


- The tensor network describes a space-like slice of AdS spacetime.
- Map the Hamiltonian/state once then time evolve.

- Essential that there is no overlapping region of causal cones in the boundary where the unitary could be implemented locally.



ATTACK IN TENSOR NETWORKS ?

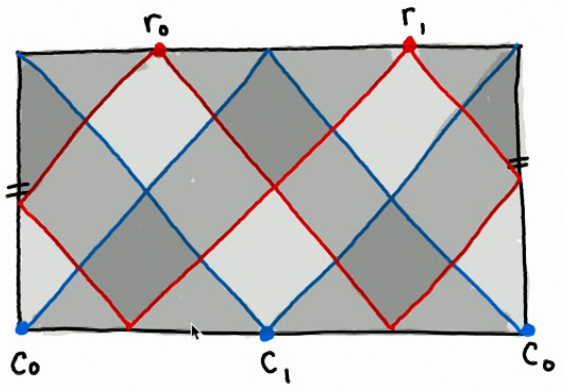


→ The tensor network describes a space-like slice of AdS spacetime.

→ Map the Hamiltonian/state once then time evolve.

→ Essential that there is no overlapping region of causal cones in the boundary where the unitary could be implemented locally.

→ There exist models with a local boundary Hamiltonian – is this enough to recover consistent bulk/boundary causality? No!



UCL

OUTLINE

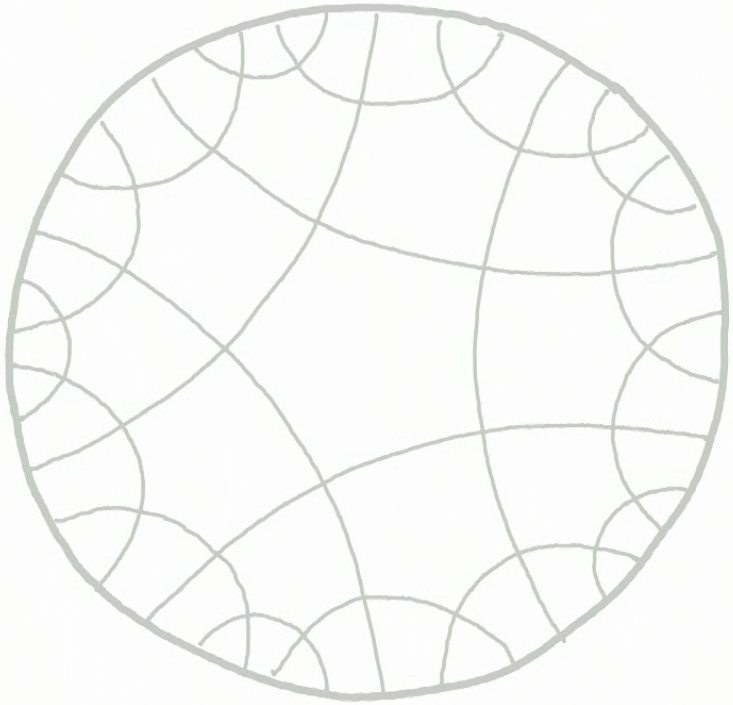
1. Recover some consistent causality features in a tensor network model of holography

