Real-Valued Somewhat-Pseudorandom Unitaries

Zvika Brakerski [*] Nir Magrafta[*]

Abstract

We explore a very simple distribution of unitaries: random (binary) phase – Hadamard – random (binary) phase – random computational-basis permutation. We show that this distribution is statistically indistinguishable from random Haar unitaries for any polynomial set of orthogonal input states (in any basis) with polynomial multiplicity. This shows that even though real-valued unitaries cannot be completely pseudorandom (Haug, Bharti, Koh, arXiv:2306.11677), we can still obtain some pseudorandom properties without giving up on the simplicity of a real-valued unitary.

Our analysis shows that an even simpler construction: applying a random (binary) phase followed by a random computational-basis permutation, would suffice, assuming that the input is orthogonal and *flat* (that is, has high min-entropy when measured in the computational basis).

Using quantum-secure one-way functions (which imply quantum-secure pseudorandom functions and permutations), we obtain an efficient cryptographic instantiation of the above.

[*] Weizmann Institute of Science. Email: {zvika.brakerski,nir.magrafta}@weizmann.ac.il. Supported by the Israel Science Foundation (Grant No. 3426/21), and by the Horizon Europe Research and Innovation Program via ERC Project ACQUA (Grant 101087742).

Contents

1 Introduction

Pseudorandomness is one of the most fundamental notions in cryptography. Prominent examples include pseudorandom generators (PRG) [HILL99], pseudorandom functions (PRF) [GGM86], and pseudorandom permutations (PRP) [LR88], which play a crucial role in various constructions in cryptography and beyond. Let us consider the concept of PRP, which is quite analogous to the object at the focus of this work. If we consider the class of all permutations $\{0,1\}^n \to \{0,1\}^n$, a random function from this class requires an exponential number of random bits to specify, and requires an exponential-size circuit to evaluate (and invert). A PRP is a distribution that can be sampled using a *polynomial* number of bits, known as the *seed*.[1] Furthermore, given the seed s, it is possible to evaluate and invert the associated permutation π_s in polynomial time. The crucial point is that any polynomial time process cannot distinguish between an interaction with a permutation π_s for a random seed s, and an interaction with a completely random permutation. It has been established [HILL99, GGM86, LR88] that PRG, PRF and PRP can all be constructed given the existence of one-way functions: the most basic (classical) cryptographic primitive. Furthermore, this connection is true even if we consider a quantum (polynomial-time) adversary [Zha12, Zha16].

In the context of quantum computing and quantum cryptography, Ji Liu and Song [JLS18] (henceforth JLS) proposed to study pseudorandomness of quantum objects. In particular, the defined the notion of *pseudorandom quantum states* (PRS) which are n-qubit states which are (indistinguishable from) Haar random n-qubit states, even with arbitrary polynomial-time interaction with a polynomial number of copies of the pseudorandom state. The notion of PRS has been the subject of extensive study since [BS19, BS20, BCQ23, AGQY22, BBSS23, GTB23, JMW23].

Another object proposed by JLS is that of pseudorandom unitaries (PRU). Similarly to PRP, these should allow to evaluate and invert a unitary given a seed of polynomially many random bits, while being computationally indistinguishable from a random Haar unitary given arbitrary polynomial time interaction. Contrary to PRS, JLS presented constructions of a PRU, but were unable to prove their security. To date, it is still unknown how to construct PRU with a security proof under any known cryptographic assumption.

Recently, some partial progress has been made towards a construction of PRU. Namely, several works introduced families of unitaries with polynomial seeds and efficient evaluation, but falling short on pdeudorandomness. Lu, Qin, Song, Yao, and Zhao [LQS$^+$23] introduced the notion of Pseudorandom State Scramblers (PRSS), which are unitaries that are only proven to act pseudorandomly on an arbitrary *single input state* with arbitrary polynomial multiplicity. Namely, any number of copies of the output on one particular input are pseudorandom. Ananth, Gulati, Kaleoglu, and Lin [AGKL23] introduced the notion of Pseudorandom Isometries (PRI), which are not unitary since their output is longer than their input (and the security of the constructions hinges on this property). They proved security of the PRI property for the case of a single input, a polynomial number of Haar-random inputs, or for an inputs which are a subset of computational basis elements (all with arbitrary polynomial multiplicity). The works of [LQS$^+$23, AGKL23] mention a number of applications for the primitives that they defined, including multi-copy security for quantum public-key encryption.

Interestingly, the constructions in [LQS$^+$23, AGKL23] are *real-valued.* Namely, the unitary

[1] In a formal definition, one has to address the subtlety of whether "efficiency" is defined with respect to the input length n, or with respect to some "security parameter". This distinction does not matter for our current discussion, and we will point out when it does down the line.

family consists of unitaries with only real values.[2] In contrast, Haug, Bharti, and Koh [HBK23] showed that *full PRU security* cannot be achieved in this way. This is done by observing that if U is real valued, then $U \otimes U$ acts as identity on the maximally entangled state, whereas this is very far from being the case if U is a random unitary. Therefore, if we consider adversaries that are allowed to make entangled queries to the unitary, then it is impossible to construct real-valued pseudorandom unitaries. Indeed, very recently, and concurrently and independently of our work, Metger, Poremba, Sinha, and Yuen [MPSY24] showed that it is possible to construct *non-adaptive PRU* that are pseudorandom with respect to any set of inputs that cannot change adaptively throughout the querying process, even when those inputs are entangled with each other and/or the environment. Indeed, their construction is inherently complex-valued. The question, therefore, remains:

What pseudorandom properties can be shown for real-valued efficiently computable unitaries?

In this work, we show that it is possible to achieve stronger security notions than [LQS$^+$23, AGKL23] using an extremely simple construction.

1.1 Our Results

We consider an extremely simple family of unitaries: $U_P U_G H^{\otimes n} U_F$, where for functions $F, G : \{0,1\}^n \to \{\pm 1\}$, the operators U_F, U_G are the unitaries $|x\rangle \to F(x)|x\rangle, |x\rangle \to G(x)|x\rangle$, and for a permutation $P : \{0,1\}^n \to \{0,1\}^n$, U_P is the unitary $|x\rangle \to |P(x)\rangle$. The functions F, G in our construction are quantum-secure pseudorandom functions, and the permutation P is a quantum-secure pseudorandom permutation. Using the security of F, G and P, we can replace them with truly random counterparts f, g and π. We then analyze the output of the construction information theoretically with f, g and π. We note that this construction is in the spirit of, but simpler than, the PRU candidates considered by [JLS18].

We show that our family of unitaries acts as a PRU so long as the inputs are (a mixture of) an *orthogonal* set of quantum states, with arbitrary polynomial multiplicity each. This in particular shows that this construction is also a PRSS. Our construction also generalizes the properties proven by [AGKL23] for PRI, without increasing the output size and using a construction of comparable complexity.

Notably, our construction can be separated into two parts, each of which is interesting in its own right. First, we show that $H^{\otimes n} U_f$ is a "state-flattener", in the sense that for any polynomial size set of input states, it holds that with overwhelming probability over a truly random function f, the output states are all "almost perfectly flat" in the computational basis. Namely, the square-magnitude of each computational basis element is bounded by $\epsilon = O(\frac{n}{2^n})$ (note that $1/2^n$ is the maximum possible flatness, and Haar random states are also expected to have $\sim \frac{n}{2^n}$ flatness). This property follows immediately from known concentration bounds, but we believe that it was not explicitly pointed out in this context. So, if we only want to approximate the flattening property of PRU, it can be done almost trivially.

We then show that the second part of our construction, $U_\pi U_g$ for random π, g, acts as PRU for flat orthogonal inputs. Again, this is an extremely simple construction that can be applied even as-is for a non-trivial set of input states (e.g. some polynomial subset of a random basis for the given Hilbert space). The technical crux of our paper is in the analysis of this component.

[2] In [LQS$^+$23] there is an additional construction which uses complex unitaries, but for the PRSS property, a real valued construction suffices.

1.2 Technical Overview

We provide an overview of the proof for our main information theoretic lemma. That is, taking f, g, π to be random functions and a permutation, then our construction is statistically indistinguishable from a Haar random unitary for orthogonal inputs.

We use an (approximate) characterization of the output of querying a Haar random unitary on orthogonal input states. For t copies of s different orthogonal inputs, the output "target" state can be approximated by the density matrix

$$\rho_{\text{target}} = \sum_{z,\sigma} |z\rangle\langle\sigma(z)| \ , \tag{1}$$

ignoring global normalization. The summation is over all $z \in (\{0,1\}^n)^{st}$ whose st entries are unique elements in $\{0,1\}^n$, and over a set of permutations σ over the set $[st]$ (or, equivalently, over $[t]^s$). Namely, the permutation σ takes a vector $z \in (\{0,1\}^n)^{st}$ and permutes its entries (the vector $\sigma(z)$ has the same set of entries as z, only in a different order). Specifically, the summation is only over "block-preserving" permutations, which are permutations that only swap elements inside each t-tuples of elements. That is, a permutation is block-preserving if it can be represented as a sequence of s permutations over $[t]$.

We then prove that the output of our construction, with random functions and permutation, is close to the state in Eq. (1), thereby showing that on our set of input states, our construction is statistically indistinguishable from a Haar random unitary.

