# Quantum Pseudoentanglement

**Scott Aaronson**
Department of Computer Science, University of Texas at Austin, TX, USA

**Adam Bouland**
Department of Computer Science, Stanford University, CA, USA

**Bill Fefferman**
Department of Computer Science, University of Chicago, IL, USA

**Soumik Ghosh**
Department of Computer Science, University of Chicago, IL, USA

**Umesh Vazirani**
Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA

**Chenyi Zhang**
Department of Computer Science, Stanford University, CA, USA

**Zixin Zhou**
Department of Computer Science, Stanford University, CA, USA

## Abstract

Entanglement is a quantum resource, in some ways analogous to randomness in classical computation. Inspired by recent work of Gheorghiu and Hoban, we define the notion of "pseudoentanglement", a property exhibited by ensembles of efficiently constructible quantum states which are indistinguishable from quantum states with maximal entanglement. Our construction relies on the notion of quantum pseudorandom states – first defined by Ji, Liu and Song – which are efficiently constructible states indistinguishable from (maximally entangled) Haar-random states. Specifically, we give a construction of pseudoentangled states with entanglement entropy arbitrarily close to $\log n$ across every cut, a tight bound providing an exponential separation between computational vs information theoretic quantum pseudorandomness. We discuss applications of this result to Matrix Product State testing, entanglement distillation, and the complexity of the AdS/CFT correspondence. As compared with a previous version of this manuscript (arXiv:2211.00747v1) this version introduces a new pseudorandom state construction, has a simpler proof of correctness, and achieves a technically stronger result of low entanglement across all cuts simultaneously.

**2012 ACM Subject Classification** Theory of computation → Quantum computation theory; Theory of computation → Pseudorandomness and derandomization; Theory of computation → Quantum complexity theory

**Keywords and phrases** Quantum computing, Quantum complexity theory, entanglement

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2024.2

**Related Version** *Full Version*: `https://arxiv.org/abs/2211.00747` [1]

**Funding** B.F. and S.G. acknowledge support from AFOSR (FA9550-21-1-0008). This material is based upon work partially supported by the National Science Foundation under Grant CCF-2044923 (CAREER) and by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers (Q-NEXT). This research was also supported in part by the National Science Foundation under Grant No. NSF PHY-1748958. A.B. and B.F. were supported in part by the DOE QuantISED grant DE-SC0020360. A.B. and C.Z. were supported in part by the AFOSR under grant FA9550-21-1-0392. A.B. was supported in part by the U.S. DOE Office of Science under Award Number DE-SC0020266. U.V. acknowledges the Vannevar Bush faculty fellowship N00014-17-1-3025, and was supported by DOE NQISRC QSA grant FP00010905, QSA grant FP00010905, and NSF QLCI Grant No. 2016245. Z.Z. was supported in part by a Stanford School of Engineering

Fellowship. S.A is supported by a Vannevar Bush Fellowship from the US Department of Defense, the Berkeley NSF-QLCI CIQC Center, a Simons Investigator Award, and the Simons "It from Qubit" collaboration.

**Acknowledgements** We thank Jordan Docter, Tudor Giurgica-Tiron, Nick Hunter-Jones, and Wilson Nguyen for helpful discussions.

## 1 Introduction

Randomness is a resource in classical computation and cryptography, and the theory of pseudorandomness plays a central role in the study of this resource. Entanglement plays an analogous role and is a central resource in quantum information and computation. Inspired by the definition of pseudorandomness, and recent work of Gheorghiu and Hoban [15], we define the notion of pseudoentanglement. Informally we say that an ensemble of quantum states is pseudoentangled if the states are efficiently constructible and have small entanglement but are indistinguishable from quantum states with maximal entanglement.

The study of quantum pseudoentanglement is closely related to the concept of quantum pseudorandom states introduced by Ji, Liu and Song [19]. *Pseudorandom states* are ensembles of quantum states which can be prepared by efficient quantum circuits, yet which masquerade as Haar-random states, even to arbitrary poly-time quantum algorithms using an arbitrary polynomial number of copies of the state. While such a strong form of pseudorandomness is impossible in the information-theoretic setting [8], Ji, Liu and Song showed it is possible to construct such states in a *computational* setting using post-quantum cryptography – in particular using any quantum secure pseudorandom function, a standard cryptographic primitive [39]. This notion has many applications in cryptography [5, 23], complexity theory [22], and quantum gravity [6, 21].

In this paper we give a new family of pseudorandom quantum states which have low entanglement rank (and therefore entropy) across every cut. A simple swap test argument shows that any pseudorandom quantum state must necessarily have $\omega(\log n)$ entanglement entropy across any cut [19]. It was an open question to exhibit pseudorandom quantum states which saturate this entanglement entropy lower bound. Here we give a construction that is optimal and achieves entanglement entropy arbitrarily close to $\log n$ across every cut. This should be contrasted with information theoretic notions of pseudorandomness, such as unitary $t$-designs, which require entanglement entropy $\Omega(n)$ across each cut[1] , and consequently our results obtain an exponential separation between computational vs information theoretic quantum pseudorandomness. Moreover, since by definition pseudorandom states are indistinguishable from Haar random states, which have maximal entropy across every cut, this ensemble of states is also pseudoentangled.

The construction of the pseudoentangled family is quite simple to describe. Let $S \subseteq \{0,1\}^n$ be a pseudorandom subset of superpolynomial support $|S| = s(n)$, and $f : \{0,1\}^n \to \{0,1\}$ a PRF. Then we prove that the state

$$\sum_{x \in S} (-1)^{f(x)} |x\rangle$$

is pseudorandom. The Schmidt rank across any cut is bounded by $s(n)$ and therefore the entanglement entropy is bounded by $\log s(n)$, and for $s(n)$ to be superpolynomial it is only necessary for the entanglement entropy to grow faster than $\log n$. Showing that this family

[1] This is true in expectation for $t \geq 2$ [12, 33] and becomes more concentrated as $t = 4$ and higher [25, 11].

of quantum states is efficiently preparable and pseudorandom therefore establishes that it is indistinguishable from the maximally entangled Haar random states, and is therefore a pseudoentangled family of states.

▶ **Theorem 1** (Pseudorandom states with low entanglement across all cuts (Informal)). *For any function $f(n) = \omega(\log n)$, there exists ensembles of pseudorandom states with entanglement entropy $\Theta(f(n))$ across all cuts of the state simultaneously* [2].

We note that a previous version of this result appeared on the arXiv with identification number `arXiv:2211.00747v1` and as a contributed talk at QIP 2023. Our prior construction was based on the random phase state construction of [19, 7], and we showed it is possible to decrease the entanglement to any $f(n) = \omega(\log n)$ across a single fixed cut, which we include in [1]. It turns out it is possible to generalize our prior construction to have low entanglement with respect to additional cuts. We achieve this by repeatedly using the same technique to reduce the entanglement across certain cuts without accidentally blowing up the entanglement across other cuts. While this allows us to produce, for example, 1D pseudorandom states with "pseudo-area law" scaling of entanglement (i.e., the entanglement of any cut is upper bounded by $A \cdot \text{poly}\log(n)$ where $A$ is the area of the cut when the qubits are arranged on a line) which we prove in [1], the technique requires a careful choice of cuts and does not give us the ability to reduce entanglement across all cuts. Compared to that result, our current construction introduces a new pseudorandom state construction, has a simpler proof of correctness, and achieves a technically stronger result of low entanglement across all cuts simultaneously. As we will show, the pseudo-area law scaling of entanglement allows us to prove strong property testing lower bounds, such as for testing Matrix Product States.

## 1.1 Applications

Given the central role played by pseudorandomness in classical computer science, we expect that the notion of pseudoentanglement will shed new light on our understanding of quantum entanglement. Here we scratch the surface by providing some initial applications.

