Pseudoentanglement

Soumik Ghosh

arxiv: 2211.00747 arxiv: 2311.12017

Joint work with…

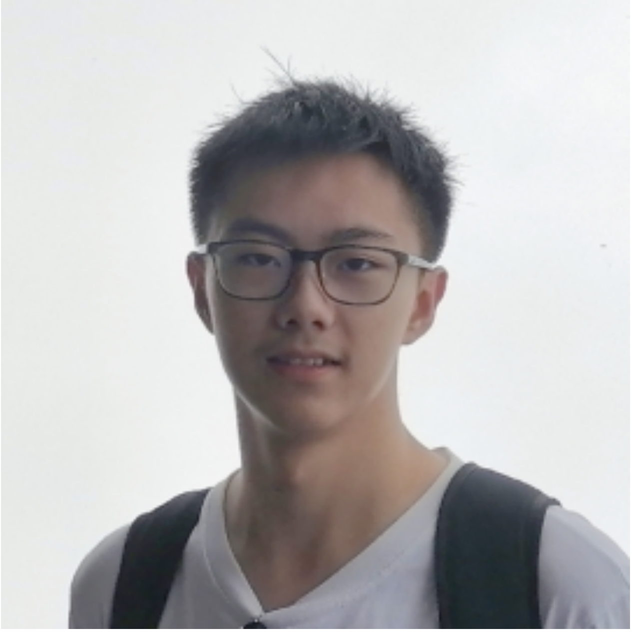
Scott Aaronson (UT Austin)

Adam Bouland (Stanford)

Bill Fefferman (UChicago)

Tony Metger (ETH)

Umesh Vazirani (UC Berkeley)



Chenyi Zhang (Stanford)

Jack Zhou (Stanford)

Based on:

Quantum Pseudoentanglement

Scott Aaronson[*1], Adam Bouland[†2], Bill Fefferman[‡3], Soumik Ghosh[§3], Umesh Vazirani[¶4], Chenyi Zhang[‖2], and Zixin Zhou[**2]

[1]Department of Computer Science, University of Texas, Austin
[2]Department of Computer Science, Stanford University
[3]Department of Computer Science, University of Chicago
[4]Department of Electrical Engineering and Computer Sciences, University of California, Berkeley

Public-key pseudoentanglement and the hardness of learning ground state entanglement structure

Adam Bouland[*1], Bill Fefferman[†2], Soumik Ghosh[‡2], Tony Metger[§3], Umesh Vazirani[¶4], Chenyi Zhang[‖1], and Zixin Zhou[**1]