In this overview we first explain how to prove the flatness property for the first part of our construction, and then consider the second part of our construction. The former is described in Section 1.2.1. For the latter, we first explain in Section 1.2.2 how to "clean up" the state by removing cross-terms and certain "asymmetric" terms. This part is similar in spirit to what is done in previous works (although we present a more general analysis that is based only on flatness and not on specific properties of the input state). Then, we are left with the most technically involved part which is to analyze bound the trace norm of the difference between our state (call it ρ_{sym}) and the state ρ_{target} above. This is explained in Section 1.2.3.

1.2.1 Flattening

Recall that we consider the unitary distribution $H^{\otimes n} U_f$, where f is a random function (i.e. a random binary phase followed by Hadamard on all qubits). We say that a vector is ϵ-flat if the square-absolute-value of each of its (standard basis) coefficients is bounded by ϵ.

Given an input state of the form $\beta = \sum_x \beta_x |x\rangle$, we consider $\gamma_y = \langle y| H^{\otimes n} U_f |\beta\rangle$, which is the amplitude of the standard basis element $|y\rangle$ in the vector $H^{\otimes n} U_f |\beta\rangle$. This value can be expressed as an exponential sum $\gamma_y = \frac{1}{2^{n/2}} \sum_x f(x)(-1)^{x \cdot y} \beta_x$. We interpret each summand as a random variable with zero mean, since f is a random function to $\{\pm 1\}$. This means that we have a sum of exponentially many independent zero-mean random variables, and furthermore the ℓ_2 norm of the vector of summands is bounded since $\sum_x |\beta_x|^2 = 1$. This means that the sum is very strongly concentrated around 0, and indeed using Hoeffding, the square-absolute-value will be at most $\frac{cn}{2^n}$ with all but an exponentially small probability. By applying the union bound, we get that for any a-priori polynomial-size set of input vectors, and for any coefficient γ_y of any of these vectors, it holds with all but exponentially small probability that they are all bounded by $\frac{cn}{2^n}$ in square-absolute-value. We note that since we consider complex vectors, the actual analysis separates β into its real and imaginary part, and analyze each separately.

From this point and on, we analyze the remainder of our construction under the assumption that the input quantum states are $\frac{cn}{2^n}$-flat.

1.2.2 Cross-Term Removal and Symmetrization

We consider the application of $(U_\pi U_g)^{\otimes st}$ on an input state consisting of s blocks, each of which contains t copies of the same (flat) state, where the vectors in the different blocks are orthogonal. Our goal is to show that, up to normalization, the output state can be expressed as

$$\rho_{\mathrm{sym}} = \sum_{z,\sigma} \nu_\sigma |z\rangle\langle\sigma(z)| \ , \tag{2}$$

where z is summed as in Eq. (1), σ ranges over *all* permutations of $[st]$ (not only block-preserving ones), and ν_σ is a term that will be explained below.

As mentioned above, the techniques here are fairly standard in the analysis of pseudorandom states and other objects [AGQY22]. However, our analysis relies only on the general notion of flatness and not on the specific expression for the coefficients of the state.

We start by using the flatness of the states. Let $\Pi^\star$ be the projector to the vectors of length st of strings in $\{0,1\}^n$ with unique entries, that is, no entry reoccurs. Then our input state is close to its $\Pi^\star$ projection, since the collision probability in the standard basis of two entries is small due to flatness. Therefore, we may consider an input state whose density matrix supported only over entries $|z\rangle\langle z'|$, where both z, z' are unique st-tuples of elements from $\{0,1\}^n$.

We first apply $U_g^{\otimes st}$, which has the effect of zeroing out the coefficients of $|z\rangle\langle z'|$ not of the form $|z\rangle\langle\sigma(z)|$. This is the result of $\mathbb{E}_g\left[\prod_i g(z_i)\prod_i g(z'_i)\right]$ being zero for all z, z' which do not have the same entry-histogram since we average over random g's.

Finally, applying $U_\pi^{\otimes st}$ means that the coefficient of $|z\rangle\langle\sigma(z)|$ becomes independent of z, and depends only on σ. This follows from taking the expectation over π, which averages the coefficients $|z\rangle\langle\sigma(z)|$ for all unique entries z (since π is a random permutation). We denote the coefficient corresponding to σ by ν_σ.

1.2.3 Bounding The Difference

The difference between Eq. (1) and Eq. (2) is two-fold. First, the target state only sums over block-preserving permutations, whereas the symmetrized state sums over all permutations. Second, the target state gives the same weight to all terms $|z\rangle\langle\sigma(z)|$ that it ranges over, whereas the symmetrized state may give different weights to different permutations.

Our crucial observation here, is to notice that if it is possible to go from a permutation σ to a permutation σ' by performing block-preserving operations, then σ and σ' have the same coefficient ν_σ. This is the case since the input state corresponds to s blocks where each block contains t identical states. Therefore, the state of the system should be invariant under block-preserving permutations, which is manifested in the corresponding terms ν_σ being equal. We may therefore define congruence classes of permutations that differ only by block-preserving operations, and associate the coefficients with the congruence class rather than a specific permutation.

Consider for every congruence class of permutations p the operator $A_{\mathsf{p}} = \sum_{\sigma\in\mathsf{p}}\sum_z |z\rangle\langle\sigma(z)|$. Then we can rewrite $\rho_{\mathrm{sym}} = \sum_{\mathsf{p}} \nu_{\mathsf{p}} A_{\mathsf{p}}$. We note that the set of all block-reserving permutations consists of a single congruence class. Therefore, all block-preserving permutations receive the same weight, as required. The remaining goal is to show that the classes that correspond to permutations that are not block-preserving are (jointly) negligible in ℓ_1 weight.

We let k be the number of "crossings" of a congruence class. That is, the number of inputs whose output belongs to a different block. The crossing number, in some sense, represents the amount of deviation from being block-preserving. Denote by p_k the set of congruence classes with k crossings. Note that there is a single congruence class with zero crossings, and it corresponds to the aforementioned set of block-preserving permutations. Our goal therefore is to bound the trace norm of $\sum_{k>1} \sum_{\mathsf{p} \in \mathsf{p}_k} \nu_{\mathsf{p}} A_{\mathsf{p}}$.[3]

The argument here contains three parts:

1. We show that for combinatorial reasons, $\|A_{\mathsf{p}}\|$ grows with $\mathrm{poly}(nst)^k$ (up to a global normalization factor). Essentially, we show that this norm is related to the number of permutations in p (which due to symmetry is the same in all p with the same k).

2. We show, again by a combinatorial argument, that the number of congruence classes with the same k also grows as $\mathrm{poly}(nst)^k$.

3. Perhaps the most technically involved part is to show that ν_{p} decays, up to a global normalization factor, with δ^k for a (negligible) factor $\delta = \frac{\mathrm{poly}(nst)}{2^n}$. This is achieved by noticing that ν_{p} contains an "inner product" term for every crossing edge. This term would ideally correspond to an inner product between two input vectors, and since these are orthogonal we would expect this value to be 0. However, the inner product is "disturbed" because permutations do not allow recurrence, which in turn creates dependence between the would-be inner products. We therefore need to come up with a fairly involved technical argument to show that whereas the value ν_{p} is not exactly 0, each of the would-be inner products contributes a δ factor, resulting in an exponential decay.

Other factors cancel out perfectly, since they represent the same combinatorial reality, and indeed when putting-together all of the above, we get sum of the form $\sum_{k>1} \left(\frac{\mathrm{poly}(nst)}{2^n}\right)^k$, which converges to a negligible value as required, bearing in mind that $s, t = \mathrm{poly}(n)$.

1.3 Other Previous Works

Alagic, Majenz, and Russell [AMR20] considered a *stateful* variant of PRU, where the adversary is interacting with a *stateful simulator* whose internal state may change and grow as the experiment proceeds. Even under this relaxed notion, they were only able to construct PRU using a simulator in (quantum) PSPACE. However, in this variant one can hope to achieve *statistical* (or even perfect) security rather than just computational.

1.4 Future Directions

Contrary to the constructions in [LQS+23], ours is not *scalable* (a notion introduced in [BS20]). That is, we consider adversaries whose running time is polynomial in the input size of the unitary n. In contrast, in a scalable construction, one specifies separately the parameters for the adversary's

[3] We notice that $k = 1$ is not possible for reasons of symmetry and therefore it does not appear in the sum, but we could have achieved our result even without this minor optimization.

complexity and for the input size. Scalable constructions are usually more involved, and in particularly require more computational depth, than non-scalable ones. It remains an open question to find a scalable version of our construction, or to prove lower bounds in this vein.

Our work shows a fairly strong notion of pseudorandomness for PRU that can be achieved using a straightforward real-valued construction. One may further wonder whether it is possible to get even closer to full-fledged PRU using constructions like ours (or even our construction as-is). For example, the negative result of [HBK23] does not seem to exclude real-valued PRU that are applicable to *tensor-product* inputs. Namely, inputs that are not necessarily orthogonal, but are not entangled with each other (recall that entangled queries stand at the core of the [HBK23] separation). We believe that answering some of these questions may be within reach, but were hurried to report our current progress due to the recent announcement of [MPSY24].

1.5 Paper Organization

Section 2 introduces notations, defines quantum-secure pseudorandom functions and permutations, and references the notion of almost invariancy under Haar random unitaries. Section 3 provides the security definition for non-adaptive orthogonal-inputs pseudorandom unitaries, presents the main theorem, describes the construction and reduce it to the information theoretic version. Section 4 contains the technical contributions. It starts with the main information theoretic lemma, continues with the analysis of the two steps of the construction separately, and concludes with proving the main lemma and theorem.

