Pseudorandom Function-like States from Common Haar Unitary

Minki Hhan*[1] and Shogo Yamada[2]

[1]The University of Texas at Austin, Texas, USA
minki.hhan@austin.utexas.edu
[2]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
shogo.yamada@yukawa.kyoto-u.ac.jp

Abstract

Recent active studies have demonstrated that cryptography without one-way functions (OWFs) could be possible in the quantum world. Many fundamental primitives that are natural quantum analogs of OWFs or pseudorandom generators (PRGs) have been introduced, and their mutual relations and applications have been studied. Among them, pseudorandom function-like state generators (PRFSGs) [Ananth, Qian, and Yuen, Crypto 2022] are one of the most important primitives. PRFSGs are a natural quantum analogue of pseudorandom functions (PRFs), and imply many applications such as IND-CPA secret-key encryption (SKE) and EUF-CMA message authentication code (MAC). However, only known constructions of (many-query-secure) PRFSGs are ones from OWFs or pseudorandom unitaries (PRUs).

In this paper, we construct classically-accessible adaptive secure PRFSGs in the invertible quantum Haar random oracle (QHRO) model which is introduced in [Chen and Movassagh, Quantum]. The invertible QHRO model is an idealized model where any party can access a public single Haar random unitary and its inverse, which can be considered as a quantum analog of the random oracle model. Our PRFSG constructions resemble the classical Even-Mansour encryption based on a single permutation, and are secure against any unbounded polynomial number of queries to the oracle and construction. To our knowledge, this is the first application in the invertible QHRO model without any assumption or conjecture. The previous best construction in the idealized model is PRFSGs secure up to $o(\lambda/\log\lambda)$ queries in the common Haar state model [Ananth, Gulati, and Lin, TCC 2024].

We develop new techniques on Haar random unitaries to prove the selective and adaptive security of our PRFSGs. For selective security, we introduce a new formula, which we call the Haar twirl approximation formula. For adaptive security, we show the unitary reprogramming lemma and the unitary resampling lemma. These have their own interest, and may have many further applications. In particular, by using the approximation formula, we give an alternative proof of the non-adaptive security of the PFC ensemble [Metger, Poremba, Sinha, and Yuen, FOCS 2024] as an additional result.

Finally, we prove that our construction is not PRUs or quantum-accessible non-adaptive PRFSGs by presenting quantum polynomial time attacks. Our attack is based on generalizing the hidden subgroup problem where the relevant function outputs quantum states.

*This work was done in part while the first author was in KIAS, Korea.

Contents

1 Introduction

In classical cryptography, one-way functions (OWFs) are the minimal assumption [IL89], because many primitives, such as pseudorandom generators (PRGs), pseudorandom functions (PRFs), secret-key encryption (SKE), message authentication code (MAC), digital signatures, and commitments, are all existentially equivalent to OWFs. Moreover, almost all primitives (including important applications such as public-key encryption and multiparty computations) imply OWFs.

In the quantum world, on the other hand, OWFs are not necessarily the minimum assumption [Kre21, MY22, AQY22]. Many fundamental primitives have been introduced such as pseudorandom unitaries (PRUs) [JLS18, MH24], pseudorandom function-like state generators (PRFSGs) [AQY22, AGQY22], pseudorandom state generators (PRSGs) [JLS18], one-way state generators (OWSGs) [MY22], one-way puzzles (OWPuzzs) [KT24], unpredictable state generators (UPSGs) [MYY24], and EFI pairs [BCQ23]. Although they are believed to be weaker than OWFs [Kre21, KQST23, LMW24], they still imply many useful applications such as private-key quantum money schemes [JLS18], SKE [AQY22], MAC [AQY22], digital signatures [MY22], commitments [MY22, AQY22], and multiparty computations [MY22, AQY22].

Among them, pseudorandom function-like state generators (PRFSGs) [AQY22, AGQY22] are one of the most important primitives. PRFSGs are a natural quantum analogue of pseudorandom functions (PRFs). A PRFSG is a quantum polynomial-time (QPT) algorithm G that takes a classical key k and a bit string x as input, and outputs a quantum state $|\phi_k(x)\rangle$. Roughly speaking, the security requires that no QPT adversary can distinguish whether it is querying to $G(k,\cdot)$ with a random k or an oracle that outputs Haar random states.[1] PRFSGs imply almost all known primitives such as UPSGs, PRSGs, OWSGs, OWPuzzs, and EFI pairs. PRFSGs also imply useful applications such as IND-CPA SKE, EUF-CMA MAC, private-key quantum money schemes, commitments, multi-party computations, (bounded-poly-time-secure) digital signatures, etc. However, all known constructions of (multi-query-secure) PRFSGs are ones from OWFs or PRUs [AQY22, AGQY22].

In classical cryptography, some idealized setups where parties can access some public source of randomness are often introduced, such as the common random string model [BFM19] or the random function or permutation oracle model [BR93, EM97]. These idealized setups reflect the reality of random source or hash functions and naturally provide the practical instantiations of basic cryptographic primitives, and they serve as a testbed for new analysis tools in classical and post-quantum settings [DKS12, ABKM22].

It is natural to consider their quantum counterparts: public sources of quantum states and unitaries. In fact, various quantum analogue of the setup models have already been introduced [CM24, DLS22, MY24, Qia24, CCS24, AGL24, BFV20], and several primitives have been constructed including commitments, PRSGs, and restricted-copy secure PRFSGs. In particular, [AGL24] recently constructed bounded-query PRFSGs in the common Haar state (CHS) model, which was shown to be optimal by the authors.

However, most previous works focus on the idealized model where the parties have access to the common *states*, except for [BFV20, CM24]. The idealized model for common unitaries must be much more useful than common states and perhaps connect the practical and heuristic constructions of quantum cryptographic objects and theory in the near future, as in the random oracle and ideal cipher models in the classical and post-quantum world. In particular, the limitation of the CHS model motivates the following question:

Are multi-copy secure PRFSGs achievable if a common random unitary is given?

[1] More precisely, the oracle works as follows. If it gets x as input and x was not queried before, it samples a Haar random state ψ_x and returns it. If x was queried before, it returns the same state ψ_x that was sampled before when x was queried for the first time.

1.1 Our Results

PRFSGs in the invertible QHRO Model. The main result of the present paper is a construction of classically-accessible adaptive secure PRFSGs in the invertible quantum Haar random oracle (QHRO) model which is a quantum analog of the random oracle model. In the invertible QHRO model, which is introduced in [CM24] and considered in [BFV20], any party can query the same Haar random unitaries $\mathcal{U} := \{U_\lambda\}_{\lambda\in\mathbb{N}}$ and their inverses $\mathcal{U}^\dagger := \{U_\lambda^\dagger\}_{\lambda\in\mathbb{N}}$, where U_λ is a λ-qubit Haar random unitary. [2]

Theorem 1.1 (Informal). *Classically-accessible adaptive secure PRFSGs exist in the invertible QHRO model.*

More precisely, given the common Haar unitaries $\mathcal{U}$, our construction of a PRFSG $G^{\mathcal{U}}(k,x) \to |\phi_k(x)\rangle$ is the following one: For any $x, k, k' \in \{0,1\}^\lambda$,

$$|\phi_k(x)\rangle := X^{k'} U_\lambda X^k |x\rangle, \tag{1}$$

where X^k applies Pauli X^{k_i} on ith qubit for each $i \in [\lambda]$. This XUX construction resembles the Even-Mansour encryption, the simplest encryption scheme based on a single permutation [EM97, DKS12].

Our PRFSG is classically-accessible adaptive secure. Roughly speaking, it means that, for each x, $|\phi_k(x)\rangle$ looks like an independent Haar random state even given access to $\mathcal{U}$ and $\mathcal{U}^\dagger$. The precise meaning is as follows: let $\mathcal{A}^{(\cdot,\cdot,\cdot)}$ be an *unbounded* adversary such that

- $\mathcal{A}^{(\cdot,\cdot,\cdot)}$ can query the first oracle only classically but adaptively at most $\mathrm{poly}(\lambda)$ times.
- $\mathcal{A}^{(\cdot,\cdot,\cdot)}$ can query the second and third oracle quantumly and adaptively at most $\mathrm{poly}(\lambda)$ times.

Then, for any such $\mathcal{A}^{(\cdot,\cdot,\cdot)}$,

$$\left| \Pr_{\mathcal{U}\leftarrow\mu, k\leftarrow\{0,1\}^\lambda}[1 \leftarrow \mathcal{A}^{\mathcal{O}^{\mathcal{U}}_{\mathrm{PRFS}}(k,\cdot),\mathcal{U},\mathcal{U}^\dagger}] - \Pr_{\mathcal{U}\leftarrow\mu,\mathcal{O}_{\mathrm{Haar}}}[1 \leftarrow \mathcal{A}^{\mathcal{O}_{\mathrm{Haar}}(k,\cdot),\mathcal{U},\mathcal{U}^\dagger}] \right| \leq \mathsf{negl}(\lambda), \tag{2}$$

where $\mathcal{U} = \{U_\lambda\}_{\lambda\in\mathbb{N}} \leftarrow \mu$ means that, for each natural number λ, U_λ is sampled from the Haar measure over λ-qubit unitary group. Here, $\mathcal{O}^{\mathcal{U}}_{\mathrm{PRFS}}$ and $\mathcal{O}_{\mathrm{Haar}}$ are defined as follows:

- $\mathcal{O}^{\mathcal{U}}_{\mathrm{PRFS}}(k,\cdot)$: It takes $x \in \{0,1\}^\lambda$ as input and outputs $G^{\mathcal{U}}(k,x) = |\phi_k(x)\rangle$.
- $\mathcal{O}_{\mathrm{Haar}}(\cdot)$: It takes $x \in \{0,1\}^\lambda$ as input and outputs $|\psi_x\rangle$, where $|\psi_x\rangle$ is sampled from the Haar measure over all λ-qubit pure states for each $x \in \{0,1\}^\lambda$.

PRSGs in the invertible QHRO Model. As in the plain model, PRFSGs trivially imply PRSGs in the invertible QHRO model. As an cororally of Theorem 1.1, we also have the following result:

Theorem 1.2 (Informal). *PRSGs exist in the invertible QHRO model.*

The construction is the trivial one, namely, $G^{\mathcal{U}}(k)$ outputs $|\phi_k\rangle := U_\lambda|k\rangle$, where $k \in \{0,1\}^\lambda$. The security means that for any polynomial t, $|\phi_k\rangle^{\otimes t}$ is statistically indistinguishable even given access to $\mathcal{U}$ and $\mathcal{U}^\dagger$.

The only known previous construction of PRSGs in the invertible QHRO model [BFV20] is more complicated and requires high query depth to the common unitary. Namely, their construction has to query a common Haar unitary U_λ $\mathrm{poly}(\lambda)$ times. On the other hand, our construction queries a common Haar unitary U_λ only at once, which is simpler construction than [BFV20].

[2] In [CM24, BFV20], they consider that anyone has access to λ-qubit unitary U_λ and its inverse for specific λ. On the other hand, in this work, we consider that any party has access to Haar random unitaries $\{U_\lambda\}_\lambda$ and their inverses, where U_λ is λ-qubit Haar random unitary for each $\lambda \in \mathbb{N}$.

Our PRFSG is not quantum-accessible secure (and therefore not PRUs). We complement this result by proving that our XUX construction is *not* secure quantum-accessible PRFSGs, even non-adaptively and without accessing inverse Haar unitary oracles. In particular, this implies that the construction is not PRUs. Concretely, our attack learns the secret keys in polynomial time[3] given non-adaptive access to U_λ and $U_\lambda P$ using a variant of Simon's algorithm [Sim96] for quantum states, inspired by the quantum attack on the Even-Mansour encryption [KM12].

We also prove that a similar attack can break UP, a naturally strengthened variant of UX, but using random Pauli P instead of random X. We believe a similar attack breaks the quantum-accessible security of the PUP construction.

Haar Twirl Approximation Formula. To show a special case of Theorem 1.1, we introduce a new formula, which we call *Haar twirl approximation formula*, which is our technical contribution. The formula is written as follows:[4]

Lemma 1.3. *Let $k, d \in \mathbb{N}$ such that $d > \sqrt{6}k^{7/4}$. Define S_k to be the set of all permutations over k elements. Let $\mathbf{A}$ be a d^k-dimentional register, and $\mathbf{B}$ be any register. Then, for any quantum state ρ on the registers $\mathbf{AB}$,*

$$\left\| (\mathcal{M}^{(k)}_{Haar,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}}[(R_{\sigma,\mathbf{A}} \otimes I_{\mathbf{B}})\rho_{\mathbf{AB}}] \right\|_1 \leq O\left(\frac{k^2}{d}\right), \tag{3}$$

where $\mathcal{M}^{(k)}_{Haar}(\cdot) := \mathbb{E}_{U \leftarrow \mu_d} U^{\otimes k}(\cdot) U^{\dagger \otimes k}$, μ_d is the Haar measure over d-dimensional unitaries, and R_π is the permutation unitary that acts $R_\pi |x_1, ..., x_k\rangle = |x_{\pi^{-1}(1)}, ..., x_{\pi^{-1}(k)}\rangle$ for all $x_1, ..., x_k \in [d]$ for each $\pi \in S_k$.

We show Lemma 1.3 based on Weingarten calculus [CŚ06]. However, for applications, we do not need any complicated facts about Wingarden calculus and Haar measure because Lemma 1.3 is stated based on only permutation unitaries.

Alternative Proof of [MPSY24]. The above formula should be of independent interest, and will have many other applications. In fact, by using the formula, we show alternative proof of the non-adaptive security of PFC emsemble [MPSY24]. In their proof, they used the Schur-Weyl duality, but our Lemma 1.3 is based on the Weingarten calculus [CŚ06]. This new approach will be useful in other applications.

Unitary reprogramming and resampling lemma. To prove Theorem 1.1 with the adaptive security, we follow the post-quantum security proof of the Even-Mansour encryption [ABKM22]. Along the way, we develop the unitary variants of their main lemmas, the (arbitrary) reprogramming lemma and resampling lemma. The unitary (arbitrary) reprogramming lemma can be understood as an adaptive version of the generalization of the lower bound of Grover's search [AMRS20], which was used in various applications including the post-quantum security of MAC. The unitary resampling lemma can be thought of as a unitary variant (and generalization) of the adaptive reprogramming lemma [GHHM21], which was widely used in e.g., Fiat-Shamir signature and transform [KLS18, SXY18] or in some of the first quantum applications of random oracles [Unr14a, Unr14b, ES15]. We believe the unitary variant presented in this paper must have further applications in quantum cryptography.

[3]A concurrent paper [ABGL24] proves that a single depth is insufficient to construct PRUs inspired by [CCS24]. However, their attack is information-theoretic, thus two results are incomparable.

[4][MPSY24] implicitly showed a similar result, but our formula is simpler. Moreover, our formula is true for any state ρ, while their result holds only for specific states ρ on the distinct subspace.

1.2 Related work

Comparison with PRFSGs in the CHS Model. A recent work [AGL24] constructed bounded-copy PRFSGs in the CHS model. Compared with their PRFSGs, our PRFSGs have an important advantage in that the number of queries allowed for the adversary is not limited: it is an unbounded polynomial time. PRFSGs in the CHS model [AGL24] allows only $o(\lambda/\log\lambda)$ number of copies, and it was shown to be optimal. Our result overcomes the barrier by considering the invertible QHRO model.

Comparison with previous works about invertible QHRO model. As mentioned, the invertible QHRO model was considered in [CM24, BFV20]. In [CM24], they conjectured the Gap-Local-Hamiltonian problem has a succinct argument in the invertible QHRO model. In [BFV20], they provide an idea of how to construct PRSGs and a security proof sketch in the invertible QHRO model based on some (unproven but very plausible) claim that might be proven through the Weingarten calculus. We give formal security proof of PRFSGs without any conjectures. Moreover, our result immediately implies the existence of PRSGs in the invertible QHRO model, which supersedes [BFV20].

Comparison with the concurrent work [ABGL24]. Ananth, Bostanci, Gulati and Lin independently and concurrently show similar results in [ABGL24]. They consider the inverseless QHRO model in which an adversary can query common Haar random unitary but cannot query its inverse, and construct PRUs, classically-accessible adaptive secure PRFSGs, and PRSGs in the inverseless QHRO model. The strength of their result is to construct PRUs. They also prove that the query depth 1 construction cannot be information-theoretic secure PRUs by suggesting the polynomial query attack. We do not construct PRUs, but our classically-accessible adaptive PRFSGs are secure even if an adversary has access to not only the common Haar random unitary but also its inverse.

The state hidden subgroup problem We consider a variant of hidden subgroup problems when breaking the quantum-accessible security. Two concurrent works [BGTW24, MZ24] observe and use the quantum state version of the hidden subgroup problem in different contexts.

1.3 Open Problems

- Can we construct quantumly-accessible adaptive secure PRFSGs in the invertible QHRO model?
- Can we construct PRUs and strong PRUs [MH24][5] in the invertible QHRO model? As mentioned, the recent concurrent work [ABGL24] shows that (inverseless) PRUs in the inverseless QHRO model. However, their construction is broken when the inverse queries are allowed using the attack presented in the same paper for the single query construction. Concretely, is $XUXUX$ strong PRUs? This candidate deviates from the known impossibility.
- For the XUX construction, can we use the same key for two X operators? Or, can we prove stronger security of the construction, e.g., secure PRUs with pure state inputs?
- Can we find further applications of the new techniques presented in this paper? Our tools are quite different from the tools used in the recent studies of the random unitaries; the Schur-Weyl duality

[5]Strong PRUs are efficiently implementable unitaries which are computationally indistinguishable from Haar random unitaries even given access to them and their inverses.

[MPSY24] or the path-recording technique [BHHP24, ABGL24] developed in [MH24]. The Haar Twirl approximation formula may be useful in the application of PRUs. The classical counterparts or relatives of the unitary reprogramming and resampling lemmas are one of the main tools in the post-quantum security analysis.

1.4 Technical Overviews

Our construction uses only single U_λ. Since each U_λ is sampled independently, it suffices to consider the case an adversary queries the same U_λ. We write it just U for notational simplicity. For $k, x \in \{0,1\}^\lambda$, we construct PRFSGs $|\phi_{k,k'}(x)\rangle$ as

$$|\phi_k(x)\rangle := UX^k |x\rangle \text{ or } X^{k'}UX^k |x\rangle, \tag{4}$$

where X^k is the λ-qubit Pauli operator defined by $\bigotimes_i X^{k_i}$. Here X^{k_i} acts on ith qubit. We show non-adaptive security for $UX^k|x\rangle$ and adaptive security for $X^{k'}UX^k|x\rangle$ based on independent techniques, which we will explain below.

1.4.1 Non-Adaptive Security

First, let us consider when an adversary can query U only non-adaptively. This precisely means that for any *unbounded* adversary $\mathcal{A}$, any polynomial t, and any bit strings $x_1, ..., x_{\ell(\lambda)} \in \{0,1\}^\lambda$ with any polynomial ℓ, $\Pr[\top \leftarrow \mathcal{C}] \leq 1/2 + \mathsf{negl}(\lambda)$ in the following security game.

1. $\mathcal{A}$ can apply U on its state. Note that n_i can be equal to n_j for any $i \neq j$.
2. $\mathcal{C}$ samples $b \leftarrow \{0,1\}$. If $b = 0$, $\mathcal{C}$ chooses $k \leftarrow \{0,1\}^\lambda$ and runs $|\phi_k(x_i)\rangle \leftarrow G^U(k, x_i)$ $t(\lambda)$ times for each $i \in [\ell(\lambda)]$. Then $\mathcal{C}$ sends $|\phi_k(x_1)\rangle^{\otimes t} \otimes ... \otimes |\phi_k(x_\ell)\rangle^{\otimes t}$ to $\mathcal{A}$. If $b = 1$, $\mathcal{C}$ sends $|\psi_1\rangle^{\otimes t} \otimes ... \otimes |\psi_\ell\rangle^{\otimes t}$ to $\mathcal{A}$, where $|\psi_i\rangle$ is a Haar random λ-qubit state for each $i \in [\ell(\lambda)]$.
3. $\mathcal{A}$ returns $b' \in \{0,1\}$. Note that $\mathcal{A}$ cannot query U after receiving the challenge state.
4. $\mathcal{C}$ outputs $\top$ if and only if $b = b'$.

As we can see in the above definition of the security game, the adversary $\mathcal{A}$ can query U *only before* it receives the challenge state.

Since our construction uses only single U, it suffices to claim that the trace norm between the following two states is at most negligible in λ for any polynomial t, ℓ, any bit strings $x_1, ..., x_\ell \in \{0,1\}^\lambda$, and any quantum state ρ:

$$\mathop{\mathbb{E}}_{\substack{U \leftarrow \mu_{2^\lambda}, \\ k \leftarrow \{0,1\}^\lambda}} \bigotimes_{i=1}^{\ell} (UX^k |x_i\rangle \langle x_i| X^{k\dagger} U^\dagger)_{\mathbf{A}}^{\otimes t} \otimes U_{\mathbf{B}}^{\otimes m} \rho_{\mathbf{BC}} U_{\mathbf{B}}^{\dagger \otimes m} \tag{5}$$

$$\bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle \leftarrow \mu_{2^\lambda}^s} |\psi_i\rangle \langle \psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{U \leftarrow \mu_{2^\lambda}} U_{\mathbf{B}}^{\otimes m} \rho_{\mathbf{BC}} U_{\mathbf{B}}^{\dagger \otimes m}. \tag{6}$$

Here μ_{2^λ} denotes the Haar measure over all λ-qubit unitary, and $\mu_{2^\lambda}^s$ denotes the Haar measure over all λ-qubit pure states.

The main challenge is to compare the above two states. One possible way is to calculate the expectation of the Haar random unitary U by invoking the Schur-Weyl duality as in [MPSY24]. However, this approach encounters challenges due to the limitations of Schur-Weyl duality in facilitating comparisons between different moments of the Haar measure. In our situation, a $(t\ell+m)$th moment of the Haar measure appears in Equation (5), but a mth moment of the Haar measure appears in Equation (6).

Solution: Approximation of the Haar Twirl. In order to overcome this challenge, we show and invoke the following approximation formula for the Haar twirl as we state it in Lemma 1.3: for any quantum state ρ,

$$\left\| (\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}}) - \sum_{\sigma\in S_k} \frac{1}{d^k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}}[(R_{\sigma,\mathbf{A}} \otimes I_{\mathbf{B}})\rho_{\mathbf{AB}}] \right\|_1 \leq O\left(\frac{k^2}{d}\right), \tag{7}$$

where $\mathcal{M}^{(k)}_{\mathrm{Haar}}(\cdot) \coloneqq \mathbb{E}_{U\leftarrow\mu_d} U^{\otimes k}(\cdot)U^{\dagger\otimes k}$, μ_d is the d-dimensional Haar measure, and R_π is the unitary that acts $R_\pi |x_1,...,x_k\rangle = |x_{\pi^{-1}(1)},...,x_{\pi^{-1}(k)}\rangle$ for all $x_1,...,x_k \in [d]$ for each $\pi \in S_k$.

From Equation (7), the Haar twirl can be approximated as the summation of permutation unitary R_π. This helps us to compare Equation (5) with Equation (6). By Equation (7) and the property of random Pauli operator, we can show Equation (5) is statistically close to Equation (6).

1.4.2 Adaptive Security

The quantitative security of the PUP construction is as follows.

Theorem 1.4. *Suppose that $\mathcal{A}$ makes p classical queries to the PRFSG oracle and q queries to the (invertible) n-qubit Haar random unitary oracle U. Then it holds that*

$$\left| \Pr_{U\leftarrow\mu,(k,k')\leftarrow\{0,1\}^n}\left[\mathcal{A}^{X^{k'}UX^k,U} \to 1\right] - \Pr_{U\leftarrow\mu,W\leftarrow\mu}\left[\mathcal{A}^{W,U}\to 1\right]\right| = O\left(\sqrt{\frac{p^3+p^2q^2}{2^n}}\right). \tag{8}$$

The proof of the above theorem closely resembles the *post-quantum* security proof of the Even-Mansour cipher [ABKM22], which uses the standard hybrid arguments by changing the oracles. To this end, we develop the following resampling and reprogramming lemmas for the unitary oracles.