2. Can we use these toy models to construct an attack on position based cryptography

UCL

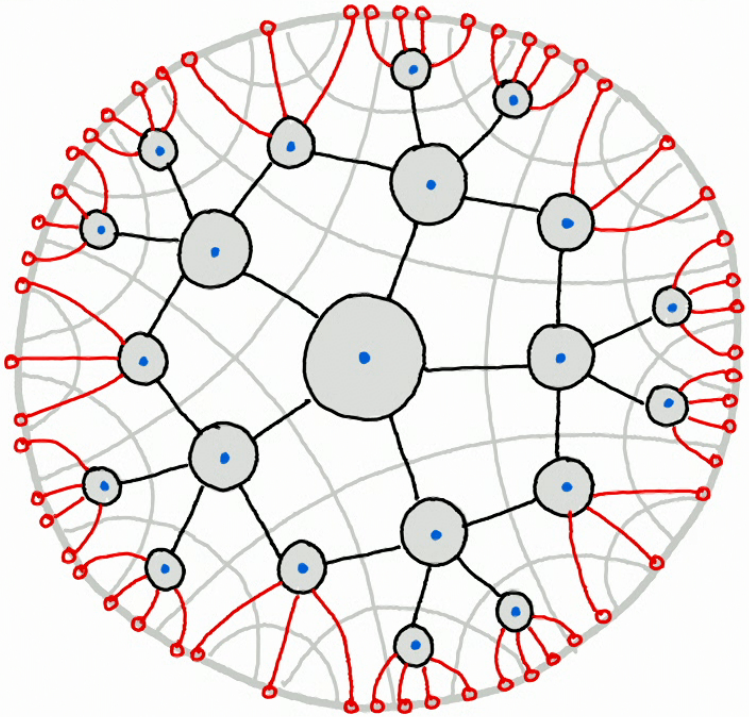
HOLOGRAPHIC TENSOR NETWORKS

[HaPPY 2015]



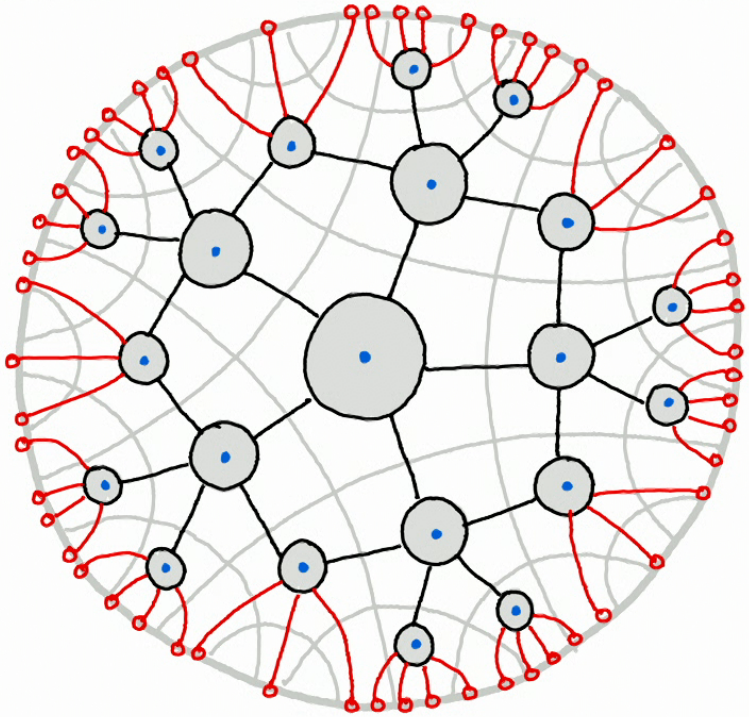
UCL

HOLOGRAPHIC TENSOR NETWORKS [HaPPY 2015]



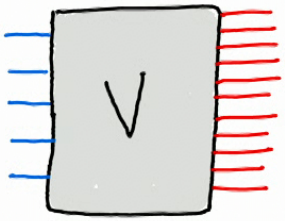
- Bulk degrees of freedom
  LOGICAL QUBITS
- Boundary degrees of freedom
  PHYSICAL QUBITS

HOLOGRAPHIC TENSOR NETWORKS [HaPPY 2015]

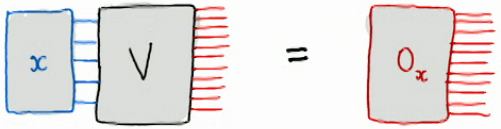


Tensor network describes a map

$\cong$



Operators are pushed through the network



Bulk operator

Boundary operator

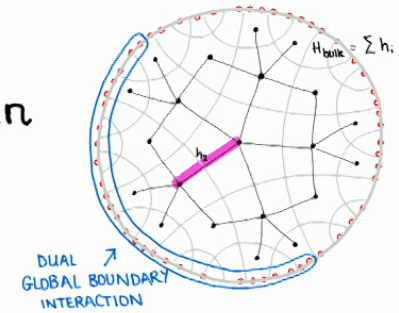
- Bulk degrees of freedom
  LOGICAL QUBITS
- Boundary degrees of freedom
  PHYSICAL QUBITS

UCL

BOUNDARY SUPERLUMINAL SIGNALLING

→ The first models mapped a local bulk Hamiltonian to a non-local boundary Hamiltonian

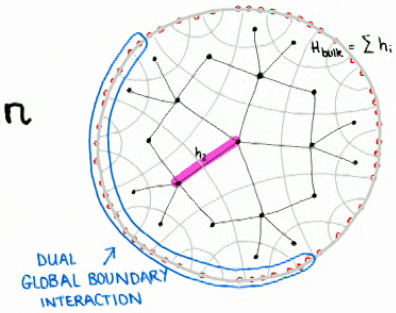
↳> Hamiltonian doesn't respect boundary metric so no causal structure