Acknowledgments

We thank Omri Shmueli for multiple contributions to the results presented in this work. We would also like to thank Yanglin Hu and Marco Patrick Tomamichel for pointing out a gap in a proof in the previous version of the manuscript.

2 Preliminaries

2.1 Notation

We denote $N = 2^n$ and $N^{\underline{st}} = \binom{N}{st}(st)! = N(N-1)\cdots(N-st+1)$. We denote the trace norm of A by $\|A\|_1 = \mathrm{Tr}(\sqrt{AA^\dagger})$, which is the sum of the singular values.

Vectors, Functions, and Permutations. Let $s, t \in \mathbb{N}$. Throughout our analysis we will consider vectors of bit-strings. Formally, an object of the form $\vec{y} \in (\{0,1\}^n)^{st}$, which indicates a t-length vector of n-bit strings. We will denote $\vec{y} = (y_1, \ldots, y_{st})$, where each coordinate in the vector is a bit-string $y_i \in \{0,1\}^n$. Let T be some set. We denote by $\mathcal{U}^{\star}_{n,st}$ the set of all length st vectors of *unique* elements from $\{0,1\}^n$, that is, no entry reoccurs.

We will consider a number of types of operations on such vectors. For any function $f : \{0,1\}^n \to D$, where D is some domain, we let $f(\vec{y}) \in D^t$ denote the pointwise application of f on each coordinate in $\vec{y}$ individually. For functions with complex range $\alpha : \{0,1\}^n \to \mathbb{C}$, we also define multiplicative notation, where we use the notation $\alpha_x = \alpha(x)$, and $\alpha_{\vec{x}} = \prod_i \alpha_{x_i}$. Note that the coefficients of quantum states constitute such functions.

For the special case of a function on the coordinates which is a permutation, we will denote it by $\pi : \{0,1\}^n \to \{0,1\}^n$. We call such a permutation an *inner permutation* since it permutes each element of $\vec{y}$ individually. We also consider an *outer permutation* (or index permutation) $\sigma \in S_{st}$ which permutes $[st] = \{1, \dots, st\}$. We will abuse the notation and think of $\sigma \in S_{st}$ also as $\sigma \in S_{[s]\times[t]}$ which takes a tuple input $(j,i), j \in [s], i \in [t]$ and outputs the tuple (j', i') s.t. $j' = \lfloor \sigma(sj+i)/s \rfloor, i' = \sigma(sj+i) \mod t$. An outer permutation permutes the indices of the elements of $\vec{y}$, i.e. $\vec{z} = \sigma(\vec{y}) \in (\{0,1\}^n)^{st}$ is such that $z_{j,i} = y_{\sigma(j,i)}$. We will also consider the subgroup $S_t^s = S_t \times \cdots \times S_t$ (s times) of outer permutations.

2.2 Concentration Bounds

Theorem 2.1 (Hoeffding's Inequality)**.** *Let Z_x, $x \in \{0,1\}^n$, be independent random variables with zero expectation such that $a_x \le Z_x \le b_x$ with probability 1. Then for all $\epsilon > 0$,*

$$\Pr\left[\sum_{x\in\{0,1\}^n} Z_x \ge \epsilon\right] \le \exp\left(\frac{-2\epsilon^2}{\sum_i (b_i - a_i)^2}\right) . \tag{3}$$

2.3 Pseudorandomness

Zhandry proved that given quantum-secure one-way functions, we can construct quantum-secure pseudorandom functions [Zha12] and pseudorandom permutations [Zha16], which we use in our construction.

Definition 2.2 (Quantum-Secure Pseudorandom Function)**.** *Let $\mathcal{K}$ be a key space. A keyed family of functions $\{F_k : \{0,1\}^n \to \{\pm 1\}\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom function (QPRF) if for any (non-uniform) quantum polynomial-time (QPT) oracle algorithm $\mathcal{A}$, F_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random function f in the sense that*

$$\left|\Pr_k[\mathcal{A}^{F_k}(1^n) = 1] - \Pr_f[\mathcal{A}^f(1^n) = 1]\right| = \mathrm{negl}(n).$$

In addition, F_k is polynomial-time computable on a classical computer.

Definition 2.3 (Quantum-Secure Pseudorandom Permutation)**.** *Let $\mathcal{K}$ be a key space. A keyed family of permutations $\{P_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom permutation (QPRP) if for any (non-uniform) QPT oracle algorithm $\mathcal{A}$, P_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random permutation π in the sense that*

$$\left|\Pr_k[\mathcal{A}^{P_k, P_k^{-1}}(1^n) = 1] - \Pr_\pi[\mathcal{A}^{\pi,\pi^{-1}}(1^n) = 1]\right| = \mathrm{negl}(n).$$

In addition, P_k is polynomial-time computable on a classical computer.

2.4 Almost Invariance Under Haar Unitaries

The following definition, claim and lemma are taken from [AGKL23].

Definition 2.4. *Let $n, q, \ell \in \mathbb{N}$. An $(\ell + n \cdot q)$-qubit state ρ is ϵ-almost invariant under q-fold Haar unitary if*

$$\mathrm{TD}\left(\rho, \underset{U \leftarrow Haar_n}{\mathbb{E}}\left[(I_\ell \otimes U^{\otimes q})\rho(I_\ell \otimes (U^\dagger)^{\otimes q})\right]\right) \leq \epsilon \tag{4}$$

Claim 2.5. *Let $n, q, \ell \in \mathbb{N}$. Suppose Φ is a quantum channel that is a probabilistic mixture of unitaries on $(\ell + n \cdot q)$ qubits. More precisely, $\Phi(\rho) \coloneqq \mathbb{E}_{k \leftarrow \mathcal{D}}\left[(I_\ell \otimes V_k^{\otimes q})\rho(I_\ell \otimes (V_k^\dagger)^{\otimes q})\right]$ where $\mathcal{D}$ a distribution over $\{0,1\}^*$, and $V_k : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ is a unitary for every k in the support of D.*

Suppose for a $(\ell + n \cdot q)$-qubit state ρ, $\Phi(\rho)$ is ϵ-almost invariant under q-fold Haar unitary, where ϵ is a negligible function, then the following holds:

$$\mathrm{TD}\left(\Phi(\rho), \underset{U \leftarrow Haar_n}{\mathbb{E}}\left[(I_\ell \otimes U^{\otimes q})\rho(I_\ell \otimes (U^\dagger)^{\otimes q})\right]\right) \leq \epsilon \tag{5}$$

Lemma 2.6. *Let $n, s, t \in \mathbb{N}$, and define*

$$\rho_{\mathsf{uni}_{s,t}} \coloneqq \frac{1}{N^{\underline{st}}} \sum_{\substack{z \in \mathcal{U}^\star_{n,st} \\ \sigma \in S_t^s}} |z\rangle\langle\sigma(z)| \ , \tag{6}$$

then for any ℓ qubit state ρ_ℓ, $\rho_\ell \otimes \rho_{\mathsf{uni}_{s,t}}$ is $O(s^2t^2/2^n)$-almost invariant under st-fold Haar unitary (I_ℓ being applied on ρ_ℓ).

This state is close to the output of applying a Haar random unitary on s different orthogonal vectors with t copies of each.

3 Somewhat Pseudorandom Unitaries

Definition 3.1 (Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary)**.** *We say that $\{Gen_n\}_{n \in \mathbb{N}}$ is a* non-adaptive orthogonal-inputs secure pseudorandom unitary family *if there exists a polynomial κ such that:*

- *For every $k \in \{0,1\}^{\kappa(n)}$, $U_k \coloneqq Gen_n(k)$ is a QPT algorithm implementing a unitary operation on n qubits.*
- *Fix $s \coloneqq s(n), t \coloneqq t(n)$ polynomials in n. Let A be a set and let $\left\{|\psi^{(1,a)}\rangle, \ldots |\psi^{(s,a)}\rangle\right\}$ be orthogonal states and ρ_a be any ℓ-qubit state for all $a \in A$. Let p_a be probabilities such that $\sum_{a\ inA} p_a = 1$. There exists a sufficiently large $n \in \mathbb{N}$, such that for any (non-uniform) QPT distinguisher $\mathcal{A}$ that makes queries of the form*

$$\rho_{in} \coloneqq \sum_{a \in A} p_a \left(\rho_a \otimes \left(\bigotimes_{j \in [s]} (|\psi^{(j,a)}\rangle\langle\psi^{(j,a)}|)^{\otimes t}\right)\right) \tag{7}$$

to the st-tensor of the unitary U_k it holds that

$$\left| \Pr_{k \leftarrow \{0,1\}^\kappa}\left[\mathcal{A}\left((I_\ell \otimes U_k^{\otimes st})\rho_{in}(I_\ell \otimes U_k^{\dagger^{\otimes st}})\right) = 1\right] \right.$$
$$\left. - \Pr_{U \leftarrow Haar_n}\left[\mathcal{A}\left((I_\ell \otimes U^{\otimes st})\rho_{in}(I_\ell \otimes U^{\dagger^{\otimes st}})\right) = 1\right] \right| \leq \mathrm{negl}(n) \tag{8}$$

Theorem 3.2. *Assuming the existence of quantum secure one way functions, there exists a family of non-adaptive orthogonal-inputs secure pseudorandom* real *unitary.*

From definition 2.4, claim 2.5, and lemma 2.6, our goal will be to construct a channel Φ such that its output for copies of orthogonal states looks like almost invariant under st-fold Haar unitary.