[1]Stanford University
[2]University of Chicago
[3]ETH Zurich
[4]UC Berkeley

Outline

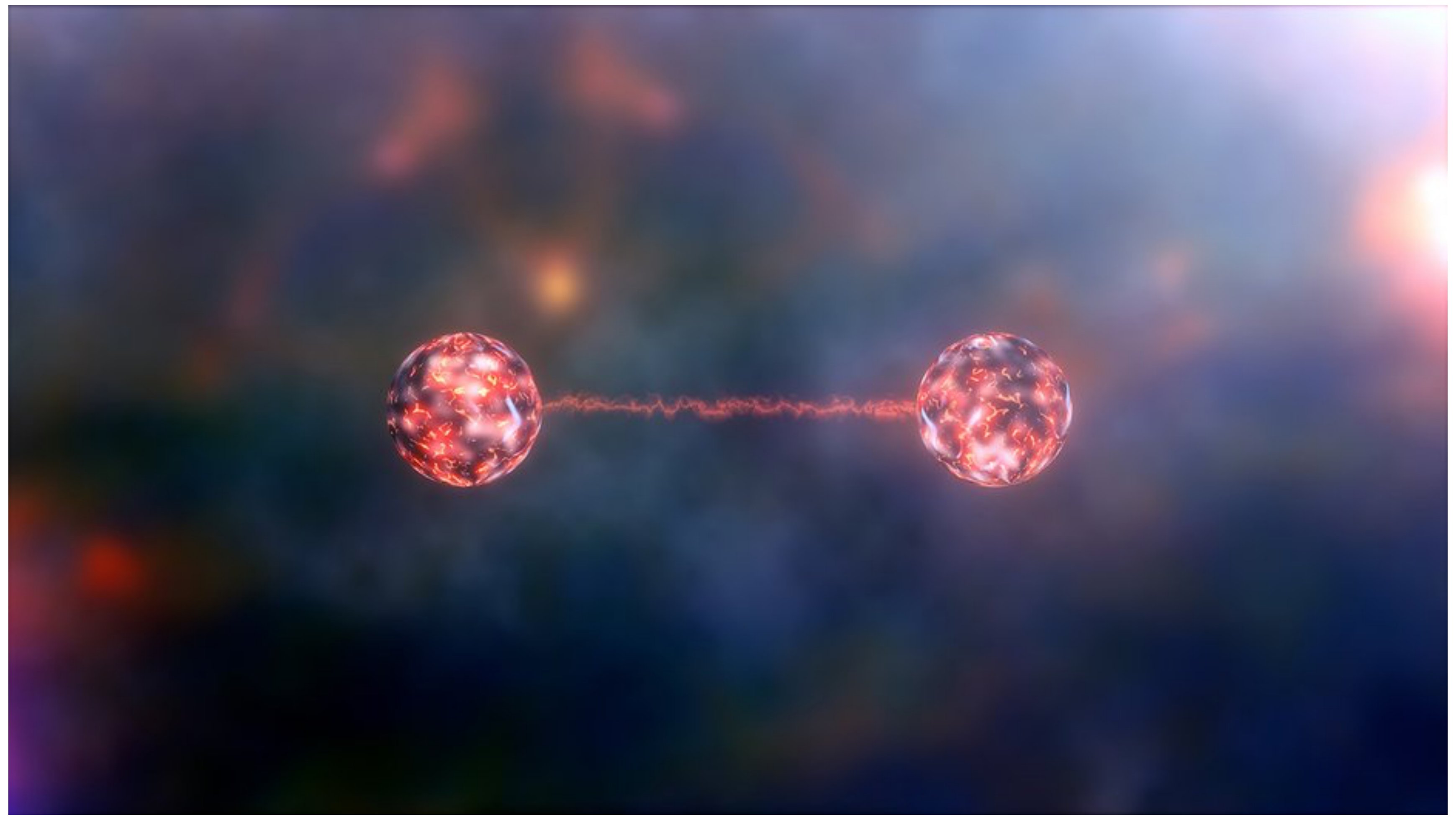
Chapter 1: Background

Chapter 2: Private Key Pseudoentanglement

Chapter 3: Public Key Pseudoentanglement

Chapter 1: Background

Entangelement is the driving force of quantum computing

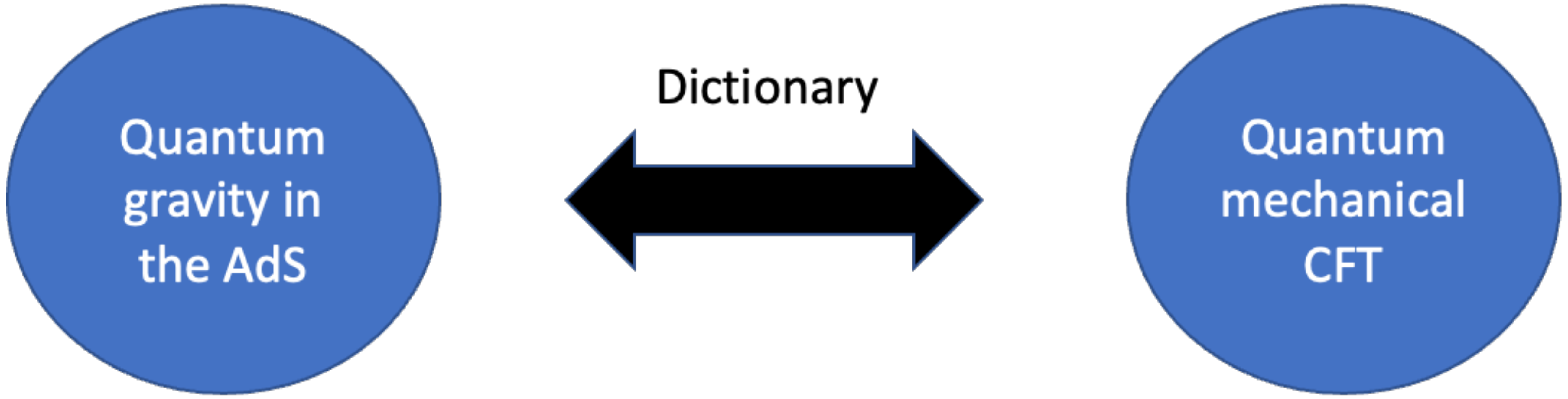


But there is a lot that we do not understand about entanglement.

This work: We will give a new property of entanglement.

Motivation:

Entanglement, Geometry, and Complexity



Major theme: Geometry in AdS = Entanglement in the CFT
(eg: Ryu-Takayanagi formula)

Our result: Entanglement cannot be felt/efficiently measured.

Are corresponding geometries feelable? If so, then the AdS/CFT dictionary must be hard to compute!

Chapter 2: Private Key Pseudoentanglement

How do we measure entanglement?

We will measure entanglement using the von Neumann entanglement entropy $S(\,\cdot\,)$ across a particular bipartition.

Definition: Two collections of states $\{ |\psi_{k_1}\rangle \}$ and $\{ |\phi_{k_2}\rangle \}$ are $(f(n), g(n))-$ pseudoentangled if