Lemma 1.5 (Unitary reprogramming lemma, informal). *Consider the following experiment:*

Phase 1: *$\mathcal{D}$ outputs a unitary $F_0 = F$ over m-qubit, and a quantum algorithm $\mathcal{C}$ that decides how to reprogram F.*

Phase 2: *$\mathcal{C}$ is executed and reprogram F on the subspace S and outputs the reprogrammed unitary F'. A random $b \in \{0,1\}$ is chosen and $\mathcal{D}$ receives oracle access (with only forward queries) to F (if $b=0$) or F' (if $b=1$).*

Phase 3: *$\mathcal{D}$ loses access to the oracle access, and is noticed how F is reprogrammed, and outputs a bit b'.*

Then, it holds that $|\Pr[\mathcal{D}\to 1|b=1] - \Pr[\mathcal{D}\to 1|b=0]| \leq q\cdot\sqrt{2\epsilon}$, where ϵ is the maximum overlap of any quantum state and the reprogrammed space.

Lemma 1.6 (Unitary resampling lemma, informal). *Consider the following experiment:*

Phase 1: *$\mathcal{D}$ specifies two distributions of quantum states D_0, D_1. $\mathcal{D}$ makes q forward or inverse queries to a m-dimensional Haar random unitary U.*

Phase 2: *A random $b \in \{0,1\}$ is chosen, and $\mathcal{D}$ makes an arbitrary many queries to U (if $b = 0$) or U' (if $b = 1$) where U' is defined by $U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$ for $|\mu_0\rangle \leftarrow D_0, |\mu_1\rangle \leftarrow D_1$.*[6]

Then, the following holds:$|\Pr[b' = 1|b = 0] - \Pr[b' = 1|b = 1]| \leq 2\sqrt{\frac{6q}{2^m}}$ *given that D_0, D_1 satisfy some uniformity conditions.*

We write $X^{k'}UX^k =: V_k^U$ for simplicity. The real-world experiment where the algorithm is given oracle access to V_k^U, U can be denoted by $\mathbf{H}_0$ below:

$$\mathbf{H}_0 : U, V_k^U, U, V_k^U, U, ... \tag{9}$$

where each U may include multiple forward and inverse queries to the unitary U, and V_k^U denotes a single classical-query to the PRFSG oracle $V_k^U = X^{k'}UX^k$.

We consider the following hybrid experiments, which are close because of the unitary resampling lemma:

$$\mathbf{H}_0 : \underbrace{U}_{\textbf{Phase 1}}, \underbrace{V_k^U, U, V_k^U, U, ...}_{\textbf{Phase 2}} \tag{10}$$

$$\mathbf{H}_0' : \underbrace{U}_{\textbf{Phase 1}}, \underbrace{V_k^{U'}, U', V_k^{U'}, U', ...}_{\textbf{Phase 2}} \tag{11}$$

where in $\mathbf{H_0}'$, we *resample* the random unitary U into U' so that $V_k^{U'}$ maps the first query to almost random state. More concretely, for the first query x_1, we define the distribution D_0 samples $x_1 \oplus k$ for the random key k, and D_1 samples a random state. Then, it holds that

$$V_k^{U'} |x_1\rangle = X^{k'}U'X^k |x_1\rangle = X^{k'}U \circ \mathrm{SWAP}_{x_1 \oplus k, \mu} |x_1 \oplus k\rangle = X^{k'}U |\mu\rangle =: |\nu\rangle \tag{12}$$

for random state $|\mu\rangle$. In turn, the output state $|\nu\rangle$ also looks random.

We define W as a random unitary that maps $|x_1\rangle$ to $|\nu\rangle$. Then, with some calculations, we can prove that the hybrid experiment $\mathbf{H}_0'$ is close to the following hybrid:

$$\mathbf{H}_0'' : U, W, U', V_k^U, U', ... \tag{13}$$

Intuitively, the first query to the PRFSG oracle is identical, and the later steps may differ slightly due to the replacement of oracles. The actual proof requires multiple hybrid experiments in between.

Then, the unitary reprogramming lemma for $F = |0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U^\dagger$ proves the following two hybrids are close:

$$\mathbf{H}_0'' : \underbrace{U, W}_{\textbf{Phase 1}}, \underbrace{U'}_{\textbf{Phase 2}}, \underbrace{V_k^U, U', ...}_{\textbf{Phase 3}} \tag{14}$$

$$\mathbf{H}_1 : \underbrace{U, W}_{\textbf{Phase 1}}, \underbrace{U}_{\textbf{Phase 2}}, \underbrace{V_k^U, U', ...}_{\textbf{Phase 3}} \tag{15}$$

$$\tag{16}$$

[6] $\mathrm{SWAP}_{x,y}$ maps $\alpha |x\rangle + \beta |y\rangle \mapsto \alpha |y\rangle + \beta |y\rangle$ in the span of $\{|x\rangle, |y\rangle\}$.

then the proof continues to reach

$$\mathbf{H}_p : U, W, U, W, U, ... \tag{17}$$

that corresponds to the ideal-world experiment. By the standard hybrid argument, we conclude that $\mathbf{H}_0$ and $\mathbf{H}_p$ are close, i.e., the p-query algorithm cannot distinguish the oracle $X^{k'}UX^k$ and W with a high probability.

Simulation of Unitary Oracles. A careful reader may notice (multiple) problems in the above arguments. In particular, if the adversary queries the same input x to the PRFSG oracle twice, some intermediate hybrid answers them using one by V_k^U and the other by W. Another subtle problem is that reprogramming and resampling may require the knowledge of some pure quantum states related to the oracle input/outputs.

We detour these problems by considering a *stronger* oracle algorithm. When an oracle W is always queried by classical inputs by A, we consider the simulation oracle $\mathsf{Sim}(W)$ and corresponding the simulation algorithm $\mathsf{Sim}(A)$ that work roughly as follows:

- When A makes the classical input query x to W and obtain a pure state $|\phi_x\rangle = W|x\rangle$, $\mathsf{Sim}(A)$ queries x to $\mathsf{Sim}(W)$ and obtains a perfect classical description of $|\phi_x\rangle$ as an answer. Then it constructs $|\phi_x\rangle$ by itself and proceeds as A. If the same query x is made by A later, $\mathsf{Sim}(A)$ does not make any query and constructs $|\phi_x\rangle$ by itself again. The other behavior of $\mathsf{Sim}(A)$ is identical to A.

Note that even if the oracle W is changed during the experiment, $\mathsf{Sim}(A)$ does the same behavior. Therefore, even if the oracle is replaced in the middle, the same input to the oracle is answered by the same output state.

By simulating the PRFSG oracles, we can extract the query information of the PRFSG oracles, thereby reprogramming and resampling relevant spaces without affecting the algorithm's success probability. This resolves the subtle problems mentioned above and completes the security proof.

2 Preliminaries

2.1 Basic Notations

This paper uses the standard notations of quantum computing and cryptography. We use λ as the security parameter. $[n]$ means the set $\{1, 2, ..., n\}$. For any set S, $x \leftarrow S$ means that an element x is sampled uniformly at random from the set S. We write negl as a negligible function and poly as a polynomial. QPT stands for quantum polynomial-time. For an algorithm A, $y \leftarrow A(x)$ means that the algorithm A outputs y on input x.

The identity operator over d-dimensional space is denoted by I_d. When the dimension is clear from the context, we sometimes write I for simplicity. We use X, Y and Z as Pauli operators. For a bit string x, $X^x := \bigotimes_i X^{x^i}$. We use Y^y and Z^z similarly. The n-qubit Pauli group is defined as $\{X^x Z^z\}_{x,z\in\{0,1\}^n}$.

For a vector $|\psi\rangle$, we define its norm as $\| \, |\psi\rangle \, \| := \sqrt{\langle\psi|\psi\rangle}$. For two density matrices ρ and σ, the trace distance is defined as $\mathrm{TD}(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\mathrm{Tr}\left[\sqrt{(\rho-\sigma)^2}\right]$, where $\|\cdot\|_1$ is the trace norm. For any matrix A, we define the Frobenius norm $\|A\|_2$ as $\sqrt{\mathrm{Tr}[A^\dagger A]}$. For any matrix A, the operator norm $\|\cdot\|_\infty$ is defined as $\|A\|_\infty := \max_{|\psi\rangle} \sqrt{\langle\psi| A^\dagger A |\psi\rangle}$, where the maximization is taken over all pure state $|\psi\rangle$. id denotes the identity channel, i.e., $\mathrm{id}(\rho) = \rho$ for any state ρ. For two channels $\mathcal{E}$ and $\mathcal{F}$ that take d dimensional states, we say $\|\mathcal{E} - \mathcal{F}\|_\diamond := \max_{|\psi\rangle} \|(\mathrm{id} \otimes \mathcal{E})(|\psi\rangle\langle\psi|) - (\mathrm{id} \otimes \mathcal{F})(|\psi\rangle\langle\psi|)\|_1$ is the diamond norm between $\mathcal{E}$ and $\mathcal{F}$, where the maximization is taken over all d^2 dimensional pure states.

The set (or group) of d-dimensional unitary matrices and states are denoted by $\mathbb{U}(d)$ and $\mathbb{S}(d)$. μ_d and μ_d^s denotes the Haar measure over $\mathbb{U}(d)$ and $\mathbb{S}(d)$, respectively. S_k denotes the permutation group over k elements. For $\pi \in S_k$ and $\sigma \in S_\ell$, $(\pi, \sigma) \in S_{k+\ell}$ is the permutation that permutates the first k elements with respect to π and the last ℓ elemensts with respect to σ. For $\pi \in S_k$, we define $d^k \times d^k$ permutation unitary R_π that satisfies $R_\pi |x_1, ..., x_k\rangle = |x_{\pi^{-1}(1)}, ..., x_{\pi^{-1}(k)}\rangle$ for all $x_1, ..., x_k \in [d]$.

2.2 Haar twirl and Unitary Design

We define the Haar twirling map.

Definition 2.1. *Let $k, d \in \mathbb{N}$ and ν be a distribution over $\mathbb{U}(d)$. We define the k-wise twirl with respect to ν $\mathcal{M}_\nu^{(k)}$ as*

$$\mathcal{M}_\nu^{(k)}(\cdot) := \mathop{\mathbb{E}}_{U \leftarrow \nu} U^{\otimes k}(\cdot) U^{\dagger \otimes k}. \tag{18}$$

In particular, for the Haar measure μ_d over $\mathbb{U}(d)$, we call it the Haar k-wise twirl, and write it by $\mathcal{M}_{\text{Haar}}^{(k)}$

Definition 2.2 (Unitary k-Design [Mel24]). *Let $k, d \in \mathbb{N}$. We say that a distribution ν over $\mathbb{U}(d)$ is a unitary k-design if the action of the k-wise twirl is the same as that of the Haar k-wise twirl. Namely, for any d^k-dimensional state ρ,*

$$\mathcal{M}_\nu^{(k)}(\rho) = \mathcal{M}_{\text{Haar}}^{(k)}(\rho). \tag{19}$$

Note that an action on any unitary 1-design ν can be written

$$\mathcal{M}_\nu^{(1)} = \frac{I}{d} \tag{20}$$

since $\mathcal{M}_{\text{Haar}}^{(1)}(\rho) = \frac{I}{d}$ for any state ρ.

The following lemma follows from the straightforward calculation.

Lemma 2.3. *For any $n \in \mathbb{N}$, the uniform distribution over n-qubit Pauli group is unitary 1-design.*

2.3 Useful Lemmas

Theorem 2.4 (Theorem 5.17 in [Mec19]). *Let μ_N be the Haar measure over $\mathbb{U}(N)$. Given $N_1, \ldots, N_k \in \mathbb{N}$, let $X = \mathbb{U}(N_1) \times \cdots \times \mathbb{U}(N_k)$. Let $\mu = \mu_{N_1} \times \cdots \times \mu_{N_k}$ be the product of Haar measures on X. Suppose that $f : X \to \mathbb{R}$ is L-Lipschitz in the ℓ^2-sum of Frobenius norm, i.e., for any $U = (U_1, ..., U_k) \in X$ and $V = (V_1, ..., V_k) \in X$, we have $|f(U) - V(U)| \le L\sqrt{\sum_i \|U_i - V_i\|_2^2}$. Then for every $\delta > 0$,*

$$\Pr_{U \leftarrow \mu}\left[f(U) \ge \mathop{\mathbb{E}}_{V \leftarrow \mu}[f(V)] + \delta\right] \le \exp\left(-\frac{N\delta^2}{24L^2}\right), \tag{21}$$

where $N := \min\{N_1, \ldots, N_k\}$.

We use that the probability that an algorithm given access to U and its inverse $U^\dagger$ is a Lipschitz function concerning U. The case when an algorithm queries only U is shown in [Kre21]. Since the proof for the case when given access to U and $U^\dagger$ is the same, we have the following.

Lemma 2.5 ([Kre21]). *Let $\mathcal{A}^{U,U^\dagger}$ be a quantum algorithm that makes T queries to $U \in \mathbb{U}(N)$ and its inverse. Then, $f(U) = \Pr[1 \leftarrow \mathcal{A}^{U,U^\dagger}]$ is $2T$-Lipschitz in the Frobenius norm, i.e., $|f(U) - f(V)| \leq 2T\|U - V\|_2$ for all $U, V \in \mathbb{U}(N)$.*

Lemma 2.6 (Gentle Measurement Lemma [Win99, Wat18]). *Let ρ be a quantum state, and $0 \leq \epsilon \leq 1$. Let M be a matrix such that $0 \leq M \leq I$ and*

$$\mathrm{Tr}[M\rho] \geq 1 - \epsilon. \tag{22}$$

Then,

$$\left\| \rho - \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{Tr}[M\rho]} \right\|_1 \leq \sqrt{\epsilon}. \tag{23}$$

Lemma 2.7 (Quantum Union Bound [Gao15, OV22]). *Apply the two-outcome projective $(P_1, I - P_1), ..., (P_m, I - P_m)$ sequentially on ρ, and let ρ_m be the final state conditioned on the outcome $P_1, ..., P_m$ all occurring. Suppose that $\mathrm{Tr}[P_i\rho] \geq 1 - \epsilon_i$ for $i = 1, ..., m$, then, it holds that*

$$\|\rho - \rho_m\|_1 \leq \sqrt{\epsilon_1 + ... + \epsilon_m}. \tag{24}$$

We also use the following lemma.

Lemma 2.8. *Let A, B and C be square matrices of the same size such that 1: A is hermitian, 2: $AB = BA$, 3: B and C are positive. Then,*

$$|\mathrm{Tr}[ABC]| \leq \|A\|_\infty \mathrm{Tr}[BC]. \tag{25}$$

Proof of Lemma 2.8. Since $AB = BA$, A and B has the spectral decomposition with the same basis $\{|\psi_i\rangle\}_i$: $A = \sum_i a_i |\psi_i\rangle\langle\psi_i|$, $B = \sum_i b_i |\psi_i\rangle\langle\psi_i|$. Note that $b_i \geq 0$ for any i since B is positive. Therefore,

$$|\mathrm{Tr}[ABC]| = |\sum_i a_i b_i \langle\psi_i| C |\psi_i\rangle| \leq \sum_i |a_i| b_i \langle\psi_i| C |\psi_i\rangle \leq (\max_i |a_i|) \sum_i b_i \langle\psi_i| C |\psi_i\rangle = \|A\|_\infty \mathrm{Tr}[BC], \tag{26}$$

where, in the first inequality, we have used the triangle inequality and $b_i \langle\psi_i| C |\psi_i\rangle \geq 0$ since $b_i \geq 0$ and C is positive. ☐

The following two lemmas follow from the straightforward calculation.

Lemma 2.9. *For any Hermitian matrix A,*

$$\|A\|_1 = 2 \max_{M: 0 \leq M \leq I} \mathrm{Tr}[MA] - \mathrm{Tr}[A]. \tag{27}$$

Lemma 2.10. *Let $\mathbf{A}$ and $\mathbf{B}$ be registers such that the dimension of $\mathbf{B}$ is larger than that of $\mathbf{A}$. Then, for any unitary V on $\mathbf{A}$ and pure state $|\phi\rangle_{\mathbf{A},\mathbf{B}}$ over the registers $\mathbf{A}$ and $\mathbf{B}$, there exist a unitary W on $\mathbf{B}$ and a quantum state ξ on $\mathbf{B}$ such that*

$$\mathrm{Tr}_{\mathbf{A}}[(V_{\mathbf{A}} \otimes I_{\mathbf{B}}) |\phi\rangle\langle\phi|_{\mathbf{AB}}] = \sqrt{\xi}_{\mathbf{B}} W (V^\Gamma \otimes I) W^\dagger \sqrt{\xi}_{\mathbf{B}}, \tag{28}$$

where Γ denotes the transpose with respect to computational basis.

For $k,d\in\mathbb{N}$, define

$$\Pi_{\mathrm{sym}}^{(d,k)}\coloneqq\frac{1}{k!}\sum_{\sigma\in S_k}R_\sigma. \tag{29}$$

$\Pi_{\mathrm{sym}}^{(d,k)}$ satisfies the following which are well-known facts. For its detail, see [Har13, Mel24].

Lemma 2.11. *Let $k,d\in\mathbb{N}$. Then, $\Pi_{sym}^{(d,k)}$ is the projection. Moreover,*

$$\mathrm{Tr}\Pi_{sym}^{(d,k)}=\binom{d+k-1}{k} \tag{30}$$

and

$$\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mu_d^s}(|\psi\rangle\langle\psi|)^{\otimes\ell}=\frac{\Pi_{sym}^{(d,k)}}{\mathrm{Tr}\Pi_{sym}^{(d,k)}}, \tag{31}$$

where μ_d^s is the Haar measure over all d-dimensional states.

Lemma 2.12. *Let $k,d\in\mathbb{N}$. Then,*

$$\frac{1}{k!}\sum_{\sigma\in S_k}R_\sigma\otimes R_\sigma=\Pi_{sym}^{(d^2,k)}. \tag{32}$$

Proof of Lemma 2.12. Let $\mathbf{A}\coloneqq\mathbf{A}_1...\mathbf{A}_k$ and $\mathbf{B}\coloneqq\mathbf{B}_1...\mathbf{B}_k$, where $\mathbf{A}_i$ and $\mathbf{B}_i$ are d-dimensional registers for each $i\in[k]$. We define $\mathbf{C}_i\coloneqq\mathbf{A}_i\mathbf{B}_i$ for each $i\in[k]$ and $\mathbf{C}\coloneqq\mathbf{C}_1...\mathbf{C}_k$. Then, $R_{\sigma,\mathbf{A}}\otimes R_{\sigma,\mathbf{B}}=R_{\sigma,\mathbf{C}}$ for any $\sigma\in S_k$. Therefore Lemma 2.12 follows from Lemma 2.11. □

3 Definition of PRSGs and PRFSGs in QHRO Model

In this section, we introduce the quantum Haar random oracle (QHRO) model and define pseudorandom state generators (PRSGs) and pseudorandom function-like state generators (PRFSGs) in the QHRO model. In the QHRO model, any party is given oracle access to a family $\mathcal{U}=\{U_n\}_{n\in\mathbb{N}}$ of Haar random unitaries, where U_n is a Haar random unitary acting on n qubits. For simplicity, $U\leftarrow\mu$ denotes $U_\lambda\leftarrow\mu_{2^\lambda}$ for each $\lambda\in\mathbb{N}$.

We consider the following two different types of oracle accesses:

- Any party can query U but cannot query its inverse $U^\dagger\coloneqq\{U_n^\dagger\}_{n\in\mathbb{N}}$.
- Any party can query both U and $U^\dagger$.

We call the former the inverseless QHRO model, and the latter the invertible QHRO model.

3.1 PRSGs in the QHRO Model

The pseudorandom state generators in the plain model were defined in [JLS18]. Here we define PRSGs in the QHRO model as follows.

Definition 3.1 (Pseduorandom States Generators (PRSGs) in the QHRO Model). *We define that an algorithm $G^{(\cdot,\cdot)}$ is a pseudorandom state generator (PRSG) in the QHRO model if it satisfies the following:*

- *Efficient generation: Let $\lambda \in \mathbb{N}$ be the security parameter and $\mathcal{K}_\lambda$ be a key space over at most* $\mathrm{poly}(\lambda)$ *bits. $G^{\mathcal{U},\mathcal{U}^\dagger}$ is a QPT algorithm that takes a key $k \in \mathcal{K}_\lambda$ as input, and outputs a quantum state $|\phi_k\rangle$.*
- *Pseudorandomness in the invertible QHRO model: For any polynomial-query adversary $\mathcal{A}^{(\cdot,\cdot)}$, and any polynomial $t(\lambda)$, there exists a negligible function* negl *such that*

$$\left| \Pr_{\mathcal{U}\leftarrow\mu, k\leftarrow\mathcal{K}_\lambda}[1 \leftarrow \mathcal{A}^{\mathcal{U},\mathcal{U}^\dagger}(|\phi_k\rangle^{\otimes t})] - \Pr_{\mathcal{U}\leftarrow\mu, |\psi\rangle\leftarrow\mu^S_{2^\lambda}}[1 \leftarrow \mathcal{A}^{\mathcal{U},\mathcal{U}^\dagger}(|\psi\rangle^{\otimes t})] \right| \leq \mathsf{negl}(\lambda). \tag{33}$$

If both the generation algorithm G and the adversary $\mathcal{A}$ are only allowed to query $\mathcal{U}$ non-adaptively before receiving challenge states, we say it is PRSGs in the non-adaptive inverseless *QHRO model.*

3.2 PRFSGs in the QHRO Models

We give the definition of PRFSGs in the QHRO model and the invertible QHRO model. PRFSGs in the plain model were defined in [AQY22, AGQY22]. As a security, we can consider selective security, classically-accessible adaptive security, and quantumly-accessible adaptive security. In this work, we focus on selective security in the QHRO model and classically-accessible adaptive security in the invertible QHRO model.

Definition 3.2 (Slectively Secure Pseudorandom Function-like State Generators (PRFSGs) in the QHRO Model). *We define that an algorithm $G^{(\cdot,\cdot)}$ is a selectively secure pseudorandom function-like state generator (PRFSG) in the QHRO model if it satisfies the following:*

- *Efficient generation: Let $\lambda \in \mathbb{N}$ be the security parameter and $\mathcal{K}_\lambda$ be a key space at most* $\mathrm{poly}(\lambda)$ *bits. $G^{\mathcal{U},\mathcal{U}^\dagger}$ is a QPT algorithm that takes a key $k \in \mathcal{K}_\lambda$ and a bit string $x \in \{0,1\}^\lambda$ as input, and outputs a quantum state $|\phi_k(x)\rangle$.*
- *Selective security in the invertible QHRO model: For any unbounded adversary $\mathcal{A}$, any polynomial t, and any bit strings $x_1, ..., x_{\ell(\lambda)} \in \{0,1\}^\lambda$ with any polynomial ℓ,*

$$\left| \Pr_{\mathcal{U}\leftarrow\mu, k\leftarrow\mathcal{K}_\lambda}[1 \leftarrow \mathcal{A}^{\mathcal{U},\mathcal{U}^\dagger}(|\phi_k(x_1)\rangle^{\otimes t}, ..., |\phi_k(x_\ell)\rangle^{\otimes t})] \right. \tag{34}$$

$$\left. - \Pr_{\mathcal{U}\leftarrow\mu, |\psi_1\rangle,...,|\psi_\ell\rangle\leftarrow\mu^S_{2^\lambda}}[1 \leftarrow \mathcal{A}^{\mathcal{U},\mathcal{U}^\dagger}(|\psi_1\rangle^{\otimes t}, ..., |\psi_\ell\rangle^{\otimes t})] \right| \leq \mathsf{negl}(\lambda). \tag{35}$$

If both the generation algorithm G and the adversary $\mathcal{A}$ are only allowed to query $\mathcal{U}$ non-adaptively before receiving challenge states, we say it is PRFSGs in the *non-adaptive inverseless* QHRO model.

