Quantum Pseudoentanglement and Pseudorandomness

Siddhant Midha[1, *]

[1] *Princeton Quantum Initiative, Princeton University, Princeton, New Jersey 08540, USA*

Insights from the theory of cryptography have led to profound developments in quantum information science in the past decade. In particular, the cryptographic notion of security against computationally bounded adversaries is naturally aligned with the perspective of a quantum pragmatist: which quantum properties can be *efficiently* observed or distinguished? The concept of *pseudorandomness* formalizes this question. In the classical setting, pseudorandom functions are efficiently computable yet indistinguishable from truly random functions to any efficient adversary. In the quantum realm, this idea extends to *pseudorandom unitaries*, which are efficiently constructible but indistinguishable from Haar-random unitaries by efficient quantum algorithms. A more constrained notion is *pseudoentanglement*, referring to ensembles of quantum states that appear genuinely entangled to efficient observers. We summarize a small but significant subset of recent developments in the theory of pseudorandom unitaries and pseudorandom states.

I. INTRODUCTION

Highly entangled quantum states—and, more generally, Haar-random unitaries—exhibit a range of powerful and theoretically useful properties. However, realizing such objects typically requires exponential resources, rendering them infeasible to construct or manipulate in practice. These systems are characterized by extremely high entanglement, but this raises a natural question: can such entanglement actually be observed or verified efficiently? This question motivates a fundamental distinction between two types of properties: *information-theoretic* and *computational*.

Information-theoretic properties describe what is possible in principle, assuming unbounded computational resources and access to an infinite number of copies of a quantum state. Quantities such as von Neumann entropy, and other combinations of entropic measures, fall into this category. They often have clear operational interpretations, revealing what a state theoretically allows in terms of communication, compression, or transformation tasks. However, these interpretations make no claims about the efficiency with which such tasks can be carried out.

In contrast, *computational* properties refer to what is achievable within bounded resources—typically measured in terms of time or memory as a function of input size of the problem. They better reflect practical considerations, since any real-world agent attempting to extract or verify a property must operate under such constraints. Crucially, this distinction implies that certain tasks may be information-theoretically possible, yet computationally infeasible. These limitations often rest on standard assumptions from computational complexity or cryptography.

Motivated by this distinction, we consider the problem of efficiently observing or detecting quantum properties. Specifically, we ask: given a quantum state promised to come from one of two possible ensembles, can an efficient algorithm distinguish between them based on their entanglement structure? More precisely, are there ensembles of efficiently preparable quantum states that cannot be efficiently distinguished from volume-law entangled (i.e., Haar-random) states? Under widely believed cryptographic assumptions, the answer is yes. This phenomenon is known as *pseudoentanglement*.

We extend this idea further to the realm of unitaries. We ask whether there exists an efficiently generable ensemble of unitaries that is computationally indistinguishable from Haar-random unitaries. We refer to such objects as *pseudorandom unitaries (PRUs)*. A PRU, if such an object exists, creates a pseudoentangled state upon application, and is thus a strictly stronger requirement.

Psuedorandom functions are classical objects which look indistinguishable from truly random functions to any polynomial time adversary [1]. In 2018, Ji, Liu, and Song proposed that certain quantum states could be constructed efficiently and yet appear indistinguishable from Haar-random states to any quantum polynomial-time adversary [2]. Building upon this notion, Aaronson et al. [3] introduced and proved some key results about pseudoentangled quantum states (PRS).

Then, PRUs were introduced as a natural extensions of PRS, and also quantum counterparts of pseudorandom functions. Follow up works [4, 5] provided constructions of PRUs robust to parallel queries, where an adversary queries all the copies *at once*. Then, the work of Ma and Huang [6] provided a proof of adaptive security as well. Quantum pseudorandomness has already been helpful in making advances in black hole physics [7, 8], building on the idea that Haar randomness, a previously conjectured model of black holes, is inherently unphysical.

This article is structured as follows. We first discuss notations and important preliminaries in Sec. II. Notably, we recap some results about designs in Sec. II B, define the oracle access model in Sec. II C and discuss some cryptographic primitives in Sec. II D. We then study pseudoentangled states in Sec. III and pseudorandom unitaries in Sec. IV. Then, we discuss the compressed oracle method in Sec. V. Finally, we discuss the adaptive

* siddhantm@princeton.edu

security proofs with path recording oracles in Sec. VI. We wrap up with outlook and discussions in VII.

II. PRELIMINARIES

A. Notations

Registers and states. A quantum system is said to be a register, denoted X. For an $n-$qubit register with $\mathsf{X} = [n]$, we have the associated Hilbert space $\mathcal{H}_{\mathsf{X}} \cong \bigotimes_{i\in\mathsf{X}} \mathcal{H}_i$ with $\mathcal{H}_i \cong \mathbb{C}^{\otimes 2}$. Pure states on X live in the Hilbert space, $|\psi\rangle_{\mathsf{X}} \in \mathcal{H}_{\mathsf{X}}$. Mixed states are unit-trace positive-semidefinite operators $\rho_{\mathsf{X}} \in \mathcal{D}(\mathcal{H}_{\mathsf{X}})$. For $\mathsf{Y} \subseteq \mathsf{X}$ we denote $\rho_{\mathsf{Y}} := \mathrm{tr}_{\mathsf{X}/\mathsf{Y}}\, \rho_{\mathsf{X}}$. Lastly, we denote $N = 2^n$. Let also Sym_n denote the symmetric group on n elements.

Entropies and Distances The von-Neumann entropy of a state $\rho \in \mathcal{D}(\mathcal{H})$ is defined as $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$. The relative entropy of two states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is defined as $S(\rho||\sigma) = \mathrm{Tr}(\rho(\log\rho - \log\sigma)) \geq 0$. The trace distance between two states ρ, σ is defined as $\mathrm{TD}(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1$, where $\|X\|_1$ is the trace norm.

Asymptotic Notations We use the following asymptotic notations: $f(n) = \mathcal{O}(g(n))$ if there exists a constant $c > 0$ such that $|f(n)| \leq c|g(n)|$ for all sufficiently large n. We say $f(n) = \Omega(g(n))$ if $g(n) = \mathcal{O}(f(n))$. We say $f(n) = \Theta(g(n))$ if $f(n) = \mathcal{O}(g(n))$ and $g(n) = \mathcal{O}(f(n))$. We say $f(n) = o(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = 0$. We say $f(n) = \omega(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = \infty$. We say that $f(n) = \mathsf{poly}(n)$ if there exists a finite $k > 0$ such that $f(n) = \mathcal{O}(n^k)$. The $\mathsf{polylog}(n)$ class of functions is defined similarly. We denote $\mathsf{negl}(n)$ to be the class of functions that are $o(1/n^c)$ for all $c > 0$, that is they are negligible in the sense that they vanish faster than any inverse polynomial.

B. Useful definitions and results

We first define the Haar measure, which formalizes the notion of the uniform distribution over the unitary group.