BOUNDARY SUPERLUMINAL SIGNALLING

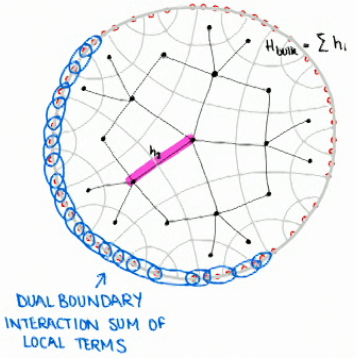
→ The first models mapped a local bulk Hamiltonian to a non-local boundary Hamiltonian

↳> Hamiltonian doesn't respect boundary metric so no causal structure



→ Later models achieve a geometrically local boundary Hamiltonian dual to the bulk. [KC19]

↳> meaningful concept of boundary distance but large interaction strengths result in information on the boundary theory propagating "too fast"

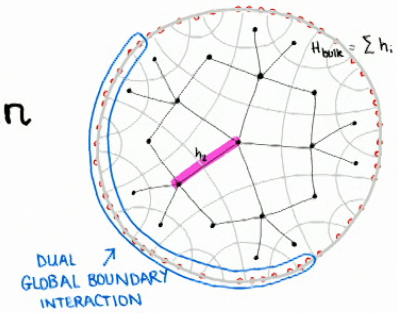


UCL

BOUNDARY SUPERLUMINAL SIGNALLING

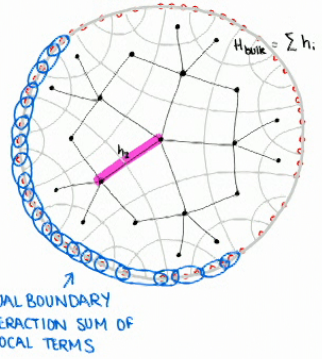
→ The first models mapped a local bulk Hamiltonian to a non-local boundary Hamiltonian

↳> Hamiltonian doesn't respect boundary metric so no causal structure

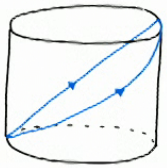


→ Later models achieve a geometrically local boundary Hamiltonian dual to the bulk.

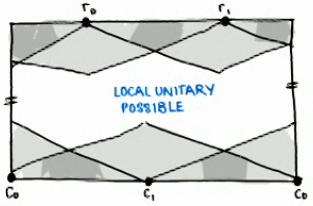
↳> meaningful concept of boundary distance but large interaction strengths result in information on the boundary theory propagating "too fast"



① inconsistent with bulk



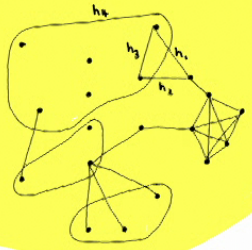
② no PBQC attack



UCL

HAMILTONIAN SIMULATION

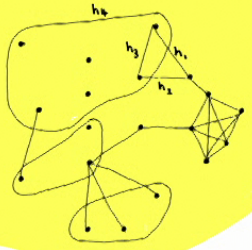
$H = \sum_i h_i$, Complex Hamiltonian with interesting physics



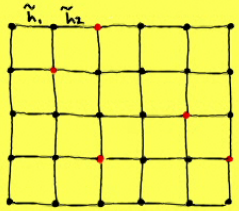
UCL

HAMILTONIAN SIMULATION

$H = \sum_i h_i$, Complex Hamiltonian with interesting physics



$\tilde{H} = \sum_i \tilde{h}_i$, Simulator Hamiltonian on a lattice

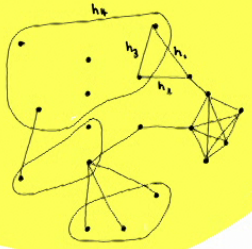


Engineer $\tilde{h}_i$'s so that $\tilde{H}$ has approximately the same physics as H

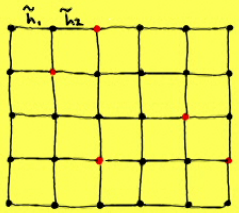
UCL

HAMILTONIAN SIMULATION

$H = \sum_i h_i$, Complex Hamiltonian with interesting physics



$\tilde{H} = \sum_i \tilde{h}_i$, Simulator Hamiltonian on a lattice



Engineer $\tilde{h}_i$'s so that $\tilde{H}$ has approximately the same physics as H