Definition 3.3 (Classically-accesible Adaptively Secure PRFSGs in the invertible QHRO Model). *Let $G^{(\cdot)}$ be a QPT algorithm that satisfies the efficient generation property in Definition 3.2. If it satisfies the following, we say it is a classically-accessible adaptive secure PRFSG in the invertible QHRO model.*

- *Classically-accessible adaptive security in the invertible QHRO model: For any unbounded adversary $\mathcal{A}^{(\cdot,\cdot,\cdot)}$ that queries each oracle at most* $\mathrm{poly}(\lambda)$ *and can query the first oracle only classically,*

$$\left| \Pr_{\mathcal{U}\leftarrow\mu, k\leftarrow\mathcal{K}_\lambda}[1 \leftarrow \mathcal{A}^{\mathcal{O}^{\mathcal{U},\mathcal{U}^\dagger}_{PRFS}(k,\cdot),\mathcal{U},\mathcal{U}^\dagger}] - \Pr_{\mathcal{U}\leftarrow\mu, \mathcal{O}_{Haar}}[1 \leftarrow \mathcal{A}^{\mathcal{O}_{Haar}(k,\cdot),\mathcal{U},\mathcal{U}^\dagger}] \right| \leq \mathsf{negl}(\lambda). \tag{36}$$

Here, $\mathcal{O}^{\mathcal{U},\mathcal{U}^\dagger}_{PRFS}$ and $\mathcal{O}_{Haar}$ are defined as follows:

- $\mathcal{O}^{\mathcal{U},\mathcal{U}^\dagger}_{PRFS}(k,\cdot)$: *It takes* $x\in\{0,1\}^\lambda$ *as input and outputs* $G^{\mathcal{U},\mathcal{U}^\dagger}(k,x)=|\phi_k(x)\rangle$.
- $\mathcal{O}_{Haar}(\cdot)$: *It takes* $x\in\{0,1\}^\lambda$ *as input and outputs* $|\psi_x\rangle$, *where* $|\psi_x\rangle\leftarrow\mu^S_{2^\lambda}$ *for each* $x\in\{0,1\}^\lambda$.

4 Haar Twirl Approximation Formula

In this section, we derive the Haar twirl approximation formula, Lemma 1.3, which plays a crucial role in proving the non-adaptive security of PRFSGs in the QHRO model. First, we intuitively explain why the approximation formula holds in Section 4.1. Next, we introduce the Weingarten matrix and the Weingarten function in Section 4.2, and give some lemmas of the Weingarten function in Section 4.3. Finally, we give a proof of the approximation formula in Section 4.4.

4.1 Intuition for Approximation Formula

Our goal of this section is to show the following approximation formula, which we call Haar twirl approximation formula: let ρ be a quantum state on the register $\mathbf{AB}$, where the dimension of $\mathbf{A}$ is d^k and $\mathbf{B}$ is some fixed register. Then, for the Haar twirl $\mathcal{M}^{(k)}_{\text{Haar}}(\cdot)=\mathbb{E}_{U\leftarrow\mu_d}U^{\otimes k}(\cdot)U^{\deg\otimes k}$ defined in Definition 2.1,

$$\left\|(\mathcal{M}^{(k)}_{\text{Haar},\mathbf{A}}\otimes\text{id}_{\mathbf{B}})(\rho_{\mathbf{AB}})-\sum_{\pi\in S_k}\frac{1}{d^k}R_{\pi,\mathbf{A}}\otimes\text{Tr}_{\mathbf{A}}[(R^\dagger_{\pi,\mathbf{A}}\otimes I_{\mathbf{B}})\rho_{\mathbf{AB}}]\right\|_1\le O\left(\frac{k^2}{d}\right),\tag{37}$$

where S_k is the set of all permutations over k elements, and R_π is the permutation unitary that acts $R_\pi|x_1,...,x_k\rangle=|x_{\pi^{-1}(1)},...,x_{\pi^{-1}(k)}\rangle$ for all $x_1,...,x_k\in[d]$.

Intuitively, the above formula is derived as follows; first, from Weingarten calculus [CŚ06],

$$(\mathcal{M}^{(k)}_{\text{Haar},\mathbf{A}}\otimes\text{id}_{\mathbf{B}})(\rho_{\mathbf{AB}})=\sum_{\sigma,\tau\in S_k}\text{Wg}(\tau\sigma^{-1};d)R^\dagger_{\sigma\mathbf{A}}\otimes\text{Tr}_{\mathbf{A}}[\rho_{\mathbf{AB}}(R_{\tau\mathbf{A}}\otimes I_{\mathbf{B}})],\tag{38}$$

where $\text{Wg}(\ \cdot\ ;d)$ is called the Weingarten function that maps an element of S_k to a real number.[7] We give its definition in Section 4.2. The Weingarten function has the following nice property[8];

$$\text{Wg}(\pi;d)\approx\begin{cases}d^{-k} & \text{if }\pi\text{ is the identity,}\\ O(d^{-k-1}) & \text{otherwise.}\end{cases}\tag{39}$$

Therefore, if we ignore all terms such that $\tau\neq\sigma$ in Equation (38), Equation (37) seems to hold. We show this formally in Section 4.4.

4.2 Weingerten Calculus

In this subsection, we review Weingarten calculus [CMN22].

We first introduce the Weingarten function as follows. Let us assume k and d are positive integers such that $k\le d$. Recall that S_k is the permutation group over k elements, and, for $\pi\in S_k$, R_π is $d^k\times d^k$ permutation unitary that satisfies $R_\pi|x_1,...,x_k\rangle=|x_{\pi^{-1}(1)},...,x_{\pi^{-1}(k)}\rangle$ for all $x_1,...,x_k\in[d]$. We define $k!\times k!$ matrix $G(d)$ whose matrix elements are specified by two permutations $\sigma,\tau\in S_k$ such that

$$G(d)_{\sigma,\tau}:=\text{Tr}[R_{\tau\sigma^{-1}}]=d^{k-|\tau\sigma^{-1}|}.\tag{40}$$

[7] Wg depends on k, but for simplicity we omit k here.

[8] For the case when π is the identity, see Lemma 4.6. For other cases, we do not use it explicitly but it is shown in [CM17].

Here, for $\pi \in S_k$, $|\pi|$ is defined by the minimum number of transpositions to represent π as a product of those transpositions. Note that $G(d)_{\sigma\pi,\tau\pi} = G(d)_{\sigma,\tau}$ for any $\pi, \sigma, \tau \in S_k$. Let $\mathrm{Wg}(d)$, which is called the Weingarten matrix, be a $k! \times k!$ matrix as the pseudo-inverse of $G(d)$. We define the Weingarten function $\mathrm{Wg}(\cdot; d) : S_k \to \mathbb{R}$ such that

$$\mathrm{Wg}(\sigma\tau^{-1}; d) := \mathrm{Wg}(d)_{\sigma,\tau}. \tag{41}$$

This is well-defined since $\mathrm{Wg}(d)_{\sigma,\tau} = \mathrm{Wg}(d)_{\sigma\pi,\tau\pi}$ for any $\pi, \sigma, \tau \in S_k$, where it follows from $G(d)_{\sigma\pi,\tau\pi} = G(d)_{\sigma,\tau}$.

Weingarten calculus is the following lemma:

Lemma 4.1 (Corollary 2.4 of [CŚ06]). *Let $k, d \in \mathbb{N}$. Let μ_d be the Haar measure over $\mathbb{U}(d)$ and S_k be the set of all permutations over $[k]$. Let $i := (i_1, ..., i_k), j := (j_1, ..., j_k), i' := (i'_1, ..., i'_k), j' := (j'_1, ..., j'_k) \in [d]^k$. Then,*

$$\mathop{\mathbb{E}}_{U \leftarrow \mu_d} U_{i_1 j_1} ... U_{i_k j_k} \overline{U}_{i'_1 j'_1} ... \overline{U}_{i'_k j'_k} = \sum_{\sigma,\tau \in S_k} \delta_{i,\sigma(i')} \delta_{j,\tau(j')} \mathrm{Wg}(\tau\sigma^{-1}; d), \tag{42}$$

where, for $\ell := (\ell_1, ..., \ell_k), \in [d]^k$ and $\pi \in S_k$, $\pi(\ell) := (\ell_{\pi(1)}, ..., \ell_{\pi(k)})$.

From Lemma 4.1 and the straightforward calculation, we have the following lemma.

Lemma 4.2. *Let $k, d \in \mathbb{N}$. Let $\mathbf{A}$ denote the d^k-dimensional register, and $\mathbf{B}$ denote any dimensional register. Let $M_{\mathbf{AB}}$ be a matrix. Then,*

$$(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(M_{\mathbf{AB}}) = \sum_{\sigma,\tau \in S_k} \mathrm{Wg}(\tau\sigma^{-1}; d) R^\dagger_{\sigma\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[M_{\mathbf{AB}}(R_{\tau\mathbf{A}} \otimes I_{\mathbf{B}})]. \tag{43}$$

Proof of Lemma 4.2. For any $d^k \times d^k$ matrix N, we have

$$\mathcal{M}^{(k)}_{\mathrm{Haar}}(N) = \sum_{\sigma,\tau \in S_k} \mathrm{Wg}(\tau\sigma^{-1}; d) \mathrm{Tr}[N R_\tau] R^\dagger_\sigma. \tag{44}$$

We give its proof later. From Equation (44),

$$(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(M_{\mathbf{AB}}) = \Big(I_{\mathbf{A}} \otimes \sum_i |i\rangle\langle i|_{\mathbf{B}}\Big)(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(M_{\mathbf{AB}})\Big(I_{\mathbf{A}} \otimes \sum_j |j\rangle\langle j|_{\mathbf{B}}\Big) \tag{45}$$

$$= \sum_{i,j} \mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}}(M^{(i,j)}_{\mathbf{A}}) \otimes |i\rangle\langle j|_{\mathbf{B}} \tag{46}$$

$$= \sum_{i,j} \sum_{\sigma,\tau \in S_k} \mathrm{Wg}(\tau\sigma^{-1}; d) \mathrm{Tr}[M^{(i,j)} R_\tau] R^\dagger_{\sigma\mathbf{A}} \otimes |i\rangle\langle j|_{\mathbf{B}} \tag{47}$$

$$= \sum_{\sigma,\tau \in S_k} \mathrm{Wg}(\tau\sigma^{-1}; d) R^\dagger_{\sigma\mathbf{A}} \otimes \Big(\sum_{i,j} \mathrm{Tr}[M^{(i,j)} R_\tau] |i\rangle\langle j|_{\mathbf{B}}\Big), \tag{48}$$

where $M^{(i,j)}_{\mathbf{A}} := (I_{\mathbf{A}} \otimes \langle i|_{\mathbf{B}}) M_{\mathbf{AB}} (I_{\mathbf{A}} \otimes |j\rangle_{\mathbf{B}})$. From the standard calculation, we have

$$\sum_{i,j} \mathrm{Tr}[M^{(i,j)} R_\tau] |i\rangle\langle j|_{\mathbf{B}} = \mathrm{Tr}_{\mathbf{A}'}[M_{\mathbf{AB}}(R_{\tau\mathbf{A}} \otimes I_{\mathbf{B}})]. \tag{49}$$

Thus, we have

$$(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}}\otimes \mathrm{id}_{\mathbf{B}})(M_{\mathbf{AB}})=\sum_{\sigma,\tau\in S_k}\mathrm{Wg}(\tau\sigma^{-1};d)R^{\dagger}_{\sigma\mathbf{A}}\otimes \mathrm{Tr}_{\mathbf{A}'}[M_{\mathbf{AB}}(R_{\tau\mathbf{A}}\otimes I_{\mathbf{B}})]. \tag{50}$$

To conclude the proof, we show Equation (44). From Lemma 4.1, we have

$$\begin{aligned}
\mathcal{M}^{(k)}_{\mathrm{Haar}}(N) &= \sum_{i,j\in[d]^k}\left(\mathcal{M}^{(k)}_{\mathrm{Haar}}(N)\right)_{i,j}|i\rangle\langle j| && (51)\\
&= \sum_{i,j,\ell,m\in[d]^k}\mathop{\mathbb{E}}_{U\leftarrow\mu_d}U_{i_1\ell_1}...U_{i_k\ell_k}N_{\ell,m}\overline{U}_{j_1m_1}...\overline{U}_{j_km_k}|i\rangle\langle j| && (52)\\
&= \sum_{i,j,\ell,m\in[d]^k}\sum_{\sigma,\tau\in S_k}N_{\ell,m}\delta_{i,\sigma(j)}\delta_{\ell,\tau(m)}\mathrm{Wg}(\tau\sigma^{-1};d)|i\rangle\langle j| && (53)\\
&= \sum_{\sigma,\tau\in S_k}\mathrm{Wg}(\tau\sigma^{-1};d)\left(\sum_{\ell,m\in[d]^k}N_{\ell,m}\delta_{\ell,\tau(m)}\right)\left(\sum_{i,j\in[d]^k}\delta_{i,\sigma(j)}|i\rangle\langle j|\right). && (54)
\end{aligned}$$

From the definition of R_σ,

$$\sum_{i,j\in[d]^k}\delta_{i,\sigma(j)}|i\rangle\langle j|=\sum_{j\in[d]^k}|\sigma(j)\rangle\langle j|=R^{\dagger}_{\sigma}. \tag{55}$$

On the other hand,

$$\sum_{\ell,m\in[d]^k}N_{\ell,m}\delta_{\ell,\tau(m)}=\sum_{\ell,m\in[d]^k}N_{\ell,m}(R_\tau)_{m,\ell}=\mathrm{Tr}[NR_\tau]. \tag{56}$$

From the above three equations, Equation (44) follows. □

4.3 Useful Lemmas of Weingarten Function

We use some properties of the Weingarten function. First, the following lemma follows from the fact that the Weingarten matrix is the pseudo-inverse of the Gram matrix.

Lemma 4.3. *Let $k,d\in\mathbb{N}$. Then, for any $\pi,\sigma\in S_k$, $\mathrm{Wg}(\pi;d)=\mathrm{Wg}(\pi^{-1};d)$ and $\mathrm{Wg}(\pi\sigma\pi^{-1};d)=\mathrm{Wg}(\sigma;d)$.*

Proof of Lemma 4.3. First, let us show the former. Since the Gram matrix is symmetric by its definition, the Weingartne matrix $\mathrm{Wg}(d)$ is also symmetric since it is the pseudoinverse of the Garm matrix. Thus, we have $\mathrm{Wg}(\pi;d)=\mathrm{Wg}(d)_{\pi,e}=\mathrm{Wg}(d)_{e,\pi}=\mathrm{Wg}(\pi^{-1};d)$.

Next, let us prove the latter. Since $\mathrm{Wg}(\sigma\tau^{-1};d)=\mathrm{Wg}(d)_{\sigma,\tau}$, it suffices to show $\mathrm{Wg}(d)_{\pi\sigma,\pi\tau}=\mathrm{Wg}(d)_{\sigma,\tau}$ for any $\pi,\sigma,\tau\in S_k$. For $\pi\in S_k$, let us define $k!\times k!$ matrix $\mathrm{Wg}^{(\pi)}(d)$ such that $\mathrm{Wg}^{(\pi)}(d)_{\sigma,\tau}:=\mathrm{Wg}(d)_{\pi\sigma,\pi\tau}$. Since $G(d)_{\pi\rho,\pi\tau}=d^{k-|\pi\rho\tau^{-1}\pi^{-1}|}=d^{k-|\sigma\tau^{-1}|}=G(d)_{\sigma,\tau}$, $\mathrm{Wg}^{(\pi)}(d)$ is also the pseudo-inverse of $G(d)$. From the uniqueness of the pseudo-inverse matrix, we have $\mathrm{Wg}^{(\pi)}(d)=\mathrm{Wg}(d)$ for any $\pi\in S_k$, which implies $\mathrm{Wg}(d)_{\pi\sigma,\pi\tau}=\mathrm{Wg}(d)_{\sigma,\tau}$ for any $\pi,\sigma,\tau\in S_k$. □

The following are lemmas about a summation of the Weingarten function. The first lemma is shown in section 3.1.1. of [CMS12].

Lemma 4.4 ([CMS12]).

$$\sum_{\pi \in S_k} \mathrm{Wg}(\pi; d) = \frac{1}{d(d+1)\cdots(d+k-1)}. \tag{57}$$

Lemma 4.5 (Lemma 6 in [ACQ22]).

$$\sum_{\pi \in S_k} |\mathrm{Wg}(\pi; d)| = \frac{1}{d(d-1)\cdots(d-k+1)}. \tag{58}$$

The following lemma is a corollary of Theorem 3.2 in [CM17].

Lemma 4.6 ([CM17]). *Let $k, d \in \mathbb{N}$ such that $d > \sqrt{6}k^{7/4}$. Then,*

$$\frac{1}{d^k}\left(1 - O\left(\frac{k}{d^2}\right)\right) \leq \mathrm{Wg}(e; d) \leq \frac{1}{d^k}\left(1 - O\left(\frac{k^{7/2}}{d^2}\right)\right). \tag{59}$$

4.4 Proof of Haar Twirl Approximation Formula

Now we are ready to prove the approximation formula.

Lemma 4.7. *Let $k, d \in \mathbb{N}$ such that $d > \sqrt{6}k^{7/4}$. Let $\mathbf{A}$ be a d^k-dimentional register, and $\mathbf{B}$ be some fixed register. Then, for any quantum state ρ on the registers $\mathbf{AB}$,*

$$\left\| (\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}}[(R_{\sigma,\mathbf{A}} \otimes I_{\mathbf{B}})\rho_{\mathbf{AB}}] \right\|_1 \leq O\left(\frac{k^2}{d}\right). \tag{60}$$

Proof of Lemma 4.7. From the concavity of 1-norm, it suffices to show the case when ρ is a pure state $|\psi\rangle\langle\psi|$. In the following, we often write $|\psi\rangle\langle\psi|$ just as ψ for the notational simplicity.

It is clear that both matrices are hermitian. Thus, from Lemma 2.9,

$$\left\| (\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] \right\|_1 \tag{61}$$

$$\begin{aligned} =&2 \max_{M: 0 \leq M \leq I} \mathrm{Tr}\left[M\left((\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] \right)\right] \\ &- \mathrm{Tr}\left[(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) - \sum_{\pi \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] \right]. \end{aligned} \tag{62}$$

Thus, it suffices to show that both the first term and the second term are at most $O(k^2/d)$.

Estimation of the first term in Equation (62). To show the first term is at most $O(k^2/d)$, we show

$$\left| \mathrm{Tr}\left[M_{\mathbf{AB}}\left((\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] \right)\right] \right| \leq O\left(\frac{k^2}{d}\right) \tag{63}$$

for any $0 \leq M \leq I$. Without loss of generality, we can assume the dimension of $\mathbf{B}$ is larger than that of $\mathbf{A}$. Otherwise, we add some register $\mathbf{C}$ such that the dimension of $\mathbf{BC}$ is larger than that of $\mathbf{A}$, and consider $M'_{\mathbf{ABC}} \coloneqq M_{\mathbf{AB}} \otimes I_{\mathbf{C}}$ and $|\psi'\rangle_{\mathbf{ABC}} \coloneqq |\psi\rangle_{\mathbf{AB}} |0...0\rangle_{\mathbf{C}}$. Thus, for any permutation $\sigma \in S_k$, there exists a quantum state ξ such that

$$\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] = \sqrt{\xi}_{\mathbf{B}} R^{\Gamma}_{\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}} = \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}} \tag{64}$$

from Lemma 2.10. Here, for simplicity, we write that $R_{\sigma,\mathbf{B}}$ is a unitary which acts as R_σ on the subregister of $\mathbf{B}$ whose dimension is the same as that of $\mathbf{A}$, and as the identity on the residual subregister of $\mathbf{B}$. By using this, we have

$$\sum_{\sigma \in S_k} \frac{1}{d^k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] = \sum_{\sigma \in S_k} \frac{1}{d^k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}}. \tag{65}$$

By combing Equation (64) and Lemma 4.2, the k-fold Haar twirl can be rewritten as follows;

$$\begin{aligned}
(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) &= \sum_{\sigma,\tau \in S_k} \mathrm{Wg}(\tau\sigma^{-1}; d) R^{\dagger}_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\tau,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] &(66)\\
&= \sum_{\sigma,\pi \in S_k} \mathrm{Wg}(\pi; d) R^{\dagger}_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\pi\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] &(67)\\
&= \sum_{\sigma,\pi \in S_k} \mathrm{Wg}(\pi; d) R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\pi\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}}, &(68)
\end{aligned}$$

where we replaced the summention of τ with π that satisfies $\tau = \pi\sigma$. Then, we have

$$\begin{aligned}
&\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\left((\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}}) - \sum_{\sigma \in S_k} \frac{1}{d^k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right)\right]\right| &(69)\\
=&\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\left(\left(\mathrm{Wg}(e; d) - \frac{1}{d^k}\right) \sum_{\sigma \in S_k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}} + \sum_{\substack{\sigma,\pi \in S_k,\\ \pi \neq e}} \mathrm{Wg}(\pi; d) R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\pi\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}}\right)\right]\right| &(70)\\
\leq&\left|\mathrm{Wg}(e; d) - \frac{1}{d^k}\right|\left|\mathrm{Tr}\left[M_{\mathbf{AB}} \sum_{\sigma \in S_k} R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}}\right]\right| + \left|\mathrm{Tr}\left[M_{\mathbf{AB}} \sum_{\substack{\sigma,\pi \in S_k,\\ \pi \neq e}} \mathrm{Wg}(\pi; d) R^{\dagger}_{\sigma,\mathbf{A}} \otimes \sqrt{\xi}_{\mathbf{B}} R^{\dagger}_{\pi\sigma,\mathbf{B}} \sqrt{\xi}_{\mathbf{B}}\right]\right|, &(71)
\end{aligned}$$

where we have used Equations (64) and (65) in the equality, and the inequality follows from the triangle inequality. In the following, we show both the first term and the second term are at most $O(k^2/d)$.

The trace of the first term in Equation (71) can be estimated as follows:

$$
\begin{aligned}
\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\Big(\sum_{\sigma\in S_k} R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}\Big)\right]\right| \leq & \left|\mathrm{Tr}\Big[\sum_{\sigma\in S_k} R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}\Big]\right| && (72)\\
\leq & \sum_{\sigma\in S_k}\left|\mathrm{Tr}[R^{\dagger}_{\sigma,\mathbf{A}}]\mathrm{Tr}[\sqrt{\xi_{\mathbf{B}}}R_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}]\right| && (73)\\
\leq & \sum_{\sigma\in S_k}\left|\mathrm{Tr}[R^{\dagger}_{\sigma,\mathbf{A}}]\right| && (74)\\
= & k!\binom{d+k-1}{k}, && (75)
\end{aligned}
$$

where we have used

- the facts that $0\leq M\leq I$ and $\sum_{\sigma\in S_k} R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}$ is positive in the first ineqaulity. The latter follows from Lemma 2.12;
- the riangle inequality and $\mathrm{Tr}[A]\mathrm{Tr}[B]=\mathrm{Tr}[A\otimes B]$ for any matrix A and B in the second equality;
- $|\mathrm{Tr}[\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}]|=|\mathrm{Tr}[\xi_{\mathbf{B}}R_{\sigma,\mathbf{B}}]|\leq 1$ for any $\sigma\in S_k$ since ξ is a quantum state and R_σ is unitary in the third inequality;
- $\mathrm{Tr}[R^{\dagger}_{\sigma}]=\mathrm{Tr}[R_\sigma]\geq 0$ for any $\sigma\in S_k$ and Lemma 2.11 in the last equality.

By combing Equation (75) and Lemma 4.6, we have[9]

$$
\begin{aligned}
\left|\mathrm{Wg}(e;d)-\frac{1}{d^k}\right|\left|\mathrm{Tr}\left[M\Big(\sum_{\sigma\in S_k} R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}\Big)\right]\right| \leq & \left|\mathrm{Wg}(e;d)-\frac{1}{d^k}\right|k!\binom{d+k-1}{k} && (76)\\
\leq & O\left(\frac{k^{7/2}}{d^{k+2}}\right)k!\binom{d+k-1}{k} && (77)\\
= & O\left(\frac{k^{7/2}}{d^2}\right) && (78)\\
\leq & O\left(\frac{k^2}{d}\right). && (79)
\end{aligned}
$$

Next, let us estimate the second term in Equation (71);

$$
\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\sum_{\substack{\sigma,\pi\in S_k,\\ \pi\neq e}}\mathrm{Wg}(\pi;d)R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}}R^{\dagger}_{\pi\sigma,\mathbf{B}}\sqrt{\xi_{\mathbf{B}}}\right]\right| \tag{80}
$$

$$
=\left|\mathrm{Tr}\Big[\sum_{\sigma,\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)(R^{\dagger}_{\sigma,\mathbf{A}}\otimes R^{\dagger}_{\pi,\mathbf{B}}R^{\dagger}_{\sigma,\mathbf{B}})(I_{\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}})M_{\mathbf{AB}}(I_{\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}})\Big]\right| \tag{81}
$$

$$
=\left|\mathrm{Tr}\left[\Big(\sum_{\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)I_{\mathbf{A}}\otimes R_{\pi,\mathbf{B}}\Big)\Big(\sum_{\sigma\in S_k}R_{\sigma,\mathbf{A}}\otimes R_{\sigma,\mathbf{B}}\Big)(I_{\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}})M_{\mathbf{AB}}(I_{\mathbf{A}}\otimes\sqrt{\xi_{\mathbf{B}}})\right]\right|. \tag{82}
$$

Here,

[9] $\frac{k^{7/2}}{d^2}=\frac{k^2}{d}\frac{k^{3/2}}{d}\leq\frac{k^2}{d}$ since $d>\sqrt{6}k^{7/4}$.