Definition II.1 (Haar measure)**.** *The Haar measure μ_H on the $n-$qubit unitary group is the unique probability measure μ_H on $\mathcal{U}(2^n)$ satisfying*

1. *For any measurable set $S \subseteq \mathcal{U}(2^n)$ and any $V \in \mathcal{U}(2^n)$ we have $\mu_H(VS) = \mu_H(S)$ and $\mu_H(SV) = \mu_H(S)$.*
2. *$\mu_H(\mathcal{U}(2^n) = 1)$*

An information theoretic way of talking about ensembles *close* to the Haar ensemble is the following.

Definition II.2 (Unitary $t-$design)**.** *We say that a distribution $\mathcal{D}$ on $n-$ qubits is a unitary $t-$design if*

$$\mathbb{E}_{U\sim\mathcal{D}}[U^{\otimes t} \otimes \bar{U}^{\otimes t}] = \int_{\mathcal{U}(2^n)} d\mu_H (U^{\otimes t} \otimes \bar{U}^{\otimes t}) \tag{1}$$

We will often refer to the notion of a $2-$design, which is an ensemble that agrees with the Haar random ensemble up to two moments. The Clifford group forms a $2-$design. An important property that we shall use is now discussed. Consider t groups of n qubits each. We define a projector on the distinct subspace, which ensures all the different blocks are 'different' upon projecting.

Definition II.3 (Distinct Subspace Projector)**.**

$$\Pi^{\mathrm{dist}} := \sum_{\mathbf{x}\in[N]^t_{\mathrm{dist}}} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_t\rangle\langle x_t| \tag{2}$$

Now, the following Lemma is exceptionally useful, as it lets us assume t groups of n qubits are essentially in the distinct subspace if they have been 'twirled' by a $2-$design.

Lemma II.1 ($2-$design collision probability)**.** *Let $|\psi\rangle$ be drawn from a two design $\mathcal{D}$ on n qubits (recall $N := 2^n$). Then we have,*

$$\mathrm{tr}\left(\mathbb{E}_{\psi\sim\mathcal{D}} \Pi^{\mathrm{dist}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] \Pi^{\mathrm{dist}}\right) \geq 1 - \mathcal{O}\left(t^2/N\right) \tag{3}$$

Thus, if we have $t = \mathsf{poly}(n)$, the bound is exponentially tight.

C. Oracles and Adversaries

A $n-$qubit quantum oracle is essentially just a unitary U. The idea is that adversaries can now have quantum registers to coherently query and process the information from oracles. The number of times the adversary can access the oracle of interest is known as the *query complexity*. A polynomial time, or 'efficient,' adversary is one which has $\mathsf{poly}(n)$ query complexity. Let us define the adversary model more formally, specializing to two natural cases.

Definition II.4 (Oracle Adversaries)**.** *Given a unitary U on $\mathcal{H}_A$, we define two adversary states:*

(a) ***Parallel Adversary****: Let $t \in \mathbb{N}$, and consider a unitary circuit A on $\mathcal{H}_A^{\otimes t}$, then the adversary state is*

$$\left|\mathcal{W}^U\right\rangle := W\left(U\left|0\right\rangle\right)^{\otimes t} \tag{4}$$

(b) ***Adaptive Adversary****: Let $m, t \in \mathbb{N}$. Then, a $t-$query adaptive adversary is defined by a $t-$tuple $(W^{(1)}, W^{(2)}, \ldots, W^{(t)})$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\mathcal{H}_B \cong \mathbb{C}^{\otimes 2^m}$*

$$\left|\mathcal{W}_t^U\right\rangle := \prod_{i=1}^{t} \left(U_A W_{AB}^{(i)}\right) \left|0\right\rangle_A \otimes \left|0\right\rangle_B \tag{5}$$

We show this schematically in Fig. 1.

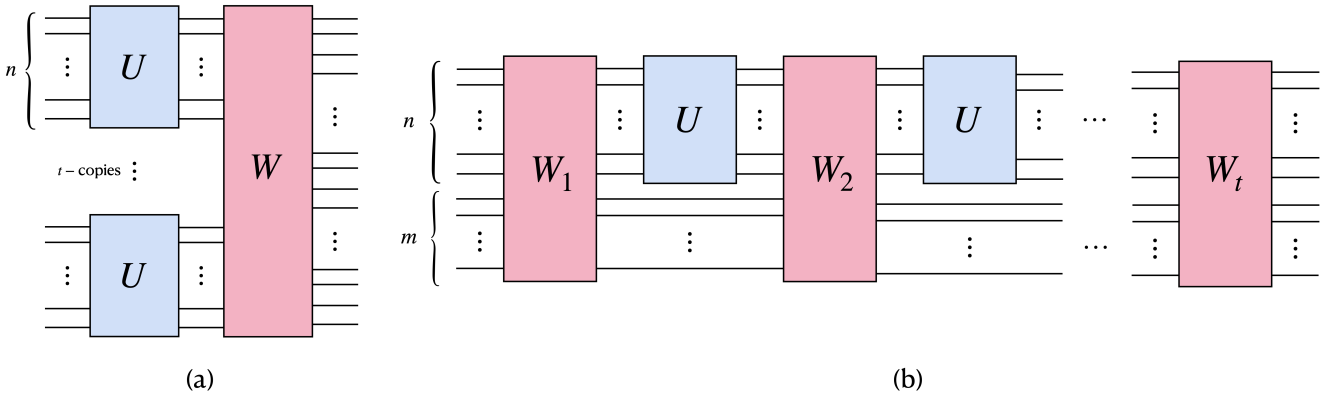

FIG. 1. **Oracle Adversaries** (a) Parallel Queries (b) Sequential (Adaptive) Queries

We consider $t = \mathsf{poly}(n)$ as well as $m = \mathsf{poly}(n)$ for efficient adversaries. The adaptive strategy is strictly powerful than the parallel one, as the intermediate operations $W_{AB}^{(i<t)}$ can be treated as swaps and $W_{AB}^{(t)}$ can take the role of W. This only requires $m = \mathcal{O}(tn)$, which is $\mathsf{poly}(n)$ as long as the number of queries is polynomial. Moreover, the parallel adversary admits a much concrete description in terms of the following mixed state

$$\rho_{\mathcal{E}} = \mathbb{E}_{|\psi\rangle \in \mathcal{E}} \left[|\psi\rangle \langle\psi| \right] \tag{6}$$

which is very useful, as one can prove properties of an ensemble by showing that this mixed state is close to the one with the desired property. This convenience is harshly taken away for the adaptive setting, where the object $\mathbb{E}[\left|\mathcal{W}_t^U\right\rangle \left\langle\mathcal{W}_t^U\right|]$ intricately encodes the adversary operations as well. We will discuss the more sophisticated techniques recently developed to attack that object.