→ Approximately the same measurement outcomes

→ Approximately preserved thermal properties

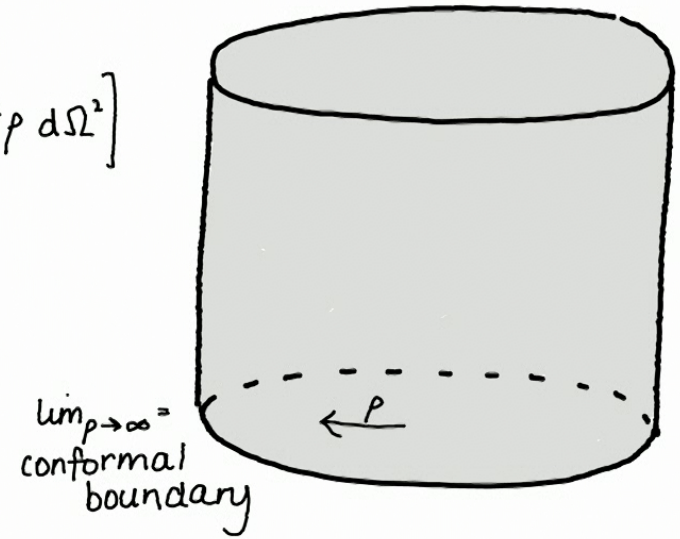
→ Approximately preserved time dynamics

UCL

BACK TO AdS/CFT...

The bulk spacetime is described by the AdS metric

$$ds^2 = \alpha^2\left[-\cosh^2\rho\, dt^2 + d\rho^2 + \sinh^2\rho\, d\Omega^2\right]$$



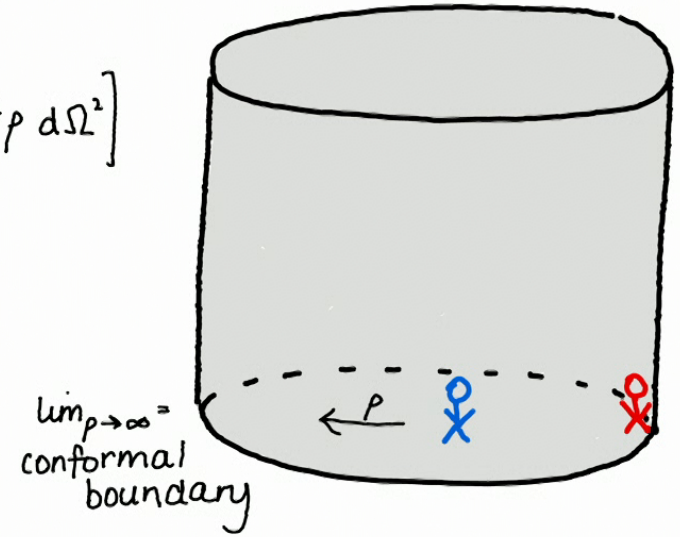
UCL

BACK TO AdS/CFT...

The bulk spacetime is described by the AdS metric

$$ds^2 = \alpha^2\left[-\cosh^2\rho\, dt^2 + d\rho^2 + \sinh^2\rho\, d\Omega^2\right]$$