- we have used $R_{\pi\sigma} = R_\sigma R_\pi$ in the first equality;
- we replaced the summation of π with π^{-1} and that of σ with σ^{-1} in the second equality.

We want to apply Lemma 2.8 to Equation (82). Note that

- $\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi,\mathbf{B}}$ is hermitian:

$$\left(\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi,\mathbf{B}}\right)^\dagger = \sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi^{-1},\mathbf{B}} \tag{83}$$

$$= \sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi^{-1};d) I_{\mathbf{A}} \otimes R_{\pi,\mathbf{B}} \tag{84}$$

$$= \sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi',\mathbf{B}}, \tag{85}$$

  where we have replaced the summation of π with π^{-1} in the second equality, and we have used Lemma 4.3 in the last equality;

- $\sum_{\sigma\in S_k} R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}}$ and $(I_{\mathbf{A}} \otimes \sqrt{\xi_{\mathbf{B}}}) M_{\mathbf{AB}} (I_{\mathbf{A}} \otimes \sqrt{\xi_{\mathbf{B}}})$ are positive, where the former follows from Lemma 2.12;

- $\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi,\mathbf{B}}$ is commutive with $\sum_{\sigma\in S_k} R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}}$ as follows;

$$\left(\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\pi,\mathbf{B}}\right)\left(\sum_{\sigma\in S_k} R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}}\right) \tag{86}$$

$$= \sum_{\sigma\in S_k} (R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}})\left(\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_\sigma^\dagger R_\pi R_{\sigma,\mathbf{B}}\right) \tag{87}$$

$$= \sum_{\sigma\in S_k} (R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}})\left(\sum_{\pi\in S_k;\pi\neq e} \mathrm{Wg}(\pi;d) I_{\mathbf{A}} \otimes R_{\sigma\pi\sigma^{-1},\mathbf{B}}\right) \tag{88}$$

$$= \sum_{\sigma\in S_k} (R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}})\left(\sum_{\pi'\in S_k;\pi'\neq e} \mathrm{Wg}(\sigma^{-1}\pi'\sigma;d) I_{\mathbf{A}} \otimes R_{\pi',\mathbf{B}}\right) \tag{89}$$

$$= \left(\sum_{\sigma\in S_k} R_{\sigma,\mathbf{A}} \otimes R_{\sigma,\mathbf{B}}\right)\left(\sum_{\pi'\in S_k;\pi'\neq e} \mathrm{Wg}(\pi';d) I_{\mathbf{A}} \otimes R_{\pi',\mathbf{B}}\right), \tag{90}$$

  where

  - we replaced the summation of π with $\pi' := \sigma\pi\sigma^{-1}$ in the third equality;
  - we have used Lemma 4.3 in the last equality.

Thus, we can apply Lemma 2.8 to Equation (82);

$$\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\sum_{\substack{\sigma,\pi\in S_k,\\ \pi\neq e}}\mathrm{Wg}(\pi;d)R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi}_{\mathbf{B}}R^{\dagger}_{\pi\sigma,\mathbf{B}}\sqrt{\xi}_{\mathbf{B}}\right]\right| \tag{91}$$

$$\leq\left\|\sum_{\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)I_{\mathbf{A}}\otimes R_{\pi,\mathbf{B}}\right\|_{\infty}\mathrm{Tr}\left[\left(\sum_{\sigma\in S_k}R_{\sigma,\mathbf{A}}\otimes R_{\sigma,\mathbf{B}}\right)(I_{\mathbf{A}}\otimes\sqrt{\xi}_{\mathbf{B}})M_{\mathbf{AB}}(I_{\mathbf{A}}\otimes\sqrt{\xi}_{\mathbf{B}})\right] \tag{92}$$

$$=\left\|\sum_{\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)I_{\mathbf{A}}\otimes R_{\pi,\mathbf{B}}\right\|_{\infty}\mathrm{Tr}\left[M_{\mathbf{AB}}\left(\sum_{\sigma\in S_k}R_{\sigma,\mathbf{A}}\otimes\sqrt{\xi}_{\mathbf{B}}R_{\sigma,\mathbf{B}}\sqrt{\xi}_{\mathbf{B}}\right)\right]. \tag{93}$$

We have already estimated the trace of Equation (93) in Equation (75). Hence, it suffices to estimate the operator norm in Equation (93);

$$\left\|\sum_{\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)I_{\mathbf{A}}\otimes R_{\pi,\mathbf{B}}\right\|_{\infty}=\left\|\sum_{\pi\in S_k;\pi\neq e}\mathrm{Wg}(\pi;d)R_{\pi,\mathbf{B}}\right\|_{\infty} \tag{94}$$

$$\leq\sum_{\pi\in S_k;\pi\neq e}|\mathrm{Wg}(\pi;d)| \tag{95}$$

$$=\frac{1}{d(d-1)\cdots(d-k+1)}-|\mathrm{Wg}(e;d)| \tag{96}$$

$$\leq\frac{1}{d^k}\left(1+O\left(\frac{k^2}{d}\right)\right)-\frac{1}{d^k}\left(1-O\left(\frac{k}{d^2}\right)\right) \tag{97}$$

$$=O\left(\frac{k^2}{d^{k+1}}\right), \tag{98}$$

where we have used

- $\|A\otimes B\|_{\infty}=\|A\|_{\infty}\|B\|_{\infty}$ for any matrix A and B in the first equality;
- triangle inequality and $\|R_{\pi}\|_{\infty}\leq 1$ for any $\pi\in S_k$ in the first inequality;
- Lemma 4.5 in the second equality, and Lemma 4.6 in the last inequality.

From Equations (75), (93) and (98), we can bund the second term in Equation (71) as follows;

$$\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\sum_{\substack{\sigma,\pi\in S_k,\\ \pi\neq e}}\mathrm{Wg}(\pi;d)R^{\dagger}_{\sigma,\mathbf{A}}\otimes\sqrt{\xi}_{\mathbf{B}}R^{\dagger}_{\pi\sigma,\mathbf{B}}\sqrt{\xi}_{\mathbf{B}}\right]\right|\leq k!\binom{d+k-1}{k}O\left(\frac{k^2}{d^{k+1}}\right)\leq O\left(\frac{k^2}{d}\right). \tag{99}$$

Therefore, from Equations (71), (79) and (99), we have

$$\left|\mathrm{Tr}\left[M_{\mathbf{AB}}\left((\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}}\otimes\mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}})-\sum_{\sigma\in S_k}\frac{1}{d^k}R^{\dagger}_{\sigma,\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A'}}[(R_{\sigma,\mathbf{A'}}\otimes I_{\mathbf{B}})\psi_{\mathbf{A'B}}]\right)\right]\right|\leq O\left(\frac{k^2}{d}\right). \tag{100}$$

for any $0\leq M\leq I$. This implies that the first term in Equation (62) is at most $O(k^2/d)$.

Estimation of the second term in Equation (62). To conclude the proof, let us estimate the second term in Equation (62). To do so, it suffices to show the following;

$$\left|\mathrm{Tr}\left[(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}}\otimes\mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}})-\sum_{\sigma\in S_k}\frac{1}{d^k}R^{\dagger}_{\sigma,\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right]\right|\leq O\left(\frac{k^2}{d}\right) \tag{101}$$

It is clear $\mathrm{Tr}[(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}}\otimes\mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}})]=1$. On the other hand,

$$\mathrm{Tr}\left[\sum_{\sigma\in S_k}\frac{1}{d^k}R^{\dagger}_{\sigma,\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right] \tag{102}$$

$$=\frac{1}{d^k}\mathrm{Tr}\left[I_{\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A}'}[\psi_{\mathbf{A}'\mathbf{B}}]\right]+\mathrm{Tr}\left[\sum_{\sigma\in S_k;\sigma\neq e}\frac{1}{d^k}R^{\dagger}_{\sigma,\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right] \tag{103}$$

$$=1+\frac{1}{d^k}\sum_{\sigma\in S_k;\sigma\neq e}\mathrm{Tr}[R_{\sigma,\mathbf{A}}]\mathrm{Tr}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}] \tag{104}$$

Thus,

$$\left|\mathrm{Tr}\left[\mathop{\mathbb{E}}_{U\leftarrow\mu_d}(U^{\otimes k}_{\mathbf{A}}\otimes I_{\mathbf{B}})\psi_{\mathbf{AB}}(U^{\dagger\otimes k}_{\mathbf{A}}\otimes I_{\mathbf{B}})-\sum_{\pi\in S_k}\frac{1}{d^k}R^{\dagger}_{\sigma,\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right]\right| \tag{105}$$

$$=\frac{1}{d^k}\left|\sum_{\sigma\in S_k;\sigma\neq e}\mathrm{Tr}[R_{\sigma,\mathbf{A}}]\mathrm{Tr}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right| \tag{106}$$

$$\leq\frac{1}{d^k}\sum_{\sigma\in S_k;\sigma\neq e}\left|\mathrm{Tr}[R_{\sigma,\mathbf{A}}]\mathrm{Tr}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right| \tag{107}$$

$$\leq\frac{1}{d^k}\sum_{\sigma\in S_k;\sigma\neq e}\left|\mathrm{Tr}[R_{\sigma,\mathbf{A}}]\right| \tag{108}$$

$$=\frac{1}{d^k}\left(\sum_{\sigma\in S_k}\mathrm{Tr}[R_{\sigma,\mathbf{A}}]-\mathrm{Tr}[I_{\mathbf{A}}]\right) \tag{109}$$

$$=\frac{1}{d^k}\left(k!\mathrm{Tr}[\Pi^{(d,k)}_{\mathrm{sym},\mathbf{A}}]-\mathrm{Tr}[I_{\mathbf{A}}]\right) \tag{110}$$

$$=\frac{1}{d^k}\left(k!\binom{d+k-1}{k}-d^k\right) \tag{111}$$

$$\leq O\left(\frac{k^2}{d}\right), \tag{112}$$

which implies that the second term in Equation (62) is at most $O(k^2/d)$. Here we have used

- Equation (104) in the first equality;
- $|\mathrm{Tr}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]|\leq 1$ for all $\sigma\in S_k$ in the second inequality;
- $|\mathrm{Tr}[R_{\sigma,\mathbf{A}}]|=\mathrm{Tr}[R_{\sigma,\mathbf{A}}]$ for all $\sigma\in S_k$ in the second equality;
- Lemma 2.11 in the third and fourth equality.

Therefore, by putting together Equations (62), (100) and (112), we have the desired result;

$$\left\|(\mathcal{M}^{(k)}_{\text{Haar},\mathbf{A}}\otimes \mathrm{id}_{\mathbf{B}})(\psi_{\mathbf{AB}})-\sum_{\sigma\in S_k}\frac{1}{d^k}R^\dagger_{\sigma,\mathbf{A}}\otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\psi_{\mathbf{A}'\mathbf{B}}]\right\|_1\leq O\left(\frac{k^2}{d}\right). \tag{113}$$

□

Remark 4.8. Our bound in Lemma 4.7 is optimal because $\rho=\frac{\Pi^{(d,k)}_{\text{sym}}}{\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}]}$ achieve the upper bound. We can check this as follows: from the concrete expression of $\Pi^{(d,k)}_{\text{sym}}$ in Lemma 2.11, we have

$$\mathcal{M}^{(k)}_{\text{Haar}}(\Pi^{(d,k)}_{\text{sym}})=\mathop{\mathbb{E}}_{U\leftarrow\mu_d}U^{\otimes k}\Pi^{(d,k)}_{\text{sym}}U^{\dagger\otimes k}=\frac{1}{k!}\sum_{\sigma\in S_k}\mathop{\mathbb{E}}_{U\leftarrow\mu_d}U^{\otimes k}R_\sigma U^{\dagger\otimes k}=\frac{1}{k!}\sum_{\sigma\in S_k}R_\sigma=\Pi^{(d,k)}_{\text{sym}}, \tag{114}$$

where we have used $R_\sigma U^{\otimes k}=U^{\otimes k}R_\sigma$ for any $\sigma\in S_k$ and any $U\in\mathbb{U}(d)$. On the other hand,

$$\begin{aligned}\sum_{\sigma\in S_k}\frac{1}{d^k}\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}R_\sigma]R^\dagger_\sigma&=\sum_{\sigma\in S_k}\frac{1}{d^k}\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}]R^\dagger_\sigma &(115)\\ &=\frac{1}{d^k}\binom{d+k-1}{k}\sum_{\sigma\in S_k}R^\dagger_\sigma &(116)\\ &=(1+O(k^2/d))\frac{1}{k!}\sum_{\sigma\in S_k}R^\dagger_\sigma &(117)\\ &=(1+O(k^2/d))\Pi^{(d,k)}_{\text{sym}}, &(118)\end{aligned}$$

where we have used $\Pi^{(d,k)}_{\text{sym}}R_\sigma=\Pi^{(d,k)}_{\text{sym}}$ for any $\sigma\in S_k$ in the first equality, and Lemma 2.11 in the second and the last equality. Therefore,

$$\left\|\mathcal{M}^{(k)}_{\text{Haar}}\left(\frac{\Pi^{(d,k)}_{\text{sym}}}{\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}]}\right)-\sum_{\sigma\in S_k}\frac{1}{d^k}\mathrm{Tr}\left[\frac{\Pi^{(d,k)}_{\text{sym}}}{\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}]}R_\sigma\right]R^\dagger_\sigma\right\|_1=O\left(\frac{k^2}{d}\right)\left\|\frac{\Pi^{(d,k)}_{\text{sym}}}{\mathrm{Tr}[\Pi^{(d,k)}_{\text{sym}}]}\right\|_1=O\left(\frac{k^2}{d}\right). \tag{119}$$

5 PRFSGs and PRSGs in the non-adaptive inverseless QHRO Model

In this section, we construct selective secure PRFSGs in the non-adaptive inverseless QHRO model.

Theorem 5.1. *Selective secure PRFSGs exist in the non-adaptive inverseless QHRO model.*

This is shown by the following theorem.

Theorem 5.2. *Let $d,m,t,\ell\in\mathbb{N}$ such that $d>\sqrt{6}(t\ell+m)^{7/4}$. Let ν be the unitary 1-design over $\mathbb{U}(d)$. Then, for any quantum state ρ and distinct $x_1,...,x_\ell\in[d]$,*

$$\begin{aligned}&\left\|\mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_d,\\ P\leftarrow\nu}}\bigotimes_{i=1}^{\ell}(UP\ket{x_i}\bra{x_i}P^\dagger U^\dagger)^{\otimes t}_{\mathbf{A}}\otimes U^{\otimes m}_{\mathbf{B}}\rho_{\mathbf{BC}}U^{\dagger\otimes m}_{\mathbf{B}}-\bigotimes_{i=1}^{\ell}\left(\mathop{\mathbb{E}}_{\ket{\psi_i}\leftarrow\mu^s_d}\ket{\psi_i}\bra{\psi_i}^{\otimes t}\right)_{\mathbf{A}}\otimes\mathop{\mathbb{E}}_{U\leftarrow\nu_d}U^{\otimes m}_{\mathbf{B}}\rho_{\mathbf{BC}}U^{\dagger\otimes m}_{\mathbf{B}}\right\|_1\\ \leq&O\left(\sqrt{\frac{m\ell}{d}}\right)+O\left(\frac{(t\ell+m)^2}{d}\right),\end{aligned} \tag{120}$$

where μ^s_d denotes the Haar mesure over all d-dimensional states.

Before proving Theorem 5.2, we show Theorem 5.1 assuming it.

Proof of Theorem 5.1. Since the proof is the same, we only show the existence of PRFSGs in the QHRO model. Let $\lambda \in \mathbb{N}$ be a security parameter and $\mathcal{U} := \{U_n\}_{n\in\mathbb{N}}$ be a single common Haar random unitary. Then, the following QPT algorithm $G^{\mathcal{U}}$ becomes a PRFSG:

- For $k, x \in \{0,1\}^\lambda$, $G^{\mathcal{U}}(k,x)$ prepares $X^k |x\rangle$ and query it to U, then outputs $|\phi_k(x)\rangle := U_\lambda X^k |x\rangle$.

Let $\mathcal{A}^{\mathcal{U}}$ be an adversary that queries $\xi_{\mathbf{BC}}$ to $U_{\lambda,\mathbf{B}}^{\otimes m(\lambda)} \otimes (\bigotimes_{i=1}^{r(\lambda)} U_{n(i)})_{\mathbf{C}}$ before receiving challenge states from the challnger, where r and m are a polynomial of λ, and $n(i) \neq \lambda$ for all $i \in [r]$. Note that this does not lose the generality. Then, for any polynomial t, ℓ, and any $x_1, ..., x_\ell \in \{0,1\}^\lambda$, the probability that $\mathcal{A}^{\mathcal{U}}$ outputs 1 when it receives $|\phi_k(x_1)\rangle^{\otimes t} \otimes ... \otimes |\phi_k(x_\ell)\rangle^{\otimes t}$ is

$$\Pr_{\substack{\mathcal{U}\leftarrow\mu,\\ k\leftarrow\{0,1\}^\lambda}}[1 \leftarrow \mathcal{A}^{\mathcal{U}}(|\phi_k(x_1)\rangle\langle\phi_k(x_1)|^{\otimes t} \otimes ... \otimes |\phi_k(x_\ell)\rangle\langle\phi_k(x_\ell)|^{\otimes t})] \tag{121}$$

$$= \mathop{\mathbb{E}}_{\substack{\mathcal{U}\leftarrow\mu,\\ k\leftarrow\{0,1\}^\lambda}} \bigotimes_{i=1}^{\ell} (U_\lambda X^k |x_i\rangle\langle x_i| X^{k\dagger} U_\lambda^\dagger)_{\mathbf{A}}^{\otimes t} \otimes (U_{\lambda,\mathbf{B}}^{\otimes m} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})\xi_{\mathbf{BC}}(U_{\lambda,\mathbf{B}}^{\otimes m} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})^\dagger \tag{122}$$

$$= \mathop{\mathbb{E}}_{\substack{U_\lambda\leftarrow\mu_{2^\lambda},\\ k\leftarrow\{0,1\}^\lambda}} \bigotimes_{i=1}^{\ell} (U_\lambda X^k |x_i\rangle\langle x_i| X^{k\dagger} U_\lambda^\dagger)_{\mathbf{A}}^{\otimes t} \otimes U_{\lambda,\mathbf{B}}^{\otimes m} \rho_{\mathbf{BC}} U_{\lambda,\mathbf{B}}^{\dagger\otimes m} \tag{123}$$

$$= \mathop{\mathbb{E}}_{\substack{U_\lambda\leftarrow\mu_{2^\lambda},\\ P\leftarrow\nu}} \bigotimes_{i=1}^{\ell} (U_\lambda P |x_i\rangle\langle x_i| P^\dagger U_\lambda^\dagger)_{\mathbf{A}}^{\otimes t} \otimes U_{\lambda,\mathbf{B}}^{\otimes m} \rho_{\mathbf{BC}} U_{\lambda,\mathbf{B}}^{\dagger\otimes m}, \tag{124}$$

where

- $\rho_{\mathbf{BC}}$ is defined as
$$\rho_{\mathbf{BC}} := (I_{\mathbf{B}} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})\xi_{\mathbf{BC}}(I_{\mathbf{B}} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})^\dagger, \tag{125}$$
and we have inserted it in the second equality since $n(i) \neq \lambda$ for all $i \in [r]$;

- ν is the uniform distribution over all λ-qubit Pauli operator, and, in the last equality, we have used
$$\mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^\lambda} X^k |x\rangle\langle x| X^{k\dagger} = \mathop{\mathbb{E}}_{k,k'\leftarrow\{0,1\}^\lambda} X^k Z^{k'} |x\rangle\langle x| Z^{\dagger k'} X^{k\dagger} = \mathop{\mathbb{E}}_{P\leftarrow\nu} P|x\rangle\langle x| P^\dagger \tag{126}$$
for any $x \in \{0,1\}^\lambda$ since any Pauli Z does not cahnge $|x\rangle$ except for a global phase.

On the other hand, we have

$$\Pr_{\substack{\mathcal{U}\leftarrow\mu_{2^\lambda},\\ |\psi_1\rangle,...,|\psi_\ell\rangle\leftarrow\mu_{2^\lambda}^s}}[1 \leftarrow \mathcal{A}^{\mathcal{U}}(|\psi_1\rangle\langle\psi_1|^{\otimes t} \otimes ... \otimes |\psi_\ell\rangle\langle\psi_\ell|^{\otimes t})] \tag{127}$$

$$= \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu_{2^\lambda}^s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{\mathcal{U}\leftarrow\mu} (U_{\lambda,\mathbf{B}}^{\otimes m} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})\xi_{\mathbf{BC}}(U_{\lambda,\mathbf{B}}^{\otimes m} \otimes \bigotimes_{i=1}^{r(\lambda)} U_{n(i),\mathbf{C}})^\dagger \tag{128}$$

$$= \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu_{2^\lambda}^s} |\psi_i\rangle\langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{U_\lambda\leftarrow\mu_{2^\lambda}} U_{\lambda,\mathbf{B}}^{\otimes m} \rho_{\mathbf{BC}} U_{\lambda,\mathbf{B}}^{\dagger\otimes m}, \tag{129}$$

where $\rho_{\mathbf{BC}}$ is defined above. Therefore

$$\begin{aligned}
&\Bigg| \Pr_{\substack{\mathcal{U}\leftarrow\mu,\\ k\leftarrow\{0,1\}^\lambda}} [1 \leftarrow \mathcal{A}^{\mathcal{U}}(|\phi_k(x_1)\rangle\langle\phi_k(x_1)|^{\otimes t}\otimes ...\otimes |\phi_k(x_\ell)\rangle\langle\phi_k(x_\ell)|^{\otimes t})] \\
&- \Pr_{\substack{\mathcal{U}\leftarrow\mu_{2\lambda},\\ |\psi_1\rangle,...,|\psi_\ell\rangle\leftarrow\mu_{2\lambda}^s}} [1 \leftarrow \mathcal{A}^{\mathcal{U}}(|\psi_1\rangle\langle\psi_1|^{\otimes t}\otimes ...\otimes |\psi_\ell\rangle\langle\psi_\ell|^{\otimes t})]\Bigg| && (130)\\
\leq&\left\| \mathop{\mathbb{E}}_{\substack{U_\lambda\leftarrow\mu_{2\lambda},\\ P\leftarrow\nu}} \bigotimes_{i=1}^{\ell}(U_\lambda P|x_i\rangle\langle x_i|P^\dagger U_\lambda^\dagger)^{\otimes t}_{\mathbf{A}}\otimes U_{\lambda,\mathbf{B}}^{\otimes m}\rho_{\mathbf{BC}}U_{\lambda,\mathbf{B}}^{\dagger\otimes m} - \bigotimes_{i=1}^{\ell}\left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu_{2\lambda}^s}|\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathbf{A}}\otimes \mathop{\mathbb{E}}_{U_\lambda\leftarrow\mu_{2\lambda}} U_{\lambda,\mathbf{B}}^{\otimes m}\rho_{\mathbf{BC}}U_{\lambda,\mathbf{B}}^{\dagger\otimes m}\right\|_1 && (131)\\
\leq& O\left(\sqrt{\frac{m\ell}{2^\lambda}}\right)+O\left(\frac{(t\ell+m)^2}{2^\lambda}\right) && (132)\\
\leq&\mathsf{negl}(\lambda), && (133)
\end{aligned}$$

which implies $G^{\mathcal{U}}$ is a PRFSG in the non-adaptive QHRO model. Here, we have used Lemma 2.3 and Theorem 5.2 in the second inequality. □

Before a proof of Theorem 5.2, we show the following lemma.