We briefly comment on the nature of oracles to be seen. A prominent kind is *quantumly-accessible* classical oracles. That is, for some classical function $g : \{0,1\}^n \to \{0,1\}^n$, the oracle O_g implements,

$$O_g |x\rangle |y\rangle \mapsto |x\rangle |y \oplus g(x)\rangle \tag{7}$$

We note two important such objects. First is the *phase oracle* defined for each $f : \{0,1\}^n \to \{0,1\}$, with the action

$$F_f |x\rangle \mapsto (-1)^{f(x)} |x\rangle . \tag{8}$$

It is not too hard to see that this is essentially same as the O_g defined above, and starting the Y register in the $|-\rangle$ state. Next up, we have the *permutation oracle* P_π defined for each $\pi \in \mathrm{Sym}_n$ as

$$P_\pi |x_1, x_2, \ldots, x_n\rangle \mapsto \left|x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \ldots, x_{\pi^{-1}(n)}\right\rangle \tag{9}$$

We note that, whenever an adversary queries a random oracle, the operational interpretation is at follows. One *fixes* a sample of the oracle, and hands it to the adversary repeatedly. This is not to be confused with sampling a new random object at each query in a single run.

D. PRPs and PRFs

All the results discussed will depend on the existence of quantum-secure pseudorandom functions (PRF) and pseudorandom permutations. These are essentially efficient objects which look random to any polytime quantum adversary.

- **Pseudorandom permutations (PRP)**. A family of permutations [9]

$$\mathcal{P} = \{\pi_k : \{0,1\}^n \to \{0,1\}^n \mid k \in \mathcal{K}_1\} \tag{10}$$

  such that for a randomly chosen key $k \in \mathcal{K}_1$ the permutation π_k is computationally indistinguishable from a truly random permutation.

- **Pseudorandom functions (PRF)**. A family of functions [10]

$$\mathcal{F} = \{f_k : \{0,1\}^n \to \{0,1\} \mid k \in \mathcal{K}_2\} \tag{11}$$

  such that for a random $k \in \mathcal{K}_2$ the function f_k is computationally indistinguishable from a trule randomf function.

Now, we define one-way functions. Classically, one way functions are of the type $\mathsf{OW} : \{0,1\}^* \to \{0,1\}^*$ with the property that there exist deterministic efficient algorithms to determine the output given the input. Crucially, they cannot be inverted efficiently. This property enables wide usage in cryptography. For our purposes, we define quantum resistant one-way functions.

Definition II.5. *A quantum resistant one-way function is an efficient classical function* $\mathsf{OWF} : \{0,1\}^\lambda \to \{0,1\}^*$ *that cannot be inverted efficiently by any quantum adversary, where* λ *is the security parameter. Specifically, for any poly-time adversary* $\mathcal{W}$*,*

$$\mathbb{P}\left[\mathsf{OWF}(\mathcal{W}(\lambda, \mathsf{OWF}(x))) = \mathsf{OWF}(x) : x \leftarrow \{0,1\}^\lambda\right] \leq \mathsf{negl}(\lambda) \tag{12}$$

Now, the key result which enables much of recent advances in pseudo-quantum things is summarized as the following theorem.

Theorem II.1 ([9, 10]). *Quantum secure pseudorandom permutations and pseudorandom functions exist assuming the existence of quantum resistent one-way functions.*

That is, all of the results rely on the widely-accepted (but not proven!) cryptographic conjecture of the existence of one-way functions. We will see how the PRP and PRF objects, presumably existing, are useful to construct pseudoentangled states and pseudorandom unitaries. Of course, the existence of one way functions is widely believed but not proven. The reader may note that proving the former will prove $\mathsf{P} \neq \mathsf{NP}$.

III. PSEUDOENTANGLEMENT

We begin with some definitions of efficient state ensembles. At the first order, we wish for our ensembles considered to be *efficient*. Borrowing some language from cryptography, we make the following definition.

Definition III.1 (Efficient Ensemble). *An efficient ensemble of states on $n-$qubits is a set of states,*

$$\mathcal{E} = \{|\psi_k\rangle \mid k \in \mathcal{K}\} \tag{13}$$

such that given key k, there exists a polynomial depth (local) quantum circuit that prepares $|\psi_k\rangle$, and $\mathcal{K} = \{0,1\}^{\mathsf{poly}(n)}$.

The *key* can be considered an efficient 'classical description' of a chosen state in the ensemble. Now, we are interested in constructing ensembles which 'spoof' entanglement. That is, they truly do not consist of a 'large' (volume-law) amount of entanglement, but to any *physical* observer, they are indistinguishable from a truly entangled ensemble. We control the true entanglement by a function $f(n)$, and make the following definition.

Definition III.2 ($f(n)-$Pseudoentanglement). *An ensemble of states $\mathcal{E}$ is said to be $f(n)-$pseudoentangled if,*

1. *It is an efficient ensemble.*
2. *With probability $1 - 1/\mathsf{poly}(n)$ over the choice of key, for any bipartition $A = A_L \cup A_R$ with $|A_L| = \Theta(n)$ the state $|\psi_k\rangle \in \mathcal{E}$ has entanglement entropy $\Theta(f(n))$.*
3. *No poly-time quantum algorithm can distinguish between a state from $\mathcal{E}$ and a Haar random state,*

$$|\mathcal{W}(\rho) - \mathcal{W}(\sigma)| \leq \mathsf{negl}(n) \tag{14}$$

for $\rho = \mathbb{E}_k[(|\psi_k\rangle\langle\psi_k|)^{\otimes p(n)}]$ and $\sigma = \mathbb{E}_{\mu_H}[(|\psi\rangle\langle\psi|)^{\otimes p(n)}]$ for $p(n) = \mathsf{poly}(n)$.

We stress that pseudoentanglement is an *ensemble property*. It makes no sense to talk about a single state to be pseudoentangled, a single state cannot spoof entanglement. The ensembles are thus important in making a sensible definition. Now, we show that any pseudoentangled ensemble has to have *some* amount of entanglement. Specifically, it must be atleast log-law.

Lemma III.1. $f(n) = \omega(\log n)$

Proof. Assume not. Then we have $S(\rho) = \mathcal{O}(\log n)$. We can perform the swap test on $n/2$ qubits, and trace the rest out. Before we do that, note,

$$S(\rho) \geq S_2(\rho) \tag{15}$$

where S_2 is the second Renyi entropy. To see this, note that

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i = \mathbb{E}[-\log(\lambda)] \geq -\log(\mathbb{E}[\lambda]) = S_2(\rho) \tag{16}$$

Now, the swap test outputs zero with probability $1/2 + 1/2^{1+S_2(\rho)}$. Thus, the Haar state results in $1/2 + 1/2^{n+1}$ and the ensemble has $1/2 + 1/\mathsf{poly}(n)$. Thus, the swap test succeeds with inverse polynomial error, which is not in $\mathsf{negl}(n)$ and thus violates the definition of pseudoentanglement. □

Now, we consider the following ensemble, among the first one to be proved pseudoentangled.