The construction Let $F, G : \{0,1\}^n \to \{\pm 1\}$ be QPRFs and $P : \{0,1\}^n \to \{0,1\}^n$ be a QPRP. We define the unitary $U_{F,G,P}$ on n qubits as follows:

$$U_{F,G,P} = U_P U_G H^{\otimes n} U_F \ , \tag{9}$$

where $U_F = \sum_{x\in\{0,1\}^n} F(x)|x\rangle\langle x|, U_G = \sum_{x\in\{0,1\}^n} G(x)|x\rangle\langle x|$, and $U_P = \sum_{x\in\{0,1\}^n} |P(x)\rangle\langle x|$.

Invoking Cryptographic Assumptions We move from pseudorandom F, G, P to truly random f, g, π. The unitary in the random case is denoted by $U_{f,g,\pi}$ and defined similarly.

Claim 3.3. *Let $U_{F,G,P}$ implicitly depend on a key k. Assuming the security of F, G and P, it holds that*

$$\begin{aligned}\Bigg| \Pr_k \left[\mathcal{A}\left(\left(I_\ell \otimes {U_{F,G,P}}^{\otimes st}\right) \rho_{in} \left(I_\ell \otimes {U^\dagger_{F,G,P}}^{\otimes st}\right)\right) = 1\right] \\ - \Pr_{f,g,\pi} \left[\mathcal{A}\left(\left(I_\ell \otimes {U_{f,g,\pi}}^{\otimes st}\right) \rho_{in} \left(I_\ell \otimes {U^\dagger_{f,g,\pi}}^{\otimes st}\right)\right) = 1\right] \Bigg| \le \mathrm{negl}(n) \ ,\end{aligned} \tag{10}$$

where $k = (k_F, k_G, k_P)$ is the key for the PRFs and PRP.

Proof. We define four hybrids. In the first one we query $U_{F,G,P}$, in the second $U_{f,G,P}$, in the third $U_{f,g,P}$, and in the forth $U_{f,g,\pi}$ (all defined similarly to $U_{F,G,P}$). Each two consecutive hybrids are indistinguishable by the security of function replaced between the two hybrids. □

4 Analysis

We now turn to analyze the application of $U_{f,g,\pi}$ information theoretically. The main lemma is:

Lemma 4.1. *Let s, t be polynomials in n and let $\{|\psi^{(j)}\rangle\}_{j\in[s]}$ be orthogonal quantum states. Then*

$$\left\| \mathop{\mathbb{E}}_{f,g,\pi} \left[{U_{f,g,\pi}}^{\otimes st} \left(\bigotimes_{j\in[s]} (|\psi^{(j)}\rangle\langle\psi^{(j)}|)^{\otimes t} \right) {U^\dagger_{f,g,\pi}}^{\otimes st} \right] - \rho_{\mathsf{uni}_{s,t}} \right\|_1 \le O(s^6 t^4 n^2 / N) \ . \tag{11}$$

Were the expectation is over sampling random functions f, g and a random permutation π.

4.1 Achieving Flatness

The first two steps in the construction, namely adding a random binary phase with U_f and performing $H^{\otimes n}$, achieve the goal of flattening the state with respect to the standard basis.

Definition 4.2. *A quantum state $|\alpha\rangle = \sum_x \alpha_x |x\rangle$, where $|x\rangle$ are the computational basis elements, is ϵ-flat if* $\max_x |\alpha_x|^2 \le \epsilon$.

Note that this is equivalent to the min-entropy of the computational-basis measurement of $|\alpha\rangle$ having min-entropy at least $\log(1/\epsilon)$.

Lemma 4.3. *Let $|\beta\rangle = \sum_{x\in\{0,1\}^n} \beta_x |x\rangle$ be a quantum state, $c > 0$, and let $f : \{0,1\}^n \to \{\pm 1\}$ be a random function. Then with probability at least $1 - 2\exp\left(-\left(\frac{c}{4} - \ln(2)\right) n\right)$ the state $H^{\otimes n} U_f |\beta\rangle$ is $c \cdot \frac{n}{2^n}$-flat.*

Proof. Denote $|\xi\rangle = H^{\otimes n} U_f |\beta\rangle$. Let $|y\rangle$ be a standard basis element, and look at $\xi_y = \langle y|\xi\rangle$:

$$\xi_y = \langle y|H^{\otimes n} U_f |\beta\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \langle x|U_f|\beta\rangle \tag{12}$$

$$= \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} f(x) \langle x|\beta\rangle \tag{13}$$

$$= \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} f(x) \beta_x \tag{14}$$

We analyze the real and imaginary parts ξ_y separately. Define the random variables Z_x to be $\Re(2^{-n/2}(-1)^{x\cdot y} f(x)\beta_x)$. It follows that $|Z_x| \le 2^{-n/2}|\beta_x|$. Using Hoeffding's inequality we get

$$\Pr\left[|\Re(\xi_y)| \ge \sqrt{\epsilon/2}\right] \le \exp\left(\frac{-2\cdot(\epsilon/2)}{\sum_x |2\cdot 2^{-n/2}\beta_x|^2}\right) = \exp\left(\frac{-\epsilon \cdot 2^n}{4\sum_x |\beta_x|^2}\right) = \exp(-\epsilon\cdot 2^n/4) \tag{15}$$

Where the second to last equality follows from $|\beta\rangle$ being a quantum state and thus a unit vector. We get $\Pr\left[|\Im(\xi_y)| \ge \sqrt{\epsilon/2}\right] \le \exp(-\epsilon \cdot 2^n/4)$ similarly. Using the bound on both the real part and imaginary part we get:

$$\Pr\left[|\xi_y| \ge \sqrt{\epsilon}\right] \le \Pr\left[|\Re(\xi_y)|^2 + |\Im(\xi_y)|^2 \ge \epsilon\right] \tag{16}$$

$$\le \Pr\left[|\Re(\xi_y)|^2 \ge \epsilon/2 \vee |\Im(\xi_y)|^2 \ge \epsilon/2\right] \tag{17}$$

$$\le \Pr\left[|\Re(\xi_y)| \ge \sqrt{\epsilon/2}\right] + \Pr\left[|\Im(\xi_y)| \ge \sqrt{\epsilon/2}\right] \tag{18}$$

$$\le 2\exp\left(-\epsilon\cdot 2^n/4\right) \tag{19}$$

Finally, we use the union bound over the 2^n entries of $|\xi\rangle$ to get that with probability at most $2\exp\left(-\epsilon\cdot 2^n/4\right)\cdot 2^n$ there exists an entry $|\xi_y| \ge \sqrt{\epsilon}$. Taking $\epsilon = c\cdot\frac{n}{2^n}$ completes the lemma. □

Using the union bound, an immediate corollary follows:

Corollary 4.4. *Let $\{|\beta^{(j)}\rangle\}_{j\in[s]}$ be quantum states, $c > 0$, and let $f : \{0,1\}^n \to \{\pm 1\}$ be a random function. Then with probability $1 - s\cdot 2\exp\left(-\left(\frac{c}{4} - \ln(2)\right) n\right)$ all states $H^{\otimes n} U_f |\beta^{(j)}\rangle$ are $c\cdot\frac{n}{2^n}$-flat.*

4.2 Getting from Flat States to Random-Looking Ones

We now prove that applying a random binary phase and a random permutation to t copies of s orthogonal flat vectors with is close in trace distance the almost invariant state from lemma 2.6. We prove the following lemma:

Lemma 4.5. *Let $g : \{0,1\}^n \to \{\pm 1\}$ be a random function and $\pi : \{0,1\}^n \to \{0,1\}^n$ be a random (inner) permutation. Let $\{|\alpha^{(j)}\rangle\}_{j\in[s]}$ be a set of s arbitrary orthogonal ϵ-flat vectors in $\mathbb{C}^{\{0,1\}^n}$. Denote:*

$$\rho := \mathbb{E}_{g,\pi}\left[(U_\pi U_g)^{\otimes st}\left(\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}\right)(U_g^\dagger U_\pi^\dagger)^{\otimes st}\right] . \tag{20}$$

Then,

$$\|\rho - \rho_{\mathsf{uni}_{s,t}}\|_1 \le O((st)^2\epsilon + Ns^6t^4\epsilon^2) . \tag{21}$$

4.2.1 Focusing on Unique States

Recall that $g_z = \prod_{j,i} g(z_{j,i})$. We notice that for all $z, z' \in \{0,1\}^{n\cdot st}$ it holds that $\mathbb{E}_g[g_z g_{z'}^*]$ is equal to 1 if and only if the binary type of z and z' (that is, the histogram of the entries modulus 2) are equal. Otherwise, the expectation is equal to 0. Expressing ρ in the standard basis we get

$$\rho = \mathop{\mathbb{E}}_{g,\pi}\left[\sum_{z,z'\in\{0,1\}^{n\cdot st}} g_z g_{z'} \prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j)}_{z(j,i)} \alpha^{*(j)}_{z'(j,i)} |\pi(z)\rangle\langle\pi(z')|\right] \tag{22}$$

$$= \mathop{\mathbb{E}}_{\pi}\left[\sum_{z,z'\in\{0,1\}^{n\cdot st}} \mathop{\mathbb{E}}_{g}[g_z g_{z'}^*] \prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j)}_{z(j,i)} \alpha^{*(j)}_{z'(j,i)} |\pi(z)\rangle\langle\pi(z')|\right] \tag{23}$$

$$= \mathop{\mathbb{E}}_{\pi}\left[\sum_{z\in\{0,1\}^{n\cdot st}} \sum_{\substack{z'\in\{0,1\}^{n\cdot st}\\ \mathsf{bintype}(z')=\mathsf{bintype}(z)}} \prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j)}_{z(j,i)} \alpha^{*(j)}_{z'(j,i)} |\pi(z)\rangle\langle\pi(z')|\right] , \tag{24}$$

where $\mathsf{bintype}(z)$ is the binary type of z.