time is dilated in the centre of the bulk

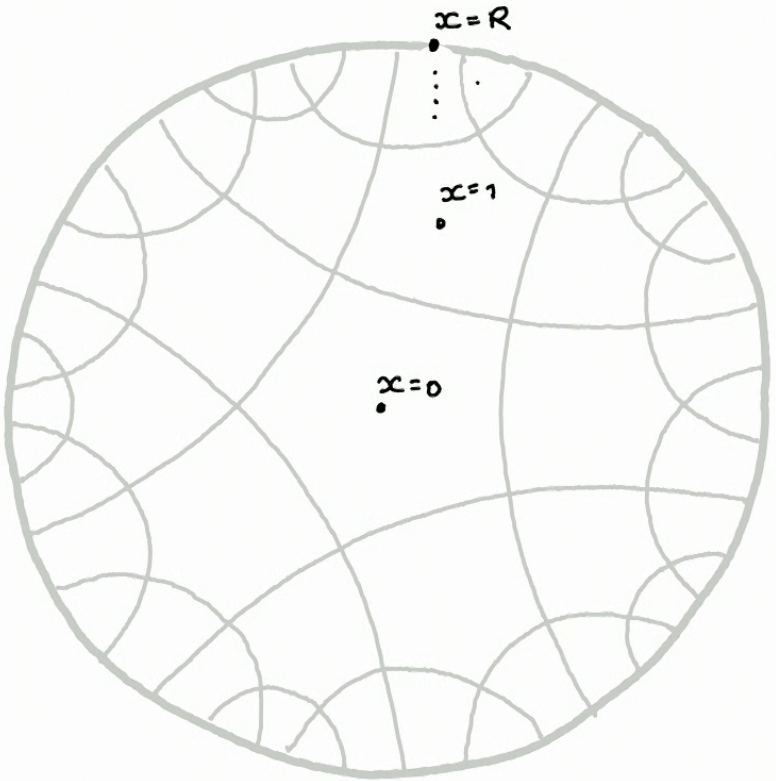


STATIONARY OBSERVER AT ρ_0 with coordinate time t_0

STATIONARY OBSERVER AT ρ_1 with coordinate time t_1

$$dt_0 = \frac{\cosh\rho_1}{\cosh\rho_0}\, dt_1 \sim e^{\rho_1-\rho_0}\, dt_1$$

TIME DILATION IN THE MODEL



$$dt_0 = \frac{\cosh \rho_1}{\cosh \rho_0} dt_1 \sim e^{\rho_1 - \rho_0} dt_1$$

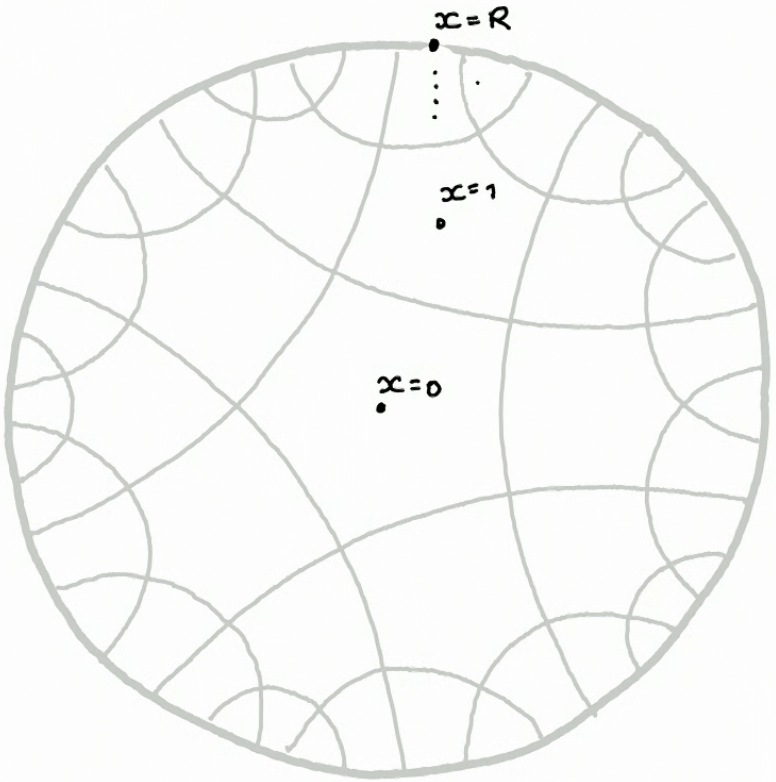
Translating to model parameters carefully ...

Coordinate time at truncated boundary t_R is related to bulk coordinate time at the x'th tensor layer

$$t_x \sim \tau^{R-x} t_R$$

τ is curvature proxy in model.

TIME DILATION IN THE MODEL



$$dt_0 = \frac{\cosh \rho_1}{\cosh \rho_0} dt_1 \sim e^{\rho_1 - \rho_0} dt_1$$

Translating to model parameters carefully ...

Coordinate time at truncated boundary t_R is related to bulk coordinate time at the x'th tensor layer

$$t_x \sim \tau^{R-x} t_R$$

τ is curvature proxy in model.