1. **Polynomial preparability:** Given the key k_1 and k_2 respectively, $|\psi_{k_1}\rangle$ and $|\phi_{k_2}\rangle$ are preparable by a polynomial time quantum algorithm.

2. **Indistinguishability:** If the keys are secret, then with high probability then for any poly time quantum distinguisher D

$$\left| \Pr[\mathrm{D}(|\psi_{k_1}\rangle^{\otimes \mathrm{poly}(n)}) = 1] - \Pr[\mathrm{D}(|\phi_{k_2}\rangle^{\otimes \mathrm{poly}(n)}) = 1] \right| = \mathrm{negl}(n) .$$

3. **Entanglement gap:** $|\psi_{k_1}\rangle$ has entanglement entropy $\Theta(f(n))$ and $|\phi_{k_2}\rangle$ has entanglement $\Theta(g(n))$ across a fixed publicly known bipartition, with $f(n) > g(n)$.

Our construction of pseudoentanglement will rely on computationally pseudorandom states…

- These are an ensemble of states such that no efficient algorithm can distinguish, with non-negligible advantage, $\mathrm{poly}(n)$ copies of the state from this ensemble from $\mathrm{poly}(n)$ copies of a Haar random state.

- These usually require complexity theoretic conjectures.

How much entanglement spoofs the Haar measure?