Definition III.3 (Subset Phase State). *Consider a subset $S \subseteq \{0,1\}^N$ and a function $f : \{0,1\}^N \to \{0,1\}$. Define the subset-phase state*

$$|\psi_{S,f}\rangle = \frac{1}{\sqrt{S}} \sum_{x \in S} (-1)^{f(x)} |x\rangle \tag{17}$$

We consider subsets S of size $|S| = 2^k$ the following form for some $k < n$. Let $\pi \in \mathrm{Sym}_n$ be a permutation. Now, define

$$S_\pi = \{\pi(x, 0^{\otimes(n-k)}) \mid x \in \{0,1\}^k\} \tag{18}$$

How do we construct a subset-phase state $|\psi_{S,f}\rangle$? Suppose we are given the oracles P_π and F_f. Then, it is not too hard to see that,

$$|\psi_{S,f}\rangle = F_f P_\pi \left(H^{\otimes k}(|0\rangle^{\otimes})\right) \equiv |\psi_{\pi,f}\rangle \tag{19}$$

The ensemble that we are then considered with is (denoting $K := 2^k$)

$$\mathcal{E}_K := \{|\psi_{\pi,f}\rangle \mid f \in [2^N], \pi \in \mathrm{sym}_n, |S| \leq K\} \tag{20}$$

The associated keys for this ensemble would then be $k = (\pi, f)$.

Theorem III.1 (Theorem 2.1 of [3]). *For any $t < K \leq N$, if we define*

$$\rho_{\mathcal{E}_K} := \mathbb{E}_{\pi,f}\left[|\psi_{\pi,f}\rangle\langle\psi_{\pi,f}|\right] \tag{21}$$

and

$$\rho_\mu := \mathbb{E}_{\psi\sim\mu_H}\left[|\psi\rangle\langle\psi|\right], \tag{22}$$

then,

$$\mathsf{TD}(\rho_{\mathcal{E}_K}, \rho_\mu) \leq \mathcal{O}\left(\frac{t^2}{K}\right). \tag{23}$$

Hence, it is sufficient to choose $K = \omega(\mathsf{poly}(n))$ to ensure that any polynomial time (parallel) adversary cannot distinguish a Haar random state to a state from this ensemble. In fact, one can *tune* the amount of entanglement in the ensemble by varying the size K of the subset. Concretely, we have [11]

$$S_{\mathsf{A}} \sim \min\{\log K, |\mathsf{A}|\log 2\} \tag{24}$$

Thus, $\omega(\mathsf{poly}(n)) \leq K \leq 2^{o(n)}$, where the left inequality ensures $f(n) = \omega(\log n)$ and the right inequality ensures sub-volume-law entanglement. Recently, it has also been shows that the phase is not exactly needed. That is, a random subset ensemble with $\omega(\mathsf{poly}(n)) \leq K \leq o(2^n/\mathsf{poly}(n))$ are also pseudoentangled [12, 13].

We now complete an important step of the argument of pseudoentanglement. The results up until now relied on *truly random* functions $f \in [2^N]$ and permutations $\pi \in \mathrm{Sym}_n$. Such objects are not efficient to begin with. Instead, we replace them by their quantum-secure pseudorandom counterparts [4]. Both PRFs and PRPs have been shown to exist assuming the existence of quantum resistant one-way functions [9, 10]. The effective key set for the subset phase ensemble would thus be $\mathcal{K} := \mathcal{K}_1 \times \mathcal{K}_2$, where $\mathcal{K}_1$ and $\mathcal{K}_2$ are the key sets of PRF and PRP respectively. Without loss of generality both $\mathcal{K}_1$ and $\mathcal{K}_2$ can be taken to have $\mathcal{O}(n)$ bits, leading to $\mathcal{K}$ having a bit length $\mathcal{O}(n)$. Hence, we conclude the following result.

Theorem III.2. *Assuming the existence of quantum-secure one-way functions, subset-phase states with $K = \omega(\mathsf{poly}(n))$ form a pseudoentangled ensemble.*

IV. PSEUDORANDOM UNITARIES

Up until now, we explored pseudoentangled states, which look indistinguishable from Haar random states given access to polynomially-many queries. A natural generalization of this is a stronger notion of *pseudorandom unitaries*, which are in some sense the quantum analogue of psuedorandom functions. Now, we begin the hunt for efficient to construct unitaries which appear indistinguishable from any Haar random unitary to any computationally-bounded adversary.

To begin with, we define a PRU. Note that we abuse notation and use the same letters to denote unitary ensembles as used for state ensembles.

Definition IV.1 ((non-adaptive) PRU). *An ensemble of unitaries $\mathcal{E} = \{U_k\}_k$ for $k \in \mathcal{K} = \{0,1\}^{\mathsf{poly}(n)}$ is pseudorandom if*

1. *For all keys $k \in \mathcal{K}$, there exists a $\mathsf{poly}(n)$ algorithm that implements the unitary U_k.*
2. *For any adversary that makes $t = \mathsf{poly}(n)$ queries, we have that,*

$$\left|\mathbb{E}_{k\in\mathcal{K}}\left|\mathcal{W}_t^{U_k}\right\rangle\left\langle\mathcal{W}_t^{U_k}\right| - \mathbb{E}_{U\sim\mu_H}\left|\mathcal{W}_t^{U}\right\rangle\left\langle\mathcal{W}_t^{U}\right|\right| = \mathsf{negl}(n) \tag{25}$$

Now, we introduce the leading PRU candidate that has been the focus of much recent work. First, we recall that the group of Clifford unitaries on $n-$qubits forms a $2-$design. It turns out, when we combine the $P_\pi \cdot F_f$ trick used for constructing (one class of) pseudoentangled states with the Clifford group, we get a PRU! Nonetheless, for later purposes it is useful to make this definition for a general unitary ensemble $\mathcal{D}$ and specialize to the Clifford group when needed.

Definition IV.2 (PF$\mathcal{D}$ Ensemble). *Given $\pi \in \mathrm{Sym}_n$, $f : \{0,1\}^n \to \{0,1\}$, define the P_π and F gates as $F_f|x\rangle := (-1)^{f(x)}|x\rangle$ and $P_\pi|x_1, x_2, \ldots, x_n\rangle = |x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}\rangle$. Then, for an ensemble of states $\mathcal{D}$, the PF$\mathcal{D}$ ensemble $\mathcal{E}_{PF\mathcal{D}}$ is defined as*

$$\mathcal{E}_{PF\mathcal{D}} := \{P_\pi F_f D \mid \pi \in Sym_n, f \in \{0,1\}^n, D \in \mathcal{D}_n\} \tag{26}$$

where each of π, f, D is chosen uniformly in the respective spaces.

The PFC ensemble is obtained by choosing $\mathcal{D}$ to be the uniformly random distribution over $n-$qubit Clifford unitaries. The central result of Ref. [4] is that the PFC ensemble forms a $t-$design for exponentially large t with negligibly small error.