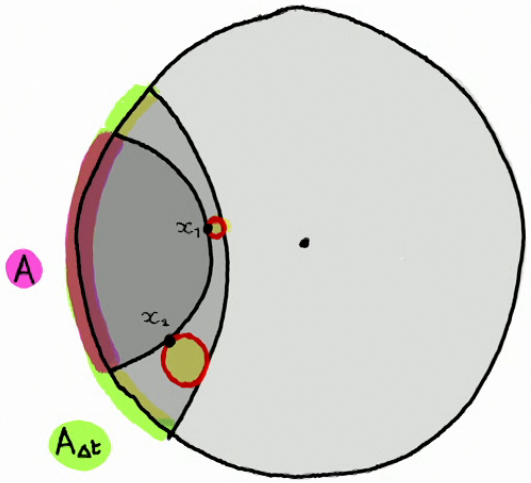
Insert time dilation by hand with bulk interaction terms decaying exp towards the centre of the bulk

$$\| h_x \| = O(\tau^{x-R})$$

UCL

BUTTERFLY VELOCITY ARGUMENT

Butterfly velocity → limits the propagation of information when restricted to the codespace on the boundary.

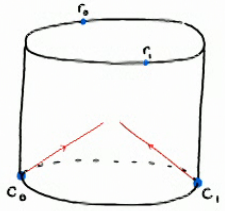


UCL

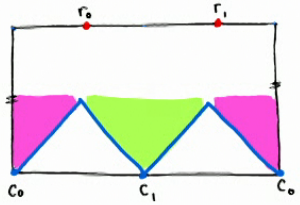
THE PROPOSED ATTACK IN TOY MODELS

① PROPAGATE IN

Local SWAPS with exp decaying weight translate inputs to the centre of the bulk.



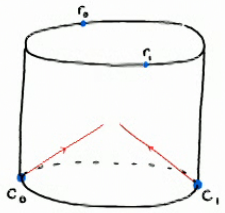
Boundary butteryfly velocity obey straight light cones.



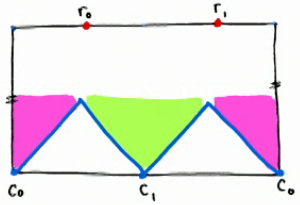
THE PROPOSED ATTACK IN TOY MODELS

① PROPAGATE IN

Local SWAPS with exp decaying weight translate inputs to the centre of the bulk.

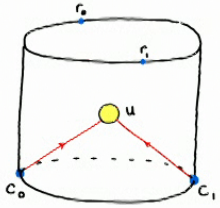


Boundary butteryfly velocity obey straight light cones.

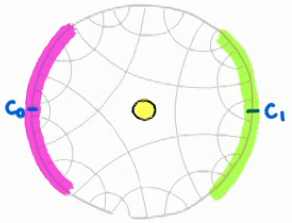


→ ② SIMULATE UNITARY

General local unitary U generated by n-local bulk Hamiltonian H.



Tensor network map → tensor product operator over two regions

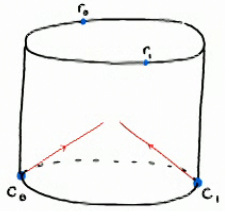


Need a GOOD simulator to keep boundary causal.

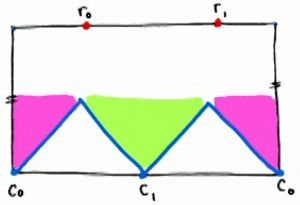
THE PROPOSED ATTACK IN TOY MODELS

① PROPAGATE IN

Local SWAPS with exp decaying weight translate inputs to the centre of the bulk.

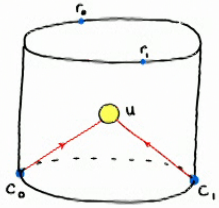


Boundary butteryfly velocity obey straight light cones.

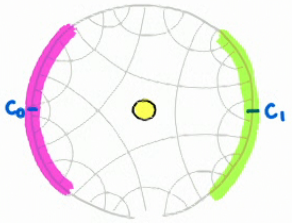


→ ② SIMULATE UNITARY

General local unitary U generated by n-local bulk Hamiltonian H.



Tensor network map → tensor product operator over two regions



Need a GOOD simulator to keep boundary causal.

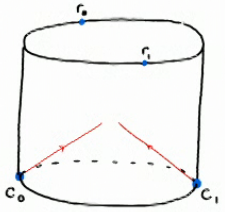
Note: Hamiltonian at this step exp small but higher weight SWAPS "turned off" here so not washed out: time dep bulk Hamiltonian.