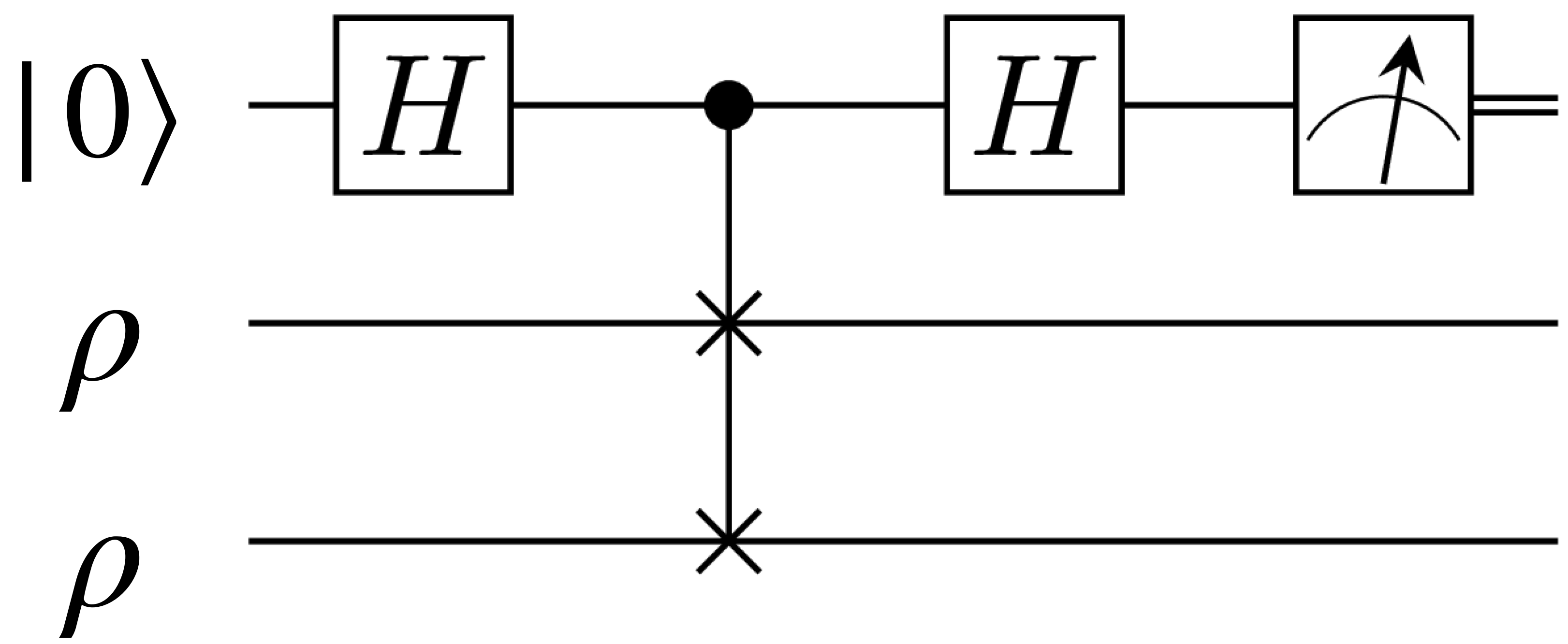
State ensemble [n qubit states]	Entanglement
Haar random	Near maximal, ie, ~ n
t-designs [t copies are info-theoretically close to t copies of Haar random states]	Near maximal, ie, ~ n [Harrow and Low, 2009]
Computationally pseudorandom	Can be as small as $\omega(\log(n))$ Our work!

How to get a lower bound? [JLS'18]

We will prove by contradiction. Assume there are pseudorandom states with entanglement $\mathcal{O}(\log n)$.

We will prove there is a distinguisher that leverages low entanglement!

Let $|\psi\rangle^{\otimes 2}$ be that state. Apply SWAP test on $\frac{n}{2}$ qubits from each copy of $|\psi\rangle$, to get



$$\text{Prob}[0] \propto \frac{1}{2} + \frac{\text{Tr}(\rho^2)}{2} \leq \frac{1}{2} + \frac{1}{2 \cdot 2^{S(\rho)}}$$

By Jensen's inequality

$\Theta(n)$

for Haar random states

If the state has very low entanglement, that is $\mathcal{O}(\log(n))$, then it can be detected by the SWAP test.

Recap: Is the SWAP test based lower bound tight?

Our result: **Yes!**

We construct ensembles of pseudorandom quantum states that saturate the entanglement lower bound.