Lemma IV.1 (PFC forms a very good $t-$design [4]). *For any $t \in \mathbb{N}$, consider the $t-$copy ensemble state $\rho_{\mathcal{E}}(|\psi\rangle) = \mathbb{E}_{U\in\mathcal{E}}\left[U|\psi\rangle\langle\psi|U^\dagger\right]$ for any state $|\psi\rangle$ on nt qubits. Then, we have that*

$$\mathsf{TD}\left(\rho_{PFC}(|\psi\rangle), \rho_{Haar}(|\psi\rangle)\right) = \mathcal{O}\left(\frac{t}{\sqrt{N}}\right) \tag{27}$$

Almost there. We must *derandomize* the random permutation and function objects just as before, and replace them with their pseudorandom counterparts. We already discussed the key set describing (π, f). Now, the Clifford group on $n-$qubits consists of $2^{\mathcal{O}(n^2)}$ elements. Thus, the PFC ensemble can be described efficiently with a key length of $\mathcal{O}(n^2)$. Thus, we have the following result.

Theorem IV.1. *Assuming the existence of quantum-secure one-way functions, the PFC ensemble is a PRU.*

V. COMPRESSED PURIFICATIONS

The compressed purification (or compressed oracle) technique introduced by Zhandry [14] is a contemporary build-up of a very basic fact in quantum information: two purifications of a (mixed) state are equivalent up to a unitary on the purifying register. The reader may be amused [15] to learn that this technique has also lead to state-of-the-art bounds on noisy quantum metrology [16, 17].

A. Warm-up example

Consider the phase state $|\psi_f\rangle$ on a register X, defined as a subset-phase with the full subset $S = \{0,1\}^N$. Now, suppose our goal is to evaluate the mixed state resulting from randomizing over the f function,

$$\rho = \mathbb{E}_f \, |\psi_f\rangle \langle\psi_f| \tag{28}$$

where the expectation is across the uniform distribution over all functions. Note that each function $f : \{0,1\}^n \to \{0,1\}$ can be be written down as a 2^N bit vector. By introducting a fictional register F of N qubits, say, we write down a *purification* of this mixed state [18] $|\Psi\rangle \propto \sum_{f\in[2^N]} |\psi_f\rangle |f\rangle$. Note that $\mathrm{tr}_{\mathsf{F}}(|\Psi\rangle\langle\Psi|) = \rho$ owing to $\langle f|f'\rangle = \delta_{ff'}$. Now, (ignoring normalization)

$$|\Psi\rangle = \sum_{f\in[2^N]} \left(\sum_{x\in[N]} (-1)^{f(x)} |x\rangle_{\mathsf{X}} \right) \otimes |f\rangle_{\mathsf{F}} \tag{29}$$

We can rearrange the phase and arrive at,

$$|\Psi\rangle = \sum_{x\in[N]} |x\rangle_{\mathsf{X}} \left(\sum_{f\in[N]} (-1)^{f\cdot e_x} |f\rangle_{\mathsf{F}} \right) \tag{30}$$

where e_x is a N bit canonical unit vector with one at position $x \in [N]$. We see that this is $\sum_{x\in[N]} |x\rangle_{\mathsf{X}} H^{\otimes n} |x\rangle_{\mathsf{F}}$. Now, any unitary on the purification register alone does not affect the state, and thus another equivalent purification is $\sum_x |x\rangle_{\mathsf{X}} |x\rangle_{\mathsf{F}}$. As a corollary, this shows that the ensemble state is maximally mixed.

B. Purifying oracles

Let us consider an adversary interacting with an oracle $f : \{0,1\}^n \to \{0,1\}$. As before, we represent every such oracle as a vector $f \in \{0,1\}^N$, thinking of this object as living in a F register. Now, we claim that the following are equivalent from the adversary's point of view,

1. *Oracle Queries.* Sample a uniformly random f. On each query, apply F_f to the register A.
2. *Purified Oracle.* Initialize F in the uniform state. On each query, apply $|x\rangle_A |f\rangle_F \mapsto (-1)^{f(x)} |x\rangle_A |f\rangle_F$

The key idea is that measuring the F register in the beginning (choosing a f) and in the end (the purified way) are equivalent as the adversary does not have access to the imaginary F register we cooked up. Now, the idea of *recording* the queries is as follows. Suppose we start with the following state (denoting the adversary register as A),

$$|\Psi_0\rangle_{\mathsf{AF}} = \sum_x |x\rangle_{\mathsf{A}} \otimes \sum_f |f\rangle_{\mathsf{F}} \tag{31}$$

Then, after one query to the oracle we get,

$$|\Psi_1\rangle_{\mathsf{AF}} = \sum_x W_0 \, |x\rangle_{\mathsf{A}} \sum_f (-1)^{f(x)} |f\rangle_{\mathsf{F}} \tag{32}$$

We re-write this object by introducing an identity,

$$|\Psi_1\rangle_{\mathsf{AF}} = \sum_{x_0 x_1} |x_1\rangle\langle x_1| \, W_0 \, |x_0\rangle_{\mathsf{A}} \sum_f (-1)^{f(x_0)} |f\rangle_{\mathsf{F}} \tag{33}$$

Now, making the second query and rewriting again,

$$|\Psi_2\rangle_{\mathsf{AF}} = \sum_{x_0 x_1 x_2} |x_2\rangle_{\mathsf{A}} \, W_1^{x_2 x_1} W_0^{x_1 x_0} \sum_f (-1)^{f(x_0)+f(x_1)} |f\rangle_{\mathsf{F}} \tag{34}$$

Hence, we build up the following general expression for the purified state at t queries

$$|\Psi_t\rangle_{\mathsf{AF}} = \sum_{\mathbf{x}} \mathcal{F}_{\mathbf{x},\mathbf{W}} \, |x_t\rangle_{\mathsf{A}} \sum_f (-1)^{f\cdot(e_{x_0}+\cdots+e_{x_{t-1}})} |f\rangle_{\mathsf{F}} \tag{35}$$

here we have the Feynman path amplitude,

$$\mathcal{F}_{\mathbf{x},\mathbf{W}} = \prod_{i=1}^{t} \langle x_i|W_i|x_{i-1}\rangle \tag{36}$$

The F state, upon applying $H^{\otimes N}$ can be mapped to the state $|e_{x_1} + e_{x_2} + \ldots e_{x_t}\rangle$. This is *much* simpler to deal with, as we can keep track of this state by just noting the (at-most) t locations where it has a one. With some abuse of notation [19]

$$|\Psi_t\rangle_{\mathsf{AF}} = \sum_{\mathbf{x}} \mathcal{F}_{\mathbf{x},\mathbf{W}} \, |x_t\rangle_{\mathsf{A}} \otimes |(x_1, x_2, \ldots, x_t)\rangle_{\mathsf{F}} \tag{37}$$

This is a fairly 'clean' description of a sequence of queries. Now, the idea is that since the imaginary purification register is *not* visible to the adversary, writing down this state and tracing out the purification register is equivalent to writing down the actual adversary state $|\mathcal{W}_t^O\rangle$. We formalize this in detail in the next section.

VI. TOWARDS ADAPTIVE PROOFS

In this section we discuss very recent progress using the compressed oracle technique in proving the security

of PRUs against adaptive adversaries. This technique, as a byproduct, furnishes a method to efficiently simulate queries to a Haar-random oracle. This is useful, as the method resulting is quite 'direct,' and does not require the typical representation-theory route to proving things about Haar-random objects.