Let $\Pi^\star := \sum_{\vec{z}\in\mathcal{U}^\star_{n,st}} |\vec{z}\rangle\langle\vec{z}|$ be the uniqueness projector, and let

$$\rho^\star := \frac{\Pi^\star\rho\Pi^\star}{\mathrm{Tr}[\Pi^\star\rho]} \tag{25}$$

be the unique restrictions of ρ. We show that ρ is close to its unique restriction.

Claim 4.5.1. *It holds that*

$$\|\rho - \rho^\star\|_1 \le O\left((st)^2\epsilon\right) . \tag{26}$$

Proof. Notice that $\Pi^\star \rho (I - \Pi^\star) = (I - \Pi^\star)\rho \Pi^\star = 0$, as $|\pi(z)\rangle$ is in the unique restriction if and only if $\langle \sigma(\pi(z))|$ is in the unique restriction too (which occurs if and only if the binary type/histogram has st entries of 1). It follows that $\rho = \Pi^\star \rho \Pi^\star + (I - \Pi^\star)\rho(I - \Pi^\star)$, and as $\Pi^\star \rho \Pi^\star$ and $(I - \Pi^\star)\rho(I - \Pi^\star)$ are positive semi-definite, it is enough to show that

$$\mathrm{Tr}[(I - \Pi^\star)\rho(I - \Pi^\star)] \leq (st)^2 \cdot \epsilon \ . \tag{27}$$

We note that $\Pi^\star$ is invariant under U_g, U_π, therefore

$$\begin{aligned} \mathrm{Tr}[(I - \Pi^\star)\rho(I - \Pi^\star)] &= \mathrm{Tr}\left[(I - \Pi^\star)\mathbb{E}_{g,\pi}\left[(U_\pi U_g)^{\otimes st}\left(\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}\right)(U_g^\dagger U_\pi^\dagger)^{\otimes st}\right]\right] &(28)\\ &= \mathbb{E}_{g,\pi}\left[\mathrm{Tr}\left[(U_\pi U_g)^{\otimes st}(I - \Pi^\star)\left(\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}\right)(U_g^\dagger U_\pi^\dagger)^{\otimes st}\right]\right] &(29)\\ &= \mathbb{E}_{g,\pi}\left[\mathrm{Tr}\left[(I - \Pi^\star)\left(\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}\right)\right]\right] &(30)\\ &= \mathrm{Tr}\left[(I - \Pi^\star)\left(\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}\right)\right] \ , &(31) \end{aligned}$$

which is exactly the probability of measuring $\otimes_{j\in[s]}|\alpha^{(j)}\rangle\langle\alpha^{(j)}|^{\otimes t}$ in the computational basis, and obtaining an (st)-tuple that contains a repetition (i.e. an element in $\{0,1\}^n$ that appears more than once). Due to ϵ-flatness, the probability for this is bounded by $(st)^2 \cdot \epsilon$. ■

Recall that $\mathcal{U}^\star_{n,st}$ is the set of all st length vectors with unique entries from $\{0,1\}^n$. From the definitions of U_g, U_π and claim 4.5.1, for $c_1 = \mathrm{Tr}[\Pi^\star \rho_{g,\pi}] \geq \frac{1}{1-\epsilon(st)^2}$ we get

$$\rho^\star = c_1 \cdot \mathop{\mathbb{E}}_{\pi}\left[\sum_{z\in\mathcal{U}^\star_{n,st}}\sum_{\sigma\in S_{st}}\prod_{\substack{j\in[s]\\ i\in[t]}}\alpha^{(j)}_{z(j,i)}{\alpha^*}^{(j)}_{\sigma(z)(j,i)}|\pi(z)\rangle\langle\sigma(\pi(z))|\right] \ . \tag{32}$$

Notice the sum over z' changed to sum over $\sigma \in S_{st}$ (an outer permutation which permutes the positions of the entries) as for z with unique entries it holds that $\mathit{bintype}(z) = \mathit{bintype}(z')$ if and only if there exists $\sigma \in S_{st}$ s.t. $z' = \sigma(z)$.

For all $(j,i) \in [s] \times [t]$ we define $\alpha^{(j,i)} = \alpha^{(j)}$ (since we implicitly think of the index (j,i) as pointing to the j'th qubit group which consists of a t-tensor of $|\alpha^{(j)}\rangle\langle\alpha^{(j)}|$). Changing the order of summation by π^{-1}. We get

$$\rho^\star = c_1 \cdot \sum_{\sigma\in S_{st}}\sum_{z\in\mathcal{U}^\star_{n,st}}\underbrace{\mathbb{E}_{\pi^{-1}}\left[\prod_{\substack{j\in[s]\\ i\in[t]}}\alpha^{(j,i)}_{\pi^{-1}(z)(j,i)}{\alpha^*}^{(j,i)}_{\sigma(\pi^{-1}(z))(j,i)}\right]}_{\text{denote } \nu_{\sigma,z}}|z\rangle\langle\sigma(z)| \ . \tag{33}$$

As π^{-1} is also a random permutation, we get that $\nu_{\sigma,z}$ is independent of z, i.e. $\nu_{\sigma,z} = \nu_\sigma$ for all $z \in \mathcal{U}^\star_{n,st}$. Making a change of variables $x = \pi^{-1}(z)$,

$$\nu_\sigma = \mathbb{E}_{x\in\mathcal{U}^\star_{n,st}}\left[\prod_{\substack{j\in[s]\\ i\in[t]}}\alpha^{(j,i)}_{x(j,i)}{\alpha^*}^{(j,i)}_{\sigma(x)(j,i)}\right] \tag{34}$$

and

$$\rho^\star = c_1 \cdot \sum_{\sigma \in S_{st}} \nu_\sigma \sum_{z \in \mathcal{U}^\star_{n,st}} |z\rangle\langle\sigma(z)| \ . \tag{35}$$

4.2.2 Using Orthogonality to Reach Closeness to an Almost Invariant State

We consider the operator

$$A = \sum_{\sigma \in S_{st}} \nu_\sigma \sum_{z \in \mathcal{U}^\star_{n,st}} |z\rangle\langle\sigma(z)| \ , \tag{36}$$

and show that it is close in trace norm to to the same operator summing only over $\sigma \in S_t^s$. For that, we define the following.

Definition 4.6. *For any permutation $\sigma \in S_{st}$, we consider the associated directed graph G_σ, whose vertex set is $[s] \times [t]$, and there is an edge $(j,i) \to (j',i')$ if and only if $\sigma((j,i)) = (j',i')$. For all $j \in [s]$, we define the j-th vertex-block as the set $\{(j,i)\}_{i\in[t]}$. We sometimes completely associate σ with G_σ.*

We associate each vertex with its outgoing edge. For any vertex $v = (j,i) \in G_\sigma$ with the outgoing edge $(j',i') = \sigma((i,j))$, we denote $j_v = j$, $j'_v = j'$, namely the block-source and block-destination of v in the graph. We say that v is a crossing vertex *if $j_v \neq j'_v$, and otherwise v is* non-crossing*. We denote the set of crossing vertices by cv_σ, and will often omit the subscript when σ is clear from the context. Likewise, we denote the set of non-crossing vertices by $\overline{\mathsf{cv}_\sigma}$.*

The block edge pattern *of σ is the vector $\mathsf{p}_\sigma \in \mathbb{N}^{[s]\times[s]}$, where $\mathsf{p}_\sigma[j,j']$ is the number of crossing vertices from block j to block j'. We say that two permutations are congruent (with respect to S_t^s) if they have the same block edge pattern. It follows that σ, σ' are congruent, denoted $\sigma \cong \sigma'$ if and only if there exist $\sigma_1, \sigma_2 \in S_t^s$ s.t. $\sigma' = \sigma_1\sigma\sigma_2$. We overload the notation and use p also to denote the congruence class corresponding to this pattern.*

The number of crossing and non-crossing vertices is thus $|\mathsf{cv}|$, and $|\overline{\mathsf{cv}}|$ respectively (so, $|\mathsf{cv}| + |\overline{\mathsf{cv}}| = st$). We note that $|\mathsf{cv}|$, $|\overline{\mathsf{cv}}|$ only depend on the congruence class p.

