Quantum Pseudoentanglement

Zhili Chen, Aditya Morolia, Yaonan Zhang

April 26, 2025

Contents

1 Introduction

Randomness is an important resource in classical computation and cryptography. The *hardness vs. randomness* connection [NW94] is an important result in the study of classical complexity, and has implications relevant for cryptography. In [JLS18], the authors define the notion of *pseudorandom quantum states* (PRS), which are efficiently preparable, but indistinguishable from perfectly random (in the Haar sense[1]) quantum states. They show that if one assumes that quantum secure one-way functions exist, one can construct in quantum polynomial time (QPT) (an ensembles of) quantum states that are pseudorandom, which means that no QPT adversary can distinguish between copies of such states and Haar random states. We note that a quantum secure one-way function exists under standard cryptographic assumptions, like the hardness of certain lattice problems [BPR12, Zha12, Zha21].

In the world of quantum information and computation, entanglement is a central resource. It is a form of *quantum correlation* that can exist between quantum states. In [ABF+24], the authors define the notion of *pseudoentanglement*, which is a computational analogue of the information-theoretic notion of entanglement. These notions have many applications in cryptography, complexity theory, and quantum gravity. Here we review some of their results and proof techniques. We note that this report is simply an exposition of their work and contains no new ideas. We first review some elementary quantum information.

1.1 Notation

For $n \in \mathbb{Z}^+$, we denote $[n] = \{0, 1, \ldots, n-1\}$. Given a string $s \in \{0,1\}^n$, the Hamming weight of s is the number of non-zero bits in s, denoted by $\mathrm{hamm}(s)$. Use Perm_t to denote the set of all permutations of t elements. For a set S, we write 2^S to denote the power set of S.

Throughout this text, we only consider finite-dimensional *Hilbert spaces*[2]. For example, a d-dimensional complex vector space equipped with the standard inner product is a Hilbert space, and we denote it by $\mathbb{C}^d$. For any set S where $|S| = k$, we use $\mathbb{C}^S$ to denote the vector space of dimension k where each entry of vectors is indexed by an element in S. It can be viewed as being isomorphic to $\mathbb{C}^k$. The *tensor product* of two vector spaces $\mathbb{C}^{S_1}$ and $\mathbb{C}^{S_2}$ is defined as $\mathbb{C}^{S_1} \otimes \mathbb{C}^{S_2} := \mathbb{C}^{S_1 \times S_2}$, where $S_1 \times S_2$ is the Cartesian product of S_1 and S_2. We use the notation $(\mathbb{C}^S)^{\otimes n}$ to denote the n-fold tensor product of $\mathbb{C}^S$, i.e., $(\mathbb{C}^S)^{\otimes n} = \mathbb{C}^S \otimes \mathbb{C}^S \otimes \cdots \otimes \mathbb{C}^S$ (n times).

1.2 A Little Bit of Quantum Mechanics

Quantum Systems. In the classical world, the *state* of a bit is either 0 or 1. However, *qubits*, analogous to bits in the quantum world, can exist in superpositions of these classical states. A qubit is a 2-dimensional quantum system. In general, a d-dimensional quantum system is represented by a Hilbert space of dimension d. For example, the n-qubit system is commonly represented by the Hilbert space $\mathbb{C}^{2^n}$.

Dirac Notation (Bra-Ket Notations). A *pure state* of a d-dimensional quantum system can be represented as a unit vector $\phi = (\alpha_0, \ldots \alpha_{d-1})^\top \in \mathbb{C}^d$. A unit vector is usually denoted by what is known

[1] The uniform distribution over the set of quantum states and operators corresponds to the distribution corresponding to the Haar measure.

[2] A Hilbert space is a vector space with an inner product that forms a complete metric space with respect to the norm induced by the inner product. This generalizes the notion of Euclidean space. Refer to Hilbert space for details.

as the *ket symbol*, i.e.,

$$|\phi\rangle := \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{bmatrix},$$

where $\sum_{i\in[d]} |\alpha_i|^2 = 1$. For example, in two dimensions, the standard basis states can be represented as the following kets

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

This is simply a convenient notation to work with quantum systems and operators, as the math can get pretty messy really quickly (as we shall demonstrate). Notice that a d-dimensional vector can be written as

$$|\phi\rangle = \sum_{i\in[d]} \alpha_i |i\rangle,$$

where $\{|i\rangle\}_{i\in[d]}$ is an orthonormal basis of $\mathbb{C}^d$. Also, notice that quantum states naturally define a probability distribution on an alphabet (identified by the basis states). Given a ket symbol $|\phi\rangle$, the corresponding *bra symbol* is the *transpose conjugate*[3] of $|\phi\rangle$, denoted by

$$\langle\phi| = (|\phi\rangle)^\dagger.$$

The *inner product* of $|\phi\rangle = \sum_{i\in[d]} \alpha_i |i\rangle$ and $|\psi\rangle = \sum_{i\in[d]} \beta_i |i\rangle$ is defined as the product of the row vector $\langle\phi|$ and the column vector $|\psi\rangle$, and we denote it by

$$\langle\phi|\psi\rangle = \sum_{i\in[d]} \bar{\alpha}_i \beta_i.$$

Similarly, the *outer product* of $|\phi\rangle$ and $\langle\psi|$ is defined as

$$|\phi\rangle\langle\psi| = \sum_{i,j\in[d]} \alpha_i \bar{\beta}_j |i\rangle\langle j|.$$