A. Path Recording Oracle

We define a $t-$relation as a tuple of the form $R = \{(x_i, y_i) \mid i \in [t], (x_i, y_i) \in [N]^2\}$. The set of $t-$relations is denoted $\mathcal{R}_t$. We further denote the domain and image of a relation as $\mathrm{Dom}(R)$ and $\mathrm{Im}(R)$ respectively. The set of all injective relations, those with $\mathbf{y} \in [N]^t_{\mathrm{dist}}$ are denoted $\mathcal{R}^{\mathrm{inj}}$. The relation state is defined as follows.

Definition VI.1 (Relation State)**.** *For a relation $R \in \mathcal{R}_t$, we have*

$$|R\rangle := \frac{1}{\mathcal{N}} \sum_{\pi \in \mathrm{Sym}_t} (P^X_\pi \otimes P^Y_\pi) \, |x_1, y_1, \ldots, x_t, y_t\rangle \in \mathcal{H}_{\mathsf{R}^t} \tag{38}$$

where $\mathcal{N}$ ensures normalization.

We now define the total relation register accounting for all relation states of different sizes,

$$\mathcal{H}_{\mathsf{R}} := \bigoplus_{t=1}^{\infty} \mathcal{H}_{\mathsf{R}^t} = \bigoplus_{t=1}^{\infty} (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes t} \tag{39}$$

The motivation for making these definitions is to form a fairly-unifying description of compressed oracles that we discussed in the previous section. With this, we define the path recording oracle.

Definition VI.2 (Path Recording Oracle (PRO))**.** *The path recording oracle V on a N dimensional register X is a linear map on $\mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{R}}$ with $\mathcal{H}_{\mathsf{R}}$ the relation register as defined above. Its action for all $R \in \mathcal{R}^{\mathrm{inj}}$ with $|R| < N$ is as follows:*

$$W_{\mathsf{XR}} \, |x\rangle_X \, |R\rangle_R := \frac{1}{\sqrt{N - |R|}} \sum_{y \in [N], y \notin Im(R)} |y\rangle_{\mathsf{X}} \otimes |R \cup \{(x,y)\}\rangle_{\mathsf{R}} \tag{40}$$

where the normalization results from counting the number of possible y values.

The space of states we are concerned with is $\mathcal{S} = \mathrm{span}\{|x\rangle \otimes |R\rangle \mid |x\rangle \in \mathbb{C}^N, R \in \mathcal{R}^{\mathrm{inj}}, |R| < N\}$. The following lemma shows us that the PRO is a isometry on this space.

Lemma VI.1 (Lemma 4.1 of [6])**.** *The path recording oracle V is an isometry on the space $\mathcal{S}$.*

Now, we define the adversary state, but instead of the query on a unitary U, we replace it with the PRO. Furthermore, we define it for a general unitary G supported on register A placed after the adversary, for a reason yet to be explained. Recall that the adversary acts on $\mathsf{A} \cup \mathsf{B}$, and the 'main system' is A. As before, R denotes the relation register, and we start in the empty relation state.

Definition VI.3 (PRO Adversary State)**.**

$$\left|\mathcal{W}^{VG}_t\right\rangle := \prod_{i=1}^{t} \left(V_{\mathsf{AR}} \cdot G_{\mathsf{A}} \cdot W^{(i)}_{\mathsf{AB}} \cdot \right) (|0\rangle_{\mathsf{A}} \otimes |0\rangle_{\mathsf{B}} \otimes |\emptyset\rangle_R) \tag{41}$$

Explicitly, this is

$$\left|\mathcal{W}^{VG}_t\right\rangle = \sqrt{\frac{(N-t)!}{N!}} \sum_{\mathbf{x} \in [N]^t, \ \mathbf{y} \in [N]^t_{\mathrm{dist}}} |y_t\rangle_{\mathsf{A}} \, |\mathcal{F}_{\mathbf{x},\mathbf{y},\mathbf{W}}\rangle_{\mathsf{B}} \, |(\mathbf{x},\mathbf{y})\rangle_{\mathsf{R}} \tag{42}$$

with the path integral denoted,

$$|\mathcal{F}_{\mathbf{x},\mathbf{y},\mathbf{W}}\rangle_{\mathsf{B}} := \langle y_t| \left[\prod_{i=1}^{t} \left(|y_i\rangle \langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot W^{(i)}_{\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \right] \tag{43}$$

and the relation state (the 'tag'),

$$|(\mathbf{x},\mathbf{y})\rangle_{\mathsf{R}} = \frac{1}{\sqrt{t!}} \sum_{\pi \in \mathrm{Sym}_t} P^X_\pi \, |\mathbf{x}\rangle \otimes P^Z_\pi \, |\mathbf{y}\rangle \, . \tag{44}$$

The fact that the path integral is a state on B is not important, as B can be trivial and then the state becomes the conventional path integral scalar.

Lemma VI.2 (Lemma 4.2 of [6])**.** *For $t \leq N$ queries, the adversary state $\left|\mathcal{W}^{VG}_t\right\rangle$ is state with unit norm in $\mathcal{H}_{\mathsf{AB}} \otimes \mathcal{H}_{\mathsf{R}}$.*

Now, the adversary cannot access information on the purification register, hence, if viable information leaks out purely into the purification register, the adversary cannot be successful. This is formalized as the following lemma.

Lemma VI.3 (Lemma 4.4 of [6])**.** *For any unitary G on A, we have*

$$\left|\mathcal{W}^{VG}_t\right\rangle = (G^{R^{(t)}_{X,1}} \otimes G^{R^{(t)}_{X,2}} \otimes \cdots \otimes G^{R^{(t)}_{X,t}}) \left|\mathcal{W}^{V\mathbb{1}}_t\right\rangle \tag{45}$$

This is surprisingly useful, and follows from basic arguments. Essentially, one has to show that

$$\sum_x |x\rangle_{\mathsf{R}^{(t)}_{X,i}} \otimes \langle x|_{\mathsf{A}} \, G_{\mathsf{A}} = \sum_x G_{\mathsf{R}^{(t)}_{X,i}} \, |x\rangle_{\mathsf{R}^{(t)}_{X,i}} \otimes \langle x|_{\mathsf{A}} \tag{46}$$

and then use the explicit form discussed above. The implication is profound, as, it follows that

$$\mathrm{tr}_{\mathsf{R}} \left(\left|\mathcal{W}^{VG}_t\right\rangle \left\langle \mathcal{W}^{VG}_t \right| \right) = \mathrm{tr}_{\mathsf{R}} \left(\left|\mathcal{W}^{V}_t\right\rangle \left\langle \mathcal{W}^{V}_t \right| \right) \quad \forall G \in \mathcal{L}(\mathcal{H}_{\mathsf{A}}) \tag{47}$$

Now, we take G to be from a $2-$ design. We know by Lemma II.1 that twirling by a $2-$design projects into the distinct subspace upto an exponentially small error. Hence, we have the following.