Under the above definition, and denoting $x(v) = x(j,i)$, we have that

$$\nu_\sigma = \mathbb{E}_{x \in \mathcal{U}^\star_{n,st}} \left[\prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j,i)}_{x(j,i)} \alpha^{*(j,i)}_{\sigma(x)(j,i)} \right] = \mathbb{E}_{x \in \mathcal{U}^\star_{n,st}} \left[\prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j,i)}_{x(j,i)} \prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{*(j,i)}_{x(\sigma^{-1}(j,i))} \right] \tag{37}$$

$$= \mathbb{E}_{x \in \mathcal{U}^\star_{n,st}} \left[\prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j,i)}_{x(j,i)} \prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{*\sigma((j,i))}_{x(j,i)} \right] = \mathbb{E}_{x \in \mathcal{U}^\star_{n,st}} \left[\prod_{\substack{j\in[s]\\ i\in[t]}} \alpha^{(j_v)}_{x(v)} \alpha^{*(j'_v)}_{x(v)} \right] \tag{38}$$

$$= \mathbb{E}_{x \in \mathcal{U}^\star_{n,st}} \left[\prod_{v\in\overline{\mathsf{cv}}} \left|\alpha^{(j_v)}_{x(v)}\right|^2 \prod_{v\in\mathsf{cv}} \alpha^{(j_v)}_{x(v)} \alpha^{*(j'_v)}_{x(v)} \right] \ . \tag{39}$$

Proposition 4.7. *If $\sigma \cong \sigma'$ then $\nu_\sigma = \nu_{\sigma'}$.*

Proof. Consider a permutation σ. Let us break the operand in the expectation in Eq. (39) into blocks. Namely, for a fixed j consider

$$\prod_{\substack{v\in\overline{\mathsf{cv}}\\ j_v=j}} \left|\alpha^{(j_v)}_{x(v)}\right|^2 \prod_{\substack{v\in\mathsf{cv}\\ j_v=j}} \alpha^{(j_v)}_{x(v)}\alpha^{*(j'_v)}_{x(v)} \ . \tag{40}$$

We notice that the expression above only depends on the number and block identities of the neighbors of the elements in the j'th block. Multiplying over all blocks we get ν_σ which remains invariant under (outer) permutations in S_t^s. □

We can therefore denote ν_{p} which is the value corresponding to ν_σ for all $\sigma \in \mathsf{p}$. Define

$$A_{\mathsf{p}} \coloneqq \sum_{z\in\mathcal{U}^\star_{n,st}} \sum_{\sigma\in\mathsf{p}} |z\rangle\langle\sigma(z)| = \sum_{z\in\mathcal{U}^\star_{n,st}} |z\rangle \sum_{\sigma\in\mathsf{p}} \langle\sigma(z)| \ . \tag{41}$$

Corollary 4.8. *It holds that*

$$A = \sum_{\mathsf{p}} \nu_{\mathsf{p}} \sum_{z\in\mathcal{U}^\star_{n,st}} \sum_{\sigma\in\mathsf{p}} |z\rangle\langle\sigma(z)| = \sum_{\mathsf{p}} \nu_{\mathsf{p}} A_{\mathsf{p}} \ , \tag{42}$$

We separate the analysis to bounding the norm of A_{p} according to the crossing number of p, counting the number of congruence classes with a certain crossing number, and bounding ν_{p} according to the crossing number of p.

Lemma 4.9. *Let* p *be with* $|\mathsf{cv}| = k$*. It holds that*

$$\|A_{\mathsf{p}}\|_1 \leq N^{\underline{st}} \cdot t^k \tag{43}$$

Proof. Partition the space $z \in \mathcal{U}^\star_{n,st}$ into parts that are invariant under "block-permutations", i.e. under S_t^s. By definition, each such set contains $(t!)^s$ different z values (recall that all $z(j,i)$ are unique), and the number of partitions is $\frac{N^{\underline{st}}}{(t!)^s}$.

For each partition P, define

$$A_{\mathsf{p},P} = \sum_{z\in P} |z\rangle \sum_{\sigma\in\mathsf{p}} \langle\sigma(z)| \ . \tag{44}$$

For all $z \in P$, the vector $\sum_{\sigma\in\mathsf{p}}\langle\sigma(z)|$ is the same, since the elements of P all differ by a $\tilde{\sigma} \in S_t^s$ permutation, and $\mathsf{p} = \mathsf{p}\tilde{\sigma}$. Thus, $A_{\mathsf{p},P}$ is a rank-1 matrix, and the norm $\|A_{\mathsf{p},P}\|_1$ is the product of the Euclidean norm of the two vectors. In our case,

$$\|A_{\mathsf{p},P}\|_1 = \sqrt{|P|} \cdot \sqrt{|\mathsf{p}|} \tag{45}$$

$$= (t!)^{s/2} \cdot \sqrt{|\mathsf{p}|} \ . \tag{46}$$

Therefore, by the triangle inequality we have that

$$\|A_{\mathsf{p}}\|_1 \leq \frac{N^{\underline{st}}}{(t!)^s} \cdot (t!)^{s/2} \cdot \sqrt{|\mathsf{p}|} \ , \tag{47}$$

Next, we bound the cardinality of p when interpreted as a congruence class (namely, the number of permutations that have edge pattern p):

$$|\mathsf{p}| \le (t!)^s \cdot t^{2k} \ . \tag{48}$$

We show this by over-counting the set of graphs with a given edge pattern and $|\mathsf{cv}| = k$. We first consider all of the crossing edges, of which there are k by definition. For each such edge, the edge pattern already specifies its source and destination blocks, so we need to choose its specific source and origin vertices within the blocks. There are at most t^2 options for each edge, and thus at most t^{2k} options in general. Then, for all of the other edges, it just remains to go over each of the s blocks of vertices in the graph, and organize the internal edges in the block. We note that any such arrangement can be completed into a permutation in S_t, by orienting the outgoing and incoming edges of the block towards each other arbitrarily. Therefore, the number of arrangements in each block is at most $|S_t| = t!$. It follows that across all blocks, the total number of internal arrangements in bounded by $(t!)^s$. The lemma follows from equations 47 and 48.

□

Lemma 4.10. *Denote*

$$\mathsf{p}_k = \{\mathsf{p} : |\mathsf{cv}| = k\} \tag{49}$$

the number of congruence classes with crossing number k. Then $|\mathsf{p}_k| \le s^{2k}$.

Proof. We over-count the elements in p_k. Each edge should be assigned to one of $\binom{s}{2} \le s^2$ pairs of origin and destination blocks. Therefore, the total number of edge patterns is at most s^{2k}. □

We now bound

Lemma 4.11. *Let p be with crossing numeber $|\mathsf{cv}|$. It holds that*

$$|\nu_{\mathsf{p}}| \le (N^{\underline{st}})^{-1}((st)^2\epsilon^2 N)^{|\mathsf{cv}|/2} \ . \tag{50}$$

Proof. Consider some $\sigma \in \mathsf{p}$, and recall that

$$\nu_\sigma = \mathbb{E}_{x\in\mathcal{U}^\star_{n,st}}\left[\prod_{v\in\overline{\mathsf{cv}}}\left|\alpha^{(j_v)}_{x(v)}\right|^2 \prod_{v\in\mathsf{cv}}\alpha^{(j_v)}_{x(v)}\alpha^{*(j'_v)}_{x(v)}\right] = (N^{\underline{st}})^{-1}\sum_{x\in\mathcal{U}^\star_{n,st}}\left[\prod_{v\in\overline{\mathsf{cv}}}\left|\alpha^{(j_v)}_{x(v)}\right|^2 \prod_{v\in\mathsf{cv}}\alpha^{(j_v)}_{x(v)}\alpha^{*(j'_v)}_{x(v)}\right] \ . \tag{51}$$

It is possible to sum over the x elements as follows. Go over all v at arbitrary order, and for each v, let $x(v)$ run over all elements in $\{0,1\}^n$ that were not selected in the previous v's, for each such value of $x(v)$ continue to pick value for the next v in the order.

In order to analyze this expression, we consider a more general expression as follows:

$$\tau = \sum_{y_1,\dots,y_m}\prod_{i\in[m]}\left|\alpha^{(j_i)}_{y_i}\right|^2 \delta(\alpha_{y_1},\dots,\alpha_{y_m})\sum_{z_1} M_1(\alpha_{z_1})\cdots\sum_{z_\ell} M_\ell(\alpha_{z_\ell}) \ , \tag{52}$$

where the indices y_i and z_i run over all of $\{0,1\}^n$ except for the preceding values of the indices. That is, the $y_1,\dots,y_m$ values are first chosen to be distinct, and then each z_i is chosen in order to be distinct from $y_1,\dots,y_m$ and all preceding z_i.

The function $\delta(\cdot)$ can be an arbitrary polynomial, and the functions M_i are monomials, where δ and M_i can act on the set of their operands and their complex conjugates. We only consider setting where the total degree of M_i is even. We note that we can always reorder the z_i's without effecting the total value of the expression (maintaining the convention that "later" z_i's take all values except those of y_i's and "previous" z_i's and).

We let d_i denote the total degree of M_i. We say that an index z_i is *loaded* if $d_i \geq 4$, otherwise we say that it is *free* (by our convention this means that $d_i = 2$). As a convention, we always order the summation so that the loaded indices are enumerated on before the free ones. We let ℓ' denote the number of loaded indices. Furthermore, in our setting, any free term i is going to be of the form $M_i(\alpha_{z_i}) = \alpha_{z_i}^{(j)} \alpha^*{}_{z_i}^{(j')}$, or its complex conjugate, for some $j \neq j'$.