First, our main result implies new lower bounds in property testing. For example, suppose one wishes to tell if an $n$-qubit state has a Matrix Product State (MPS) description of bond dimension $k$, or is far from any such state? This is the "MPS-testing" problem. Soleimanifar and Wright [34] recently showed MPS testing requires $\Omega(\sqrt{n})$ copies of the state in an info-theoretic sense. We show that MPS testing requires $\Omega\big(\sqrt{k}\big)$ copies of the state, either in info-theoretic or computational settings, as a corollary of our low-entropy PRS construction. While incomparable to the Soleimanifar-Wright bound, this is a stronger lower bound in the regime of high bond dimension $k$ – so is saying that it gets more and more difficult to determine if a state is an MPS as the bond dimension grows. We describe this application in more detail in Section 3.3.

Another classic property testing problem is to estimate the Schmidt rank of many copies of an unknown quantum state [27]. While it is known that in general this is a difficult problem [10], prior lower bounds for this problem have relied on input quantum states which are not efficiently constructible. Our work implies that Schmidt rank testing remains intractable in the setting where states are efficiently constructible, and gives analogous

[2] Technically, this is across all cuts of the state where one size of the partition is of size $\Omega(f(n))$, as the statement is trivially false otherwise.

lower bounds for a number of related property testing/tomography problems, such as estimating the largest Schmidt coefficients of an unknown state (see Section 4). In addition, our pseudoentanglement construction can be used to prove lower bounds on entanglement distillation protocols for extracting entanglement from Haar random states via the Schur transform (see Section 3.1).

Finally our work has applications to quantum gravity theory. A central theme of quantum gravity is that entanglement is related to the geometry of general relativity, through dualities such as the AdS/CFT correspondence. The construction of pseudoentangled states within these theories might give additional evidence that the duality maps must be exponentially difficult to compute [6], which was also part of Hoban and Gheorghiu's motivation for their work [15]. We discuss this further in Section 3.4.

## 1.2 A formal definition of pseudo-entanglement

We now proceed to define pseudoentanglement. A pseudoentangled state ensemble (PES) with gap $f(n)$ vs. $g(n)$ consists of two ensembles of $n$-qubit states $|\Psi_k\rangle, |\Phi_k\rangle$ indexed by a secret key $k \in \{0,1\}^{\text{poly}(n)}$, with the following properties:

- Given $k$, $|\Psi_k\rangle$ ($|\Phi_k\rangle$, respectively) is efficiently preparable by a uniform, poly-sized quantum circuit.
- With probability at least $1 - \frac{1}{\text{poly}(n)}$ over the choice of $k$, the entanglement entropy across every cut of $|\Psi_k\rangle$ ($|\Phi_k\rangle$, respectively) is $\Theta(f(n))$ ($\Theta(g(n))$, respectively)
- For any polynomial $p(n)$, no poly-time quantum algorithm can distinguish between the ensembles $\rho = \mathbb{E}_k \left[ |\Psi_k\rangle \langle\Psi_k|^{\otimes p(n)} \right]$ and $\sigma = \mathbb{E}_k \left[ |\Phi_k\rangle \langle\Phi_k|^{\otimes p(n)} \right]$ with more than negligible probability. That is, for any poly-time quantum algorithm $\mathcal{A}$, we have that

$$|\mathcal{A}(\rho) - \mathcal{A}(\sigma)| \leq \frac{1}{\text{negl}(n)}$$

Our definition is inspired by prior work of Gheorghiu and Hoban [15], who implicitly considered a similar notion. In our language, [15] showed that PES ensembles exist with gap $n$ vs $n-k$ for any $k = O(1)$, based on LWE. Our main result improves this construction to the maximum gap possible:

▶ **Corollary 2** (High gap pseudoentangled states (informal)). *There exists a pseudoentangled state ensemble (PES) with entanglement gap $\Theta(n)$ vs $\omega(\log n)$ across all cuts simultaneously, which is simultaneously a pseudorandom state ensemble, assuming there exists any quantum-secure OWF.*

In contrast to Gheorghiu and Hoban's result, we achieve the maximum possible entanglement gap, which is agnostic to the choice of quantum-secure OWF, applies to all cuts simultaneously, and simultaneously maintain indistinguishability from the Haar measure[3]. We similarly show our state can be instantiated in logarithmic depth.

# 2 Main result

In this section, we will prove our main result, Theorem 1. To do this we first construct a pseudorandom quantum state with optimally low entropy across any cut. As discussed, this is the strongest possible notion of pseudoentanglement for a pseudorandom state ensemble, matching the lower bound established by Ji, Liu, and Song [19].

[3] One can indeed show [15]'s construction is not itself a pseudorandom state ensemble, as we describe in [1]

We then show how to *tune* the entanglement entropy of our construction to achieve a pseudorandom state with entanglement entropy $\Theta(f(n))$ across each cut, for any function $f = \omega(\log(n))$.

## 2.1 The subset phase state construction

For particular choices of $S$ and a binary phase function $f : \{0,1\}^n \to \{0,1\}$, our pseudorandom state will have the following form.

$$|\psi_{f,S}\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} (-1)^{f(x)} |x\rangle . \tag{1}$$

Let us call states that are denoted by (1) "subset phase states". Our next arguments are as follows.

- **Efficient preparation:** We show how to efficiently prepare subset phase states, when the subset and phases are chosen pseudorandomly, using appropriate quantum–secure pseudorandom functions and permutations.
- **Proof of statistical closeness:** First, we will show that if $|S| = 2^{\omega(\log n)}$, and if $f$ is randomly chosen in (1), then polynomially many copies of the corresponding density matrix are close in trace distance to polynomially many copies of a Haar random state. Qualitatively, this result means that a randomly chosen subset phase state is statistically close to a Haar random state, even with polynomially many copies.
- **Proof of computational indistinguishability:** Then, we will show that conditioned on a cryptographic conjecture, we can efficiently prepare pseudorandom subset phase states that are computationally indistinguishable to a random subset phase state. The proof of security will hinge on a sequence of hybrids.
- **Analysis of pseudoentanglement:** We will have a discussion on how our construction can be made to achieve the desired optimally low pseudoentanglement properties across any cut.
- **Tight tunability:** Finally, we will discuss how to tightly tune the entanglement of our construction by varying the size of the subset.

## 2.2 Notations

We will use $\mathsf{TD}(\cdot\ ,\ \cdot)$ to denote the trace distance between two density matrices. Use $\mathrm{Perm}_t$ to denote the set of all permutations among $t$ items. For any subset $S \subseteq \{0,1\}^n$ and any $\sigma \in \mathrm{Perm}_t$, we define

$$P_S(\sigma) \coloneqq \sum_{x_1,\ldots,x_t \in S} |x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(t)}\rangle \langle x_1, \ldots, x_t| . \tag{2}$$

Then,

$$\Pi^{S,t}_{\mathrm{sym}} = \frac{1}{t!} \sum_{\sigma \in \mathrm{Perm}_t} P_S(\sigma) \tag{3}$$

is the projector onto the symmetric subspace of $(\mathbb{C}^S)^{\otimes t}$.

There are two sources of randomness in the subset phase state: randomness in choosing the subset and randomness in choosing the phase. To simplify notations, we use $|\psi_S\rangle$ to denote the subset phase state defined in Eq. (1) with a random phase function and a fixed subset $S$, $|\psi_f\rangle$ to denote the subset phase state with a random subset and a fixed phase

function, and $|\psi\rangle$ to denote the subset phase state where both the components are chosen at random. Sometimes, when the choice of the subset is specified by a function $p$, as we will see in the very next section, we slightly modify the notation in Eq. (1) and use $|\psi_{f,p}\rangle$ to denote such an ensemble.

In the next section, we will show that we can efficiently instantiate these states using pseudorandom functions and permutations. We will reference this section later, in our final proof of the pseudorandom and pseudoentangled properties of these states.