To start with, consider the following ensemble..

$$|\psi_{f_k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f_k(x)} |x\rangle \,.$$

any quantum secure
pseudorandom function

Divvy up the state into two registers:

$$|\psi_{f_k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i,j \in \{0,1\}^{n/2}} (-1)^{f_k(i,j)} |i_A\rangle |j_B\rangle \,.$$

For ease of presentation, define a pseudorandom matrix

Subsystem B

$$\mathsf{C_f} = \begin{pmatrix} f(0^{\frac{n}{2}},0^{\frac{n}{2}}) & \dots & f(0^{\frac{n}{2}},1^{\frac{n}{2}}) \\ \vdots & \ddots & \vdots \\ f(1^{\frac{n}{2}},0^{\frac{n}{2}}) & \cdots & f(1^{\frac{n}{2}},1^{\frac{n}{2}}) \end{pmatrix}$$

Subsystem A

has a one to one correspondence with the pseudorandom state

The reduced density matrix across subsystem A, given by ρ_{A} is

$$\rho_{\mathsf{A}} = \frac{1}{2^n}\mathsf{C_f} \cdot \mathsf{C_f^T}\,.$$

Note that the entanglement entropy is….

$$S(\rho_{\mathsf{A}}) = \mathcal{O}(\log \mathsf{rank}(\mathsf{C_f}))\,.$$

By Jensen's inequality

How to reduce the entanglement entropy?

$\boxed{\text{Reduce the rank of } \mathsf{C_f}\text{! But do it in a quantum-secure way.}}$

The idea is to reduce the rank of this matrix by using quantum secure 2^k to 1 functions.

- We construct a new pseudorandom matrix C'_f : the i^{th} row of C'_f is the $g(i)^{\text{th}}$ row of C_f .

- We let the function $g(i) = f_1(f_2(i) \text{ mod } 2^{\frac{n}{2}-k})$, where f_1 and f_2 are quantum secure pseudorandom permutations. By a variant of the collision bound, g is a valid pseudorandom function!

By choosing k appropriately, we can make the entanglement as small as $\omega(\log n)$!

- The construction is "private key"! Describing g reveals what the entanglement is.

This gives a pseudoentangled state across one cut…

We can get a maximal entanglement difference of $\Omega(n)$ versus $\mathcal{O}(\text{polylog}(n))$.

Can we strengthen the construction to have maximal pseudoentanglement across multiple cuts?

Let us take the qubits to be arranged in a 1D line

The key idea is to go from left to right and iteratively reduce the rank of the corresponding pseudorandom matrices by using fresh quantum secure PRFs.

Step i:

Step $i+1$:

Then by sub-additivity of entanglement entropy, this gives pseudoentanglement with scaling