Linear Operators. Given a Hilbert space $\mathcal{H}$, the space of all linear operators on $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. This represents all operations *physically possible* on a quantum system. Since we only deal with finite-dimensional Hilbert spaces, we can identify these operators with the set of complex matrices. For any operator $A \in \mathcal{L}(\mathcal{H})$, we denote the (i,j)-th entry of it by $A_{i,j}$ and denote its *conjugate transpose* by $A^\dagger$. The *trace* of an operator A is defined as $\mathrm{Tr}(A) := \sum_{i=1}^d A_{ii}$. We define the 1-norm of A as $\|A\|_1 := \mathrm{Tr}(\sqrt{A^\dagger A})$.

Density Operators and Entropy. In quantum mechanics, any state can be represented by a density operator.

Definition 1.1 (Density Operators)**.** *A density operator $\rho \in \mathcal{L}(\mathcal{H})$ is an operator satisfying*

1. *positive semidefinite, i.e., exists $A \in \mathcal{L}(\mathcal{H})$ such that $\rho = A^\dagger A$,*
2. *$\mathrm{Tr}(\rho) = 1$.*

Then we have the following definition of *trace distance*, a measure of distinguishability between two density operators.

[3]The transpose conjugate of a matrix A is obtained by applying transpose on A and applying complex conjugation to each entry. Refer to conjugate transpose.

Definition 1.2 (Trace Distance)**.** *The trace distance between two density operators ρ and σ is defined as*

$$\mathrm{TD}(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1.$$

For any density operator, we can always find a decomposition of it in terms of its eigenvalues and eigenvectors. This is known as the *spectral theorem*, and it applies to any *normal operators*. Here, we only consider density operators for simplicity.

Fact 1.3 (Spectral Theorem)**.** *For any density operator $\rho \in \mathcal{L}(\mathcal{H})$, there exists a spectral decomposition of ρ as follows:*

$$\rho = \sum_{i \in [d]} \lambda_i \left|\phi_i\right\rangle \left\langle\phi_i\right|,$$

where λ_i is the ith eigenvalue of ρ and $\left|\phi_i\right\rangle$ is the corresponding eigenvector. The eigenvalues are real numbers, and the eigenvectors are orthonormal.

A function of a density operator is defined as the function applied to its eigenvalues. For any function $f : \mathbb{R} \to \mathbb{R}$ and a density operator $\rho = \sum_{i \in [d]} \lambda_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$, $f(\rho)$ is defined as follows:

$$f(\rho) := \sum_{i \in [d]} f(\lambda_i) \left|\phi_i\right\rangle \left\langle\phi_i\right|.$$

This allows us to define a measure called *von Neumann (quantum) entropy*[4] capturing the randomness of a quantum state.

Definition 1.4 (von Neumann Entropy)**.** *The von Neumann entropy of a density operator ρ is defined as*

$$S(\rho) := -\operatorname{Tr}(\rho \log \rho) = -\sum_{i \in [d]} \lambda_i \log \lambda_i,$$

where λ_i is the ith eigenvalue of ρ.

Entanglement. Consider an n-qubit system, a *cut* $(\mathsf{X} : \mathsf{Y})$ of it satisfies that $\mathsf{X} \cup \mathsf{Y} = [n]$ and $\mathsf{X} \cap \mathsf{Y} = \emptyset$. Denote the Hilbert space of X and Y to be $\mathcal{H}_{\mathsf{X}}$ and $\mathcal{H}_{\mathsf{Y}}$, respectively. Let ρ be a state of this system. The *reduced density operator* ρ_{X} of ρ on the subsystem X is obtained by tracing out the subsystem Y from the density operator ρ of the whole system. Formally, we have

$$\rho_{\mathsf{X}} = \operatorname{Tr}_{\mathsf{Y}}(\rho) := \sum_{y} (I_{\mathsf{X}} \otimes \langle y|)\rho(I_{\mathsf{X}} \otimes |y\rangle),$$

where I_{X} is the identity operator in $\mathcal{H}_{\mathsf{X}}$. We can define ρ_{Y} similarly. When ρ is a pure state, i.e., $\rho = \left|\psi\right\rangle \left\langle\psi\right|$, we have the following fact stating that the randomness of ρ_{X} is same as the randomness of ρ_{Y}.

Fact 1.5. *For a pure state $\left|\phi\right\rangle \in \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}}$, the reduced density operators ϕ_{X} and ϕ_{Y} are related as follows:*

$$S(\phi_{\mathsf{X}}) = S(\phi_{\mathsf{Y}}).$$

The *entanglement* between X and Y on a pure state is measured by the von Neumann entropy of the reduced density operator.

