Pseudoentanglement

Soumik Ghosh

arxiv: 2211.00747 arxiv: 2311.12017

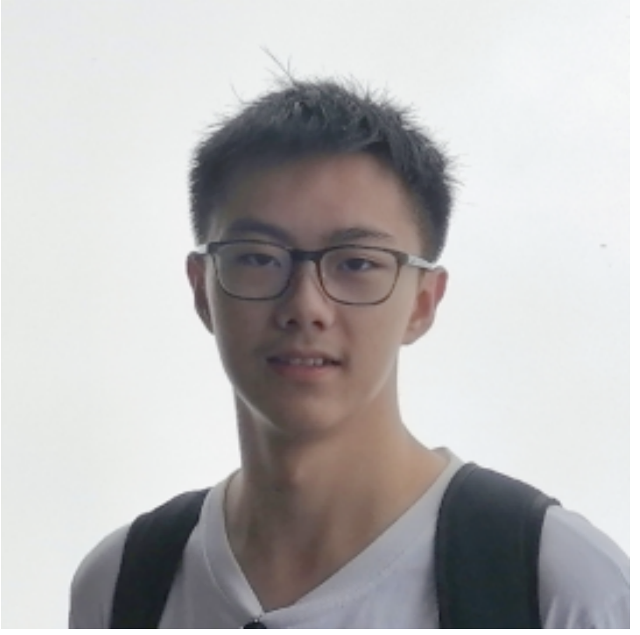
Joint work with…

Scott Aaronson (UT Austin)

Adam Bouland (Stanford)

Bill Fefferman (UChicago)

Umesh Vazirani (UC Berkeley)

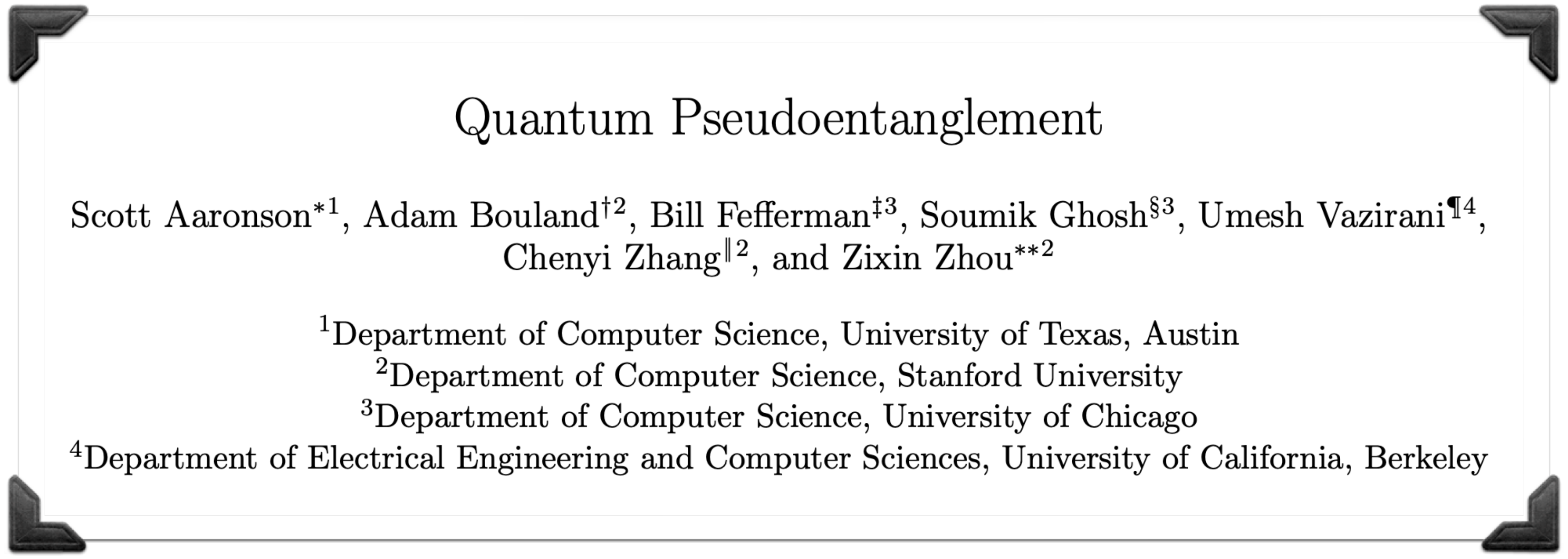


Chenyi Zhang (Stanford)

Jack Zhou (Stanford)

Tony Metger (ETH)