UCL

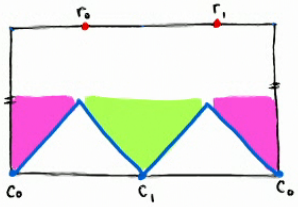
THE PROPOSED ATTACK IN TOY MODELS

① PROPAGATE IN

Local SWAPS with exp decaying weight translate inputs to the centre of the bulk.



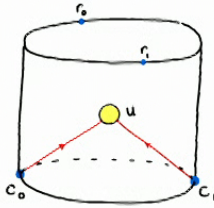
Boundary butteryfly velocity obey straight light cones.



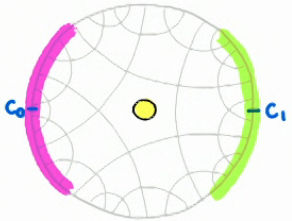
→

② SIMULATE UNITARY

General local unitary U generated by n-local bulk Hamiltonian H.



Tensor network map → tensor product operator over two regions

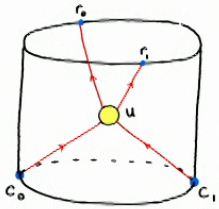


Need a GOOD simulator to keep boundary causal.

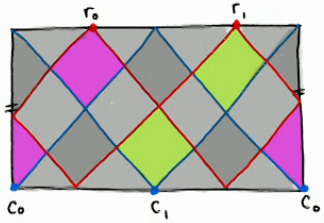
→

③ PROPAGATE OUT

Local SWAPS again to deliver outputs

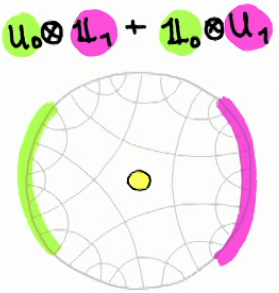


Causal structure on boundary maintained during protocol.



Tensor network obeys RT so can bound entanglement of non-local attack.

CASES TO CONSIDER



(1) PBQC known to be insecure

→ bulk unitary produces non-interacting Boundary Hamiltonian

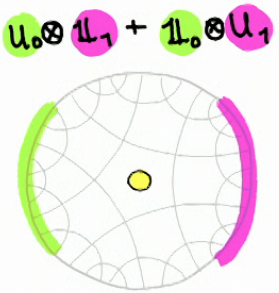
→ bulk unitary has low complexity - generated by a very weak Hamiltonian

CASES TO CONSIDER

① PBQC known to be insecure

→ bulk unitary produces non-interacting Boundary Hamiltonian

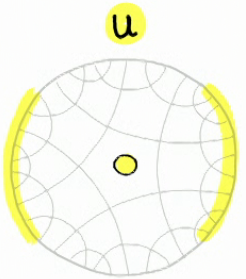
→ bulk unitary has low complexity - generated by a very weak Hamiltonian



② PBQC security not known with linear entanglement

→ with $\|H_{bulk}\| = \frac{4I^{-R}}{cn}$ can do arbitrarily complex unitary

→ $\|H_{boundary}\| = \frac{4I^{-R}}{cn}$ but need to simulate with a local Hamiltonian with particular properties to maintain causality



UCL

HOW GOOD CAN HAMILTONIAN SIMULATIONS BE ?

- To maintain causal structure during boundary implementation of U require a simulating Hamiltonian that is geometrically 2-local
* with interaction strengths scaling as $\text{poly}\left[\frac{n^a}{\varepsilon^b}\|H_{target}\|\right]$ with $a+b\leq 1$ while ε-simulating a $O(n)$ local Hamiltonian, H_{target}

UCL

HOW GOOD CAN HAMILTONIAN SIMULATIONS BE ?

- To maintain causal structure during boundary implementation of U require a simulating Hamiltonian that is geometrically 2-local
* with interaction strengths scaling as $\text{poly}\left[\frac{n^a}{\varepsilon^b}\|H_{target}\|\right]$ with $a+b\leq 1$ while ε-simulating a $O(n)$ local Hamiltonian, H_{target}

- We construct new universal simulation techniques that are exponentially better than existing methods given the boundary Hamiltonian is sparse however can only ACHIEVE $a+b=1.5$

UCL

HOW GOOD CAN HAMILTONIAN SIMULATIONS BE ?