[4]The von Neumann entropy is the generalization of Shannon entropy to quantum states. Refer to von Neumann entropy.

Definition 1.6 (Entanglement Entropy)**.** *The entanglement entropy of a pure state $|\phi\rangle$ on a bipartite system X and Y is defined as*

$$S(\phi_{\mathsf{X}:\mathsf{Y}}) := S(\phi_{\mathsf{X}}) = S(\phi_{\mathsf{Y}}).$$

Quantum Polynomial-Time Adversaries. Since we want to study security in the quantum setting, the definition for adversaries with quantum resources is needed. A quantum polynomial-time (QPT) adversary is a quantum algorithm that runs in polynomial time. One can also think of it as a *quantum circuit*[5] with polynomial size.

Symmetric Subspace. For a subset $S \subseteq \{0,1\}^n$ and $t \in \mathbb{Z}^+$, the symmetric subspace of $(\mathbb{C}^S)^{\otimes t}$ is the subspace of $(\mathbb{C}^S)^{\otimes t}$ that is invariant under permutation of t subspaces. For any $\sigma \in \mathrm{Perm}_t$, we define

$$P_S(\sigma) := \sum_{x_1,\ldots,x_t \in S} \left|x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(t)}\right\rangle \langle x_1,\ldots,x_t|.$$

Then,

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

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

1.3 Quantum-Secure Pseudorandomness

In this report, we focus on the pseudorandomness notions that are secure against quantum adversaries. We begin with quantum-secure pseudorandom functions and permutations, which are the building blocks of the construction of quantum pseudoentanglement.

Quantum-Secure Pseudorandom Functions and Permutations. The definitions for quantum-secure pseudorandom functions and permutations are similar to the classical ones, but with the requirement that the adversary is a QPT algorithm. Informally, a function f (permutation p) sampled uniformly at random from a family of quantum-secure pseudorandom functions (permutations) is indistinguishable from a truly random function (permutation) to any QPT adversary.

Haar Random Quantum States and Pseudorandom Quantum States. In the quantum setting, we want to construct pseudorandom quantum states that are computationally indistinguishable from 'random' quantum states. Like the classical random string sampled uniformly from $\{0,1\}^n$, we want a 'random' quantum state to be sampled uniformly from the space of all quantum states. The distribution of such 'random' quantum states corresponds to the *Haar measure*. Informally, the Haar measure on a Hilbert space $\mathcal{H}$ is a uniform distribution over the unit sphere in $\mathcal{H}$. We denote a Haar random state $|\phi\rangle$ sampled according to the Haar measure on $\mathcal{H}$ by $|\phi\rangle \leftarrow \mathscr{H}(\mathcal{H})$.

The notion of quantum pseudorandom states (PRS) was first introduced by Ji, Liu, and Song in [JLS18]. Informally, the quantum pseudorandom states are computationally indistinguishable from Haar random states by any QPT algorithms.

Pseudoentanglement. Now we move on to the pseudoentangled state. The pseudoentangled states are quantum states that are computationally indistinguishable from Haar random states, but have low entanglement across any cut. The pseudoentangled state ensemble was defined in [ABF+24] as follows.

Definition 1.7. *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 $k \in \{0,1\}^{\mathsf{poly}(n)}$, with the following properties:*

[5] The analogue of Boolean circuits. Refer to quantum circuit.

- *Given k, $|\Psi_k\rangle$ ($|\Phi_k\rangle$, respectively) is efficiently preparable by a uniform, poly-sized quantum circuit.*
- *With probability at least $1 - \frac{1}{\mathsf{poly}(n)}$ 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 non-negligible probability. That is, for any QPT algorithm $\mathcal{A}$, we have that*

$$|\mathcal{A}(\rho) - \mathcal{A}(\sigma)| \leq \mathsf{negl}(n).$$

1.4 Subset Phase State

Let $S \subseteq \{0,1\}^n$, $n \in \mathbb{Z}^+$ be a subset. Note that elements of S can be identified with integers $[N]$, where $N = 2^n$. Let $f : \{0,1\}^n \to \{0,1\}$ be a binary function. A *subset phase state* is a quantum state of the following form

$$|\psi_{f,S}\rangle := \frac{1}{\sqrt{|S|}} \sum_{x \in S} (-1)^{f(x)} |x\rangle . \tag{1.1}$$

In [ABF+24], the authors identify such states and show the following results.

- **Efficient preparation.** They show that when the subset S and the function f are pseudorandomly chosen, then one can efficiently prepare a subset phase state. Note that a pseudorandom subset S can be identified with a pseudorandom permutation applied to strings of up to a certain Hamming weight.
- **Statistical closeness to Haar random states.** They show that if $|S| = 2^{\omega(\log n)}$, and if f is *truly* random, then polynomially many copies of (the density matrix corresponding to) the state in eq. (1.1) is statistically close (in trace distance) to polynomially many copies of a Haar random state.
- **Computational indistinguishability from Haar random states.** They use a hybrid argument to show that if a certain cryptographic conjecture is true, then one can efficiently prepare pseudorandom subset phase states that are computationally indistinguishable from a truly random subset phase state to a QPT adversary.