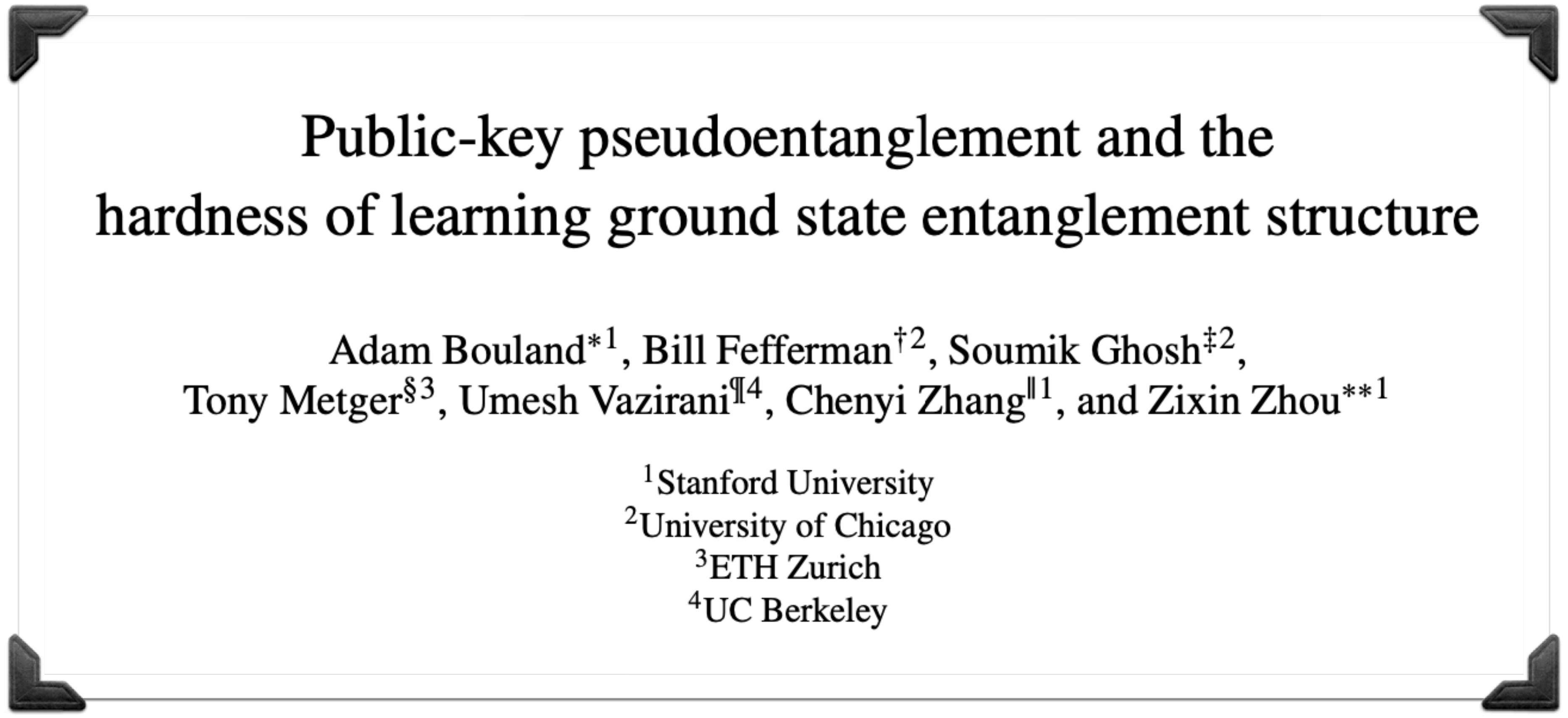
Based on:



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

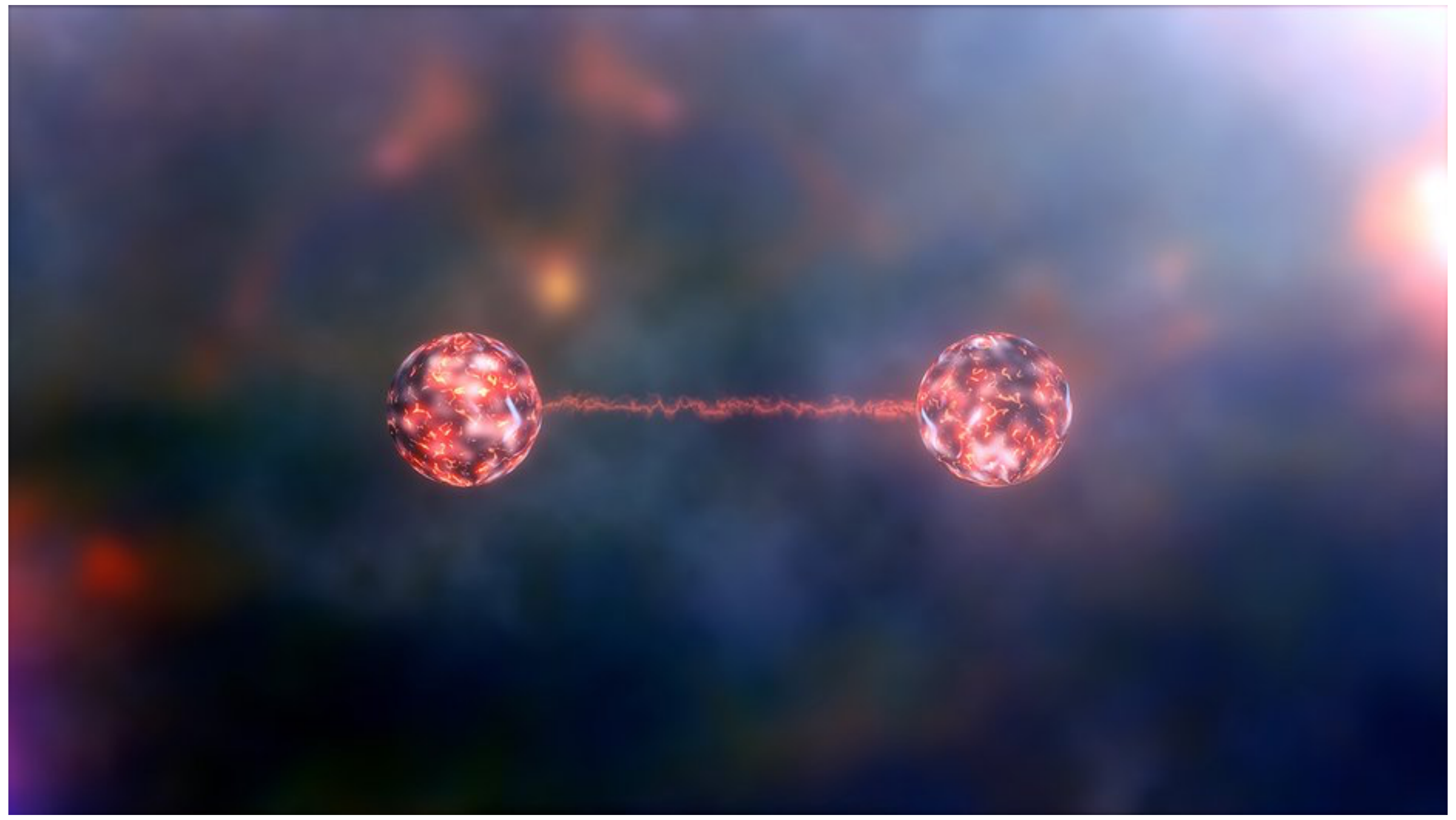
Chapter 1: Background

Chapter 2: Private Key Pseudoentanglement

Chapter 3: Public Key Pseudoentanglement

Chapter 1: Background

Entanglement 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.

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

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

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!

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….

$$S(\rho_A) = \mathcal{O}(\log \mathrm{rank}(C_f))\,.$$

By Jensen's inequality

How to reduce the entanglement entropy?

Reduce the rank of C_f! But do it in a quantum-secure way.

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

Remarks

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?

Yes! Using LWE: a post-quantum cryptography variant

Application

Ground State Entanglement Structure

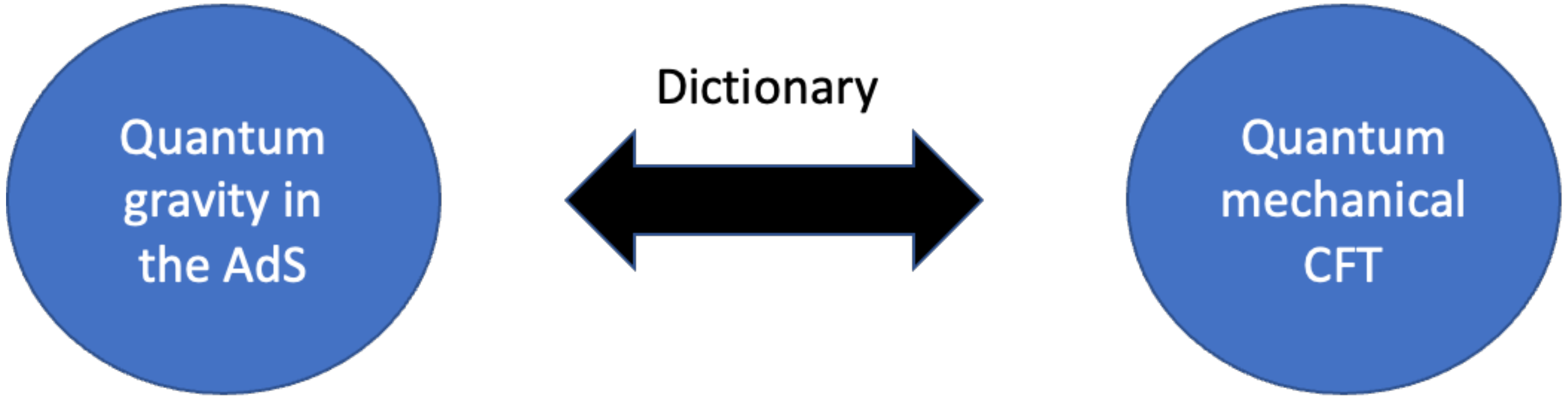
Given a Hamiltonian H, decide if….

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

This work: LWE-hard

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

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!

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?

Thank you!