## 2.3 Efficiently preparing the state

Let $p$ be sampled uniformly at random from a family of quantum–secure pseudorandom permutations $P$ with

$$P = \{p : [2^n] \to [2^n]\} \tag{4}$$

and $f$ be sampled uniformly at random from a family of quantum–secure pseudorandom functions $F$ with

$$F = \{f : [2^n] \to \{1, -1\}\}. \tag{5}$$

Let us suppose we know $f$, $p$ and $p^{-1}$. We will give a recipe of how to efficiently prepare the state:

$$|\psi_{f,p}\rangle = \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))} |p(x0^{\otimes(n-k)})\rangle \tag{6}$$

The steps are as follows:

- Start with $|0^n\rangle$.
- Let the size of the subset $\mathsf{S}$ be $2^k$ for some integer $k \leq n$.
- Apply $H^{\otimes k} \otimes I^{\otimes(n-k)}$ to $|0^n\rangle$.
- We get the state

$$\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x0^{\otimes(n-k)}\rangle\,, \tag{7}$$

  where $x0^{\otimes(n-k)}$ means we pad $n-k$ zeros to to end of $x$ to get an $n$-bit string.
- We apply $p$ to this state to get

$$\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x0^{\otimes(n-k)}\rangle\, |p(x0^{\otimes(n-k)})\rangle\,. \tag{8}$$

- Finally, we apply the inverse of $p$, denoted by $p^{-1}$, to un-compute the first register. We get

$$\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |p(x0^{\otimes(n-k)})\rangle\,. \tag{9}$$

  Observe that if $p$ were sampled from the set of truly random permutations, then this process would output a subset set state $\frac{1}{\sqrt{2^k}} \sum\limits_{x\in S} |x\rangle$ uniformly at random from all subset states with size $2^k$.

- Finally, we construct a phase oracle using the description of $f$ to get the state

$$\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))} \left|p(x0^{\otimes(n-k)})\right\rangle . \tag{10}$$

  Note that if $P$ were a truly random permutation family and $f$ a truly random phase function, then the output distribution of this process is exactly the uniform distribution over subset phase states with $|\mathsf{S}| = 2^k$.

## 2.4 Proof of statistical closeness to Haar random states

We will prove that polynomially many copies of a subset phase state, where both the subset and the phases have been chosen at random, are statistically close to polynomially many copies of a Haar random state. More formally, we establish the following theorem.

▶ **Theorem 3.** *For any $t < K \leq 2^n$, it holds that*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S \text{ with } |S|=K,\ f}\left[\left|\psi_{f,S}\right\rangle\left\langle\psi_{f,S}\right|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathscr{H}(\mathbb{C}^N)}\left[\left|\phi\right\rangle\left\langle\phi\right|^{\otimes t}\right]\right) < O\left(\frac{t^2}{K}\right),$$

*where $|\psi_{f,S}\rangle$ is defined in (1). That is to say,*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S \text{ with } |S|=K,\ f}\left[\left|\psi_{f,S}\right\rangle\left\langle\psi_{f,S}\right|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathscr{H}(\mathbb{C}^N)}\left[\left|\phi\right\rangle\left\langle\phi\right|^{\otimes t}\right]\right) < \frac{1}{\mathrm{poly}(n)},$$

*for $K = 2^{\omega(\log n)}$, any polynomially bounded $t$, and any $\mathrm{poly}(n)$, where $\mathscr{H}(\mathbb{C}^N)$ denotes the ensemble of Haar random states in the Hilbert space with dimension $N = 2^n$.*

The proof can be found in [1], and uses techniques from representation theory to represent a random subset phase state ensemble as a "truncated" projector onto the symmetric subspace, where the truncation depends on the size of the subset. Then, using standard facts, we compute its statistical distance from the Haar random ensemble.

## 2.5 Proof of computational indistinguishability

In this section, we will prove the following theorem.

▶ **Theorem 4.** *Consider an ensemble of subset phase states $|\psi_{f,p}\rangle$ given by*

$$\left|\psi_{f,p}\right\rangle = \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))} \left|p(x0^{\otimes(n-k)})\right\rangle , \tag{11}$$

*where $p$ is sampled uniformly at random from a family of quantum–secure pseudorandom permutations $P$ with*

$$P = \{p : [2^n] \to [2^n]\}$$

*and $f$ is sampled uniformly at random from a family of quantum–secure pseudorandom functions $F$ with*

$$F = \{f : [2^n] \to \{1, -1\}\}.$$

*Then, (11) defines an ensemble of pseudorandom quantum states, with the secret key $\mathsf{K}$ being the description of $f$, $p$, and $p^{-1}$, where $p^{-1}$ is the inverse permutation of $p$.*

Note that the efficient preparability of the states in (11) follow from Section 2.3. The rest of the proof will be a security analysis: to prove that this construction is computationally indistinguishable from Haar random states. Finally, in a separate section, we will analyze the entropy of this state ensemble.

### 2.5.1 Security analysis

In this subsection, we prove the following proposition.

▶ **Proposition 5.** *The ensemble of subset phase states defined in (10) is computationally indistinguishable from Haar random states, with the secret key being the description of $f$ and $p$, when $|\mathsf{S}| = 2^{\omega(\log n)}$.*

**Proof.** Note that $f$ is oracle indistinguishable from a random function $r_{\mathsf{f}}$, from an analysis in Section B.2.3 of [1]. Additionally, by definition, $p$ is oracle indistinguishable from a truly random permutation $r_{\mathsf{p}}$. Moreover, again by definition, the oracle indistinguishability result holds even when the adversary is given access to the inverse of the permutation. That is, no adversary can distinguish between $(p, p^{-1})$ and $(r_{\mathsf{p}}, r_{\mathsf{p}}^{-1})$ when given black box access and promised one of these is the case.

So, when given access to three black boxes, promised to either $(f, p, p^{-1})$, or $(r_{\mathsf{f}}, r_{\mathsf{p}}, r_{\mathsf{p}}^{-1})$, no polynomial time adversary, with query access, can distinguish between these two cases. Now, the following sequence of hybrids completes the proof.

**Hybrid 0.** This is the case where the adversary is given polynomially many copies of the state

$$|\psi_{f,p}\rangle = \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))} \, |p(x0^{\otimes(n-k)})\rangle \, . \tag{12}$$

**Hybrid 1.** This is the case where the adversary is given polynomially many copies of the state

$$|\psi_{R,r}\rangle = \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{r_{\mathsf{f}}(r_{\mathsf{p}}(x0^{\otimes(n-k)}))} \, |r_{\mathsf{p}}(x0^{\otimes(n-k)})\rangle \, . \tag{13}$$

This is computationally indistinguishable from **Hybrid 0** because, otherwise, we can efficiently distinguish between $(f, p, p^{-1})$ and $(r_{\mathsf{f}}, r_{\mathsf{p}}, r_{\mathsf{p}}^{-1})$ when given black box access, by using the unknown black box to prepare polynomially many copies of a state that has to be either (12) or (13).

**Hybrid 2.** The adversary is given polynomially many copies of a Haar random state. This is indistinguishable from **Hybrid 1** from Theorem 3. ◀

## 2.6 Entanglement entropy of pseudorandom subset phase states

Let $|\psi_{f,p}\rangle$ be a pseudorandom subset phase state and let

$$\rho_{f,p} = |\psi_{f,p}\rangle\langle\psi_{f,p}|.$$

To prevent cluttering notations, we will drop $f$ and $p$ from the subscript of $\rho$ and take them to be implicit whenever we use the symbol, unless otherwise stated. Let $S$ be the size of the subset defined by $p$ and let $\mathsf{S}(\cdot)$ be the von Neumann entanglement entropy of a density matrix.

For an $n$–qubit state $|\psi\rangle$, let $(\mathsf{X}, \mathsf{Y})$ be any partition of the $n$ qubits. Then, for reduced density matrices $\rho_{\mathsf{X}}$ and $\rho_{\mathsf{Y}}$, let the von Neumann entropy, for each, be denoted by $\mathsf{S}(\rho_{\mathsf{X:Y}})$.

The following statements are immediate.

▶ **Corollary 6.** *For* any *cut* $(\mathsf{X},\mathsf{Y})$ *of* $n$ *qubits, such that* $|\mathsf{X}|+|\mathsf{Y}|=n$,

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) = \mathcal{O}(\log|S|).$$

**Proof.** The proof follows trivially from noting that the rank of the density matrix $\rho$ is at most $|S|$, as it is a density matrix corresponding subset state over a subset of size $|S|$ and has, at most $|S|$ linearly independent rows or columns. ◀

▶ **Corollary 7.** *For* $|S| = 2^{\text{poly}\log n}$, *for* any *cut* $(\mathsf{X},\mathsf{Y})$ *of* $n$ *qubits, such that* $|\mathsf{X}|+|\mathsf{Y}|=n$,

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) = \Theta(\text{poly}\log n). \tag{14}$$

**Proof.** The upper bound follows from Corollary 6 and the lower bound follows from the SWAP test, as described in [1]. ◀

This shows that when $|S| = 2^{\text{poly}\log n}$, we get optimally low pseudoentanglement across every cut, no matter what the spatial geometry is. We will now see a way of tuning the entanglement entropy by varying the size of the subset.