In addition to this, they also show that one can construct subset phase states such that there is an optimally low pseudoentanglement across any cut, and show that one can, in fact tune the amount of entanglement by varying the size of the subset S.

2 Construction of Subset Phase State

We now show how to efficiently prepare a (pseudorandom) subset phase state, given a pseudorandom function $f : [2^n] \to \{0,1\}$, a pseudorandom permutation p and an integer $k \in \mathbb{Z}^+$. The subset S is identified as follows: S consists of all strings one can get by applying the permutation p to strings of the

form $x0^{n-k}$, where $x \in \{0,1\}^k$, that is, zeros appended to an arbitrary string of length k. The quantum algorithm follows the following sequence of transformations[6].

$$|0^n\rangle \xmapsto{H^{\otimes k}\otimes I^{\otimes(n-k)}} \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x0^{\otimes(n-k)}\rangle \tag{2.1}$$

$$\xmapsto{p} \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x0^{\otimes(n-k)}\rangle\, |p(x0^{\otimes(n-k)})\rangle \tag{2.2}$$

$$\xmapsto{p^{-1}} \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |p(x0^{\otimes(n-k)})\rangle \tag{2.3}$$

$$\xmapsto{f} \frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))}\, |p(x0^{\otimes(n-k)})\rangle \tag{2.4}$$

$$= \frac{1}{\sqrt{2^k}} \sum_{x\in S} (-1)^{f(x)}\, |x\rangle\,. \tag{2.5}$$

3 Statistical Indistinguishability from Haar Random States

In this section we sketch the proof from [ABF+24] of the fact that (polynomially many copies of) the subset phase state in eq. (1.1), for a *truly* random subset S and function f, is close in trace distance to (polynomially many copies of) a Haar random state. The proof follows from a sequence of hybrids that relate the expectation over Haar random states to subset phase states. We will first state some results that we need to prove. The following fact says that polynomially many copies of a Haar random state can be interpreted as a normalized projector onto the symmetric subspace of the Hilbert space spanned by the basis states corresponding to the strings in $[N]$. Here, t is polynomial in n. A proof of this fact can be found in [Har13].

Fact 3.1.

$$\mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathscr{H}(\mathbb{C}^N)} \left[|\phi\rangle\langle\phi|^{\otimes t}\right] = \frac{\Pi_{sym}^{N,t}}{\mathrm{Tr}\left(\Pi_{sym}^{N,t}\right)}. \tag{3.1}$$

Next, they show that the normalized projector over *all* basis states is close in trace distance to a normalized projector onto the span of basis vectors corresponding to elements of a *randomly chosen subset* of all basis states. The distance naturally depends on the size of the subset chosen. We provide a short proof sketch.

Lemma 3.2 (Lemma 2.2, [ABF+24])**.**

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S \text{ with } |S|=K}\left[\frac{\Pi_{sym}^{S,t}}{\mathrm{Tr}(\Pi_{sym}^{S,t})}\right], \frac{\Pi_{sym}^{N,t}}{\mathrm{Tr}(\Pi_{sym}^{N,t})}\right) \leq \mathcal{O}\left(t^2/K\right) \tag{3.2}$$

where the expectation is taken over all subsets $S \subseteq \{0,1\}^n$ with fixed size $|S| = K$, and $K \geq t$.

Proof Sketch. To prove this lemma, they first define a *type* of a basis vector as follows. Let $v \in [N]^t$. Then $\mathrm{type}(v) \in [t+1]^N$ is a vector of N dimensions that counts the frequency of each of the N possible

[6]We abuse notation and only introduce ancillas as needed.

entries of v. Then, for one such vector $T \in [t+1]^N$, define

$$|\mathrm{type}_T\rangle := \beta \sum_{\substack{v \in [N]^t \\ \mathrm{type}(v)=T}} |v\rangle\,, \tag{3.3}$$

where β is a normalization parameter. Next, they define

$$\mathcal{T}(S,t) := \{\, T \in \{\,0,1\,\}^N \mid \mathrm{hamm}(T) = t \text{ and the non-zero entries of } T \text{ have indices in } S\,\}\,. \tag{3.4}$$

They show that the following inequalities hold for all $N, t \in \mathbb{Z}^+$ with $N = 2^n$, and for any $S \subseteq \{\,0,1\,\}^n$ with $|S| = K$ and $K \geq t$.