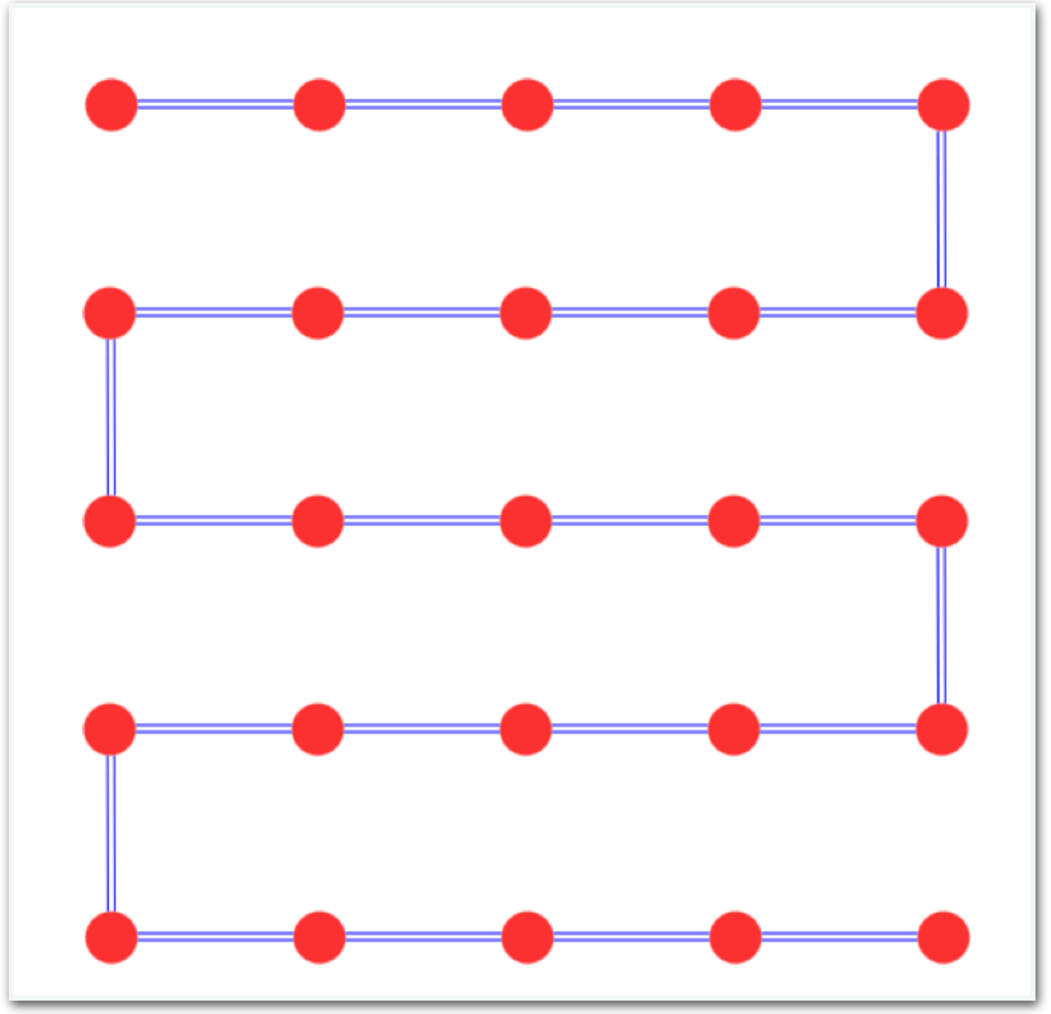
$$\Omega(n) \text{ versus } \mathcal{O}(|\mathrm{B}|\,\mathrm{polylog}(\mathrm{n}))$$

size of the cut

…across any cut!

Remarks

- Simple generalization to 2D, by snaking the 2D grid!



- Another construction also gives pseudoentanglement across multiple cuts, using subset phase states!
    - See Adam Bouland’s Simons colloquium on “Quantum Pseudoentanglement.”

Applications and other constructions

- Time-complexity lower bounds on problems that are as hard as entanglement testing, like spectrum testing, Schmidt rank testing, testing matrix product states etc.

- Time complexity lower bounds on entanglement distillation.

- Check out LOCC-based pseudoentanglement [Arnon-Friedman, Brakerski, Vidick ’23]. Nice generalization to operational mixed state measures!

Chapter 3: Public Key Pseudoentanglement

Observation

Remember that for our private-key constructions, the distinguisher only got to see many copies of the unknown (low or high entanglement) state.

- The distinguisher did not know the circuit that prepared the state!

Can we construct pseudoentangled states even when the circuit is revealed?

Motivation: Hamiltonian complexity!

Can we get Hamiltonians whose ground states are pseudoentangled?

Equivalent to asking for public-key pseudoentanglement, by circuit to Hamiltonian constructions [GH'20]!

More on this later!

Gives public-key post-quantum cryptography!

Use LWE to construct two sets of indistinguishable functions: an (almost) injective one to build high entanglement states and a lossy one to build low entanglement states!

Our work in context

Previous work [GH'20]:

n versus $n - \mathcal{O}(1)$ (Single cut)

Our work:

$\Omega(n)$ versus $\mathcal{O}(|B|\,\mathrm{polylog}(n))$ (All cuts!)