## 2.7 Tuning the entanglement entropy of the random subset phase state construction

By varying the size of the subset, we can tune the entanglement entropy of our random subset phase state construction. However, since the SWAP test lower bound of $\Omega(\log n)$ is no longer tight for these cases, we need a different way of proving a tight lower bound. For that, we will consider a very specific form of the pseudorandom phase function.

This is what we will motivate and discuss in the next parts. Before that discussion, just for convenience of analysis, we will define a pseudorandom matrix.

### 2.7.1 Pseudorandom matrices for subset phase states

Let a given subset be $S$, a subset state $|\psi_{f,S}\rangle$, and a given partition $(\mathsf{X},\mathsf{Y})$, where $|\mathsf{X}|=m$ and $|\mathsf{Y}|=n-m$. Let us write the reduced density matrix across the partition $\mathsf{X}$. Let $|S|=2^k$.

$$\begin{aligned}
\rho_{\mathsf{X}} &= \frac{1}{2^k}\left(\sum_{i\in\{0,1\}^m, j\in\{0,1\}^{n-m}, ij\in S}\ \sum_{k\in\{0,1\}^m, l\in\{0,1\}^{n-m}, kl\in S} (-1)^{f(i,j)+f(k,l)}\,\mathrm{Tr}_2(|i\rangle|j\rangle\langle k|\langle l|)\right)\\
&= \frac{1}{2^k}\left(\sum_{i,k\in\{0,1\}^m, j\in\{0,1\}^{n-m}, ij\in S, kj\in S} (-1)^{f(i,j)+f(k,j)}\,|i\rangle\langle k|\right) &(15)\\
&= \frac{1}{2^k}\left(\sum_{i,k\in\{0,1\}^m, j\in\{0,1\}^{n-m}, ij\in S, kj\in S} B_{i,j}B_{k,j}\,|i\rangle\langle k|\right) &(16)\\
&= \frac{1}{2^k}\left(\sum_{i,k\in\{0,1\}^m, j\in\{0,1\}^{n-m}, ij\in S, kj\in S} B_{i,j}B_{k,j}\,|i\rangle\langle j|j\rangle\langle k|\right) &(17)\\
&= \frac{1}{2^k}\left(\sum_{i\in\{0,1\}^m}\ \sum_{j\in\{0,1\}^{n-m}, ij\in S} B_{i,j}\,|i\rangle\langle j|\right)\left(\sum_{j\in\{0,1\}^{n-m}}\ \sum_{k\in\{0,1\}^m, kj\in S} B_{k,j}\,|j\rangle\langle k|\right) &(18)\\
&= \frac{1}{2^k}BB^{\mathsf{T}}, &(19)
\end{aligned}$$

where we define a pseudorandom matrix $B_{\mathsf{X}:\mathsf{Y},f}$ as follows.

$$\begin{aligned} B_{\mathsf{X}:\mathsf{Y},f,i,j} &= f(i,j) \qquad \text{when } \; ij \in S,\; i \in \{0,1\}^m,\; j \in \{0,1\}^{n-m} \\ &= 0 \qquad\quad \text{otherwise.} \end{aligned} \tag{20}$$

When the context is clear, we drop the corresponding subscripts from our notation, which we have done in (16), (17), (18), and (19).

### 2.7.2 Tuning the entanglement entropy

For tuning the entanglement entropy, we will consider an ensemble of pseudorandom subset phase states $|\psi_{f,p}\rangle$, where $f$ is chosen as

$$f(i) := h(q(i)), \tag{21}$$

where $h$ is uniformly drawn from a 4-wise independent function family

$$H = \{h : [2^n] \to \{1, -1\}\},$$

and $q$ is uniformly drawn from $Q$ – a quantum-secure pseudorandom permutation (PRP) family – where

$$Q = \{q : [2^n] \to [2^n]\}.$$

Note that by a simple hybrid argument, $f$ is computationally indistinguishable from a truly random function: so, it is both pseudorandom and 4-wise independent. This is proven in detail in [1]. We will now prove the following theorem.

▶ **Theorem 8.** *Let $\omega(\log n) \leq k \leq n$ and let $|S| = 2^k$. Consider a cut $(\mathsf{X}, \mathsf{Y})$ of $n$ qubits, such that $|\mathsf{X}| + |\mathsf{Y}| = n$ and $|\mathsf{X}|, |\mathsf{Y}| \geq k$. Let the pseudorandom phase function satisfy* (21)*. Then, with high probability over the choice of the state,*

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) = \Theta(k).$$

**Proof.** The upper bound follows from Corollary 6. For the lower bound, we will use the inequality,

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) \geq -\log\left(\left|\left|\frac{1}{2^k} B_{\mathsf{X}:\mathsf{Y}} {B_{\mathsf{X}:\mathsf{Y}}}^{\mathsf{T}}\right|\right|_F\right), \tag{22}$$

where $B_{\mathsf{X}:\mathsf{Y}}$ is the pseudorandom matrix corresponding to the partition $(\mathsf{X}, \mathsf{Y})$. (22) can be derived by Jensen's inequality. Hence, it suffices to lower bound the quantity

$$\log\left(\left|\left|\frac{1}{2^k} B_{\mathsf{X}:\mathsf{Y}} {B_{\mathsf{X}:\mathsf{Y}}}^{\mathsf{T}}\right|\right|_F\right).$$

In this proof, for simplicity, we prove the statement for partitions of size $n/2$. Note that the same proof follows for any other partition, just by changing the dimensions of the matrix $B_{\mathsf{X}:\mathsf{Y}}$.

Having fixed the partition, let us drop the subscripts from $B$, to avoid any redundant notational clutter. Note that,

$$\begin{aligned}
&\mathrm{E}\left[\left\|\frac{1}{2^k}BB^{\mathsf{T}}\right\|_F^2\right]\\
&=\frac{1}{2^{2k}}\mathrm{E}\left[\left\|BB^{\mathsf{T}}\right\|_F^2\right]\\
&=\frac{1}{2^{2k}}\sum_{i=1}^{2^{k/2}}\sum_{j=1}^{2^{n/2}}\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\cdot B_{jl}\right)^2\right]\\
&=\frac{1}{2^{2k}}\sum_{i=1}^{2^{n/2}}\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\cdot B_{il}\right)^2\right]+\frac{1}{2^{2k}}\sum_{i\neq j,i,j=1}^{2^{n/2}}\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\cdot B_{jl}\right)^2\right]\\
&=\frac{1}{2^{2k}}\sum_{i=1}^{2^{n/2}}\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\right)+2\left(\sum_{l\neq l',l,l'=1}^{2^{n/2}}B_{il}\cdot B_{il'}\right)\right]+\\
&\quad\frac{1}{2^{2k}}\sum_{i\neq j,i,j=1}^{2^{n/2}}\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\cdot B_{jl}\right)^2\right]\\
&\leq\frac{1}{2^{2k}}\left(2^k+2^{n/2+1}\cdot 2^n\cdot\left(\frac{2^k}{2^n}\right)^2\right)+\frac{1}{2^{2k}}\sum_{i\neq j,i,j=1}^{2^{n/2}}\sum_{l=1}^{2^{n/2}}\mathrm{E}\left[\left(B_{il}\cdot B_{jl}\right)^2\right]\\
&\leq\frac{1}{2^{k-1}}+\frac{2^n}{2^{2k}}2^{n/2}\frac{2^{2k}}{2^{2n}}\\
&\leq\frac{1}{2^{k/2-1}},
\end{aligned}$$

where we have used the fact that because $f$ is 4–wise independent, conditioned on any choice of $\mathsf{S}$ we have

$$\begin{aligned}
\mathrm{E}\left[\left(\sum_{l=1}^{2^{n/2}}B_{il}\cdot B_{jl}\right)^2\right]&=\sum_{l=1}^{2^{n/2}}\mathrm{E}\left[\left(B_{il}\cdot B_{jl}\right)^2\right]\\
&\leq 2^{n/2}\frac{2^{2k}}{2^{2n}}.
\end{aligned}$$

Finally, by the Markov's inequality, we have

$$\Pr\left[\left\|\frac{1}{2^k}BB^{\mathsf{T}}\right\|_F^2>2^{-k/4}\right]\leq 2^{1-k/2}. \tag{23}$$

Therefore,

$$\Pr\left[\left\|\frac{1}{2^k}BB^{\mathsf{T}}\right\|_F>2^{-k/8}\right]\leq 2^{1-k/2}. \tag{24}$$

Hence, the proof follows. ◀

## 2.8 Instantiating our constructions using low depth circuits

A natural question to ask is how we can explicitly construct our two pseudorandom states. Note that pseudorandom functions, 4-wise independent functions, and pseudorandom permutations can be instantiated using one-way functions [38, 20]. So, our pseudorandom states can also be instantiated using quantum-secure one-way functions.