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{T \leftarrow \{\,0,1\,\}^N \\ \mathrm{hamm}(T)=t}} |\mathrm{type}_T\rangle\langle\mathrm{type}_T|\,, \frac{\Pi_{\mathrm{sym}}^{N,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{N,t})}\right) \leq \mathcal{O}\left(\frac{t^2}{N}\right). \tag{3.5}$$

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{T \leftarrow \mathcal{T}(S,t)} |\mathrm{type}_T\rangle\langle\mathrm{type}_T|\,, \frac{\Pi_{\mathrm{sym}}^{S,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{S,t})}\right) \leq \mathcal{O}\left(\frac{t^2}{N}\right). \tag{3.6}$$

Now, observe that is S is a random subset of $\{\,0,1\,\}^n$, then for any $T \in \{\,0,1\,\}^N$ with $\mathrm{hamm}(T) = t$, the probability

$$p_T := \mathop{\Pr}_{\substack{T' \leftarrow \mathcal{T}(S,t) \\ S \leftarrow 2^{\{\,0,1\,\}^n}}} [T' = T]$$

is uniform over T such that $\mathrm{hamm}(T) = t$. To see this, simply observe that a random choice from $\mathcal{T}(S,t)$, when S is random, behaves as a random choice from all types T. Note that the size of the subset has to be $K = |S| \geq t$. This immediately gives us the following.

$$\mathop{\mathbb{E}}_{S:|S|=K}\left[\mathop{\mathbb{E}}_{T \leftarrow \mathcal{T}(S,t)} [|\mathrm{type}_T\rangle\langle\mathrm{type}_T|]\right] = \mathop{\mathbb{E}}_{\substack{T \leftarrow \{0,1\}^N \\ \mathrm{hamm}(T)=t}} [|\mathrm{type}_T\rangle\langle\mathrm{type}_T|]\,. \tag{3.7}$$

Hence,

$$\begin{aligned}\mathsf{TD}\left(\mathop{\mathbb{E}}_{S:|S|=K}\left[\frac{\Pi_{\mathrm{sym}}^{S,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{S,t})}\right], \frac{\Pi_{\mathrm{sym}}^{N,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{N,t})}\right) &\leq \mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{T \leftarrow \{0,1\}^N \\ \mathrm{hamm}(T)=t}} [|\mathrm{type}_T\rangle\langle\mathrm{type}_T|]\,, \frac{\Pi_{\mathrm{sym}}^{N,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{N,t})}\right) &(3.8)\\ &\quad + \mathop{\mathbb{E}}_{S:|S|=K}\left[\mathsf{TD}\left(\mathop{\mathbb{E}}_{T \leftarrow \mathcal{T}(S,t)} [|\mathrm{type}_T\rangle\langle\mathrm{type}_T|]\,, \frac{\Pi_{\mathrm{sym}}^{S,t}}{\mathrm{Tr}(\Pi_{\mathrm{sym}}^{S,t})}\right)\right] \\ &\leq \mathcal{O}\left(t^2/K\right). &(3.9)\end{aligned}$$

□

We are now ready to show the main result.

Theorem 3.3. *For any $t < K \leq 2^n$, it holds that*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S:|S|=K}\left[|\psi_{f,S}\rangle\langle\psi_{f,S}|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle \leftarrow \mathscr{H}(\mathbb{C}^N)}\left[|\phi\rangle\langle\phi|^{\otimes t}\right]\right) \leq \mathcal{O}\left(\frac{t^2}{K}\right), \tag{3.10}$$

where $\mathcal{H}(\mathbb{C}^N)$ denotes the ensemble of Haar random states in the complex Hilbert space with dimension $N = 2^n$.

Notice that when $K = 2^{\omega(\log n)}$ and t is polynomially bounded, the RHS of eq. (3.10) is bounded by $\frac{1}{\mathsf{poly}(n)}$, which is negligible in n.

Proof Sketch. The proof follows from a hybrid argument. Consider the following distributions, when S is a fixed subset.

Hybrid 1. Choose a binary function $f : \{0,1\}^n \to \{0,1\}$ uniformly at random. Output t copies of the subset phase state corresponding to this S and f. In expectation, the output density matrix is

$$\mathop{\mathbb{E}}_{f} \left[|\psi_{f,S}\rangle \langle \psi_{f,S}|^{\otimes t} \right].$$

Hybrid 2. Sample a vector $w \in S^t$ uniformly at random. Let $T = \text{type}(w) \pmod 2$. Define

$$|\text{bintype}_T\rangle := \beta_T \sum_{\substack{v \in S^t \\ \text{type}(v) \pmod 2 = T}} |v\rangle .$$

Output $|\text{bintype}_T\rangle$.

Hybrid 3. Sample $T \in \mathcal{T}(S,t)$ uniformly at random and output the state $|\text{type}_T\rangle$.

They claim that Hybrid 1 and Hybrid 2 are identical. Here is a short proof. Hybrid 1 outputs