- To maintain causal structure during boundary implementation of U require a simulating Hamiltonian that is geometrically 2-local
* with interaction strengths scaling as $\text{poly}\left[\frac{n^a}{\varepsilon^b}\|H_{target}\|\right]$ with $a+b\leq 1$ while ε-simulating a $O(n)$ local Hamiltonian, H_{target}

- We construct new universal simulation techniques that are exponentially better than existing methods given the boundary Hamiltonian is sparse however can only ACHIEVE $a+b=1.5$

- Can argue via Lieb-Robinson bounds that simulations with properties * cannot exist with controllable error in the state
  ↳ giving a lower bound on how good simulators can be

UCL

HOW GOOD CAN HAMILTONIAN SIMULATIONS BE ?

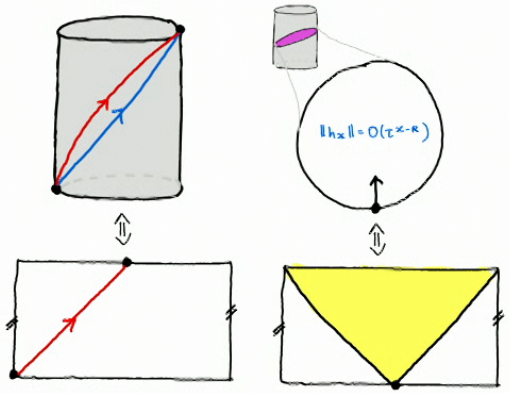
*
- To maintain causal structure during boundary implementation of U require a simulating Hamiltonian that is geometrically 2-local with interaction strengths scaling as $\text{poly}\left[\frac{n^a}{\varepsilon^b}\|H_{target}\|\right]$ with $a+b\leq 1$ while ε-simulating a $O(n)$ local Hamiltonian, H_{target}

- We construct new universal simulation techniques that are exponentially better than existing methods given the boundary Hamiltonian is sparse however can only ACHIEVE $a+b=1.5$

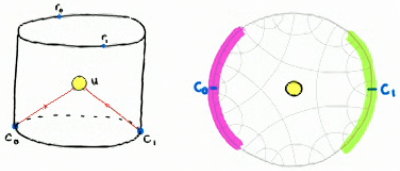
- Can argue via Lieb-Robinson bounds that simulations with properties * cannot exist with controllable error in the state
  ↳ giving a lower bound on how good simulators can be

- Best known simulation bounds say cannot simulate 2-local all to all with 2-geometrically local using $O(1)$ strengths [AZ18]

SUMMARY

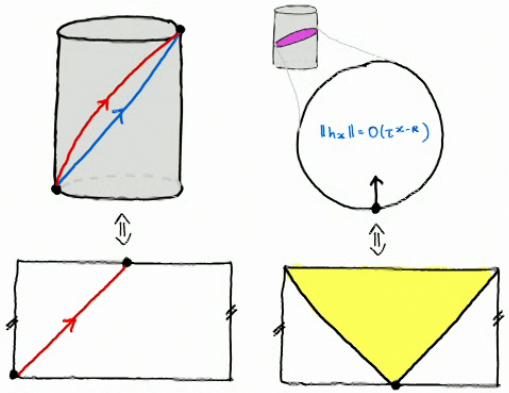
1. 

2. Provably no simulation techniques to construct attacks in these types of toy models even with recovery of some causal structure.

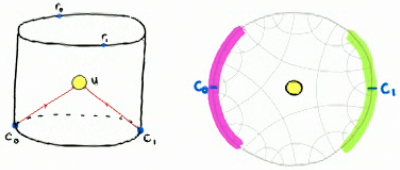


↳ Led to more precise lower bounds on Hamiltonian simulation from causality.

SUMMARY

1. 

2. Provably no simulation techniques to construct attacks in these types of toy models even with recovery of some causal structure.



↳ Led to more precise lower bounds on Hamiltonian simulation from causality.

Other application of toy models with improved causality?

Capture space-time more completely in models?

Simulation of more restricted classes of Hamiltonians?

Thank you

References

[May19] Alex May, Geoff Penington, and Jonathan Sorce. "*Holographic scattering requires a connected entanglement wedge*."

[HaPPY15] Fernando Pastawski et al. "*Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence*".

[Dolev+22] K Dolev, S Cree *"Non-local computation of quantum circuits with small light cones"* arXiv:2203.10106, 2022

[KC19] Tamara Kohler and Toby Cubitt. *"Toy Models of Holographic Duality between local Hamiltonians."* arXiv: 1810.08992v3.

[AKC] Harriet Apel, Tamara Kohler, and Toby Cubitt. *"Holographic duality between local Hamiltonians from random tensor networks"*. In: (2021). arXiv: 2105.12067.