Corollary VI.1. *Let $\mathcal{D}$ be any $2-$design, and let $C \in \mathcal{D}$. Now, define*

$$\rho := \mathbb{E}_{C\sim\mathcal{D}}\left[\left|\mathcal{W}_t^{V\cdot C}\right\rangle\!\left\langle\mathcal{W}_t^{V\cdot C}\right|_{\mathsf{ABR}}\right] \tag{48}$$

Then, we have that

$$\mathsf{TD}\left(\mathrm{tr}_{\mathsf{R}}\left[\Pi^{\mathrm{dist}}_{R_X^{(t)}}\rho\Pi^{\mathrm{dist}}_{R_X^{(t)}}\right] - \mathrm{tr}_{\mathsf{R}}\left[\rho\right]\right) \leq \mathcal{O}\left(\frac{t^2}{N}\right) \tag{49}$$

This enables us to show that queries to a Haar random unitary can be efficiently simulated with the path-recording oracle.

Theorem VI.1 (Efficient simulation of Haar-Random Queries)**.** *Let $\mathcal{W}$ be a $t-$query adaptive oracle adversary*

$$\rho_{\mathcal{W}} := \mathbb{E}_{U\sim\mu_H}\left|\mathcal{W}_t^{U}\right\rangle\!\left\langle\mathcal{W}_t^{U}\right|_{\mathsf{AB}} \tag{50}$$

$$\rho_{V} := \mathrm{tr}_{\mathsf{R}}\left|\mathcal{W}_t^{V}\right\rangle\!\left\langle\mathcal{W}_t^{V}\right|_{\mathsf{ABR}} \tag{51}$$

$$\mathsf{TD}(\rho_{\mathcal{W}},\rho_V) = \mathcal{O}\left(\frac{t^2}{N}\right) \tag{52}$$

The proof of this will follow from a more general result, that we discuss in the next subsection. However, the intuition is essentially resulting from taking care of the collision probabilities, as enabled by Lemma II.1.

B. Purifying PFO

Now, extending our developments in the realm of compressed purifications, we define two imaginary register P, for the permutation, and F for the phase function as before. With this, we have the purified PF oracle as follows.

Definition VI.4 (Purified pf Oracle)**.**

$$\mathsf{pfO}\left|x\right\rangle_{\mathsf{A}}\left|f\right\rangle_{\mathsf{F}}\left|\pi\right\rangle_{\mathsf{P}} := (-1)^{f(x)}\left|\pi(x)\right\rangle_{\mathsf{A}}\left|f\right\rangle_{\mathsf{F}}\left|\pi\right\rangle_{\mathsf{P}} \tag{53}$$

With this, we define the pf relation states, analogous to the relation states before. Then, we will show that queries to the pfO can be written down in terms of these relation states.

Definition VI.5. *For $0 \leq t \leq N$, and $R = \{(x_1,y_1),\ldots,(x_t,y_t)\} \in \mathcal{R}_t$ we define*

$$\left|\mathsf{PF}_R\right\rangle \propto \sum_{\pi\in\mathrm{Sym}_N, f\in[2^N]} \delta_{\pi,R}\left|\pi\right\rangle_{\mathsf{P}} \otimes (-1)^{\sum_{i=1}^t f(x_t)}\left|f\right\rangle_{\mathsf{F}} \tag{54}$$

where the normalization factor is $1/\sqrt{2^N\cdot(N-t)!}$

Starting with the empty relation $R=\emptyset$, we note that $\left|\mathsf{PF}_\emptyset\right\rangle$ is the uniform superposition over all functions and permutations. Also, we note that for bijective relations, the PF relation states are orthonormal. Then, we have the following description of the purified oracle in terms of the relation states.

Lemma VI.4. *We have the following action of the PF oracle for $0 \leq t < N$ and $R \in \mathcal{R}_t$*

$$\mathsf{pfO}\left|x\right\rangle_{\mathsf{A}}\left|\mathsf{PF}_R\right\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{N-|R|}}\sum_{y\in[N]}\left|y\right\rangle_{\mathsf{A}}\left|\mathsf{PF}_{R\cup\{(x,y)\}}\right\rangle_{\mathsf{PF}} \tag{55}$$

for all $x \in [N]$.

Proof.

$$(-1)^{f(x)}\left|\pi(x)\right\rangle_{\mathsf{A}}\sum_{\pi,f]}\delta_{\pi,R}\left|\pi\right\rangle_{\mathsf{P}}\otimes(-1)^{\sum_{i=1}^t f(x_t)}\left|f\right\rangle_{\mathsf{F}} \tag{56}$$

$$\sum_y\left|y\right\rangle_{\mathsf{A}}\sum_{\pi,f}\delta_{\pi,R}\delta_{y=\pi(x)}(-1)^{\sum_{i=1}^t(x_i)+f(x)}\left|\pi\right\rangle_{\mathsf{P}}\left|f\right\rangle_{\mathsf{F}} \tag{57}$$

Now note that $\delta_{y=\pi(x)} \equiv \delta_{\pi,\{(x,y)\}}$, and thus $\delta_{y=\pi(x)}\delta_{\pi,R} = \delta_{\pi,R}\delta_{\pi,\{(x,y)\}} = \delta_{\pi,R\cup\{(x,y)\}}$. □

Now, if we replace queries with the pfO, then the adversary state has the following form.

Definition VI.6 (PFO Adversary State)**.**

$$\left|\mathcal{W}_t^{\mathsf{pfO}G}\right\rangle := \prod_{i=1}^t\left(\mathsf{pfO}\cdot G_{\mathsf{A}}\cdot W^{(i)}_{\mathsf{AB}}\cdot\right)\left(\left|0\right\rangle_{\mathsf{AB}}\otimes\left|\mathsf{PF}_\emptyset\right\rangle_{\mathsf{PF}}\right) \tag{58}$$

Explicitly, this is

$$\sqrt{\frac{(N-t)!}{N!}}\sum_{\mathbf{x},\mathbf{y}\in[N]^t}\left|y_t\right\rangle_{\mathsf{A}}\left|\mathcal{F}_{\mathbf{x},\mathbf{y},\mathbf{W}}\right\rangle_{\mathsf{B}}\left|\mathsf{PF}_{\{(\mathbf{x},\mathbf{y})\}}\right\rangle_{\mathsf{PF}} \tag{59}$$

with the path integral denoted,

$$\left|\mathcal{F}_{\mathbf{x},\mathbf{y},\mathbf{W}}\right\rangle_{\mathsf{B}} := \left\langle y_t\right|\left[\prod_{i=1}^t\left(\left|y_i\right\rangle\left\langle x_i\right|_{\mathsf{A}}\cdot G_{\mathsf{A}}\cdot W^{(i)}_{\mathsf{AB}}\right)\left|0\right\rangle_{\mathsf{AB}}\right] \tag{60}$$

Now, we relate the path recording construction and the PRO adversary with the pfO adversary. The key idea is that there exists a bijection between the relation registers if we have no collisions.