We define the *magnitude* of τ as follows, letting δ_0 be the maximal value of δ over all possible inputs that it can take:

$$\mathsf{Mag}(\tau) = \delta_0 \prod_{i \in [\ell']} (\epsilon^{d_i/2} N) \tag{53}$$

$$= \delta_0 N^{\ell'} \epsilon^{(\sum_i d_i)/2} \ . \tag{54}$$

We let $d = \sum_{i \in [\ell']} d_i$ denote the total degree of all loaded elements.

We now recall that $|\alpha^{(j)}\rangle, |\alpha^{(j')}\rangle$ are orthogonal for $j \neq j'$, and therefore $\sum_{z \in \{0,1\}^n} \alpha_z^{(j)} \alpha^*{}_z^{(j')} = 0$. It therefore follows that if τ has any free indices, i.e. by our convention if its ℓ index is free, then we have that (up to complex conjugation)

$$\sum_{z_\ell} M_\ell(\alpha_{z_\ell}) = \sum_{z_\ell} \alpha_{z_\ell}^{(j)} \alpha^*{}_{z_\ell}^{(j')} = 0 - \sum_{i < \ell} \alpha_{z_i}^{(j)} \alpha^*{}_{z_i}^{(j')} + \delta_\ell(\alpha_{y_1}, \ldots \alpha_{y_m}) \ . \tag{55}$$

where $|\delta_\ell| \leq \epsilon \cdot (st)$ from ϵ flatness.

Each term of the form $\alpha_{z_i}^{(j)} \alpha^*{}_{z_i}^{(j')}$ now "joins" M_i and so it either creates a new loaded term, if z_i was not previously loaded, decreasing the value of Mag by $\epsilon^2 N$, or adds 2 to the degree of a pre-existing loaded term if z_i was previously loaded, decreasing the value of Mag by ϵ. Furthermore, multiplying by δ_ℓ would decrease the value of the "global" delta by a factor of $\epsilon \cdot (st)$. Therefore, we can write τ as a sum of ℓ terms, each of which conforms with the general form of Eq. (52), but with only $\ell - 1$ indices (rather than ℓ), namely:

$$\tau = \sum_{i \in [\ell]} \tau_i \ , \tag{56}$$

and it holds that

$$\mathsf{Mag}(\tau_i) \leq \max\{\epsilon^2 N, \epsilon, \epsilon \cdot (st)\} \mathsf{Mag}(\tau) \leq (\epsilon^2 N(st)) \cdot \mathsf{Mag}(\tau) \ . \tag{57}$$

We can now prove the following inductive claim:

Claim 4.11.1. *Let τ be with parameters m, ℓ, ℓ' as above, and assume $(\epsilon^2 N(st)\ell) < 1$ then it holds that*

$$|\tau| \leq (\epsilon^2 N(st)\ell)^{\frac{\ell - \ell'}{2}} \cdot \mathsf{Mag}(\tau) \ . \tag{58}$$

Proof. We prove this inductively over the value of $\ell - \ell'$. For the base case, consider the setting where $\ell' = \ell$. Notice that $\sum_{y_1,\ldots,y_m} \prod_{i\in[m]} \left|\alpha^{(j_i)}_{y_i}\right|^2 \le 1$. Therefore, τ is a (sub) convex combination of elements of the form $\delta(\alpha_{y_1},\ldots,\alpha_{y_m}) \sum_{z_1} M_1(\alpha_{z_1}) \cdots \sum_{z_\ell} M_\ell(\alpha_{z_\ell})$, that are each bounded in absolute value by $\delta_0 N^{\ell'} \epsilon^{d/2}$, which we show below. It follows that if τ has no free terms, then $|\tau| \le \mathsf{Mag}(\tau)$, where $\mathsf{Mag}(\tau)$ is given by Eq. (53).

Indeed, each such element is a product of δ, times a product of ℓ' loaded sums. The total number of summands over all the sums is at most $N^{\ell'}$ (as $l' = l$). Each element in the sum is a product of d_i elements from α. By flatness, each element of α has absolute value at most $\sqrt{\epsilon}$, and therefore each element in the sum has absolute value at most $\epsilon^{d_i/2}$. We get a value that is bounded by $\delta_0 N^{\ell'} \epsilon^{d/2}$ as required.

Now consider the case where $\ell > \ell'$. In this case, we can write $\tau = \sum_{i\in[\ell]} \tau_i$ as above. We notice that for each τ_i, we have $\ell_i = \ell - 1$, and $\ell'_i \le \ell' + 1$, so $\ell - \ell'$ shrinks by at most 2. Therefore we get the bound

$$
\begin{aligned}
|\tau| &\le \sum_{i\in[\ell]} |\tau_i| && \quad (59)\\
&\le \sum_i (\epsilon^2 N(st)\ell_i)^{\frac{\ell_i-\ell'_i}{2}} \cdot \mathsf{Mag}(\tau_i) && \text{(induction)} \quad (60)\\
&\le \sum_i (\epsilon^2 N(st)\ell)^{\frac{\ell-\ell'}{2}-1} \cdot \mathsf{Mag}(\tau_i) && (l_i \le l,\ \ell_i - \ell'_i \ge \ell - \ell' - 2) \quad (61)\\
&\le \ell \cdot (\epsilon^2 N(st)\ell)^{\frac{\ell-\ell'}{2}-1} \cdot (\epsilon^2 N(st)) \cdot \mathsf{Mag}(\tau) && \text{(Eq. (57))} \quad (62)\\
&\le (\epsilon^2 N(st)\ell)^{\frac{\ell-\ell'}{2}} \cdot \mathsf{Mag}(\tau) && \quad (63)
\end{aligned}
$$

and the claim thus follows. ■

Now, let us go back to our expression for ν_σ. We can write it as $\nu_\sigma = (N^{\underline{st}})^{-1}\tau$, where τ has the form as above, with $\delta = 1$, $\ell = |\mathsf{cv}| \le st$, and $\ell' = 0$, thus $\mathsf{Mag}(\tau) = 1$. Claim 4.11.1 therefore guarantees that

$$|\tau| \le (\epsilon^2 N(st)^2)^{|\mathsf{cv}|/2}\ , \tag{64}$$

and the bound for ν_σ thus follows. □

Corollary 4.12. *Let $\gamma = \epsilon^2 N(st)^2$, and assume $t^2 s^4 \gamma < 1/4$, then it holds that*

$$\sum_{\mathsf{p}:|\mathsf{cv}|>0} \|\nu_{\mathsf{p}} A_{\mathsf{p}}\|_1 \le 2t^2 s^4 \gamma = 2t^4 s^6 \epsilon^2 N \tag{65}$$

Proof. We derive the bound in the following equation. We note that $|\mathsf{cv}|$ cannot be equal to 1 since for every outgoing edge from a block there needs to be an incoming edge. We also recall the notation of $\mathsf{p}_k = \{\mathsf{p} : |\mathsf{cv}| = k\}$, introduced in Lemma 4.10 (namely, p_k is a set whose elements are congruence classes p).

$$\sum_{\mathsf{p}:|\mathsf{cv}|>0} \|\nu_{\mathsf{p}} A_{\mathsf{p}}\|_1 = \sum_{k=2}^{st} \sum_{\mathsf{p}\in\mathsf{p}_k} |\nu_{\mathsf{p}}| \, \|A_{\mathsf{p}}\|_1 \tag{66}$$

$$\leq \sum_{k=2}^{st} \sum_{\mathsf{p}\in\mathsf{p}_k} \gamma^{k/2} t^k \qquad \text{Lemmas 4.11 and 4.9} \tag{67}$$

$$\leq \sum_{k=2}^{st} \gamma^{k/2} t^k s^{2k} \qquad \text{Lemma 4.10} \tag{68}$$

$$= \sum_{k=2}^{st} (ts^2\sqrt{\gamma})^k \tag{69}$$

$$\leq \frac{(ts^2\sqrt{\gamma})^2}{1 - ts^2\sqrt{\gamma}} \tag{70}$$

$$\leq 2t^2 s^4 \gamma \tag{71}$$

and the lemma follows. □

We can now prove lemma 4.5

Proof of lemma 4.5. Using the triangle inequality,

$$\|\rho - \rho_{\mathsf{uni}_{s,t}}\|_1 \leq \|\rho - \rho^\star\|_1 + \left\|\rho^\star - c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|=0} \nu_{\mathsf{p}} A_{\mathsf{p}}\right\|_1 + \left\|c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|=0} \nu_{\mathsf{p}} A_{\mathsf{p}} - \rho_{\mathsf{uni}_{s,t}}\right\|_1 . \tag{72}$$

We bound each term separately.

$$\|\rho^\star - c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|=0} \nu_{\mathsf{p}} A_{\mathsf{p}}\|_1 = \|c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|>0} \nu_{\mathsf{p}} A_{\mathsf{p}}\|_1 \tag{73}$$

$$\leq c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|>0} \|\nu_{\mathsf{p}} A_{\mathsf{p}}\|_1 \tag{74}$$

$$\leq c_1 \cdot 2t^2 s^4 \gamma \tag{75}$$

$$= c_1 \cdot 2\epsilon^2 N s^6 t^4 \tag{76}$$

We note that there is one congruence class with zero crossing, which contains the permutations $\sigma \in S_t^s$. Denote this congruence class by p_0, so $\sum_{\mathsf{p}:|\mathsf{cv}|=0} A_{\mathsf{p}} = A_{\mathsf{p}_0}$. Recall that

$$\rho_{\mathsf{uni}_{s,t}} = \frac{1}{N^{\underline{st}}} \sum_{\substack{z\in\mathcal{U}^\star_{n,st} \\ \sigma\in S_t^s}} |z\rangle\langle\sigma(z)| = \frac{1}{N^{\underline{st}}} A_{\mathsf{p}_0} \tag{77}$$