Lemma 5.3. *Let $d,k,\ell\in\mathbb{N}$ and ν be a unitary 1-design over $\mathbb{U}(d)$. For ℓ distinct $x_1,...,x_\ell\in[d]$, define $x:=(x_1,...,x_\ell)$ and*

$$\Lambda^{(x)} := \sum_{y_1,...,y_k\in[d]/\{x_1,...,x_\ell\}}\bigotimes_{i=1}^{k}|y_i\rangle\langle y_i|. \tag{134}$$

Then, for any d^k-dimensional state ρ,

$$\mathrm{Tr}[\Lambda^{(x)}\mathop{\mathbb{E}}_{P\leftarrow\nu}P^{\otimes k}\rho P^{\dagger\otimes k}]\geq 1-\frac{m\ell}{d}. \tag{135}$$

Proof of Lemma 5.3. Note that

$$I-\Lambda^{(x)} = \sum_{\substack{y_1,...,y_k\in[d]\\ y_i=x_j \text{ for some } i\in[k] \text{ and } j\in[\ell]}}\bigotimes_{i=1}^{k}|y_i\rangle\langle y_i| \leq \sum_{i\in[k],j\in[\ell]}\Lambda_{i,j}, \tag{136}$$

where $\Lambda_{i,j}:=I^{\otimes i-1}\otimes|x_j\rangle\langle x_j|\otimes I^{\otimes k-i}$. Then,

$$\begin{aligned}
\mathrm{Tr}[(I-\Lambda^{(x)})\mathop{\mathbb{E}}_{P\leftarrow\nu}P^{\otimes k}\rho P^{\dagger\otimes k}] &\leq \sum_{i\in[k],j\in[\ell]}\mathrm{Tr}[\Lambda_{i,j}\mathop{\mathbb{E}}_{P\leftarrow\nu}P^{\otimes k}\rho P^{\dagger\otimes k}] && (137)\\
&=\sum_{i\in[k],j\in[\ell]}\mathrm{Tr}[\rho\mathop{\mathbb{E}}_{P\leftarrow\nu}P^{\dagger\otimes k}\Lambda_{i,j}P^{\otimes k}] && (138)\\
&=\sum_{i\in[k],j\in[\ell]}\mathrm{Tr}[\rho\frac{I^{\otimes k}}{d}] && (139)\\
&=\frac{m\ell}{d}, && (140)
\end{aligned}$$

which implies Equation (135). Here, the inequality follows from Equation (136), and the second equality follows from the definition of $\Lambda_{i,j}$ and ν is a 1-design as follows:

$$\mathop{\mathbb{E}}_{P \leftarrow \nu} P^{\dagger \otimes k} \Lambda_{i,j} P^{\otimes k} = \mathop{\mathbb{E}}_{P \leftarrow \nu} I^{\otimes i-1} \otimes P^{\dagger} \left| x_j \right\rangle \left\langle x_j \right| P \otimes I^{\otimes k-i} = \frac{1}{d} I^{\otimes k}. \tag{141}$$

$\square$

Now we are reday to prove Theorem 5.2.

Proof of Theorem 5.2. Let $x \coloneqq (x_1, ..., x_\ell)$ and

$$\Lambda^{(x)} \coloneqq \sum_{y_1,...,y_k \in [d]/\{x_1,...,x_\ell\}} \bigotimes_{i=1}^{k} \left| y_i \right\rangle \left\langle y_i \right|. \tag{142}$$

Define

$$\xi_{\mathbf{BC}} = \mathop{\mathbb{E}}_{P \leftarrow \nu} P_{\mathbf{B}}^{\otimes k} \rho_{\mathbf{BC}} P_{\mathbf{B}}^{\dagger \otimes k} \tag{143}$$

and

$$\xi'_{\mathbf{BC}} \coloneqq \frac{\Lambda_{\mathbf{B}}^{(x)} \xi_{\mathbf{BC}} \Lambda_{\mathbf{B}}^{(x)}}{\mathrm{Tr}[\Lambda_{\mathbf{B}}^{(x)} \xi_{\mathbf{BC}}]}. \tag{144}$$

Note that

$$\|\xi_{\mathbf{BC}} - \xi'_{\mathbf{BC}}\|_1 \leq O\left(\sqrt{\frac{m\ell}{d}}\right) \tag{145}$$

from Lemmata 2.6 and 5.3. Let us consider the following sequence of matrices:

$$\rho^{(0)}_{\mathbf{ABC}} \coloneqq \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_d,\\ P\leftarrow\nu}} \bigotimes_{i=1}^{\ell} (UP\,|x_i\rangle\langle x_i|\,P^\dagger U^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U^{\otimes m}_{\mathbf{B}} \rho_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{146}$$

$$\rho^{(1)}_{\mathbf{ABC}} \coloneqq \mathop{\mathbb{E}}_{U\leftarrow\mu_d} \bigotimes_{i=1}^{\ell} (U\,|x_i\rangle\langle x_i|\,U^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U^{\otimes m}_{\mathbf{B}} \xi_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{147}$$

$$\rho^{(2)}_{\mathbf{ABC}} \coloneqq \mathop{\mathbb{E}}_{U\leftarrow\mu_d} \bigotimes_{i=1}^{\ell} (U\,|x_i\rangle\langle x_i|\,U^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U^{\otimes m}_{\mathbf{B}} \xi'_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{148}$$

$$\rho^{(3)}_{\mathbf{ABC}} \coloneqq \sum_{\pi\in S_{t\ell+m}} \frac{1}{d^{t\ell+m}} R_{\pi,\mathbf{AB}} \otimes \mathrm{Tr}_{\mathbf{AB}}[R^\dagger_{\pi,\mathbf{AB}}(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}})] \tag{149}$$

$$\rho^{(4)}_{\mathbf{ABC}} \coloneqq \left(\sum_{\sigma\in S_t} \frac{1}{d^t} R_\sigma\right)^{\otimes\ell}_{\mathbf{A}} \otimes \sum_{\tau\in S_m} \frac{1}{d^m} R_{\tau,\mathbf{B}} \otimes \mathrm{Tr}_{\mathbf{B}}[R^\dagger_{\tau,\mathbf{B}} \xi'_{\mathbf{BC}}] \tag{150}$$

$$\rho^{(5)}_{\mathbf{ABC}} \coloneqq \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu^s_d} |\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathbf{A}} \otimes \sum_{\tau\in S_m} \frac{1}{d^m} R_{\tau,\mathbf{B}} \otimes \mathrm{Tr}_{\mathbf{B}}[R^\dagger_{\tau,\mathbf{B}} \xi'_{\mathbf{BC}}] \tag{151}$$

$$\rho^{(6)}_{\mathbf{ABC}} \coloneqq \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu^s_d} |\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{U\leftarrow\nu_d} U^{\otimes m}_{\mathbf{B}} \xi'_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{152}$$

$$\rho^{(7)}_{\mathbf{ABC}} \coloneqq \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu^s_d} |\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{U\leftarrow\nu_d} U^{\otimes m}_{\mathbf{B}} \xi_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{153}$$

$$\rho^{(8)}_{\mathbf{ABC}} \coloneqq \bigotimes_{i=1}^{\ell} \left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu^s_d} |\psi_i\rangle\langle\psi_i|^{\otimes t}\right)_{\mathbf{A}} \otimes \mathop{\mathbb{E}}_{U\leftarrow\nu_d} U^{\otimes m}_{\mathbf{B}} \rho_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}}. \tag{154}$$

We argue $\rho^{(i-1)}$ is indistinguishable from $\rho^{(i)}$ for each $i \in [8]$:

- $\rho^{(0)}_{\mathbf{ABC}} = \rho^{(1)}_{\mathbf{ABC}}$ follows from the left and right invariance of the Haar measure:

$$\rho^{(0)}_{\mathbf{ABC}} = \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_d,\\ P\leftarrow\nu}} \bigotimes_{i=1}^{\ell} (UP\,|x_i\rangle\langle x_i|\,P^\dagger U^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U^{\otimes m}_{\mathbf{B}} \rho_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{155}$$

$$= \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_d,\\ P\leftarrow\nu}} \bigotimes_{i=1}^{\ell} (U'\,|x_i\rangle\langle x_i|\,U'^\dagger)^{\otimes t}_{\mathbf{A}} \otimes (U'P^\dagger)^{\otimes k}_{\mathbf{B}} \rho_{\mathbf{BC}} (U'P^\dagger)^{\dagger\otimes k}_{\mathbf{B}} \tag{156}$$

$$= \mathop{\mathbb{E}}_{U'\leftarrow\nu_d} \bigotimes_{i=1}^{\ell} (U'\,|x_i\rangle\langle x_i|\,U'^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U'^{\otimes k}_{\mathbf{B}} (\mathop{\mathbb{E}}_{P\leftarrow\nu} P^{\otimes k}_{\mathbf{B}} \rho_{\mathbf{BC}} P^{\otimes k}_{\mathbf{B}}) U^{\dagger\otimes m}_{\mathbf{B}} \tag{157}$$

$$= \mathop{\mathbb{E}}_{U'\leftarrow\nu_d} \bigotimes_{i=1}^{\ell} (U'\,|x_i\rangle\langle x_i|\,U'^\dagger)^{\otimes t}_{\mathbf{A}} \otimes U'^{\otimes k}_{\mathbf{B}} \xi_{\mathbf{BC}} U^{\dagger\otimes m}_{\mathbf{B}} \tag{158}$$

$$= \rho^{(1)}_{\mathbf{ABC}}, \tag{159}$$

  where we replaced the expectation of U with that of $U' \coloneqq UP$ in the second equality.

- $\|\rho^{(1)}_{\mathbf{ABC}} - \rho^{(2)}_{\mathbf{ABC}}\|_1 \le O(\sqrt{m\ell/d})$ from Equation (145).

- $\|\rho^{(2)}_{\mathbf{ABC}} - \rho^{(3)}_{\mathbf{ABC}}\|_1 \leq O((t\ell+m)^2/d)$ by Lemma 4.7.
- $\rho^{(3)}_{\mathbf{ABC}} = \rho^{(4)}_{\mathbf{ABC}}$ from the following observation. Suppose that $\pi \in S_{t\ell+m}$ cannot be decomposed into $\pi = (\sigma_1, ..., \sigma_\ell, \tau)$ for any $\sigma_1, ..., \sigma_\ell \in S_t$ and $\tau \in S_m$. Then, for any state $|\phi\rangle_{\mathbf{B}}$,

$$(I_{\mathbf{A}} \otimes \Lambda^{(x)}_{\mathbf{B}}) R_{\pi,\mathbf{AB}} (\bigotimes_{i=1}^{\ell} |x_i\rangle^{\otimes t})_{\mathbf{A}} |\phi\rangle_{\mathbf{B}} = 0 \tag{160}$$

from the definition of $\Lambda^{(x)}$, which implies

$$\mathrm{Tr}_{\mathbf{AB}}[R^{\dagger}_{\pi,\mathbf{AB}}(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}})] = \mathrm{Tr}_{\mathbf{AB}}[R^{\dagger}_{\pi,\mathbf{AB}}(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}})\Lambda_{\mathbf{B}}] = 0 \tag{161}$$

for such $\pi \in S_{t\ell+m}$. On the other hand, if $\pi \in S_{t\ell+m}$ can be decomposed into $\pi = (\sigma_1, ..., \sigma_\ell, \tau)$ for some $\sigma_1, ..., \sigma_\ell \in S_t$ and $\tau \in S_m$, we have

$$\mathrm{Tr}_{\mathbf{AB}}\left[R^{\dagger}_{\pi,\mathbf{AB}}\left(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}}\right)\right] = \mathrm{Tr}_{\mathbf{AB}}\left[R^{\dagger}_{(\sigma_1,...,\sigma_\ell,\tau),\mathbf{AB}}\left(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}}\right)\right] \tag{162}$$

$$= \mathrm{Tr}_{\mathbf{AB}}\left[\left(\left(\bigotimes_{i=1}^{\ell} R_{\sigma_i}\right)_{\mathbf{A}} \otimes R_{\tau,\mathbf{B}}\right)^{\dagger}\left(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}}\right)\right] \tag{163}$$

$$= \left(\prod_{i\in[\ell]} \mathrm{Tr}[R^{\dagger}_{\sigma_i} |x_i\rangle\langle x_i|^{\otimes t}]\right) \mathrm{Tr}_{\mathbf{B}}[R^{\dagger}_{\tau,\mathbf{B}}\xi'_{\mathbf{BC}}] \tag{164}$$

$$= \mathrm{Tr}_{\mathbf{B}}[R^{\dagger}_{\tau,\mathbf{B}}\xi'_{\mathbf{BC}}]. \tag{165}$$

Thus,

$$\rho^{(3)}_{\mathbf{ABC}} = \sum_{\pi\in S_{t\ell+m}} \frac{1}{d^{t\ell+m}} R_{\pi,\mathbf{AB}} \otimes \mathrm{Tr}_{\mathbf{AB}}\left[R^{\dagger}_{\pi,\mathbf{AB}}\left(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}}\right)\right] \tag{166}$$

$$= \sum_{\sigma_1,...,\sigma_\ell\in S_t, \tau\in S_m} \frac{1}{d^{t\ell+m}} R_{(\sigma_1,...,\sigma_\ell,\tau),\mathbf{AB}} \otimes \mathrm{Tr}_{\mathbf{AB}}\left[R^{\dagger}_{(\sigma_1,...,\sigma_\ell,\tau),\mathbf{AB}}\left(\bigotimes_{i=1}^{\ell} |x_i\rangle\langle x_i|^{\otimes t}_{\mathbf{A}} \otimes \xi'_{\mathbf{BC}}\right)\right] \tag{167}$$

$$= \sum_{\sigma_1,...,\sigma_\ell\in S_t, \tau\in S_m} \frac{1}{d^{t\ell+m}} \left(\bigotimes_{i=1}^{\ell} R_{\sigma_i}\right)_{\mathbf{A}} \otimes R_{\tau,\mathbf{B}} \otimes \mathrm{Tr}_{\mathbf{B}}[R^{\dagger}_{\tau,\mathbf{B}}\xi'_{\mathbf{BC}}] \tag{168}$$

$$= \left(\sum_{\sigma\in S_t} \frac{1}{d^t} R_\sigma\right)^{\otimes\ell}_{\mathbf{A}} \otimes \sum_{\tau\in S_m} \frac{1}{d^m} R_{\tau,\mathbf{B}} \otimes \mathrm{Tr}_{\mathbf{B}}[R^{\dagger}_{\tau,\mathbf{B}}\xi'_{\mathbf{BC}}] \tag{169}$$

$$= \rho^{(4)}_{\mathbf{ABC}}. \tag{170}$$

- $\|\rho^{(4)}_{\mathbf{ABC}} - \rho^{(5)}_{\mathbf{ABC}}\|_1 \leq O(\ell t^2/d)$ as follows: for each $j \in [\ell+1]$, define

$$\rho'^{(j)}_{\mathbf{ABC}} := \left(\bigotimes_{i=1}^{j-1}\left(\mathop{\mathbb{E}}_{|\psi_i\rangle\leftarrow\mu^s_d} |\psi_i\rangle\langle\psi_i|^{\otimes t}\right) \otimes \left(\sum_{\sigma\in S_t} \frac{1}{d^t} R_\sigma\right)^{\otimes\ell-j+1}\right)_{\mathbf{A}} \otimes \sum_{\tau\in S_m} \frac{1}{d^m} R_{\tau,\mathbf{B}} \otimes \mathrm{Tr}_{\mathbf{B}}[R^{\dagger}_{\tau,\mathbf{B}}\xi'_{\mathbf{BC}}]. \tag{171}$$

From Lemma 2.11,

$$\underset{|\psi_i\rangle \leftarrow \mu_d^s}{\mathbb{E}} |\psi_i\rangle \langle\psi_i|^{\otimes t} = \sum_{\sigma \in S_t} \frac{1}{d(d-1)...(d-t+1)} R_\sigma = \left(1 + O\left(\frac{t^2}{d}\right)\right) \sum_{\sigma \in S_t} \frac{1}{d^t} R_\sigma, \tag{172}$$

which implies $\|\rho'^{(j)}_{\mathbf{ABC}} - \rho'^{(j+1)}_{\mathbf{ABC}}\|_1 \leq O(t^2/d)$ for all $j \in [\ell]$. Since $\rho'^{(1)}_{\mathbf{ABC}} = \rho^{(4)}_{\mathbf{ABC}}$ and $\rho'^{(\ell+1)}_{\mathbf{ABC}} = \rho^{(5)}_{\mathbf{ABC}}$, we have $\|\rho^{(4)}_{\mathbf{ABC}} - \rho^{(5)}_{\mathbf{ABC}}\|_1 \leq O(\ell t^2/d)$.

- $\|\rho^{(5)}_{\mathbf{ABC}} - \rho^{(6)}_{\mathbf{ABC}}\|_1 \leq O(m^2/d)$ from Lemma 4.7.
- $\|\rho^{(6)}_{\mathbf{ABC}} - \rho^{(7)}_{\mathbf{ABC}}\|_1 \leq O(\sqrt{m\ell/d})$ from Equation (145).
- $\rho^{(7)}_{\mathbf{ABC}} = \rho^{(8)}_{\mathbf{ABC}}$ follows from the left and right invariance of the Haar measure:

$$\begin{aligned}
\rho^{(7)}_{\mathbf{ABC}} &= \bigotimes_{i=1}^{\ell} \left(\underset{|\psi_i\rangle \leftarrow \mu_d^s}{\mathbb{E}} |\psi_i\rangle \langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \underset{U \leftarrow \nu_d}{\mathbb{E}} U_{\mathbf{B}}^{\otimes m} \xi_{\mathbf{BC}} U_{\mathbf{B}}^{\dagger \otimes m} &(173)\\
&= \bigotimes_{i=1}^{\ell} \left(\underset{|\psi_i\rangle \leftarrow \mu_d^s}{\mathbb{E}} |\psi_i\rangle \langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \underset{U \leftarrow \nu_d}{\mathbb{E}} U_{\mathbf{B}}^{\otimes m} (\underset{P \leftarrow \nu}{\mathbb{E}} P_{\mathbf{B}}^{\otimes k} \rho_{\mathbf{BC}} P^{\dagger \otimes k}) U_{\mathbf{B}}^{\dagger \otimes m} &(174)\\
&= \bigotimes_{i=1}^{\ell} \left(\underset{|\psi_i\rangle \leftarrow \mu_d^s}{\mathbb{E}} |\psi_i\rangle \langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \underset{U \leftarrow \nu_d, P \leftarrow \nu}{\mathbb{E}} (UP)_{\mathbf{B}}^{\otimes k} \rho_{\mathbf{BC}} (UP)_{\mathbf{B}}^{\dagger \otimes k} &(175)\\
&= \bigotimes_{i=1}^{\ell} \left(\underset{|\psi_i\rangle \leftarrow \mu_d^s}{\mathbb{E}} |\psi_i\rangle \langle\psi_i|^{\otimes t} \right)_{\mathbf{A}} \otimes \underset{U' \leftarrow \nu_d}{\mathbb{E}} U_{\mathbf{B}}'^{\otimes k} \rho_{\mathbf{BC}} U_{\mathbf{B}}'^{\dagger \otimes k} &(176)\\
&= \rho^{(8)}_{\mathbf{ABC}}, &(177)
\end{aligned}$$

where we replaced the expectation of U with that of $U' := UP$ in the last equality.

Therefore, from the triangle inequality, we have

$$\|\rho^{(0)}_{\mathbf{ABC}} - \rho^{(7)}_{\mathbf{ABC}}\|_1 \leq O\left(\sqrt{\frac{m\ell}{d}}\right) + O\left(\frac{(t\ell + m)^2}{d}\right), \tag{178}$$

which concludes the proof. □

6 Adaptively-secure PRFSGs in the invertible QHRO Model

In this section, we prove the following theorem.

Theorem 6.1. *Classically-accessible adaptively-secure PRFSGs exist in the invertible QHRO model.*

6.1 Construction

We consider the following construction:

$$V_k^U |\phi\rangle = X^{k_1} \circ U \circ X^{k_0} |\phi\rangle \tag{179}$$

where a key $k = (k_0, k_1) \in K$ specifies two independent operators $X^{k_0}, X^{k_1} \in \mathbb{U}(d)$.[10] The following theorem shows that V_k^U is a pseudorandom unitary if the queries are all *classical*, meaning that the input register of V_k^U is measured in a computational basis before every query. This implies Theorem 6.1, combining with the proof of [AGQY22, Theorem 5.14], which says that if U is a Haar random unitary, then $|x\rangle \mapsto |x\rangle \otimes U|x\rangle$ is adaptively-secure PRFSGs.

Theorem 6.2. *Let V_k be in Equation (179). Suppose that $\{X^{k_b}\}_k$ is such that, for any $b \in \{0,1\}$ and $x \in \{0, ..., d-1\}$, $X^{k_b}|x\rangle$ is uniformly distributed over $\{|0\rangle, ..., |d-1\rangle\}$ for random k. For any $\mathcal{A}$ having access to two oracles that makes p classical-input queries to the first oracle and q queries[11] to the second oracle (including inverse queries), it holds that*

$$\left| \Pr_{U \leftarrow \mu_d, k \leftarrow K}\left[\mathcal{A}^{V_k^U,(U,U^\dagger)} \to 1\right] - \Pr_{U \leftarrow \mu_d, W \leftarrow \mu_d}\left[\mathcal{A}^{W,(U,U^\dagger)} \to 1\right] \right| = O\left(\sqrt{\frac{p^3 + p^2 q^2}{d}}\right). \tag{180}$$

6.2 Preparation I: Lemmas

We use the following lemmas to prove the security of Equation (179).

For two quantum states $|a\rangle$ and $|b\rangle$, define the generalized swap operation

$$\mathrm{SWAP}_{|a\rangle,|b\rangle} : \alpha|a\rangle + \beta|b\rangle + |c\rangle \mapsto \alpha|b\rangle + \beta|a\rangle + |c\rangle$$

for any $|c\rangle \in \mathrm{span}(|a\rangle, |b\rangle)^\perp$.[12] It is the swap operation between two states if $\langle a|b\rangle = 0$. We sometimes use $\mathrm{SWAP}_{a,b}$ for brevity.

Our two main lemmas are stated below. We give the proofs in Sections 6.5 and 6.6.

Lemma 6.3 (Unitary reprogramming lemma). *Let $\mathcal{D}$ be a distinguisher in the following experiment:*

Phase 1: *$\mathcal{D}$ outputs a unitary $F_0 = F$ over m-qubit and a quantum algorithm $\mathcal{C}$ whose output is a quantum state ρ and a classical string that specifies a classical description of the following data: a set S of m-qubit pure states and a unitary U_S such that, for the span $\mathcal{S}$ of all states in S, U_S acts as the identity on the image of $I - \Pi_{\mathcal{S}}$, where $\Pi_{\mathcal{S}}$ is the projection to $\mathcal{S}$. Let*

$$\epsilon := \sup_{|\phi\rangle : m\text{-qubit state}} \mathop{\mathbb{E}}_{\mathcal{C}}\left[\|\Pi_{\mathcal{S}}|\phi\rangle\|^2\right]. \tag{181}$$

Phase 2: *$\mathcal{C}$ is executed and outputs ρ, S and U_S. Let $F_1 := F \circ U_S$. A bit b is chosen uniformly at random, and $\mathcal{D}$ is given ρ and quantum access to F_b and makes q queries in expectation if $b = 0$, and sends the quantum state ν_b to the next phase.*

Phase 3: *$\mathcal{D}$ loses access to F_b and receives ν_b and the classical string specifying the classical descriptions S and U_S outputted by $\mathcal{C}$ in the second phase. Finally, $\mathcal{D}$ outputs a guess b'.*

Then, it holds that

$$|\Pr[\mathcal{D} \to 1 | b = 1] - \Pr[\mathcal{D} \to 1 | b = 0]| \le q \cdot \sqrt{2\epsilon}. \tag{182}$$

In fact, the trace distance $\mathsf{TD}(\nu_0, \nu_1)$ between two cases after Phase 2 is at most $q\sqrt{2\epsilon}$.