$$\begin{aligned}
\rho &= \mathop{\mathbb{E}}_{f} \left[\left(\frac{1}{\sqrt{|S|^t}} \sum_{x_1,\dots x_t \in S} (-1)^{f(x_1)+\dots+f(x_t)} |x_1,\dots x_t\rangle \right) \left(\frac{1}{\sqrt{|S|^t}} \sum_{y_1,\dots y_t \in S} (-1)^{f(y_1)+\dots+f(y_t)} \langle y_1,\dots y_t| \right) \right] \\
&= \frac{1}{|S|^t} \mathop{\mathbb{E}}_{f} \left[\left(\sum_{\substack{x_1,\dots x_t \in S \\ y_1,\dots y_t \in S}} (-1)^{f(x_1)+\dots+f(x_t)+f(y_1)+\dots+f(y_t)} |x_1,\dots x_t\rangle \langle y_1,\dots y_t| \right) \right] \\
&= \frac{1}{|S|^t} \left(\sum_{\substack{x_1,\dots x_t \in S \\ y_1,\dots y_t \in S}} \mathop{\mathbb{E}}_{f} \left[(-1)^{f(x_1)+\dots+f(x_t)+f(y_1)+\dots+f(y_t)} \right] |x_1,\dots x_t\rangle \langle y_1,\dots y_t| \right) \\
&= \frac{1}{|S|^t} \left(\sum_{\substack{x,y \in S^t \\ \text{type}(x)=\text{type}(y) \pmod 2}} |x\rangle \langle y| \right).
\end{aligned}$$

Hybrid 2 outputs

$$\begin{aligned}
\rho' &= \mathop{\mathbb{E}}_{w \in S^t} \left[\left(\beta_w \sum_{\substack{v \in S^t \\ \text{type}(v)=\text{type}(w) \pmod 2}} |v\rangle \right) \left(\beta_w \sum_{\substack{v' \in S^t \\ \text{type}(v')=\text{type}(w) \pmod 2}} \langle v'| \right) \right] \\
&= \frac{1}{|S|^t} \left(\sum_{\substack{v,v' \in S^t \\ \text{type}(v)=\text{type}(v') \pmod 2}} |v\rangle \langle v'| \right).
\end{aligned}$$

Notice that their outputs are identical.

Now we turn to Hybrids 2 and 3. Notice that when $w \in S^t$ is sampled uniformly at random, the probability that w has no collisions in its entries is at least $1 - t^2/|S|$. Therefore, if $T = \text{type}(w) \pmod 2$ then the probability that $\text{hamm}(T) = t$ is at least $1 - t^2/|S|$. Therefore, the trace distance between the outputs of Hybrids 2 and 3 is $\mathcal{O}\left(t^2/|S|\right)$. Then by eq. (3.6), and by chaining together the Hybrids 1, 2, and 3, we get that

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{f}\left[|\psi_{f,S}\rangle\langle\psi_{f,S}|\right], \frac{\Pi_{\text{sym}}^{S,t}}{\text{Tr}(\Pi_{\text{sym}}^{S,t})}\right) \leq \mathcal{O}\left(\frac{t^2}{|S|}\right). \tag{3.11}$$

Equation (3.11) says that for a *fixed* S but randomly chosen binary phases, the expected state is close in trace distance to the normalized projector onto the Hilbert subspace defined on the span of that subset. The distance, naturally, depends on the size of the set chosen. We are now ready to prove the final result. In the following, we use fact 3.1 in the second line, lemma 3.2 and the triangle inequality in the third line, and the joint convexity of trace distance in the fourth line, that is,

$$\mathsf{TD}\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \leq \sum_i p_i\,\mathsf{TD}(\rho_i,\sigma_i),$$

and eq. (3.11) in the last line to get

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S:|S|=K,f}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{|\phi\rangle\leftarrow\mathscr{H}(\mathbb{C}^N)}\left[|\phi\rangle\langle\phi|^{\otimes t}\right]\right) \tag{3.12}$$

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{S:|S|=K,f}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \frac{\Pi_{\text{sym}}^{N,t}}{\text{Tr}(\Pi_{\text{sym}}^{N,t})}\right) \tag{3.13}$$

$$\leq \mathsf{TD}\left(\mathop{\mathbb{E}}_{S:|S|=K,f}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \mathop{\mathbb{E}}_{S:|S|=K}\left[\frac{\Pi_{\text{sym}}^{S,t}}{\text{Tr}(\Pi_{\text{sym}}^{S,t})}\right]\right) + \mathcal{O}\left(t^2/K\right) \tag{3.14}$$

$$\leq \mathop{\mathbb{E}}_{S:|S|=K}\left[\mathsf{TD}\left(\mathop{\mathbb{E}}_{f}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \frac{\Pi_{\text{sym}}^{S,t}}{\text{Tr}(\Pi_{\text{sym}}^{S,t})}\right)\right] + \mathcal{O}\left(t^2/K\right) \tag{3.15}$$

$$\leq \max_{S:|S|=K}\left[\mathsf{TD}\left(\mathop{\mathbb{E}}_{f}\left[|\psi\rangle\langle\psi|^{\otimes t}\right], \frac{\Pi_{\text{sym}}^{S,t}}{\text{Tr}(\Pi_{\text{sym}}^{S,t})}\right)\right] + \mathcal{O}\left(t^2/K\right) \tag{3.16}$$

$$\leq \mathcal{O}\left(t^2/K\right). \tag{3.17}$$

This concludes the proof sketch. □

4 Computational Indistinguishability from Haar Random States

Now we show that when the binary function f and the subset S are pseudorandomly chosen from a family of pseudorandom functions and permutations that are secure against a quantum adversary, then the corresponding subset phase state is computationally indistinguishable from a Haar random state. That is, such states form an ensemble of pseudorandom quantum states, with the secret key being the description of the function and the permutation. Formally, [ABF+24] shows the following theorem.