Lemma VI.5 (Relating PRO and pfO)**.** *Define a compression map $\mathsf{Comp} : \mathcal{H}_{\mathsf{P}}\otimes\mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{R}}$ as,*

$$\mathsf{Comp} := \sum_{R\in\mathcal{R}^{\mathrm{bij}}}\left|R\right\rangle\left\langle\mathsf{PF}_R\right| \tag{61}$$

Further, we define the distinct projector on PF relations as

$$\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} := \sum_{R\in\mathcal{R}^{\mathrm{bij}},|R|=t}\left|\mathsf{PF}_R\right\rangle\!\left\langle\mathsf{PF}_R\right| \tag{62}$$

Then, we have the following relation

$$\mathsf{Comp}\cdot\left(\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}\cdot\left|\mathcal{W}^{\mathsf{pfO}G}_t\right\rangle\right)=\Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\left|\mathcal{W}^{V\cdot G}_t\right\rangle \tag{63}$$

Hence, we can now show that upon projecting onto the suitable distinct subspaces, the adversary's view while using the pfO is the same as that of the PRO.

Corollary VI.2.

$$\rho_{\mathsf{pfO}}:=\mathbb{E}_{C\sim\mathcal{D}}\left[\left|\mathcal{W}^{\mathsf{pfO}C}_t\right\rangle\!\left\langle\mathcal{W}^{\mathsf{pfO}C}_t\right|_{\mathsf{ABPF}}\right] \tag{64}$$

$$\rho_{V}:=\mathbb{E}_{C\sim\mathcal{D}}\left[\left|\mathcal{W}^{V\cdot C}_t\right\rangle\!\left\langle\mathcal{W}^{V\cdot C}_t\right|_{\mathsf{ABR}}\right] \tag{65}$$

$$\mathrm{tr}_{\mathsf{PF}}\left(\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}\rho_{\mathsf{pfO}}\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}\right)=\mathrm{tr}_{\mathsf{R}}\left(\Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\rho_V\Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\right) \tag{66}$$

Now, a similar result as Lemma VI.3 holds for the pfO oracle, hence we have the following corollary.

Corollary VI.3. *Let $\mathcal{D}$ be any $2-$design, and let $C\in\mathcal{D}$. Now, define*

$$\rho:=\mathbb{E}_{C\sim\mathcal{D}}\left[\left|\mathcal{W}^{\mathsf{pfO}C}_t\right\rangle\!\left\langle\mathcal{W}^{\mathsf{pfO}C}_t\right|_{\mathsf{ABPF}}\right] \tag{67}$$

Then, we have that

$$\mathsf{TD}\left(\mathrm{tr}_{\mathsf{PF}}\left[\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}\rho\tilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}\right]-\mathrm{tr}_{\mathsf{PF}}\left[\rho\right]\right)\leq\mathcal{O}\left(\frac{t^2}{N}\right) \tag{68}$$

Theorem VI.2. *Let $\mathcal{D}$ be any $2-$design and $\mathcal{W}$ be a $t-$query adaptive oracle adversary with the mixed state,*

$$\rho_{\mathcal{W}}:=\mathbb{E}_{U\sim PF\mathcal{D}}\left|\mathcal{W}^{U}_t\right\rangle\!\left\langle\mathcal{W}^{U}_t\right|_{\mathsf{AB}} \tag{69}$$

Define the corresponding path recording state, upon tracing out the relation register

$$\rho_V:=\mathrm{tr}_{\mathsf{R}}\left|\mathcal{W}^{V}_t\right\rangle\!\left\langle\mathcal{W}^{V}_t\right|_{\mathsf{ABR}} \tag{70}$$

Then we have

$$\mathsf{TD}(\rho_{\mathcal{W}},\rho_V)=\mathcal{O}\left(\frac{t^2}{N}\right) \tag{71}$$

Proof. This follows by a series of triangle inequalities. The $PF\mathcal{D}$ query state is a pfO state with $G\sim\mathcal{D}$, which by Lemma VI.3 can be approximated well within the distinct subspace. Then, we have shown that within the distinct subspace the pfO query is approximated well by the PRO query in the distinct subspace. Finally, we have also shown that the support of PRO with the $2-$design is essentially in the distinct subspace. Lastly, since the G unitaries can be distilled out on the relation register, by eq. (46) the adversary view is the traced out state. Each approximation was within a $\mathcal{O}(t^2/N)$ error, thus we are done. □

As a corollary, this also shows that queries to a Haar random unitary are efficiently simulated through the path recording oracle. This follows by the invariance properties of the Haar equation, we have $\mu_H=PF\mu_H$. Collecting these results together, we have the following.

Theorem VI.3. *Pseudorandom unitaries with adaptive security exist assuming quantum-secure one way functions.*

VII. CONCLUSIONS

Pseudorandom quantum ensembles are efficient object which are indistinguishable from Haar random ensembles given arbitrary polynomial queries by an adversary. We briefly discussed the key techniques and results in pseudoentangled quantum states and pseudorandom unitaries. All of these objects were shown to exist given the widely accepted conjecture of quantum-secure one-way functions. We discussed the key differences in proof techniques between parallel and adaptive proofs. As a byproduct, the compressed oracle technique has now furnished a novel formalism to simulate queries to Haar random unitaries, which may find applications in other areas such as chaos and holography.

[1] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[2] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[3] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement. *arXiv preprint arXiv:2211.00747*, 2022.

[4] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 485–492. IEEE, 2024.

[5] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751*, 2024.

[6] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. *arXiv preprint arXiv:2410.10116*, 2024.

[7] 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), June 2020.

[8] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo)random dynamics of black holes and

other chaotic systems, 2023.

[9] Mark Zhandry. A note on quantum-secure prps. *Quantum*, 9:1696, 2025.

[10] Mark Zhandry. How to construct quantum random functions. *Journal of the ACM (JACM)*, 68(5):1–43, 2021.

[11] Xiaozhou Feng and Matteo Ippoliti. Dynamics of pseudoentanglement. *Journal of High Energy Physics*, 2025(2):1–53, 2025.

[12] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Pseudorandom and pseudoentangled states from subset states. *arXiv preprint arXiv:2312.15285*, 2023.

[13] Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states. *arXiv preprint arXiv:2312.09206*, 2023.

[14] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 239–268. Springer, 2019.

[15] The author likes to talk about metrology, as the reader may realize.

[16] Rafał Demkowicz-Dobrzański, Jan Kołodyński, and Mădălin Guţă. The elusive heisenberg limit in quantum-enhanced metrology. *Nature communications*, 3(1):1063, 2012.

[17] Sisi Zhou, Mengzhen Zhang, John Preskill, and Liang Jiang. Achieving the heisenberg limit in quantum metrology using quantum error correction. *Nature communications*, 9(1):78, 2018.

[18] the randomness causes the mixing.

[19] strictly speaking we need no *collisions* to write this, but we will see how to deal with that in the PFC case.