Moreover, we can instantiate our states using low-depth circuits. This is discussed in detail in Section 2.8 of [1].

# 3 Applications

In this section, we will describe the applications of our construction.

## 3.1 Low entanglement pseudorandom states imply inefficient entropy distillation protocols

In this section, we will discuss connections between our pseudorandom state constructions and entanglement distillation.

Consider $m$ copies of an uknown $d$-dimensional quantum state $|\psi\rangle$. Consider a bipartition $(A, B)$ of the qubits in $|\psi\rangle$. Let $\rho^A$ and $\rho^B$ be the reduced density matrix across each bipartition, and, to avoid clutter of notation, let $\mathsf{S}(\rho) = \mathsf{S}(\rho^A) = \mathsf{S}(\rho^B)$ be the von Neumann entropy across each bipartition. Then we know, due to previous results:

▶ **Lemma 9** ([17, 16]). *Given an unknown $|\psi\rangle^{\otimes m}$, there is an* LOCC *protocol, which runs in poly$(n)$ time, to get at least $p$ EPR pairs, where*

$$p \geq m\left(\mathsf{S}(\rho) - \eta(\delta) - \delta \log d\right) - \frac{1}{2} d(d+1) \log(m+d), \tag{25}$$

*with probability at least*

$$1 - \exp\left(\frac{-n\delta^2}{2}\right)(n+d)^{d(d+1)/2},$$

*where $\eta(\cdot)$ is the binary entropy function.*

The protocol involves applying a Schur transform to $|\psi\rangle^{\otimes m}$ and then measuring in the standard basis. Note that the Schur transform can be efficiently implemented in $\mathrm{poly}(n, \log d)$ time, using [24], up to inverse exponential precision. A trivial upper bound to $p$ is $\mathsf{S}(\rho)$ – one cannot distill more EPR pairs than the amount of distillable entanglement entropy present, which, for pure states, is equal to the von Neumann entropy $\mathsf{S}(\rho)$ [18]. However, distilling all of the distillable entanglement entropy is non-trivial and the upper bound could potentially be very loose.

Note that when $d = 2^n$, and $m = \mathrm{poly}(n)$, the RHS in (25) is negative, for any value of $\mathsf{S}(\rho)$. Hence, the lower bound on $p$ is vacuous as $p \geq 0$. Tighter lower bounds to $p$ are not known. So, the distillation protocol could essentially terminate without generating a single EPR pair.

We will sketch an argument that for any efficient distillation protocol, working with polynomially many copies of $|\psi\rangle$, the lower bounds on $p$ are unlikely to be too tight. At a high level, our sketch would show that assuming a cryptographic conjecture, no efficient entanglement distillation protocol, working with polynomially many copies of an unknown quantum state, can guarantee a distillation of more than polylogarithmically many EPR pairs.

▶ **Proposition 10.** *For an unknown quantum state $|\psi\rangle^{\otimes m}$ with $m = \mathrm{poly}(n)$, $d = 2^n$, and for a bipartition where each side has $\Omega(n)$ qubits, there is no efficient distillation protocol such that the number of EPR pairs produced $p = \omega(\mathrm{poly} \log \mathsf{S}(\rho))$ with non-negligible probability, assuming the existence of quantum secure one-way functions.*

**Proof.** Assume the contrapositive. Choose a bipartition of size $n/2$ [4]. For a Haar random state, $\mathsf{S}(\rho) = \Theta(n)$ [30]. Consequently, we can distill between $\omega(\text{poly}\log n)$ to $\mathcal{O}(n)$ EPR pairs from this state. However, we can distill between $\omega(\log(\log n))$ to $\mathcal{O}(\text{poly}\log n)$ EPR pairs from our low entropy pseudorandom state (where the entropy is taken to be $\text{poly}\log n$ across the chosen bipartition.) So, just by looking at the number of EPR pairs, we can distinguish between these two states, which breaks the pseudo-entanglement proof. ◀

## 3.2 Applications to property testing: An overview

To motivate our results, consider the two following tasks.

▶ **Task 1.** *Efficiently estimate the largest $t$ eigenvalues of an $n$ qubit mixed state $\rho \in \mathbb{C}^{2^n \times 2^n}$ to $\epsilon = \frac{1}{2^{\mathcal{O}(\text{poly}\log n)}}$ in additive error, starting from $\rho^{\otimes m}$.*

▶ **Task 2.** *Efficiently estimate whether the Schmidt rank of an $n$ qubit pure state $|\psi\rangle$ is at most $2^{\mathcal{O}(\text{poly}\log n)}$, across an equipartition of qubits, starting from $|\psi\rangle^{\otimes m}$.*

Note that for Task 1, when $t = \omega(\text{poly}(n))$, by a Holevo bound, $m = \omega(\text{poly}(n))$. For $t = \mathcal{O}(\text{poly}(n))$, there could potentially be algorithms for which $m$ is polynomially bounded. However, from the collision bound from quantum query complexity [3],

$$m = 2^{\Omega(\text{poly}\log n)/3}, \tag{26}$$

for both Task 1 and Task 2. Here is the proof sketch. Consider two states,

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle ,$$

and

$$|\psi_g\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |g(x)\rangle ,$$

where $f$ is a random 1-to-1 function, and $g$ is a random $2^{n-\text{poly}\log n}$-to-1 function. Then, if $m$ does not satisfy (26), this violates the quantum collision lower bound from query complexity between a 1-to-1 and a $2^{n-\text{poly}\log n}$-to-1 function [3]. However, even though the proof holds, note that neither $|\psi_f\rangle$ or $|\psi_g\rangle$ has a polynomial sized circuit description.

Our pseudorandom constructions allow us to boost the lower bound in (26) to states that have an efficient description [5].

### 3.2.1 Lower bound on eigenvalue estimation for efficiently preparable states

▶ **Task 3.** *Efficiently estimate the largest $t$ eigenvalues of an $n$ qubit mixed state $\rho \in \mathbb{C}^{2^n \times 2^n}$ to $\epsilon = \frac{1}{2^{\mathcal{O}(\text{poly}\log n)}}$ in additive error starting from $\rho^{\otimes m}$ with high probability, where it is promised that $\rho$ has a polynomial sized circuit description* [6].

[4] A similar argument works for any bipartition where each side has size $\Omega(n)$.

[5] Although not explicitly studied, previous pseudoentangled state constructions [15] also imply such lower bounds, but for inverse exponentially small $\epsilon$ or exponentially large Schmidt rank. So, our lower bounds are stronger.

[6] The circuit is allowed to have trace-out gates.