Cut size

A recap of the construction

Start with pseudorandom phase states, just as in the "private-key" case:

$$|\psi_{f_k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i,j \in \{0,1\}^n} (-1)^{f_k(i,j)} |i,j\rangle \,.$$

Consider the corresponding pseudorandom matrix:

$$\begin{array}{cc} & \text{Subsystem B} \\ C_f = & \begin{pmatrix} f(0^{\frac{n}{2}},0^{\frac{n}{2}}) & \dots & f(0^{\frac{n}{2}},1^{\frac{n}{2}}) \\ \vdots & \ddots & \vdots \\ f(1^{\frac{n}{2}},0^{\frac{n}{2}}) & \cdots & f(1^{\frac{n}{2}},1^{\frac{n}{2}}) \end{pmatrix} \text{ Subsystem A} \end{array}$$

Idea: Repeat rows using a function g which is either 1-to-1 or has many collisions, ie "lossy".

Property: Even when a description of g is public, hard to tell apart the two cases.

Note:

$$g : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$

How will we get our function? Through LWE!

A recap of LWE

The task is to distinguish between

$$(A, \overrightarrow{u}) \quad \text{versus} \quad (A, A \cdot \vec{s} + \overrightarrow{e})$$

Uniformly random vector

Secret string

Gaussian noise

$A \leftarrow U_q^{r \times l}$

$\overrightarrow{u} \leftarrow U_q^r$

$\vec{s} \leftarrow U_q^l$

$\overrightarrow{e} \leftarrow D_{q,\sigma}^r$

Standard LWE: every polynomial time algorithm has negligible advantage in distinguishing the samples, even with many samples.

Subexponential LWE: every polynomial time algorithm has sub-exponentially small advantage in distinguishing the samples, even with many samples.

Refresher on goal: We need to construct our function g using LWE…

To sample a one to one function $f: \{0,1\}^{n/2} \rightarrow \{0,1\}^{\text{poly}(n)}$…

- Sample a poly(n) $\times \frac{n}{2}$ matrix U and let $f(x) = Ux$.

Chosen uniformly at random, w.h.p a full rank matrix

To sample a "lossy" function $g : \{0,1\}^{n/2} \rightarrow \{0,1\}^{\text{poly(n)}}$…

- Sample a poly(n) $\times \frac{n}{2}$ matrix $B^T \cdot C + E$ and let $g(x) = (B^T \cdot C + E)x$.

w.h.p a low rank matrix, <u>how low depends on length of secret + other parameters</u>

Gaussian noise

Distinguishing these functions, given their description, is as hard as breaking LWE with many samples [Peikert and Waters, 2007]!

There is a problem with this approach!

For the constructions to work, the functions need to be from $\{0,1\}^{\frac{n}{2}}$ to $\{0,1\}^{\frac{n}{2}}$: ie, the co-domain needs to be much smaller than what we have.

How to solve this problem?

Use a hash function to hash down the co-domain from $\{0,1\}^{\text{poly}(n)}$ back to $\{0,1\}^n$ and ensure there aren't too many collisions in the injective case.

Our result:

Assuming subexponential hardness of LWE, we get public key pseudoentangled states with maximal gap $(\Omega(n), \Theta(\text{polylog}n))$.

Assuming standard LWE, we get public key pseudoentangled states with gap $(\Omega(n), \Theta(n^c))$ for $0 < c < 1$.

How do we generalize to multiple cuts? Same way as the private key construction!

Think of the qubits to be on a 1-D line:

Iteratively apply the injective or lossy functions to hash down the rank of the pseudorandom matrix, just like we saw before.

Technical challenge: Need to make sure collisions don't compound in the almost injective function.

Application

$\boxed{\text{Ground State Entanglement Structure}}$

Given a Hamiltonian H, decide if….

The ground state $|\psi\rangle$ has low or high entanglement…

$\boxed{\text{This work: LWE-hard}}$

As hard as breaking a particular type of post-quantum cryptography!

Key idea: Pass the circuit description through Kitaev clocks.

More open problems

- Other constructions!
  - For subset state based constructions, check out [Tudor Giurgica-Tiron, Bouland’ 23] [Geronimo, Magrafta, Wu’ 23] [Fermi Ma, unpublished].
- Can we have geometrically local Hamiltonians with large spectral gap for which ground states are pseudoentangled?
- Can we find pseudoentangled states compatible with holography?
  - Check out Lijie Chen’s next talk!

Thank you!