[10] The independency of k_0 and k_1 are used in the proof of Claim 1.
[11] We do not count the queries used by V_k^U.
[12] This map is well-defined unitary as a (rotated) reflection in $\mathrm{span}(|a\rangle, |b\rangle)$.

Lemma 6.4 (Unitary resampling lemma). *Let $\mathcal{D}$ be a distinguisher in the following experiment:*

Phase 1: *$\mathcal{D}$ specifies two distributions of d-dimensional qudit pure quantum states D_0^μ, D_1^μ such that $\mathbb{E} |\mu_i\rangle \langle\mu_i| = I/d$ for $i = 0, 1$. $\mathcal{D}$ makes at most q forward or inverse queries to a d-dimensional Haar random unitary $U^{(0)} := U$, and sends the quantum state ν to the next phase.*

Phase 2: *Sample $|\mu_0\rangle \leftarrow D_0^\mu, |\mu_1\rangle \leftarrow D_1^\mu$. A bit $b \in \{0, 1\}$ is uniformly chosen, and $\mathcal{D}$, given ν and classical descriptions of $|\mu_0\rangle, |\mu_1\rangle$, is allowed to make arbitrarily many (forward or inverse) queries to an oracle that is either $U^{(0)}$ if $b = 0$ or $U^{(1)} := U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$ if $b = 1$. Finally, $\mathcal{D}$ outputs a bit b'.*

Then, the following holds:

$$\left|\Pr\left[b' = 1 | b = 0\right] - \Pr\left[b' = 1 | b = 1\right]\right| \le 2\sqrt{\frac{6q}{d}}. \tag{183}$$

In fact, the trace distance between two distributions $(\nu, |\mu_0\rangle, |\mu_1\rangle, U^{(0)})$ and $(\nu, |\mu_0\rangle, |\mu_1\rangle, U^{(1)})$ is at most $2\sqrt{\frac{6q}{d}}$ where U and U' are perfectly given as their classical description.

The following fact is (implicitly) used in this section multiple times.

6.3 Preparation II: Simulations

We occasionally consider that the algorithms or oracles have perfect knowledge of quantum states or unitaries, *without hurting the algorithm's behavior*. This section explains the classical simulation or descriptions of quantum objects. Here and below, we fix a way to express (unnormalized) pure quantum states $|\phi\rangle$ and unitary U by classical strings $\mathsf{str}(|\phi\rangle)$ and $\mathsf{str}(U)$—for example by the amplitudes of the state or matrix that describes the unitary.

We define the classical simulation of the unitary oracle U with the classical-input access as follows.

Definition 6.5. *Let U be a $d \times d$ unitary. We define a classical simulation oracle $\mathsf{Sim}(U)$ with the classical-input queries that are defined as follows:*

- *It maintains a list T of tuples of two strings representing quantum states, initialized by $T = \emptyset$.*
- *For the j-th query $x_j \in \{0, ..., d-1\}$, it does:*
  - *If there is* no *$\ell < j$ such that $(x_\ell, \mathsf{str}(|\psi_\ell\rangle))$ in T, it defines $|\psi_j\rangle := U|x_j\rangle$ and returns $\mathsf{str}(|\psi_j\rangle)$. It appends $(x_j, \mathsf{str}(|\psi_j\rangle))$ at the end of T.*
  - *If there is $\ell < j$ such that $(x_\ell, \mathsf{str}(|\psi_\ell\rangle))$ in T, it returns $\mathsf{str}(|\psi_\ell\rangle)$. It samples a new $x' \in \{0, ..., d-1\}$ where there is no $\ell < j$ satisfying the above condition, and appends $(x', \mathsf{str}(U|x'\rangle))$ at the end of T.* [13]

The list T after the j-th query is denoted by

$$T_j = \{(x_j, \mathsf{str}(|\psi_i\rangle))\}_{i\in[j]}. \tag{184}$$

We define $X_j := \mathrm{span}(|x_1\rangle, ..., |x_j\rangle)$ and $\Psi_j := \mathrm{span}(|\psi_1\rangle, ..., |\psi_j\rangle)$.

[13] This step is to maintain the same size of the list.

Lemma 6.6. *Let $\mathcal{A}^W$ be an oracle algorithm that only makes classical-input queries to W. Then, there exists an oracle algorithm $\mathsf{Sim}(\mathcal{A})^{\mathsf{Sim}(W)}$ with the same number of queries whose output is identical to $\mathcal{A}^W$. In particular,* $\Pr[\mathcal{A}^W \to 1] = \Pr[\mathsf{Sim}(\mathcal{A})^{\mathsf{Sim}(W)} \to 1]$.

Proof. We define $\mathcal{B} := \mathsf{Sim}(\mathcal{A})$ as follows:

- It runs $\mathcal{A}$, but when $\mathcal{A}$ makes the j-th query x_j to W, $\mathcal{B}$ makes query x_j to $\mathsf{Sim}(W)$ and obtain $\mathsf{str}(|\psi_j\rangle)$. It recovers $|\psi_j\rangle$ and returns to $\mathcal{A}$ as the output of the j-th query.
- If $\mathcal{A}$ terminates, $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs.

From the perspective of $\mathcal{A}$, the oracle answers are always identical, proving the lemma. $\square$

6.4 Security Proof

Given the lemmas, we will prove Theorem 6.2. In other words, we will prove Equation (180).

Proof of Theorem 6.2. We call the algorithms in the real world when accessing the oracles V_k^U, $(U, U^\dagger)$, and in the ideal world when accessing W, $(U, U^\dagger)$. Below, we occasionally write U to denote the oracle access to both U and $U^\dagger$. We let $\mathcal{B} := \mathsf{Sim}(\mathcal{A})$ and prove the indistinguishability with respect to the simulation algorithm $\mathcal{B}$ with the simulated oracle $\mathsf{Sim}(W)$ or $\mathsf{Sim}(V_k^U)$.

Recall $\mathcal{B}$ maintains the list T; after the j-th pure state query, we write

$$T_j = \{x_j, \mathsf{str}(|\psi_i\rangle))\}_{i\in[j]} \tag{185}$$

to denote the current T, where it holds $|\psi_i\rangle = W\,|x_i\rangle$ in the ideal world, and

$$|\psi_i\rangle = V_k^U\,|x_i\rangle = X^{k_1} \circ U \circ X^{k_0}\,|x_i\rangle \tag{186}$$

for some k in the real-world experiment for $i \in [j]$.

We write $\Pi_{i=1}^j f_i$ to denote $f_1 \circ ... \circ f_j$; the order is important because we use the notation Π for the product of unitary operations. Following [ABKM22, pp. 9-10], for any unitary U, we define:

$$\overrightarrow{Q}_{T_j,U,k} := \prod_{i=1}^{j} \mathrm{SWAP}_{X^{k_0}|x_i\rangle, U^\dagger\circ(X^{k_1})^\dagger|\psi_i\rangle}, \qquad \overrightarrow{S}_{T_j,U,k} := \prod_{i=1}^{j} \mathrm{SWAP}_{UX^{k_0}|x_i\rangle,(X^{k_1})^\dagger|\psi_i\rangle}, \tag{187}$$

and define

$$U_{T_j,k} = [U]_{T_j,k} := U \circ \overrightarrow{Q}_{T_j,U,k} \tag{188}$$

for unitaries U. For any $|x_1\rangle, |x_2\rangle, |y_1\rangle, |y_2\rangle$ and U, $\mathrm{SWAP}_{U|x_1\rangle,U|y_1\rangle} \circ U \circ \mathrm{SWAP}_{|x_2\rangle,|y_2\rangle}$ equals to

$$\mathrm{SWAP}_{U|x_1\rangle,U|y_1\rangle} \circ \mathrm{SWAP}_{U|x_2\rangle,U|y_2\rangle} \circ U = U \circ \mathrm{SWAP}_{|x_1\rangle,|y_1\rangle} \circ \mathrm{SWAP}_{|x_2\rangle,|y_2\rangle}, \tag{189}$$

which gives

$$U_{T_j,k} = \overrightarrow{S}_{T_j,U,k} \circ U. \tag{190}$$

We divide the execution of $\mathcal{B}$ into $p+1$ phases $P_0, ..., P_p$ where P_i describes the execution between the i-th and $(i+1)$-st queries to the first oracle; P_0 corresponds to the execution before the first pure state query. Let q_j denote the expected query number of B to the second oracle during P_j. It holds that $q = \sum_{j=0}^{p} q_j$.

We define the following sequences of experiments:

$$\mathbf{H}_{j,0}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{V_k^U, U_{T_j,k},}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^U, \cdots, V_k^U, U_{T_j,k}}_{P_{j+2},\ldots,P_p} \tag{191}$$

$$\mathbf{H}_{j,1}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{V_k^{U_j}, [U_j]_{T_j,k},}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^{U_j}, \cdots, V_k^{U_j}, [U_j]_{T_j,k}}_{P_{j+2},\ldots,P_p} \tag{192}$$

$$\mathbf{H}_{j,2}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{W, U_{T_{j+1},k},}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^{U_j}, \cdots, V_k^{U_j}, U_{T_{j+1},k}}_{P_{j+2},\ldots,P_p} \tag{193}$$

$$\mathbf{H}_{j,3}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{W, U_{T_{j+1},k},}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^U, \cdots, V_k^U, U_{T_{j+1},k}}_{P_{j+1},\ldots,P_p} \tag{194}$$

$$\mathbf{H}_{j+1,0}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{W, U,}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^U, \cdots, V_k^U, U_{T_{j+1},k}}_{P_{j+1},\ldots,P_p} \tag{195}$$

where U_j will be specified later in the proof of Claim 2 where its actual definition is used. The characters (with super/subscripts) in the descriptions of hybrids denote:

U**:** It denotes the phases $P_0, \ldots, P_p$ that may contain multiple queries to the unitary U.

V, W**:** They denote a *single* pure state query to the corresponding *simulation* oracle $\mathsf{Sim}(V)$ or $\mathsf{Sim}(W)$. Recall the oracles also store the query list T. If the j-th query input $|x_j\rangle$ coincides with the previous ℓ-th query for some $\ell < j$, the simulation oracle returns $|\psi_\ell\rangle$ *without making the actual query.*[14]

Note that $\mathbf{H}_{0,0}$ and $\mathbf{H}_{p,0}$ correspond to the real- and ideal-world experiments, respectively.

We write $\mathcal{B}(\mathbf{H}_{j,k})$ to denote the algorithm with the hybrid experiment $\mathbf{H}_{j,k}$. We will prove the following claims, which correspond (parts of) [ABKM22, Lemma 6,7]. Note that in Claim 3 we connect the hybrid $\mathbf{H}_{j,1}$ and $\mathbf{H}_{j,3}$ and $\mathbf{H}_{j,2}$ appears as an intermediate hybrid in between.

Claim 1. $|\Pr[\mathcal{B}(\mathbf{H}_{j,3}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j+1,0}) \to 1]| \le 4q_{j+1}\sqrt{6p^2/d}$ for $j = 0, \ldots, p-1$.

Claim 2. $|\Pr[\mathcal{B}(\mathbf{H}_{j,0}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j,1}) \to 1]| \le 2\sqrt{6q/d}$ for $j = 0, \ldots, p-1$.

Claim 3. $|\Pr[\mathcal{B}(\mathbf{H}_{j,1}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j,3}) \to 1]| \le 4\sqrt{p/d}$ for $j = 0, \ldots, p-1$.

We prove these claims later. Given these claims, we prove our main result as follows.

$$|\Pr[\mathcal{B}(\mathbf{H}_{0,0}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{p,0}) \to 1]| \tag{196}$$

$$\le \sum_{j=0}^{p-1} \left(4q_{j+1}\sqrt{\frac{6p^2}{d}} + 2\sqrt{\frac{6q}{d}} + 4\sqrt{\frac{p}{d}} \right) \tag{197}$$

$$\le 4q\sqrt{\frac{6p^2}{d}} + 2p\sqrt{\frac{6q}{d}} + 4p\sqrt{\frac{p}{d}} \tag{198}$$

$$= O\left(\sqrt{\frac{p^3 + p^2q^2}{d}} \right). \tag{199}$$

This proves the desired result. □

[14] For example, even if $|\psi_\ell\rangle = W|x_\ell\rangle$ holds and the j-th oracle query is to V_k^U, the oracle returns the stored output $|\psi_\ell\rangle$. This resembles the assumptions that no same queries are made in the (classical or post-quantum) random oracle/permutations.

Proof of Claim 1. Recall this claim compares the following two hybrids:

$$\mathbf{H}_{j,3}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{W, U_{T_{j+1},k},}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^U, \cdots, V_k^U, U_{T_{j+1},k}}_{P_{j+1},\ldots,P_p} \tag{200}$$

$$\mathbf{H}_{j+1,0}: \underbrace{U, W, U, \cdots, W, U,}_{P_0,\ldots,P_j} \quad \underbrace{W, U,}_{(j+1)\text{-st pure state query and } P_{j+1}} \quad \underbrace{V_k^U, \cdots, V_k^U, U_{T_{j+1},k}}_{P_{j+1},\ldots,P_p} \tag{201}$$

Note that the only difference between the two hybrids is the second oracle in the phase P_{j+1}. We define the following distinguisher $\mathcal{D}$ using $\mathcal{B}$ to invoke the unitary reprogramming lemma (Lemma 6.3):

Phase 1: $\mathcal{D}$ samples Haar random unitary U and defines a unitary

$$F_0 = F = |0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U^\dagger. \tag{202}$$

It defines the following algorithm:

$\mathcal{C}$**:** It samples Haar random unitary W and $k \leftarrow \mathcal{K}$. It runs $\mathcal{B}$ by answering the queries to the second oracles using U and one to the first oracles using $\mathsf{Sim}(W)$, until after answering the $(j+1)$-st query to the first oracle with the intermediate state ρ. Until this point, $\mathcal{D}$ gets the list

$$T_{j+1} = \{(x_i, \mathsf{str}(|\psi_i\rangle))\}_{i\in[j+1]} \tag{203}$$

of the input-output states to W. It then computes S and U_S such that

$$F_1 = F \circ U_S = |0\rangle\langle 0| \otimes U_{T_{j+1},k} + |1\rangle\langle 1| \otimes U_{T_{j+1},k}^\dagger \tag{204}$$

holds by choosing $U_S := |0\rangle\langle 0| \otimes \overrightarrow{Q}_{T_j,U,k} + |1\rangle\langle 1| \otimes \overrightarrow{Q}_{T_j,U,k}^\dagger$.
Explicitly, the following choice of S suffices by definition of $U_{T_{j+1},k}$ and Equation (190):

$$\{|0\rangle \otimes X^{k_0}|x_i\rangle, |0\rangle \otimes U^\dagger \circ (X^{k_1})^\dagger|\psi_i\rangle, |1\rangle \otimes UX^{k_0}|x_i\rangle, |1\rangle \otimes (X^{k_1})^\dagger|\psi_i\rangle\}_{i=1}^{j+1}. \tag{205}$$

We define the following subsets:

$$S_{00} := \{|0\rangle \otimes X^{k_0}|x_i\rangle\}_{i=1}^{j+1}, \qquad S_{01} := \{|0\rangle \otimes U^\dagger \circ (X^{k_1})^\dagger|\psi_i\rangle\}_{i=1}^{j+1}, \tag{206}$$

$$S_{10} := \{|1\rangle \otimes UX^{k_0}|x_i\rangle\}_{i=1}^{j+1}, \qquad S_{11} := \{|1\rangle \otimes (X^{k_1})^\dagger|\psi_i\rangle\}_{i=1}^{j+1}. \tag{207}$$

Phase 2: $\mathcal{C}$ is executed and outputs S and ρ, and $\mathcal{D}$ is given quantum access to F_b. $\mathcal{D}$ resumes running $\mathcal{B}$ given ρ, by answering the queries using F_b. When $\mathcal{B}$ makes the $(j+2)$-nd pure-state query, this phase is finished.

Phase 3: $\mathcal{D}$ is now given the classical string specifying k, W, T_{j+1}. $\mathcal{D}$ resumes running $\mathcal{B}$, answering the queries to the first oracle using $\mathsf{Sim}(V_k^U)$ (with the list T_{j+1}) and the queries to the second oracle using $U_{T_{j+1},k}$. Finally, $\mathcal{D}$ outputs whatever $\mathcal{B}$ outputs.

This distinguisher $\mathcal{D}$ fits in Lemma 6.3. Also, if $b = 0$, the distinguisher accesses the oracle exactly as in $\mathbf{H}_{j+1,0}$, whereas $b = 1$ gives $\mathbf{H}_{j,3}$.

The expected number of queries in Phase 2 is exactly the expected number of queries in P_{j+1}, that is, q_{j+1}. To bound ϵ, note that the last register of each vector in S, described in Equation (205), is applied by 1-design unitaries over random k. We will show that the following inequality holds:

$$\mathop{\mathbb{E}}_{\mathcal{C}}\left[\|\Pi_{\mathcal{S}}|\phi\rangle\|^2\right] \le \frac{12p^2}{d}. \tag{208}$$

The claim is followed by the unitary reprogramming lemma. $\square$

Proof of Equation (208). For any $b, c \in \{0,1\}$, S_{bc} is the set of $j+1$ orthonormal states. Let Π_{bc} and Π_b be the projections to the span of S_{bc} and $S_{b0} \cup S_{b1}$. Also note that the states in $S_{00} \cup S_{01}$ and the states in $S_{10} \cup S_{11}$ are orthogonal. Thus it holds that

$$\|\Pi_{\mathcal{S}} |\phi\rangle\|^2 = \|\Pi_0 |\phi\rangle\|^2 + \|\Pi_1 |\phi\rangle\|^2 \tag{209}$$

and we bound each term. Below, we give the upper bound of $\|\Pi_0 |\phi\rangle\|^2$, and the same argument gives the same upper bound for $\|\Pi_1 |\phi\rangle\|^2$.

Note that $\Pi_0 \Pi_{0b} = \Pi_{0b}$. The following can be easily verified:

$$\Pi_0^2 = (\Pi_0 - \Pi_{00} - \Pi_{01})^2 + (\Pi_{00} - \Pi_{01})^2 \tag{210}$$

which gives

$$\begin{aligned}
\|\Pi_0 |\phi\rangle\|^2 &= \|(\Pi_0 - \Pi_{00} - \Pi_{01}) |\phi\rangle\|^2 + \|(\Pi_{00} - \Pi_{01}) |\phi\rangle\|^2 && (211)\\
&\le \|\Pi_{00}(\Pi_0 - \Pi_{00} - \Pi_{01}) |\phi\rangle\|^2 + \|(\Pi_0 - \Pi_{00})(\Pi_0 - \Pi_{00} - \Pi_{01}) |\phi\rangle\|^2 && (212)\\
&\quad + (\|\Pi_{00} |\phi\rangle\| + \|\Pi_{01} |\phi\rangle\|)^2 && (213)\\
&= \|\Pi_{00}\Pi_{01} |\phi\rangle\|^2 + \|(\Pi_0 - \Pi_{00})(\Pi_0 - \Pi_{01}) |\phi\rangle\|^2 + (\|\Pi_{00} |\phi\rangle\| + \|\Pi_{01} |\phi\rangle\|)^2 && (214)\\
&\le \|\Pi_{00}\Pi_{01}\|_2^2 + \|(\Pi_0 - \Pi_{00})(\Pi_0 - \Pi_{01})\|_2^2 + 2\|\Pi_{00} |\phi\rangle\|^2 + 2\|\Pi_{01} |\phi\rangle\|^2 && (215)
\end{aligned}$$

where the first equality is obtained by considering $\langle\phi| (\cdot) |\phi\rangle$ on Equation (210), and the inequality holds because 1) we decompose the first term by the range of Π_{00} and $(\Pi_0 - \Pi_{00})$, and 2) we apply the triangle inequality on the second term. In the last inequality, we use the property of the matrix 2-norm and $(a+b)^2 \le 2a^2 + 2b^2$. Using this inequality, we will prove that, using $j \le p-1$,

$$\mathop{\mathbb{E}}_{\mathcal{C}} \|\Pi_0 |\phi\rangle\|^2 = \frac{2(j+1)^2 + 4(j+1)}{d} \le \frac{6p^2}{d}. \tag{216}$$

By similarly bounding $\mathbb{E}\, \|\Pi_1 |\phi\rangle\|^2$, we have the inequality $\|\Pi_{\mathcal{S}} |\phi\rangle\|^2 \le \frac{12p^2}{d}$, which concludes the proof of Equation (208).

Recall that $|\psi_i\rangle = W |x_i\rangle$ for all i. For convenience, write $S_{00} = \{|a_1\rangle, ..., |a_{j+1}\rangle\}$ and $S_{01} = \{|b_1\rangle, ..., |b_{j+1}\rangle\}$ where $|a_i\rangle := |0\rangle \otimes X^{k_0} |x_i\rangle \in S_{00}$ and $|b_\ell\rangle := |0\rangle \otimes U^\dagger (X^{k_1})^\dagger W |x_\ell\rangle \in S_{01}$. For any $i, \ell \in \{1, ..., j+1\}$, it holds that

$$\mathop{\mathbb{E}}_{k} \| |a_i\rangle \langle a_i| \cdot |b_\ell\rangle \langle b_\ell| \|_2^2 = \mathop{\mathbb{E}}_{k} |\langle b_\ell | a_i\rangle|^2 = \mathop{\mathbb{E}}_{k} |\langle x_\ell| W^\dagger X^{k_1} U X^{k_0} |x_i\rangle|^2 = \frac{1}{d} \tag{217}$$

because $\mathbb{E}_k[X^{k_0} |x_i\rangle \langle x_i| (X^{k_0})^\dagger] = I/d$.

We now give the upper bounds on the terms in Equation (215) in expectation over W, k, which are randomness chosen by $\mathcal{C}$. The third and last terms can be bounded by $2(j+1)/d$ each easily.

Note that S_{0b} is an orthonormal set for $b = 0, 1$, thus $\Pi_{00} = \sum |a_i\rangle \langle a_i|$, $\Pi_{01} = \sum |b_i\rangle \langle b_i|$. It holds that

$$\begin{aligned}
\mathop{\mathbb{E}}_{k} \|\Pi_{00}\Pi_{01}\|_2^2 &= \mathop{\mathbb{E}}_{k} \Big\| \sum_{1 \le i, \ell \le j+1} |a_i\rangle \langle a_i| \cdot |b_\ell\rangle \langle b_\ell| \Big\|_2^2 && (218)\\
&\le \mathop{\mathbb{E}}_{k} \sum_{1 \le i, \ell \le j+1} \| |a_i\rangle \langle a_i| \cdot |b_\ell\rangle \langle b_\ell| \|_2^2 = \frac{(j+1)^2}{d} && (219)
\end{aligned}$$

where we use $\|A+B\|_2 \le \max(\|A\|_2, \|B\|_2) \le \sqrt{\|A\|_2^2 + \|B\|_2^2}$ for two orthogonal projectors A, B such that $AB = 0$, and $\|AB\|_2 = \|BA\|_2$ for two matrices. This gives an upper bound on the first term.

For the second term, note that $\|(\Pi_0 - \Pi_{00})(\Pi_0 - \Pi_{01})\|_2 = \|\Pi_{01}\Pi_{00}\|_2$ is well-known[15] if their ranges have only a trivial intersection $\{0\}$, which happens with probability 1. This gives the same upper bound on the second term. $\square$

Proof of Claim 2. Recall this claim compares the following two hybrids:

$$\mathbf{H}_{j,0} : \underbrace{U, W, U, \cdots, W, U}_{P_0,\ldots,P_j}, \qquad \underbrace{V_k^{U}, U_{T_j,k}}_{(j+1)\text{-st pure state query and } P_{j+1}}, \qquad \underbrace{V_k^{U}, \cdots, V_k^{U}, U_{T_j,k}}_{P_{j+2},\ldots,P_p} \tag{220}$$

$$\mathbf{H}_{j,1} : \underbrace{U, W, U, \cdots, W, U}_{P_0,\ldots,P_j}, \qquad \underbrace{V_k^{U_j}, [U_j]_{T_j,k}}_{(j+1)\text{-st pure state query and } P_{j+1}}, \qquad \underbrace{V_k^{U_j}, \cdots, V_k^{U_j}, [U_j]_{T_j,k}}_{P_{j+2},\ldots,P_p} \tag{221}$$

Note that U_j is yet to be defined; we will define U_j by $U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$ for some d-dimensional qudit states $|\mu_0\rangle, |\mu_1\rangle$. The only difference between the two hybrids is that the unitary U in $\mathbf{H}_{j,0}$ from the $(j+1)$-st phase is replaced by U_j in $\mathbf{H}_{j,1}$.