▶ **Lemma 11.** *For Task 3 with* $\epsilon = \frac{1}{2^{\mathcal{O}(\text{poly}\log n)}}$ *and* $t = \mathcal{O}(\text{poly}(n))$*, assuming the existence of quantum secure one-way functions*

$$m = \omega\left(\text{poly}(n)\right).$$

**Proof.** Follows from the security of our pseudoentanglement construction. If we can perform Task 3 with $\mathcal{O}\left(\text{poly}(n)\right)$ copies, it means we can distinguish our high-entanglement pseudorandom state from our low-entanglement pseudorandom state. ◀

▶ Remark 12. Note that an upper bound for Task 3 is given in [29]. They show

$$m = \mathcal{O}\left(t^2/\epsilon^2\right).$$

For $\epsilon = \frac{1}{2^{\mathcal{O}(\text{poly}\log n)}}$ and $t = \text{poly}(n)$,

$$m = 2^{\mathcal{O}(\text{poly}\log n)}.$$

### 3.2.2 Lower bound on estimating the Schmidt rank for efficiently preparable states

▶ **Task 4.** *Efficiently estimate whether an* $n$ *qubit pure state* $|\psi\rangle$ *has Schmidt rank at most* $2^{\mathcal{O}(\text{poly}\log n)}$*, across an equipartition of qubits, starting from* $|\psi\rangle^{\otimes m}$ *with high probability, where it is promised* $|\psi\rangle$ *has a polynomial sized circuit description.*

▶ **Lemma 13.** *For Task 4, assuming the existence of quantum secure one way functions,* $m = \omega\left(\text{poly}(n)\right)$*.*

**Proof.** Follows from the security of our pseudoentanglement construction. If we can efficiently determine whether a state has Schmidt rank at most $r$ for $r = 2^{\mathcal{O}(\text{poly}\log n)}$, with polynomially many copies of $|\psi\rangle$, then we can use that algorithm to distinguish our high-entanglement pseudorandom state, which has Schmidt rank $2^{\Omega(n)}$, from a tunable-entanglement pseudorandom state, which has Schmidt rank $2^{\mathcal{O}(r)}$ [7]. ◀

▶ Remark 14. Note that an upper bound for Task 4, of $m = \mathcal{O}(r)$, is proven in [10]. So, when $r$ is superpolynomially large, $m$ is also superpolynomially bounded.

## 3.3 Improved lower bound for testing matrix product states

Note that pseudorandom states have interesting connections to the learnability of matrix product states, as discussed in [1]. Using pseudoentanglement, we can make these connections much stronger. Specifically, optimally quasi–area law pseudoentanglement means an improved lower bound to the number of copies required to test a matrix product state.

We show that it is difficult to test if a state is an $n$–qubit MPS with bond dimension $r$, or far from such a state, using fewer than $\Omega(\sqrt{r})$ copies of the state, in either information-theoretic or computational settings.

[7] Although our entropy calculations are based on von Neumann entropy, we implicitly also have upper and lower bounds for another entropy measure – the logarithm of the Schmidt rank, which, by virtue of our construction, is just the logarithm of the rank of the high entropy matrix $A$ in B.2.4 or the tunable entropy matrix $B$ in B.4 of [1] From there, we can get corresponding bounds on the Schmidt rank of our constructed states.

### 3.3.1 Previous work

This problem was previously studied in a very recent work by [34], who proved a lower bound of $\Omega(\sqrt{n})$. The lower bound on [34] had no dependence on $r$. The authors also prove an upper bound of $\mathcal{O}(nr^2)$: so, their bounds are significantly loose when $r$ is at least superpolynomially large.

### 3.3.2 Definitions

First, we will introduce some definitions.

▶ **Definition 15** (Matrix product state, [34, Definition 1]). *A quantum state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$ consisting of $n$ qudits is a matrix product state with bond dimension $r$ if it can be written as*

$$|\psi_{1,\ldots,n}\rangle = \sum_{i_1 \in [d_1], \ldots, i_n \in [d_n]} \mathrm{Tr}\left[A_{i_1}^{(1)} \cdots A_{i_n}^{(n)}\right] \cdot |i_1 \cdots i_n\rangle\,,$$

*where each matrix $A_j^{(i)}$ is an $r \times r$ complex matrix, for $i \in [n]$ and $j \in [d_i]$. We write $\mathsf{MPS}_n(r)$ for the set of such states, or more simply $\mathsf{MPS}(r)$ when the dependency on $n$ is clear from the context.*

*Further, for any state $|\phi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, the distance of $|\phi\rangle$ to the set $\mathsf{MPS}(r)$ is defined as*

$$\mathrm{Dist}_r(|\phi\rangle) = \min_{|\psi\rangle \in \mathsf{MPS}(r)} \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \tag{27}$$

[34] also introduced the concept of $\mathsf{MPS}(r)$ tester.

▶ **Definition 16** ($\mathsf{MPS}(r)$ tester). *An algorithm $\mathcal{A}$ is a property tester for $\mathsf{MPS}(r)$ using $m = m(n, r, \delta)$ copies if, given $\delta > 0$ and $m$ copies of $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, it acts as follows.*

- *(Completeness) If $|\psi\rangle \in \mathsf{MPS}(r)$, then*

$$\Pr\left[\mathcal{A} \text{ accepts given } |\psi\rangle^{\otimes m}\right] \geq \frac{2}{3}.$$

- *(Soundness) If $\mathrm{Dist}_r(|\psi\rangle) \geq \delta$, then*

$$\Pr\left[\mathcal{A} \text{ accepts given } |\psi\rangle^{\otimes m}\right] \leq \frac{1}{3}.$$

### 3.3.3 Our results

Following the language of Definition 16, [34] showed that an $\mathsf{MPS}(r)$ tester using $m = O(nr^2/\delta^2)$ copies of the unknown state $|\psi\rangle$ can be constructed, while any $\mathsf{MPS}(r)$ tester must use at least $\Omega(n^{1/2}/\delta^2)$ copies of $|\psi\rangle$.

In this work, we show that this lower bound can be improved to order $\Omega(\sqrt{r})$, which may scale exponentially in terms of $n$. In particular, we prove the following theorem.

▶ **Theorem 17.** *Following the language of Definition 16, for any $r \leq 2^{n/8}$ and $\delta \leq \frac{1}{\sqrt{2}}$, testing whether a state $|\psi\rangle \in \mathbb{C}^{\otimes n}$, is in $\mathsf{MPS}(r)$ requires $\Omega\left(\sqrt{r}\right)$ copies of $|\psi\rangle$.*

Before proving the theorem, we first state some useful results.

▶ **Fact 1** ([37]). *For any state $|\psi\rangle \in \mathbb{C}^{\otimes n}$ and any partition of the state into two parts $A$ and $B$, we denote*

$$\chi_A(|\psi\rangle) \coloneqq \operatorname{rank}(\rho_A), \qquad \rho_A(|\psi\rangle) \coloneqq \operatorname{Tr}_B(|\psi\rangle\langle\psi|)$$

*and*

$$\chi(|\psi\rangle) \coloneqq \max_A \chi_A(|\psi\rangle),$$

*where the maximum is taken over all possible partitions. Then,*

$$|\psi\rangle \in \mathsf{MPS}(\chi(|\psi\rangle)).$$

▶ **Lemma 18** (Young-Eckart Theorem, [13]). *Consider a bipartite state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ with $d_1 \geq d_2$ and let*

$$|\psi\rangle = \sum_{i=1}^{d_2} \sqrt{\lambda_i}\,|a_i\rangle\,|b_i\rangle$$

*be its Schmidt decomposition, where $\lambda_1 \geq \cdots \geq \lambda_{d_2}$. Then,*

$$\operatorname{Dist}_r(|\psi\rangle) = \sqrt{1 - \sum_{i=1}^{r} \lambda_i}.$$

Equipped with Fact 1 and Lemma 18, we are now ready to prove Theorem 17.

**Proof of Theorem 17.** Note that any $\mathsf{MPS}(r)$ tester defined in Definition 16 can distinguish with success probability at least $2/3$ between any two ensembles of quantum states, one only containing matrix product states with bond dimension at most $r$, the other only containing states whose distance to $\mathsf{MPS}(r)$ is at least $\frac{1}{\sqrt{2}}$. In this proof, we explicitly construct such two ensembles and demonstrate that any quantum algorithm having less than $O(\sqrt{r})$ copies of a state $|\psi\rangle$ cannot determine with success probability $2/3$ which of the two ensembles $|\psi\rangle$ is in, thus establishing an $\Omega(\sqrt{r})$ lowerbound for MPS testing.