As $\mathrm{Tr}(\rho^\star) = 1$, we have

$$\left|1 - c_1 \cdot \nu_{\mathsf{p}_0} N^{\underline{st}}\right| = \left|1 - \mathrm{Tr}\left(c_1 \cdot \nu_{\mathsf{p}_0} A_{\mathsf{p}_0}\right)\right| \leq c_1 \cdot 2\epsilon^2 N s^6 t^4 \ . \tag{78}$$

It follows that

$$\frac{1 - c_1 \cdot 2\epsilon^2 N s^6 t^4}{c_1} \frac{1}{N^{\underline{st}}} \leq \nu_{\mathsf{p}_0} \leq \frac{1 + c_1 \cdot 2\epsilon^2 N s^6 t^4}{c_1} \frac{1}{N^{\underline{st}}} \tag{79}$$

and so,

$$\left\| c_1 \cdot \sum_{\mathsf{p}:|\mathsf{cv}|=0} \nu_{\mathsf{p}} A_{\mathsf{p}} - \rho_{\mathsf{uni}_{s,t}} \right\|_1 = \left\| c_1 \cdot \nu_{\mathsf{p}_0} A_{\mathsf{p}_0} - \frac{1}{N^{\underline{st}}} A_{\mathsf{p}_0} \right\|_1 \leq c_1 \cdot 2\epsilon^2 N s^6 t^4 \tag{80}$$

and it follows that

$$\|\rho^\star - \rho_{\mathsf{uni}_{s,t}}\|_1 \leq O(\epsilon^2 N s^6 t^4) \tag{81}$$

□

4.3 Proving the main lemma and theorem

We combine the results of sections 4.1 and 4.2 to prove the main lemma.

Proof of lemma 4.1. Let s, t be polynomials in n and let $\{|\psi^{(j)}\rangle\}_{j\in[s]}$ be orthogonal quantum states. From corollary 4.4, choosing $c = 8$ we get that $\forall_{j\in[s]} H^{\otimes n} U_f |\psi^{(j)}\rangle$ is $\frac{8n}{N}$-flat with probability at least $1 - s \cdot 2\exp\left(-\left(\frac{8}{4} - \ln(2)\right) n\right) \geq 1 - 2^{-n} = 1 - \frac{1}{N}$.

Assuming flatness of these states, we can now use lemma 4.5 and get that:

$$\left\| \mathop{\mathbb{E}}_{f,g,\pi} \left[{U_{f,g,\pi}}^{\otimes st} \left(\bigotimes_{j\in[s]} (|\psi^{(j)}\rangle\langle\psi^{(j)}|)^{\otimes t} \right) {U^\dagger_{f,g,\pi}}^{\otimes st} \right] - \rho_{\mathsf{uni}_{s,t}} \right\|_1 \leq O\left(\frac{(st)^2 8n}{N} + N s^6 t^4 \left(\frac{9n}{N}\right)^2 + \frac{1}{N} \right) \tag{82}$$

$$= O\left(\frac{s^6 t^4 n^2}{N}\right) \; . \tag{83}$$

□

We conclude with a proof for theorem 3.2.

Proof of theorem 3.2. Taking $Gen_n(k) = U_k$ to be $U_{F,G,P}$ (where k is split into keys for F, G and P), we get that it is indeed a QPT algorithm on n qubits. We now prove the security requirement.

Recall that ρ_{in} is promised to be of the form

$$\rho_{in} = \sum_{a\in A} p_a \left(\rho_a \otimes \left(\bigotimes_{j\in[s]} (|\psi^{(j,a)}\rangle\langle\psi^{(j,a)}|)^{\otimes t} \right) \right) \tag{84}$$

for orthogonal sets of states $\left\{|\psi^{(1,a)}\rangle, \ldots, |\psi^{(s,a)}\rangle\right\}$. Define the channel Φ to be $\Phi(\rho) = \mathbb{E}_{f,g,\pi}\left[\left(I_\ell \otimes {U_{f,g,\pi}}^{\otimes st}\right) \rho \left(I_\ell \otimes\right.\right.$
Performing Φ on ρ_{in} results in the state

$$\Phi(\rho_{in}) = \sum_{a\in A} p_a \left(\rho_a \otimes \mathop{\mathbb{E}}_{f,g,\pi} \left[{U_{f,g,\pi}}^{\otimes st} \left(\bigotimes_{j\in[s]} (|\psi^{(j,a)}\rangle\langle\psi^{(j,a)}|)^{\otimes t} \right) {U^\dagger_{f,g,\pi}}^{\otimes st} \right] \right) \; . \tag{85}$$

By lemma 4.1 and the fact that $\sum_{a\in A} p_a = 1$ we get that

$$\left\|\Phi(\rho_{in}) - \sum_{a\in A} p_a(\rho_a \otimes \rho_{\mathsf{uni}_{s,t}})\right\|_1 \le O\left(\frac{s^6t^4n^2}{N}\right) . \tag{86}$$

Together with lemma 2.6, we get by the triangle inequality that $\Phi(\rho_{in})$ is an $O(s^6t^4n^2/N + s^2t^2/N) = O(s^6t^4n^2/N)$ almost invariant state. Using claim 2.5 we get

$$\mathrm{TD}\left(\Phi(\rho_{in}), \mathop{\mathbb{E}}_{U\leftarrow Haar_n}\left[(I_\ell \otimes U^{\otimes st})\rho_{in}(I_\ell \otimes (U^\dagger)^{\otimes st})\right]\right) \le O(s^6t^4n^2/N) . \tag{87}$$

By claim 3.3 we have

$$\begin{aligned}\Bigg|\Pr_k\left[\mathcal{A}\left(\left(I_\ell \otimes U_{F,G,P}{}^{\otimes st}\right)\rho_{in}\left(I_\ell \otimes U^\dagger_{F,G,P}{}^{\otimes st}\right)\right) = 1\right]& \\ - \Pr_{f,g,\pi}\left[\mathcal{A}\left(\left(I_\ell \otimes U_{f,g,\pi}{}^{\otimes st}\right)\rho_{in}\left(I_\ell \otimes U^\dagger_{f,g,\pi}{}^{\otimes st}\right)\right) = 1\right]\Bigg| &\le \mathrm{negl}(n) .\end{aligned} \tag{88}$$

We finish by combining equations 88 and 87 to get

$$\begin{aligned}\Bigg|\Pr_k\left[\mathcal{A}\left(\left(I_\ell \otimes U_{F,G,P}{}^{\otimes st}\right)\rho_{in}\left(I_\ell \otimes U^\dagger_{F,G,P}{}^{\otimes st}\right)\right) = 1\right]& \\ - \Pr_{U\leftarrow Haar_n}\left[\mathcal{A}\left((I_\ell \otimes U^{\otimes st})\rho_{in}(I_\ell \otimes U^{\dagger\otimes st})\right) = 1\right]\Bigg| &\le \mathrm{negl}(n) + O(s^6t^4n^2/N) = \mathrm{negl}(n) ,\end{aligned} \tag{89}$$

as needed to satisfy the security definition 3.1.

□

References

[AGKL23] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. *arXiv preprint arXiv:2311.02901*, 2023.

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In *Proceedings of the Theory of Cryptography Conference (TCC)*, pages 237–265. Springer, 2022.

[AMR20] Gorjan Alagic, Christian Majenz, and Alexander Russell. Efficient simulation of random states and random unitaries. In *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III 39*, pages 759–787. Springer, 2020.

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. Pseudorandomness with proof of destruction and applications. *Cryptology ePrint Archive*, 2023.

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. In *Proceedings of the 14th Innovations in Theoretical Computer Science Conference (ITCS)*, 2023.

[BS19] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Proceedings of the Theory of Cryptography Conference (TCC)*, pages 229–250. Springer, 2019.

[BS20] Zvika Brakerski and Omri Shmueli. Scalable pseudorandom quantum states. In *Proceedings of the 40th Annual International Cryptology Conference (CRYPTO)*, pages 417–440. Springer, 2020.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

[GTB23] Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states. *arXiv preprint arXiv:2312.09206*, 2023.

[HBK23] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. Pseudorandom unitaries are neither real nor sparse nor noise-robust. *arXiv preprint arXiv:2306.11677*, 2023.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Proceedings of the 38th Annual International Cryptology Conference (CRYPTO)*, pages 126–152. Springer, 2018.

[JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Subset states and pseudorandom states. *arXiv preprint arXiv:2312.15285*, 2023.

[LQS$^+$23] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. *arXiv preprint arXiv:2309.08941*, 2023.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Pseudorandom unitaries with non-adaptive security. *arXiv preprint arXiv:2402.14803*, 2024.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *Proceedings of the IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 679–687. IEEE, 2012.

[Zha16] Mark Zhandry. A note on quantum-secure prps. *arXiv preprint arXiv:1611.05564*, 2016.