We define the following distinguisher $\mathcal{D}$ using $\mathcal{B}$ to invoke Lemma 6.4:

Phase 1: $\mathcal{D}$ samples a d-dimensional Haar unitary W and specifies the following two distributions of $|\mu_0\rangle, |\mu_1\rangle$:

$$D_0^{\mu} := \{|0\rangle, \ldots, |d-1\rangle\}, \tag{222}$$
$$D_1^{\mu} := \{d\text{-dimensional pure states}\}. \tag{223}$$

Given access to a d-dimensional Haar random unitary $U^{(0)} := U$, $\mathcal{D}$ runs $\mathcal{B}^{\mathsf{Sim}(W), U}$ until $\mathcal{B}$ asks the $(j+1)$-st query x_{j+1} to $\mathsf{Sim}(W)$. This phase is finished before answering this query. Until this point, $\mathcal{D}$ gets the list $T_j = ((x_i, \mathsf{str}(|\psi_i\rangle)))_{i\in[j]}$ of the input-output states to W.

Phase 2: Samples $|\mu_0\rangle \leftarrow D_0^{\mu}$, i.e., $\mu_0 \leftarrow \{0, \ldots, d-1\}$, and $|\mu_1\rangle \leftarrow D_1^{\mu}$ and $b \leftarrow \{0,1\}$. Now $\mathcal{D}$ got the $(j+1)$-st query $|x_{j+1}\rangle$ for some $x_{j+1} \in \{0, \ldots, d-1\}$. $\mathcal{D}$ defines k so that $X^{k_0}|x_{j+1}\rangle = |\mu_0\rangle$ and randomly chooses k_1. Given oracle access to $U^{(b)}$, $\mathcal{D}$ resumes running $\mathcal{B}$, answering the remaining queries to the first oracle using $V_k^{U^{(b)}}$ and the remaining queries to the second oracle using $[U^{(b)}]_{T_j,k}$. In particular, the $(j+1)$-st query x_{j+1} to the first oracle is answered by $U|\mu_1\rangle$.

The distinguisher fits in Lemma 6.4. Also, by defining $U_j := U^{(1)}$, the case of $b = 0$ corresponds to $\mathbf{H}_{j,0}$ and $b = 1$ corresponds to $\mathbf{H}_{j,1}$, respectively. Since $\mathbb{E}|\mu_i\rangle\langle\mu_i| = I/d$ holds for $i = 0, 1$, the unitary resampling lemma proves the claim, where the number of queries in the first phase is $q_0 + \ldots + q_j \le q$. $\square$

Proof of Claim 3. We consider the following variations of the second phase of the experiment in the proof of Claim 2, where we highlight the changed parts by red and the omitted parts are identical to Phase 2:

Phase 2-1: Samples $|\mu_0\rangle \leftarrow D_0^{\mu}$ and $|\mu_1'\rangle \leftarrow D_1^{\mu}$ and $b \leftarrow 1$. Define $|\mu_1\rangle := \frac{(I - \Pi_{U^\dagger(\Psi_j)})|\mu_1'\rangle}{\|(I - \Pi_{U^\dagger(\Psi_j)})|\mu_1'\rangle\|}$. Here $\Phi_j = \mathrm{span}(|\psi_1\rangle, \ldots, |\psi_j\rangle)$ as defined in Definition 6.5.

[15] It can be proven as follows. Let R_0, R_{00}, R_{01} be the ranges of the projectors $\Pi_0, \Pi_{00}, \Pi_{01}$. Then it holds that $R_0 = R_{00} \oplus R_{01} = R_{01}^{\perp} \oplus R_{01} = R_{01}^{\perp} \oplus R_{00}^{\perp}$, which implies that there exist unitary U_0, U_1 such that $U_0 : R_{00} \to R_{01}^{\perp}$ and $U_1 : R_{01} \to R_{00}^{\perp}$. For $U = U_0 \oplus U_1$, it holds that $\Pi_0 - \Pi_{00} = U\Pi_{01}U^\dagger$ and vice versa, which proves $\|(\Pi_0 - \Pi_{00})(\Pi_0 - \Pi_{01})\|_2 = \|U\Pi_{01}U^\dagger U\Pi_{00}U^\dagger\|_2 = \|\Pi_{01}\Pi_{00}\|$.

Phase 2-2: Samples $|\mu_0\rangle \leftarrow D_0^\mu$ and $|\mu_1\rangle$ is defined by $U^\dagger W |x_{j+1}\rangle$ and $b \leftarrow 1$. ... In particular, the $(j+1)$-st query x_{j+1} to the first oracle is answered by $U|\mu_1\rangle = W|x_{j+1}\rangle$.

Phase 2-3: Samples $|\mu_0\rangle \leftarrow D_0^\mu$ and $|\mu_1\rangle$ is defined by $U^\dagger W |x_{j+1}\rangle$ and $b \leftarrow 1$. ... answering the remaining queries to the first oracle using $V_k^{U^{(1)}}(I - \Pi_{\mathrm{span}(|x_{j+1}\rangle,(X^{k_0})^\dagger|\mu_1\rangle)})$ and the remaining queries to the second oracle using $[U^{(1)}]_{T_j,k}$. The $(j+1)$-st query x_{j+1} to the first oracle is answered by $U|\mu_1\rangle = W|x_{j+1}\rangle$.

Phase 2-4: Samples $|\mu_0\rangle \leftarrow D_0^\mu$ and $|\mu_1\rangle$ is defined by $U^\dagger W |x_{j+1}\rangle$ and $b \leftarrow 1$. ... answering the remaining queries to the first oracle using $V_k^{U^{(0)}}$ and the remaining queries to the second oracle using $[U^{(1)}]_{T_j,k}$.

We write $\mathbf{H}_{j,1}^{(1)}$,..., $\mathbf{H}_{j,1}^{(4)}$ to denote these changed hybrids. In Phase 2-3, we only change the output $|\psi\rangle$ according to the oracle's answers in the list T.

- Note that $\mathbf{H}_{j,1}$ coincides with **Phase 2** with $b=0$, and $\mathbf{H}_{j,1}^{(1)}$ only differs the projective measurement. We think $\mathbf{H}_{j,1}^{(1)}$ as applying the projection $(I - \Pi_{U^\dagger(\Psi_j)})$ on $|\mu_1'\rangle$ *and proceeding conditioned on its success*. Note that $|\mu_1'\rangle$ is independent from U and the states in Ψ_j are orthogonal to each other. Thus, the projection fails with probability

$$\|\Pi_{U^\dagger(\Psi_j)}|\mu_1'\rangle\|^2 = \sum_{i=1}^{j} |\langle\psi_i| U |\mu_1'\rangle|^2 = \frac{j}{d} \le \frac{p}{d}. \tag{224}$$

  By the gentle measurement lemma, we have $|\Pr[\mathcal{B}(\mathbf{H}_{j,1}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j,1}^{(1)}) \to 1]| \le \sqrt{p/d}$.

- Phase 2-2 is identical to Phase 2-1 because $|\mu_1\rangle$ is uniformly distributed over $\mathsf{Im}(I - \Pi_{U^\dagger(\Psi_j)})$ in both cases. Note that this corresponds to

$$\mathbf{H}_{j,2} : \underbrace{U, W, U, \cdots, W, U}_{P_0,\dots,P_j}, \qquad \underbrace{W, U_{T_{j+1},k}}_{(j+1)\text{-st pure state query and } P_{j+1}}, \qquad \underbrace{V_k^{U_j}, \cdots, V_k^{U_j}, U_{T_{j+1},k}}_{P_{j+2},\dots,P_p}. \tag{225}$$

- For Phase 2-3, for any $x \in \{0,...,d-1\} \setminus \{x_{j+1}\}$, the expectation over U, W, k satisfies

$$\mathbb{E}\left|\langle\mu_1| X^{k_0} |x\rangle\right|^2 = \mathbb{E}\left|\langle x_{j+1}| U W^\dagger X^{k_0} |x\rangle\right|^2 = \frac{1}{d} \tag{226}$$

  which represents that the projection on input x fails. Therefore, by the quantum union bound (Lemma 2.7), we have

$$\left|\Pr[\mathcal{B}(\mathbf{H}_{j,1}^{(2)}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j,1}^{(3)}) \to 1]\right| \le \sqrt{\frac{p}{d}}. \tag{227}$$

- Finally, Phase 2-4 corresponds to

$$\mathbf{H}_{j,3} : \underbrace{U, W, U, \cdots, W, U}_{P_0,\dots,P_j}, \qquad \underbrace{W, U_{T_{j+1},k}}_{(j+1)\text{-st pure state query and } P_{j+1}}, \qquad \underbrace{V_k^{U}, \cdots, V_k^{U}, U_{T_{j+1},k}}_{P_{j+2},\dots,P_p}. \tag{228}$$

  Since V_k^U and $V_k^{U_j}$ are identical in $\mathsf{Im}(\Pi_{\mathrm{span}(|x_{j+1}\rangle,(X^{k_0})^\dagger|\mu_1\rangle)})$, the same argument above shows that

$$\left|\Pr[\mathcal{B}(\mathbf{H}_{j,1}^{(3)}) \to 1] - \Pr[\mathcal{B}(\mathbf{H}_{j,1}^{(4)}) \to 1]\right| \le \sqrt{\frac{p}{d}}. \tag{229}$$

Combining the above, we prove the claim. □

6.5 Proof of Unitary Reprogramming Lemma

This section proves Lemma 6.3. We recall the statement below for convenience.

Lemma 6.7 (Unitary reprogramming lemma). *Let $\mathcal{D}$ be a distinguisher in the following experiment:*

Phase 1: *$\mathcal{D}$ outputs a unitary $F_0 = F$ over m-qubit and a quantum algorithm $\mathcal{C}$ whose output is a quantum state ρ and a classical string that specifies a classical description of the following data: a set S of m-qubit pure states and a unitary U_S such that, for the span $\mathcal{S}$ of all states in S, U_S acts as the identity on the image of $I - \Pi_{\mathcal{S}}$, where $\Pi_{\mathcal{S}}$ is the projection to $\mathcal{S}$. Let*

$$\epsilon := \sup_{|\phi\rangle : m\text{-qubit state}} \mathop{\mathbb{E}}_{\mathcal{C}} \left[\|\Pi_{\mathcal{S}} |\phi\rangle\|^2 \right]. \tag{230}$$

Phase 2: *$\mathcal{C}$ is executed and outputs ρ, S and U_S. Let $F_1 := F \circ U_S$. A bit b is chosen uniformly at random, and $\mathcal{D}$ is given ρ and quantum access to F_b and makes q queries in expectation if $b = 0$, and sends the quantum state ν_b to the next phase.*

Phase 3: *$\mathcal{D}$ loses access to F_b and receives ν_b and the classical string specifying the classical descriptions S and U_S outputted by $\mathcal{C}$ in the second phase. Finally, $\mathcal{D}$ outputs a guess b'.*

Then, it holds that

$$|\Pr[\mathcal{D} \to 1 | b = 1] - \Pr[\mathcal{D} \to 1 | b = 0]| \le q \cdot \sqrt{2\epsilon}. \tag{231}$$

In fact, the trace distance $\mathsf{TD}(\nu_0, \nu_1)$ between two cases after Phase 2 is at most $q\sqrt{2\epsilon}$.

Proof. Let $\mathcal{M}_{\mathbf{C}}(\rho_{\mathbf{AC}}) = |0\rangle\langle 0|_C \rho_{\mathbf{AC}} |0\rangle\langle 0|_C + |1\rangle\langle 1|_C \rho_{\mathbf{AC}} |1\rangle\langle 1|_C$ for a single-qubit register C and arbitrary ancillary register $\mathbf{A}$. Let F be a unitary over $\{0,1\}^m$. The controlled version of F is defined by

$$cF = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes F \tag{232}$$

so that $cF : |c\rangle|x\rangle \mapsto |c\rangle F^c |x\rangle$.[16] The execution of $\mathcal{D}$ can be described by

$$(\Phi \circ cF \circ \mathcal{M}_C)^{q_{\max}} \tag{233}$$

which is applied to some initial state ρ where $q_{\max}$ is the upper bound of the number of queries and Φ is an arbitrary quantum channel.[17] Let $\Gamma_b = \Phi \circ cF_b \circ \mathcal{M}_C$ and define

$$\rho_k := (\Gamma_1^{q_{\max}-k} \circ \Gamma_0^k)(\rho) \tag{234}$$

which corresponds to the final state where the first k queries are answered by cF_0, and the remaining queries are answered by cF_1. The intermediate state after the k-th query is denoted by $\rho_k^{(0)} := \Gamma_0^k(\rho)$. The final state of the algorithm using the F_0 (or F_1) oracle entirely is ρ_0 ($\rho_{q_{\max}}$, respectively). We also define $p_k := \mathrm{Tr}\left[|1\rangle\langle 1|_C \rho_k^{(0)}\right]$ to represent the probability that the oracle query is made in the $(k+1)$-th iteration for $0 \le k < q_{\max}$.

[16] The controlled queries reflect the expected number of queries. See [ABKM22, Section 4.1] for a more detailed discussion.

[17] Each layer may have different channels $\Phi_1, \ldots, \Phi_{q_{\max}}$. The standard argument with the counter, i.e. $\Phi = \sum_{j=1}^{q_{\max}} |j\rangle\langle j-1| \otimes \Phi_j$ allows us to use a single channel Φ without loss of generality.

We give an upper bound

$$\mathop{\mathbb{E}}_{r}\left[\mathsf{TD}\left(|r\rangle\langle r|\otimes\rho_{q_{\max}},|r\rangle\langle r|\otimes\rho_{0}\right)\right]\leq q\sqrt{2\epsilon} \tag{235}$$

where r is the randomness used by $\mathcal{C}$. Note that $cF_0^\dagger\circ cF_1 = cU_S$. By the monotonicity of TD under quantum channels, for any r we have

$$\begin{aligned}\mathsf{TD}\left(|r\rangle\langle r|\otimes\rho_{k},|r\rangle\langle r|\otimes\rho_{k-1}\right) &\leq \mathsf{TD}\left(cF_0\circ\mathcal{M}_C\left(\rho_{k-1}^{(0)}\right),cF_1\circ\mathcal{M}_C\left(\rho_{k-1}^{(0)}\right)\right) &(236)\\ &= \mathsf{TD}\left(\mathcal{M}_C\left(\rho_{k-1}^{(0)}\right),cU_S\circ\mathcal{M}_C\left(\rho_{k-1}^{(0)}\right)\right). &(237)\end{aligned}$$

We can write

$$cU_S\circ\mathcal{M}_C\left(\rho_{k-1}^{(0)}\right) = U_S\left(|1\rangle\langle 1|_C\,\rho_{k-1}^{(0)}\,|1\rangle\langle 1|_C\right)+|0\rangle\langle 0|_C\,\rho_{k-1}^{(0)}\,|0\rangle\langle 0|_C\,, \tag{238}$$

thus Equation (237) can be written as

$$\begin{aligned}&\mathsf{TD}\left(|1\rangle\langle 1|_C\,\rho_{k-1}^{(0)}\,|1\rangle\langle 1|_C\,,U_S\left(|1\rangle\langle 1|_C\,\rho_{k-1}^{(0)}\,|1\rangle\langle 1|_C\right)\right) &(239)\\ &= p_{k-1}\cdot\mathsf{TD}\left(\sigma_{k-1},U_S(\sigma_{k-1})\right) &(240)\end{aligned}$$

where we recall $p_{k-1}=\mathrm{Tr}\left[|1\rangle\langle 1|_C\,\rho_{k-1}^{(0)}\right]$ and define σ_{k-1} be the normalization of $|1\rangle\langle 1|_C\,\rho_{k-1}^{(0)}\,|1\rangle\langle 1|_C$. This gives

$$\begin{aligned}\mathop{\mathbb{E}}_{r}\left[\mathsf{TD}\left(|r\rangle\langle r|\otimes\rho_{q_{\max}},|r\rangle\langle r|\otimes\rho_{0}\right)\right] &\leq \sum_{k=1}^{q_{\max}}\mathop{\mathbb{E}}_{r}\left[\mathsf{TD}\left(|r\rangle\langle r|\otimes\rho_{q_k},|r\rangle\langle r|\otimes\rho_{k-1}\right)\right] &(241)\\ &\leq \sum_{k=1}^{q_{\max}}p_{k-1}\cdot\mathop{\mathbb{E}}_{S}\left[\mathsf{TD}\left(\sigma_{k-1},U_S(\sigma_{k-1})\right)\right] &(242)\\ &\leq q\cdot\sup_{\sigma}\mathop{\mathbb{E}}_{S}\left[\mathsf{TD}\left(\sigma,U_S(\sigma)\right)\right]. &(243)\end{aligned}$$

Using the fact that any mixed state is a convex combination of pure states and $\mathsf{TD}(|\phi\rangle,|\psi\rangle)=\sqrt{1-\langle\phi|\psi\rangle^2}=\|\,|\phi\rangle-|\psi\rangle\,\|_2/\sqrt{2}$, we have

$$\sup_{\sigma}\mathop{\mathbb{E}}_{r}\left[\mathsf{TD}(\sigma,U_S(\sigma))\right]\leq\sup_{|\phi\rangle}\mathop{\mathbb{E}}_{S}\left[\mathsf{TD}(|\phi\rangle,U_S|\phi\rangle)\right]=\frac{\sup_{|\phi\rangle}\mathbb{E}_S\left[\|\,|\phi\rangle-U_S|\phi\rangle\,\|_2\right]}{\sqrt{2}}\leq\sqrt{2\epsilon}. \tag{244}$$

Plugging Equation (244) into Equation (243) concludes the proof. The last inequality of Equation (244) is derived by, recalling the map U_S acts as the identity on the image of $I-\Pi_{\mathcal{S}}$,

$$\begin{aligned}&\mathop{\mathbb{E}}_{S}\left[\|\,|\phi\rangle-U_S|\phi\rangle\,\|_2\right] &(245)\\ &=\mathop{\mathbb{E}}_{S}\left[\|\Pi_{\mathcal{S}}|\phi\rangle-U_S\Pi_{\mathcal{S}}|\phi\rangle\,\|_2\right] &(246)\\ &\leq\mathop{\mathbb{E}}_{S}\left[\|\Pi_{\mathcal{S}}|\phi\rangle\,\|_2\right]+\mathop{\mathbb{E}}_{S}\left[\|U_S\Pi_{\mathcal{S}}|\phi\rangle\,\|_2\right] &(247)\\ &=2\mathop{\mathbb{E}}_{S}\left[\|\Pi_{\mathcal{S}}|\phi\rangle\,\|_2\right] &(248)\\ &\leq 2\sqrt{\mathop{\mathbb{E}}_{S}\left[\|\Pi_{\mathcal{S}}|\phi\rangle\,\|_2^2\right]}\leq 2\sqrt{\epsilon} &(249)\end{aligned}$$

for any $|\phi\rangle$, where we use Jensen's inequality in the last step. $\square$

6.6 Unitary Resampling Lemma

This section proves Lemma 6.4. We recall the statement below for convenience.

Lemma 6.8 (Unitary resampling lemma). *Let $\mathcal{D}$ be a distinguisher in the following experiment:*

Phase 1: *$\mathcal{D}$ specifies two distributions of d-dimensional qudit pure quantum states D_0^μ, D_1^μ such that $\mathbb{E}\left|\mu_i\right\rangle\left\langle\mu_i\right| = I/d$ for $i = 0, 1$. $\mathcal{D}$ makes at most q forward or inverse queries to a d-dimensional Haar random unitary $U^{(0)} := U$, and sends the quantum state ν to the next phase.*

Phase 2: *Sample $\left|\mu_0\right\rangle \leftarrow D_0^\mu, \left|\mu_1\right\rangle \leftarrow D_1^\mu$. A bit $c \in \{0, 1\}$ is uniformly chosen, and $\mathcal{D}$, given ν, is allowed to make arbitrarily many (forward or inverse) queries to an oracle that is either U if $b = 0$ or $U' := U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$ if $b = 1$. Finally, $\mathcal{D}$ outputs a bit b'.*

Then, the following holds:

$$\left|\Pr\left[b' = 1 | b = 0\right] - \Pr\left[b' = 1 | b = 1\right]\right| \leq 2\sqrt{\frac{2q}{d}}. \tag{250}$$

In fact, the trace distance between two distributions (ν, U) and (ν, U') is at most $2\sqrt{\frac{2q}{d}}$ where U and U' are perfectly given as their classical description.

Proof. We assume that the execution of the first phase of $\mathcal{D}$ can be described by[18]

$$\mathcal{D}_1^U := \Phi \circ U^{\pm 1} \circ \ldots \circ U^{\pm 1} \circ \Phi \circ U \circ \Phi \tag{251}$$

where Φ is an arbitrary quantum channel that may include the intermediate measurements.

We consider the following two continuous distributions:

$D_0(\nu_U, U)$**:** It samples a Haar random unitary U, $\left|\mu_0\right\rangle, \left|\mu_1\right\rangle$. It runs $\mathcal{D}_1^U$ on input $\left|0\right\rangle\left\langle 0\right|$ and obtains ν_U. Then it outputs (ν_U, U) where U specifies the full classical description of U.

$D_1(\nu_U, U')$**:** It samples a Haar random unitary U, $\left|\mu_0\right\rangle, \left|\mu_1\right\rangle$. It runs $\mathcal{D}_1^U$ on input $\left|0\right\rangle\left\langle 0\right|$ and obtains ν_U. Define $U' := U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$. Then it outputs (ν_U, U').

By the right-invariant property of Haar measure, the following distribution is identical to D_1:

$D_2(\nu_{U'}, U)$**:** It samples a Haar random unitary U, $\left|\mu_0\right\rangle, \left|\mu_1\right\rangle$. Define $U' := U \circ \mathrm{SWAP}_{\mu_0,\mu_1}$. It runs $\mathcal{D}_1^{U'}$ on input $\left|0\right\rangle\left\langle 0\right|$ and obtains $\nu_{U'}$. Then it outputs $(\nu_{U'}, U)$.

We will prove that for any U, the following two mixed states are close:

$$\mathsf{TD}\left(\nu_U, \nu_{U'}\right) \leq 2\sqrt{\frac{6q}{d}}. \tag{252}$$

Assuming this, we conclude the proof of the resampling lemma.

[18]Technically, multiple projective measurements may exist between two oracle queries, which cannot be deferred because of the pure state queries. The general case can be proven exactly the same way, and considering the general case only makes the description of $\mathcal{D}$ complicated.

Now we prove Equation (252). Let $S = \mathrm{span}(|\mu_0\rangle, |\mu_1\rangle)$. We first define the projection $P_+ := I - \Pi_S$. By the same analysis as in Equation (211), we can prove that

$$\mathop{\mathbb{E}}_{\mu_0,\mu_1}\left[\|\Pi_S |\phi\rangle\|_2^2\right] \leq \frac{6}{d}. \tag{253}$$

Also note that $U' = U \circ \mathrm{SWAP}_{\mu_0,\mu_1} = \mathrm{SWAP}_{U^{-1}|\mu_0\rangle, U^{-1}|\mu_1\rangle} \circ U$. We define $T = \mathrm{span}(U^{-1}|\mu_0\rangle, U^{-1}|\mu_1\rangle)$ and $P_- := I - \Pi_T$, which satisfies by the same reason:

$$\mathop{\mathbb{E}}_{\mu_0,\mu_1}\left[\|\Pi_T |\psi\rangle\|_2^2\right] \leq \frac{6}{d}. \tag{254}$$

Observe that

$$UP_+ |\phi\rangle = U'P_+ |\phi\rangle \text{ and } U^{-1}P_- |\psi\rangle = (U')^{-1}P_- |\psi\rangle \tag{255}$$

for any quantum states $|\phi\rangle, |\psi\rangle$. Therefore, we have

$$\mathsf{TD}\left(\nu_U, \nu_{U'}\right) \tag{256}$$
$$\leq \mathsf{TD}\left(\Phi \circ U^{\pm 1} \circ \ldots \circ U^{\pm 1} \circ \Phi(|0\rangle\langle 0|), \Phi \circ U^{\pm 1}P_\pm \circ \ldots \circ U^{\pm 1}P_\pm \circ \Phi(|0\rangle\langle 0|)\right) \tag{257}$$
$$+ \mathsf{TD}\left(\Phi \circ (U')^{\pm 1}P_\pm \circ \ldots \circ (U')^{\pm 1}P_\pm \circ \Phi(|0\rangle\langle 0|), \Phi \circ (U')^{\pm 1} \circ \ldots \circ (U')^{\pm 1} \circ \Phi(|0\rangle\langle 0|)\right) \tag{258}$$

where the terms in $U^{\pm 1}P_\pm$, $(U')^{\pm 1}P_\pm$ always have the same signs. The quantum union bound (Lemma 2.7) ensures that each term is bounded above by $\sqrt{6q/d}$. Thus we have

$$\mathsf{TD}\left(\nu_U, \nu_{U'}\right) \leq 2\sqrt{\frac{6q}{d}} \tag{259}$$

for any U. This proves Equation (252). $\square$

7 Breaking quantum-accessible PRFSG security

We prove that the constructions in this section are not quantum-accessible PRFSGs.