We use $\mathcal{E}_r$ to denote the ensemble of subset phase states with subset size $r$ and random phase. Quantitatively,

$$\mathcal{E}_r \coloneqq \left\{\, |\psi_{f,S}\rangle \;\middle|\; |S| = r \right\},$$

where $|\psi_{f,S}\rangle$ is defined in (1). Observe that for any partition of any subset phase state $|\psi_{f,S}\rangle$ into two parts $A$ and $B$, the rank of the corresponding reduced density matrix $\rho_A \coloneqq \operatorname{Tr}_B(|\psi\rangle\langle\psi|)$ is upper bounded by $r$. Then by Fact 1, we have

$$\mathcal{E}_r \subseteq \mathsf{MPS}(r).$$

Next, we construct an ensemble of quantum states that are far from $\mathsf{MPS}(r)$. Specifically, we consider the ensemble $\mathcal{E}_{\text{phase}}$ consisting of phase states with random phases,

$$\mathcal{E}_{\text{phase}} \coloneqq \{|\psi_f\rangle\}, \qquad |\psi_f\rangle = \frac{1}{2^n}\sum_x (-1)^{f(x)}\,|x\rangle\,.$$

For any cut $(\mathsf{A}, \mathsf{B})$ of $n$ qubits such that $|\mathsf{A}| = |\mathsf{B}| = n/2$, by calculations in Section B.2 of [1] and Markov's inequality, we know that

$$\Pr_{|\psi_f\rangle \leftarrow \mathcal{E}_{\text{phase}}}\left[\|\rho_{\mathsf{A}:\mathsf{B}}\|_F \leq \frac{1}{2^{n/4}}\right] \geq 1 - 2^{-n/4}.$$

That is to say, if we uniformly randomly select a state $|\psi_f\rangle$ from $\mathcal{E}_{\text{phase}}$, with probability at least $1 - 2^{-n/4}$, its Schmidt decomposition

$$|\psi_f\rangle = \sum_{i=1}^{d_2} \sqrt{\lambda_i}\, |a_i\rangle\, |b_i\rangle$$

satisfies

$$\sum_{i=1}^{d_2} \lambda_i^2 \leq 2^{-n/4},$$

where $\lambda_1 \geq \cdots \geq \lambda_{d_2}$. By Cauchy's ineuqality,

$$\sum_{i=1}^{r} \lambda_i \leq \sqrt{r \cdot 2^{-n/4}} \leq 2^{-n/8} \leq \frac{1}{2}.$$

Then by Lemma 18, we have

$$\Pr_{|\psi_f\rangle \leftarrow \mathcal{E}_{\text{phase}}} \left[ \text{Dist}_r(|\psi_f\rangle) \geq \frac{1}{\sqrt{2}} \right] \geq 1 - 2^{-n/4}. \tag{28}$$

We define $\mathcal{E}'_{\text{phase}}$ to be the set of phase states that are at least $1/\sqrt{2}$-far from $\mathsf{MPS}(r)$. In particular,

$$\mathcal{E}'_{\text{phase}} := \left\{ |\psi_f\rangle \,\middle|\, \text{Dist}_r(|\psi_f\rangle) \geq \frac{1}{\sqrt{2}} \right\}.$$

Based on (28), we have

$$\mathsf{TD}\left( \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}'_{\text{phase}}} \left[ |\psi\rangle\langle\psi|^{\otimes t} \right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathcal{E}_{\text{phase}}} \left[ |\phi\rangle\langle\phi|^{\otimes t} \right] \right) \leq 2^{-n/4}$$

for any $t$. Further, since

$$\mathsf{TD}\left( \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_{\text{phase}}} \left[ |\psi\rangle\langle\psi|^{\otimes t} \right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathscr{H}(\mathbb{C}^N)} \left[ |\phi\rangle\langle\phi|^{\otimes t} \right] \right) < O\left( \frac{t^2}{2^n} \right),$$

we can derive that

$$\mathsf{TD}\left( \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}'_{\text{phase}}} \left[ |\psi\rangle\langle\psi|^{\otimes t} \right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathscr{H}(\mathbb{C}^N)} \left[ |\phi\rangle\langle\phi|^{\otimes t} \right] \right) < O\left( \frac{t^2}{2^{n/4}} \right),$$

where $\mathscr{H}(\mathbb{C}^N)$ denotes the ensemble of Haar random states in the Hilbert space with dimension $N = 2^n$. Moreover, by Theorem 3,

$$\mathsf{TD}\left( \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_r} \left[ |\psi\rangle\langle\psi|^{\otimes t} \right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathscr{H}(\mathbb{C}^N)} \left[ |\phi\rangle\langle\phi|^{\otimes t} \right] \right) < O\left( \frac{t^2}{r} \right),$$

which further leads to

$$\mathsf{TD}\left( \mathop{\mathbb{E}}_{|\psi\rangle \leftarrow \mathcal{E}_r} \left[ |\psi\rangle\langle\psi|^{\otimes t} \right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathcal{E}'_{\text{phase}}} \left[ |\phi\rangle\langle\phi|^{\otimes t} \right] \right) < O\left( \frac{t^2}{2^{n/4}} \right) + O\left( \frac{t^2}{r} \right) < O\left( \frac{t^2}{r} \right).$$

Hence, any quantum algorithm distinguishing between $\mathcal{E}_r$ and $\mathcal{E}_{\text{phase}'}$ with $\Omega(1)$ success probability requires at least $t = \Omega(\sqrt{r})$ copies of the unknown state, which is also the lower bound for MPS testing. ◀

▶ Remark 19. By using appropriate security conjectures and appropriate cryptographic primitives to efficiently instantiate our pseudorandom functions – for example, by one–way functions which are secure upto subexponential time against quantum adversaries [8] – we can get the same lower bounds as in Theorem 17 in the computational setting, when the matrix product state under consideration is guaranteed to have an efficient description.

## 3.4 Applications to quantum gravity

Another application of our result is to quantum gravity. The AdS/CFT correspondence [26] is one of the leading candidates for a theory of quantum gravity. It postulates a duality between a theory of quantum gravity in anti-de Sitter space (AdS) and simple quantum mechanical theory (namely, a conformal field theory (CFT)). The AdS/CFT "dictionary" maps states in one theory to the other, and through this dictionary observables and states are mapped from one theory to the other. In this way one can study properties of quantum gravity via studying a simpler quantum mechanical system. This has led to a series of remarkable results connecting quantum gravity with topics in quantum information such as quantum error correction [4], quantum tensor networks [31], the Eastin-Knill Theorem [14], and quantum circuit complexity [35]. There has even the suggestion that future quantum computers might shed light into quantum gravity [9, 28].

Recently, Bouland, Fefferman and Vazirani [6] showed that the AdS/CFT dictionary might be exponentially complex to compute, even for a quantum computer. This stands in sharp contrast to other dualities in computer science, such as LP and SDP duality, which are efficiently computable. Their argument used the fact that certain information about the geometry of the gravitational theory – in particular information about the interior of a wormhole – seems to be pseudorandomly scrambled in the quantum theory, in a manner analogous to a block cipher such as DES. Therefore efficient computation of the dictionary to reconstruct wormhole interiors allows one to break certain forms of cryptography, which is not believed to be tractable for quantum computers. Their result seems to challenge the quantum Extended Church-Turing thesis, i.e. the conjecture that all physical processes are efficiently simulable by a universal quantum computer.

The arguments of [6] require the presence of a black hole. It is natural to ask if similar arguments might show the dictionary might be exponentially complex in more general gravitational geometries. Indeed, Susskind [36] has suggested this might not be possible, i.e. that without black holes (and outside of the event horizon of black holes) the dictionary is easy to compute.

A potential starting point to investigate this issue is the more general connection between entanglement and geometry in AdS/CFT. It is believed that in AdS/CFT, the entanglement entropy between certain regions of the quantum theory is directly proportional to certain geometrical quantities in the gravity theory (namely, the shortest geodesic between corresponding boundary points in the spacetime), up to small corrections, via the Ryu-Takanayagi formula [32]. Therefore the entanglement entropy of CFT is directly connected to the geometry.