Theorem 4.1. *Suppose*

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

is a family of quantum-secure pseudorandom permutations, and

$$F = \{\, f : [2^n] \to \{0,1\} \,\}$$

is a family of quantum-secure pseudorandom functions. Suppose $k \in \omega(\log n)$. Then, the ensemble of subset phase states is defined as

$$|\psi_{f,p}\rangle = \frac{1}{\sqrt{2^k}} \sum_{x \in \{0,1\}^k} (-1)^{f(p(x0^{\otimes(n-k)}))} |p(x0^{\otimes(n-k)})\rangle \,, \tag{4.1}$$

where $p \in P, f \in F$ form an ensemble of pseudorandom quantum states, with the secret key being the description of f, p, p^{-1}.

Proof Sketch. The efficiency of construction follows from section 2. We show security, that is, the fact that such states are indistinguishable from Haar random states. By definition of pseudorandom functions and permutations, it is clear that f is indistinguishable from r_f, and p is indistinguishable from r_p, where r_p and r_f are truly random permutations and function. This indistinguishability holds even when the adversary is given the inverse permutation. Therefore, no polynomial time adversary can distinguish between (f, p, p^{-1}) and $(r_f, r_p, r_{p^{-1}})$, given black box query access to them. Now they use a hybrid argument to complete the proof. Consider the following sequence of hybrids.

Hybrid 1. Prepare and return the state $|\psi_{f,p}\rangle^{\otimes t}$, where

$$|\psi_{f,p}\rangle = \frac{1}{\sqrt{2^k}} (-1)^{f(p(x0^{\otimes(n-k)}))} |p(x0^{\otimes(n-k)})\rangle \,. \tag{4.2}$$

Hybrid 2. Prepare and return the state $|\psi_{r_f,r_p}\rangle^{\otimes t}$, where

$$|\psi_{r_f,r_p}\rangle = \frac{1}{\sqrt{2^k}} (-1)^{r_f(r_p(x0^{\otimes(n-k)}))} |r_p(x0^{\otimes(n-k)})\rangle \,. \tag{4.3}$$

Hybrid 3. Prepare and return polynomially many copies of a Haar random state.

Suppose there is an efficient adversary $\mathcal{A}$ that can distinguish between Hybrids 1 and 2 with a non-negligible advantage. Then, there exists another efficient adversary that prepares that given oracle access to either (f, p, p^{-1}) or $(r_f, r_p, r_{p^{-1}})$, prepares the state corresponding to either eq. (4.2) or eq. (4.3), and uses $\mathcal{A}$ to distinguish between the two cases. Further, Hybrids 2 and 3 are indistinguishable by theorem 3.3 (statistical indistinguishability). This concludes the proof. □

5 Construction of Pseudoentangled State

We have proved that a family of subset phase states $\{|\psi_{f,p}\rangle\}$, with p from a family of quantum–secure pseudorandom permutations, f from a family of quantum–secure pseudorandom functions, and $k = \omega(\log n)$, is a family of pseudorandom quantum states (PRS). In this section we analyze the entanglement entropy for the optimally low case $k = \mathsf{poly}\log n$, and then show how to tightly tune the entanglement by varying the subset size. These give us the construction of PES satisfying Definition 1.7 for any $\omega(\log n) \leq f(n), g(n) \leq n$.

5.1 Entanglement Entropy of pseudorandom subset phase states

Fact 5.1 ([JLS18])**.** *A simple SWAP test argument shows that any pseudorandom quantum state must necessarily have $\omega(\log n)$ entanglement entropy across any cut.*

Theorem 5.2. *Let $|\psi_{f,p}\rangle$ be an n-bit pesudorandom subset phase state with $k \in \mathsf{poly}\log n \cap \omega(\log n)$, and let $\rho = |\psi_{f,p}\rangle\langle\psi_{f,p}|$ be the corresponding density matrix. Then for any cut (X, Y) of n qubits, the von Neumann entanglement entropy*

$$S(\rho_{X:Y}) = \Theta(\mathsf{poly}\log n). \tag{5.1}$$

Proof. The upper bound follows from the definition of $|\psi_{f,p}\rangle$. The rank of ρ is at most $|S|$, so

$$S(\rho_{X:Y}) = \mathcal{O}\left(\log|S|\right) = \mathcal{O}\left(\mathsf{poly}\log n\right). \tag{5.2}$$

The lower bound follows from the SWAP test since $|\psi_{f,p}\rangle$ is a PRS. □

This shows that when $|S| = 2^{\mathsf{poly}\log n}$, 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.

5.2 Tuning the entanglement entropy

Consier a family of pseudorandom subset phase states $\{|\psi_{f,p}\rangle\}$ where

$$f := h(q(i)), \tag{5.3}$$

h is from a 4-wise independent function family $H = \{h : [2^n] \to \{0,1\}\}$, q is from a quantum–secure pseudorandom permutation family $Q = \{q : [2^n] \to [2^n]\}$. Therefore f is both pseudorandom and 4-wise independent.