It is natural to ask if this connection between entanglement and geometry already implies the dictionary is exponentially hard to compute. If so this would provide complementary evidence to [6] for the exponential complexity of the dictionary, and potentially remove the need for a black hole in those arguments. This was precisely the suggestion of Hoban and Gheorghiu in their construction of what we call pseudoentanglement [15]. By showing that

[8] One way functions based on LWE are conjectured to have this property.

entanglement entropy is exponentially difficult to compute, even on average, they argued this was evidence for the exponential complexity of the dictionary. Their work left open many future directions to further develop this argument. Most salient is whether or not it is possible to create pseudoentanglement within the subset of holographic states, i.e. states for which the AdS/CFT dictionary is well-defined. Such states exhibit many atypical features, for example sub-volume law (but super-area law) entanglement, which are not properties of Hoban and Gheorghiu's construction.

Our result strengthens the case for this argument, as we show that it is possible to construct pseudorandomness or pseudoentanglement with subvolume law entanglement. This is a necessary but not sufficient condition to construct pseudorandomness and pseudoentanglement within the domain of validity of AdS/CFT, and therefore paves the way to potentially constructing pseudoentanglement with holographic entanglement structures. More speculatively, we believe the "tunable" nature of our construction might be useful for constructing pseudoentanglement with varying geometries, which might form the basis of a future challenge to the quantum ECT without the presence of black holes. We leave further development of this argument to future work.

Finally, we note this line of argument is complementary to very recent work of Aaronson and Pollack [2], who showed that given as input a list of entropies of a CFT state obeying certain conditions, that there is an efficient algorithm to produce a bulk state with the corresponding entropies. In contrast, our work shows that it is difficult to produce the list of entanglement entropies given as input a quantum state. If our argument could be made holographic, this might show the difficulty of the dictionary stems from the ability of quantum states to hide their entanglement entropies.

## 4 Future directions

We close with some natural future directions that are left open by this work.

1. A natural question left open in this work is to understand the importance of the random phases in our subset phase state construction. That is, consider states of the form:

$$|\psi_S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle \tag{29}$$

   Are these states pseudorandom and pseudoentangled if $S \in \{0,1\}^n$ is a pseudo-randomly chosen subset of appropriate size? Note that this is similar to the construction in Section 2 which we discussed in this paper without the pseudorandom phases.
2. Do other families of quantum states achieve tightly tuned pseudoentanglement across any cut? We discuss two variants in [1], where we prove a pseudo–area law scaling of entanglement. However, we only prove an upper bound on the entanglement entropy: It remains to see if our upper bound is tight.
3. Finally, are there further applications of pseudoentanglement to cryptography, complexity theory, and quantum computing?

## References

1 Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement, 2023. arXiv:2211.00747.

2 Scott Aaronson and Jason Pollack. Discrete bulk reconstruction. *arXiv preprint*, 2022. arXiv:2210.15601.

3 Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, July 2004. doi:10.1145/1008731.1008735.

4 Ahmed Almheiri, Xi Dong, and Daniel Harlow. Bulk locality and quantum error correction in AdS/CFT. *Journal of High Energy Physics*, 2015(4):1–34, 2015.

5 Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. *arXiv preprint*, 2021. arXiv:2112.10020.

6 Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality. *arXiv preprint*, 2019. arXiv:1910.14646.

7 Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019.

8 Fernando G.S.L. Brandao, Aram W. Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346(2):397–434, 2016.

9 Adam R. Brown, Hrant Gharibyan, Stefan Leichenauer, Henry W. Lin, Sepehr Nezami, Grant Salton, Leonard Susskind, Brian Swingle, and Michael Walter. Quantum gravity in the lab: teleportation by size and traversable wormholes. *arXiv preprint*, 2019. arXiv:1911.06314.

10 Andrew M. Childs, Aram W. Harrow, and Paweł Wocjan. Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 598–609. Springer, 2007.

11 Jordan Cotler, Nicholas Hunter-Jones, and Daniel Ranard. Fluctuations of subsystem entropies at late times. *Physical Review A*, 105(2):022416, 2022.

12 Oscar Dahlsten and Martin B Plenio. Exact entanglement probability distribution of bi-partite randomised stabilizer states. *arXiv preprint quant-ph/0511119*, 2005.

13 Carl Eckart and Gale Young. The approximation of one matrix by another of lower rank. *Psychometrika*, 1(3):211–218, 1936.

14 Philippe Faist, Sepehr Nezami, Victor V Albert, Grant Salton, Fernando Pastawski, Patrick Hayden, and John Preskill. Continuous symmetries and approximate quantum error correction. *Physical Review X*, 10(4):041018, 2020.

15 Alexandru Gheorghiu and Matty J Hoban. Estimating the entropy of shallow circuit outputs is hard. *arXiv preprint*, 2020. arXiv:2002.12814.

16 Aram Wettroth Harrow. *Applications of coherent classical communication and the Schur transform to quantum information theory*. PhD thesis, Massachusetts Institute of Technology, 2005.

17 Masahito Hayashi and Keiji Matsumoto. Universal distortion-free entanglement concentration, 2002. doi:10.48550/ARXIV.QUANT-PH/0209030.

18 Michał Horodecki. Entanglement measures. *Quantum Info. Comput.*, 1(1):3–26, January 2001.

19 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Lecture Notes in Computer Science*, pages 126–152. Springer International Publishing, 2018. doi:10.1007/978-3-319-96878-0_5.

20 Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, November 2014. doi:10.1201/b17668.

21 Isaac Kim, Eugene Tang, and John Preskill. The ghost in the radiation: Robust encodings of the black hole interior. *Journal of High Energy Physics*, 2020(6):1–65, 2020.

22 William Kretschmer. Quantum pseudorandomness and classical complexity. *arXiv preprint*, 2021. arXiv:2103.09320.

23 William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. *arXiv preprint*, 2022. arXiv:2212.00879.

24 Hari Krovi. An efficient high dimensional quantum schur transform. *Quantum*, 3:122, February 2019. doi:10.22331/q-2019-02-14-122.

**25** Richard A. Low. Large deviation bounds for k-designs. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 465(2111):3289–3308, 2009.

**26** Juan Maldacena. The large-n limit of superconformal field theories and supergravity. *International journal of theoretical physics*, 38(4):1113–1133, 1999.

**27** Ashley Montanaro, Ronald de Wolf, et al. A survey of quantum property testing. *Theory of Computing*, 2016.

**28** Sepehr Nezami, Henry W. Lin, Adam R. Brown, Hrant Gharibyan, Stefan Leichenauer, Grant Salton, Leonard Susskind, Brian Swingle, and Michael Walter. Quantum gravity in the lab: teleportation by size and traversable wormholes, part II. *arXiv preprint*, 2021. arXiv:2102.01064.

**29** Ryan O'Donnell and John Wright. Efficient quantum tomography, 2015. doi:10.48550/ARXIV.1508.01907.

**30** Don N. Page. Average entropy of a subsystem. *Physical Review Letters*, 71(9):1291–1294, August 1993. doi:10.1103/physrevlett.71.1291.

**31** Fernando Pastawski, Beni Yoshida, Daniel Harlow, and John Preskill. Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence. *Journal of High Energy Physics*, 2015(6):1–55, 2015.

**32** Shinsei Ryu and Tadashi Takayanagi. Holographic derivation of entanglement entropy from the anti–de sitter space/conformal field theory correspondence. *Physical review letters*, 96(18):181602, 2006.

**33** Graeme Smith and Debbie Leung. Typical entanglement of stabilizer states. *Physical Review A*, 74(6):062314, 2006.

**34** Mehdi Soleimanifar and John Wright. Testing matrix product states. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1679–1701. SIAM, 2022.

**35** Leonard Susskind. Computational complexity and black hole horizons. *Fortschritte der Physik*, 64(1):24–43, 2016.

**36** Leonard Susskind. Horizons protect church-turing. *arXiv preprint*, 2020. arXiv:2003.01807.

**37** Guifré Vidal. Efficient simulation of one-dimensional quantum many-body systems. *Physical Review Letters*, 93(4), July 2004. doi:10.1103/physrevlett.93.040502.

**38** Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981. doi:10.1016/0022-0000(81)90033-7.

**39** Mark Zhandry. How to construct quantum random functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 679–687. IEEE, 2012.