Theorem 5.3 (Theorem 2.7, [ABF+24])**.** *Let $\omega(\log n) \le k \le n$ and let $|S| = 2^k$. Consider a cut (X, Y) of n qubits, such that $|\mathsf{X}| + |\mathsf{Y}| = n$ and $|\mathsf{X}|, |\mathsf{Y}| \ge k$. Let the pseudorandom phase function satisfy eq. (5.3). Then, with at least $1 - \frac{1}{\mathsf{poly}(n)}$ probability over the choice of the state,*

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) = \Theta(k). \tag{5.4}$$

Proof. The upper bound still follows from that rank of ρ is at most $|S|$. For the lower bound, we will use the inequality,

$$\mathsf{S}(\rho_{\mathsf{X}:\mathsf{Y}}) \ge -\log\left(\left|\left|\frac{1}{2^k} B_{\mathsf{X}:\mathsf{Y}} B_{\mathsf{X}:\mathsf{Y}}{}^{\mathsf{T}}\right|\right|_F\right), \tag{5.5}$$

where $B_{\mathsf{X}:\mathsf{Y}}$ is the pseudorandom matrix corresponding to the partition (X, Y):

$$B_{\mathsf{X}:\mathsf{Y},i,j} := \begin{cases} f(i,j) & \text{if } ij \in S, i \in \{0,1\}^m, j \in \{0,1\}^{n-m}, \\ 0 & \text{otherwise.} \end{cases} \tag{5.6}$$

Equation (5.5) can be derived by Jensen's inequality. Hence, it suffices to lower bound the quantity

$$\log\left(\left|\left|\frac{1}{2^k} B_{\mathsf{X}:\mathsf{Y}} B_{\mathsf{X}:\mathsf{Y}}{}^{\mathsf{T}}\right|\right|_F\right). \tag{5.7}$$

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,

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

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

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

Finally, by the Markov's inequality, we have

$$\Pr\left[\left\|\frac{1}{2^k}BB^{\mathsf{T}}\right\|_F^2 > 2^{-k/4}\right] \leq 2^{1-k/2}. \tag{5.8}$$

Therefore,

$$\Pr\left[\left\|\frac{1}{2^k}BB^{\mathsf{T}}\right\|_F > 2^{-k/8}\right] \leq 2^{1-k/2}. \tag{5.9}$$

Hence, the proof follows. □

6 Applications and Open Problems

6.1 Applications

1. Low-entropy pseudorandom states imply inefficient entropy distillation protocols. Given an unknown $|\psi\rangle^{\otimes m}$, there is an LOCC protocol, which runs in $\mathsf{poly}(n)$ time, to get at least p EPR pairs,

where

$$p \geq m\left(\mathsf{S}(\rho) - \eta(\delta) - \delta \log d\right) - \frac{1}{2} d(d+1) \log(m+d), \tag{6.1}$$

with probability at least

$$1 - \exp\left(\frac{-n\delta^2}{2}\right)(n+d)^{d(d+1)/2}, \tag{6.2}$$

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

2. The main result implies new lower bounds in property testing. It can be used to 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 ("MPS-testing" problem), and to estimate the Schmidt rank of many copies of an unknown quantum state ("Schmidt rank estimation" problem).

3. Applications to quantum gravity. The AdS/CFT correspondence 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 a simple quantum mechanical theory. One of the most salient open problems 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 [GH24].

   The main result of this paper shows 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.

6.2 Open Problems

1. To better understand the importance of the random phases in our subset phase state construction. That is, consider states of the form:

$$|\psi_S\rangle = \frac{1}{|S|} \sum_{x \in S} |x\rangle . \tag{6.3}$$

   Are these states pseudorandom and pseudoentangled if $S \in \{0,1\}^n$ is a pseudorandomly chosen subset of appropriate size?

2. Do other families of quantum states achieve tightly tuned pseudoentanglement across any cut? This paper discusses some variants in the Appendix, but only proves an upper bound on the entanglement entropy. It remains to see if the upper bound is tight.

3. Are there further applications of pseudoentanglement to cryptography, complexity theory, and quantum computing?

References

[ABF+24] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum Pseudoentanglement. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:21, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 2, 5, 6, 7, 10, 12

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Proceedings of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'12, page 719–737, Berlin, Heidelberg, 2012. Springer-Verlag. 2

[GH24] Alexandru Gheorghiu and Matty J. Hoban. On estimating the entropy of shallow circuit outputs, 2024. 14

[Har13] Aram W. Harrow. The church of the symmetric subspace, 2013. 7

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in cryptology—CRYPTO 2018. Part III*, volume 10993 of *Lecture Notes in Comput. Sci.*, pages 126–152. Springer, Cham, 2018. 2, 5, 11

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, October 1994. 2

[Zha12] Mark Zhandry. How to construct quantum random functions. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, FOCS '12, page 679–687, USA, 2012. IEEE Computer Society. 2

[Zha21] Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), August 2021. 2