Theorem 7.1. *Let U be an n-qubit Haar random unitary given as an oracle and a, b be random n-bit strings. Then, X^aUX^b is not a quantum-accessible (nonadaptively-secure) PRFSGs in the QHRO model even without inverse access to the QHRO. More explicitly, a polynomial-time algorithm exists given non-adaptive oracle access to U and X^aUX^b that finds a, b with overwhelming probability.*

We also consider the random Pauli variant and prove the following theorem.

Theorem 7.2. *Let U be an n-qubit Haar random unitary given as an oracle and P be a random Pauli operator over n qubits. Then, UP is not a quantum-accessible (nonadaptively-secure) PRFSGs in the QHRO model even without inverse access to the QHRO. More explicitly, a polynomial-time algorithm exists given non-adaptive oracle access to U and UP that finds P with overwhelming probability.*

Before proceeding to the attack, we use the following variant of Simon's algorithm for quantum states.

Lemma 7.3. *Let $(|\xi_x\rangle)_{x\in\{0,1\}^n}$ be quantum states. Suppose that there exists $t\in\{0,1\}^n\setminus\{0^n\}$ such that $\langle\xi_x|\xi_{x\oplus t}\rangle=1$ for any $x\in\{0,1\}^n$ and there exists a constant $0\le c<1$ such that $|\langle\xi_x|\xi_{x'}\rangle|\le c$ if $x\oplus x'\notin\{0^n,t\}$. Suppose that there is an efficient algorithm A that prepares*

$$\frac{\sum_{x\in\{0,1\}^n}|x\rangle|\xi_x\rangle^{\otimes t}}{\sqrt{2^n}} \tag{260}$$

for t such that $c^t\le 2^{-2n+4}$. Then, there exists an algorithm that recovers t using $O(n)$ calls to A with overwhelming probability.

Proof. Consider the following subroutine

$$\begin{aligned}\frac{\sum_{x\in\{0,1\}^n}|x\rangle|\xi_x\rangle^{\otimes t}}{\sqrt{2^n}} &\mapsto \frac{\sum_{x,y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle|\xi_x\rangle^{\otimes t}}{2^n} &(261)\\ &=\frac{\sum_{y\in\{0,1\}^n}|y\rangle\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}|\xi_x\rangle^{\otimes t}}{2^n} &(262)\\ &=\frac{\sum_{y\in\{0,1\}^n}|y\rangle\sum_{x\in X}((-1)^{x\cdot y}+(-1)^{(x\oplus t)\cdot y})|\xi_x\rangle^{\otimes t}}{2^n} &(263)\end{aligned}$$

for $X\subset\{0,1\}^n$ of size 2^{n-1} such that $X\cup\{x\oplus t: x\in X\}=\{0,1\}^n$, where the first state is prepared by A then we apply the inverse QFT on the first register. Measuring the first n qubits, we obtain y such that $y\cdot t=0$. Specifically, the probability of obtaining y is,

$$\begin{aligned}&\left|\frac{\|2\sum_{x\in X}(-1)^{x\cdot y}|\xi_x\rangle^{\otimes t}\|^2}{4^n}-\frac{1}{2^{n-1}}\right| &(264)\\ &=\left|\frac{2^{n+1}+\sum_{x,x'\in X,x\ne x'}(-1)^{(x\oplus x')\cdot y}\langle\xi_x|\xi_{x'}\rangle^t}{4^n}-\frac{1}{2^{n-1}}\right| &(265)\\ &\le\sum_{x,x'\in X,x\ne x'}\frac{|\langle\xi_x|\xi_{x'}\rangle^t|}{4^n}\le\frac{2^{2n-2}c^t}{4^n}=\frac{c^t}{4}\le\frac{1}{2^{2n-2}}. &(266)\end{aligned}$$

Therefore, the output is $(1/2^{n-1})$-close in the statistical distance to the uniform distribution over y such that $y\cdot t=0$. Repeating this procedure $O(n)$ times, we can recover t with overwhelming probability. □

7.1 Breaking XUX

Proof of Theorem 7.1. Let U be Haar random unitary and $V:=X^aUX^b$ for random n-bit strings a,b. Let $|\Phi\rangle=\sum_{x\in\{0,1\}^n}|x,x\rangle/\sqrt{2^n}$ be the maximally entangled state. We have

$$\begin{aligned}&(X^x\otimes I)\cdot(U\otimes U)\cdot(X^y\otimes I)|\Phi\rangle\otimes(X^x\otimes I)\cdot(V\otimes U)\cdot(X^y\otimes I)|\Phi\rangle &(267)\\ &=(X^xUX^y\otimes U)|\Phi\rangle\otimes(X^{a\oplus x}UX^{b\oplus y}\otimes U)|\Phi\rangle. &(268)\end{aligned}$$

We write $(X^xUIX^y\otimes U)|\Phi\rangle=:|U_{x,y}\rangle$. We then consider the state

$$\begin{aligned}|\xi_{x,y}\rangle&=\frac{(X^xUX^y\otimes U)\otimes(X^{a\oplus x}UX^{b\oplus y}\otimes U)+(X^{a\oplus x}UX^{b\oplus y}\otimes U)\otimes(X^xUX^y\otimes U)}{\sqrt{2}}|\Phi,\Phi\rangle &(269)\\ &=\frac{|U_{x,y}\rangle\otimes|U_{a\oplus x,b\oplus y}\rangle+|U_{a\oplus x,b\oplus y}\rangle\otimes|U_{x,y}\rangle}{\sqrt{2}}. &(270)\end{aligned}$$

Note that $|\xi_{x\oplus a,y\oplus b}\rangle = |\xi_{x,y}\rangle$ holds. On the other hand, we later prove that $|\langle\xi_{x,y}|\xi_{x',y'}\rangle| \le 2n/2^{n/2}$ holds for all pairs such that $(x,y)\oplus(x',y') \neq (0,0)$ or (a,b) with an overwhelming probability over random U. Assuming this, $t = O(1)$ satisfies the condition of Lemma 7.3 with overwhelming probability.

To prepare the target state, we prepare

$$\sum_{x,y} \frac{1}{2^n} |x,y\rangle \otimes (|\Phi\rangle^{\otimes 2})^{\otimes t} \mapsto \sum_{x,y} \frac{1}{2^n} |x,y\rangle \otimes (|U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle)^{\otimes t} \tag{271}$$

using Equations (267) and (268). Then compute the projection $I_{2^{2n}} \otimes \Pi_{\text{sym}}^{\otimes t}$ where $\Pi_{\text{sym}} := \Pi_{\text{sym}}^{(2^{2n},2)}$ is the projection to the space $\left\{\frac{|p,q\rangle+|q,p\rangle}{\sqrt{2}} : p,q \in \{0,1\}^{2n}\right\}$ as defined in Lemma 2.11. The probability of success is at least $1/2^t$, because

$$\left\| (I_{2^{2n}} \otimes \Pi_{\text{sym}}^{\otimes t}) \sum_{x,y} \frac{1}{2^n} |x,y\rangle \otimes (|U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle)^{\otimes t} \right\|^2 \tag{272}$$

$$= \frac{1}{2^{2n}} \sum_{x,y} \| \Pi_{\text{sym}} |U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle \|^{2t} \tag{273}$$

$$\ge \frac{1}{2^{2n}} \cdot \sum_{x,y} \left(\frac{1}{2}\right)^t = \frac{1}{2^t} \tag{274}$$

where we use the fact that $|U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle$ is identical to

$$\frac{|U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle + |U_{a\oplus x,b\oplus y}\rangle \otimes |U_{x,y}\rangle}{2} + \frac{|U_{x,y}\rangle \otimes |U_{a\oplus x,b\oplus y}\rangle - |U_{a\oplus x,b\oplus y}\rangle \otimes |U_{x,y}\rangle}{2} \tag{275}$$

which implies the projection onto the symmetric subspace succeeds with probability $1/2$ each. In particular, if all the projections succeed, the outcome becomes

$$\sum_{x,y} \frac{1}{2^n} |x,y\rangle \otimes |\xi_{x,y}\rangle^{\otimes t}. \tag{276}$$

It remains to prove that $|\langle\xi_{x,y}|\xi_{x',y'}\rangle|$ is small for $(x,y)\oplus(x',y') \neq (0,0)$ or (a,b). We use the following lemma.

Lemma 7.4. *Let a, b and c be n bit strings such that $a \neq c$. Then,*

$$|\langle 0| X^a U X^b U^\dagger X^c |0\rangle|^2 \le \frac{n}{\sqrt{2^n}} \tag{277}$$

with probability at least $1 - e^{-O(n^2)}$ over the choice of U with respect to μ_{2^n}.

The proof is given below. Assume that this lemma is true. Then, by the union bound, with probability at least $1 - 2^{2n} e^{-O(n^2)} = 1 - \mathsf{negl}(n)$, Equation (277) holds for any $a \neq c$. The inner product is, using Equation (270),

$$\langle\xi_{x,y}|\xi_{x',y'}\rangle = \langle U_{x,y}|U_{x',y'}\rangle \langle U_{a\oplus x,b\oplus y}|U_{a\oplus x',b\oplus y'}\rangle + \langle U_{x,y}|U_{a\oplus x',b\oplus y'}\rangle \langle U_{a\oplus x,b\oplus y}|U_{x',y'}\rangle. \tag{278}$$

For $y' \neq y$, we have

$$|\langle U_{x,y}|U_{x',y'}\rangle| = |\langle\Phi|(X^x U X^y \otimes U)^\dagger (X^{x'} U X^{y'} \otimes U)|\Phi\rangle| \tag{279}$$

$$= |\langle\Phi|(X^y U^\dagger X^{x\oplus x'} U X^{y'} \otimes I)|\Phi\rangle| \tag{280}$$

$$= \left|\frac{\sum_{i,j\in\{0,1\}^n}\langle i,i|(X^y U^\dagger X^{x\oplus x'} U X^{y'} \otimes I)|j,j\rangle}{2^n}\right| \tag{281}$$

$$= \left|\frac{\sum_{i\in\{0,1\}^n}\langle i|X^y U^\dagger X^{x\oplus x'} U X^{y'}|i\rangle}{2^n}\right| \tag{282}$$

$$\leq \sum_{i\in\{0,1\}^n}\frac{|\langle i|X^y U^\dagger X^{x\oplus x'} U X^{y'}|i\rangle|}{2^n} \leq (\frac{n}{\sqrt{2^n}})^{1/2}. \tag{283}$$

The same inequality holds for $|\langle U_{a\oplus x,b\oplus y}|U_{a\oplus x',b\oplus y'}\rangle|$ and $|\langle U_{x,y}|U_{a\oplus x',b\oplus y'}\rangle|$ if $y' \notin \{y, y\oplus b\}$. Also, if $x \neq x'$, we have

$$|\langle U_{x,y}|U_{x',y'}\rangle| = |\langle\Phi|(X^x U X^y \otimes I)^\dagger (X^{x'} U X^{y'} \otimes I)|\Phi\rangle| \tag{284}$$

$$= |\langle\Phi|(I \otimes (X^x U X^y)^T)^\dagger (I \otimes (X^{x'} U X^{y'})^T)|\Phi\rangle| \tag{285}$$

$$= |\langle\Phi|(I \otimes X^x (U^T)^\dagger X^{y\oplus y'} U^T X^{x'})|\Phi\rangle| \tag{286}$$

using the ricochet property of the maximally mixed state $(A\otimes I)|\Phi\rangle = (I\otimes A^T)|\Phi\rangle$. A simple calculation gives the same inequality holds for this case. If $(x', y') \notin \{(x,y), (x\oplus a, y\oplus b)\}$, by the case-by-case analysis on each term of Equation (278), it must hold that

$$|\langle\xi_{x,y}|\xi_{x',y'}\rangle| \leq \frac{2n}{2^{n/2}}. \tag{287}$$

Therefore, we can prepare the state in Equation (276) in polynomial time which satisfies the conditions of Lemma 7.3. Applying the attack in the lemma, we conclude the proof. □

The proof of Lemma 7.4 relies on the following lemma.

Lemma 7.5 ([EAŻ05]). *Let A, B and C be $d\times d$ matrix. Then,*

$$\mathop{\mathbb{E}}_{U\leftarrow\mu_d} UAU^\dagger CUBU^\dagger = \frac{\mathrm{Tr}[AB]\mathrm{Tr}[C]}{d}\frac{I}{d} + \frac{d\mathrm{Tr}[A]\mathrm{Tr}[B]-\mathrm{Tr}[AB]}{d(d^2-1)}\left(C - \mathrm{Tr}[C]\frac{I}{d}\right) \tag{288}$$

Proof of Lemma 7.4. We show by the concentration inequality. To invoke it, we need the following expectation:

$$\mathop{\mathbb{E}}_{U\leftarrow\mu_{2^n}} |\langle 0|X^a U X^b U^\dagger X^c|0\rangle|^2 \tag{289}$$

$$= \mathop{\mathbb{E}}_{U\leftarrow\mu_{2^n}} |\langle a|UX^bU^\dagger|c\rangle|^2 \tag{290}$$

$$= \mathop{\mathbb{E}}_{U\leftarrow\mu_{2^n}} \langle a|UX^bU^\dagger|c\rangle\langle c|UX^bU^\dagger|a\rangle \tag{291}$$

$$= \langle a|\frac{\mathrm{Tr}[(X^b)^2]\mathrm{Tr}[|c\rangle\langle c|]}{2^n}\frac{I}{2^n} + \frac{2^n\mathrm{Tr}[X^b]\mathrm{Tr}[X^b]-\mathrm{Tr}[(X^b)^2]}{2^n(2^{2n}-1)}\left(|c\rangle\langle c| - \mathrm{Tr}[|c\rangle\langle c|]\frac{I}{2^n}\right)|a\rangle \tag{292}$$

$$= \langle a|\frac{I}{2^n} + \frac{2^n(2^{2n-2h(b)}-1)}{2^n(2^{2n}-1)}\left(|c\rangle\langle c| - \frac{I}{2^n}\right)|a\rangle \tag{293}$$

$$= \Theta(2^{-n}), \tag{294}$$

where we have used

- Lemma 7.5 in the third equality;
- $\text{Tr}[X^b] = 2^{n-h(b)}$ in the fourth equality, where $h(b)$ is the hamming distance of b;
- $a \neq c$ and $0 \leq \frac{2^n(2^{2n-2h(b)}-1)}{2^n(2^{2n}-1)} \leq 1$ in the last equality.

Note that we can see $\langle 0| X^a U X^b U^\dagger X^c |0\rangle |^2$ is the probability that some algorithm given access to U and $U^\dagger$ outputs 1. From this and Lemma 2.5, $\langle 0| X^a U X^b U^\dagger X^c |0\rangle |^2$ is 4-Lipshcitz for U. Therefore, from the concentration inequality Theorem 2.4,

$$\Pr_{U \leftarrow \mu_{2^n}}[| \langle 0| X^a U X^b U^\dagger X^c |0\rangle |^2 \leq \frac{n}{\sqrt{2^n}}] \geq \Pr_{U \leftarrow \mu_{2^n}}\left[\left| | \langle 0| X^a U X^b U^\dagger X^c |0\rangle |^2 - \Theta(2^{-n}) \right| \leq \frac{n}{2\sqrt{2^n}}\right] \tag{295}$$

$$\geq 1 - \exp\left(- O\left(2^n \frac{n^2}{2^n}\right)\right) \tag{296}$$

$$\geq 1 - e^{-O(n^2)}. \tag{297}$$

□

7.2 Breaking UP

Proof of Theorem 7.2. We construct the quantum states $|\xi\rangle$ given oracle access to U and $UP =: V$ for random Pauli operator P over n qubits. More concretely, for $(x, z) \in \{0,1\}^n \times \{0,1\}^n$, write $P_{x,z}$ to denote

$$i^{x \cdot z} X^{\otimes x} Z^{\otimes z} = i^{x \cdot z}(X^{x_1} Z^{z_1}) \otimes \ldots \otimes (X^{x_n} Z^{z_n}). \tag{298}$$

We define $V = UP$ for random Pauli $P = P_{a,b}$. Note that $P_{x,z} \cdot P_{x',z'} = i^{x \cdot z' - x' \cdot z} P_{(x,z) \oplus (x',z')} = (-1)^{x \cdot z' - x' \cdot z} P_{x',z'} \cdot P_{x,z}$. It well known that $\{|P_{x,z}\rangle := (P_{x,z} \otimes I) |\Phi\rangle\}_{x,z}$ consists the orthonormal basis for the maximally mixed state $|\Phi\rangle$.

Let $(x', z') = (x, z) \oplus (a, b)$. It holds that

$$P_{a,b} P_{x',z'} = i^{a \cdot z' - x' \cdot b} \cdot P_{x,z} = i^{a \cdot z - x \cdot b} \cdot P_{x,z}, \text{ and } P_{x',z'} = i^{a \cdot z - x \cdot b} \cdot P_{a,b} P_{x,z}. \tag{299}$$

Consider

$$|\phi_{x,z}\rangle := \frac{1}{\sqrt{2}} \left[(V \otimes I \otimes U \otimes I) + (U \otimes I \otimes V \otimes I) \right] (P_{x,z} \otimes I \otimes P_{x,z} \otimes I) |\Phi, \Phi\rangle \tag{300}$$

$$= (U \otimes I)^{\otimes 2} \left[\frac{(PP_{x,z} \otimes I) |\Phi\rangle \otimes (P_{x,z} \otimes I) |\Phi\rangle + (P_{x,z} \otimes I) |\Phi\rangle \otimes (PP_{x,z} \otimes I) |\Phi\rangle}{\sqrt{2}} \right] \tag{301}$$

$$= i^{a \cdot z - x \cdot b} (U \otimes I)^{\otimes 2} \left[\frac{|P_{x',z'}, P_{x,z}\rangle + |P_{x,z}, P_{x',z'}\rangle}{\sqrt{2}} \right]. \tag{302}$$

Similarly, $(U^\dagger \otimes I)^{\otimes 2} |\phi_{x',z'}\rangle$ can be expressed by

$$\frac{(P_{a,b} P_{x',z'} \otimes I) |\Phi\rangle \otimes (P_{x',z'} \otimes I) |\Phi\rangle + (P_{x',z'} \otimes I) |\Phi\rangle \otimes (P_{a,b} P_{x',z'} \otimes I) |\Phi\rangle}{\sqrt{2}} \tag{303}$$

$$= (-1)^{a \cdot z - x \cdot b} \cdot \frac{(P_{x,z} \otimes I) |\Phi\rangle \otimes (P_{a,b} P_{x,z} \otimes I) |\Phi\rangle + (P_{a,b} P_{x,z} \otimes I) |\Phi\rangle \otimes (P_{x,z} \otimes I) |\Phi\rangle}{\sqrt{2}} \tag{304}$$

$$= (-i)^{a \cdot z - x \cdot b} \frac{|P_{x',z'}, P_{x,z}\rangle + |P_{x,z}, P_{x',z'}\rangle}{\sqrt{2}}. \tag{305}$$

From this and the orthogonality of $\{(P_{x,z} \otimes I)\,|\Phi\rangle\}_{x,z}$, we derive that $|\phi_{x,z}\rangle^{\otimes 2}, |\phi_{x',z'}\rangle^{\otimes 2}$ are identical for $(x', z') \in \{(x, z), (x, z) \oplus (a, b)\}$ and otherwise orthogonal. Therefore, $|\xi_{x,z}\rangle := |\phi_{x,z}\rangle^{\otimes 2}$ be our target states. To construct $\sum_{x,z} |x, z, \xi_{x,z}\rangle$, we prepare

$$\sum_{x,z} \frac{1}{2^n} |x, z\rangle \otimes |\Phi\rangle^{\otimes 4} \mapsto \sum_{x,z} \frac{1}{2^n} |x, z\rangle \otimes |P_{x,z}\rangle^{\otimes 4} \tag{306}$$

$$\mapsto \sum_{x,z} \frac{1}{2^n} |x, z\rangle \otimes (U \otimes I)^{\otimes 4} |P_{x',z'}, P_{x,z}\rangle^{\otimes 2} \tag{307}$$

where the first step is to apply $(P_{x,z} \otimes I)^{\otimes 4}$ and the second step apply $(V \otimes I \otimes U \otimes I)^{\otimes 2}$.[19] Then compute the projection $I_{2^{2n}} \otimes \Pi_{\text{sym}}^{\otimes 2}$ where $\Pi_{\text{sym}} := \Pi_{\text{sym}}^{(2^{2n},2)}$ is the projection to the space $\left\{\frac{|p,q\rangle + |q,p\rangle}{\sqrt{2}} : p, q \in \{0,1\}^{2n}\right\}$ as defined in Lemma 2.11. It is not hard to see that the probability of success is at least $1/4$. This is because

$$\left\| (I_{2^{2n}} \otimes \Pi_{\text{sym}}^{\otimes 2}) \sum_{x,z} \frac{1}{2^n} |x, z\rangle \otimes (U \otimes I \otimes U \otimes I)^{\otimes 2} |P_{x',z'}, P_{x,z}\rangle^{\otimes 2} \right\|^2 \tag{308}$$

$$= \frac{1}{2^{2n}} \sum_{x,z} \left\| \Pi_{\text{sym}} |P_{x',z'}, P_{x,z}\rangle \right\|^4 \tag{309}$$

$$\geq \frac{1}{2^{2n}} \cdot \sum_{x,z} \left(\frac{1}{2}\right)^2 = \frac{1}{4} \tag{310}$$

where we use the invariant of the symmetric subspace under any unitary in the first equality, and

$$|P_{x',z'}, P_{x,z}\rangle = \frac{|P_{x',z'}, P_{x,z}\rangle + |P_{x,z}, P_{x',z'}\rangle}{2} + \frac{|P_{x',z'}, P_{x,z}\rangle - |P_{x,z}, P_{x',z'}\rangle}{2}. \tag{311}$$

Therefore, given U, UP we can efficiently construct the state in Equation (260) for $|\xi_{x,z}\rangle = |\phi_{x,z}\rangle^{\otimes 2}$ for $|\phi_{x,z}\rangle$ defined in Equation (300). By Lemma 7.3, we can extract (a, b) for $P = P_{a,b}$, thus UP cannot be a secure quantum-accessible PRFSG. □

8 Application of Haar Twirl Approximation: Alternative Proof of Non-Adaptive Security of PFC Ensemble

In this section, we give an alternative proof of the non-adaptive security of PFC ensemble [MPSY24]. They essentially use the Schur-Weyl duality in the proof of [MPSY24]. However, our proof does not invoke it and essentially uses the Weingarten calculus.

8.1 Definitions and Lemmas

First, we define the action of a permutation unitary and a binary phase unitary.

Definition 8.1 (Permutation Unitaries on $\mathbb{C}^d$). *Let S_d be a set of all permutations over d elements. For each $\pi \in S_d$, we define the permutation unitary P_π on $\mathbb{C}^d$ that acts*

$$P_\pi |x\rangle = |\pi(x)\rangle \tag{312}$$

for all $x \in [d]$.

[19] We ignore the phase which becomes irrelevant.

Definition 8.2 (Binary Phase Unitaries). *For a function $f:[d]\to\{0,1\}$, we define the binary phase unitary F_f on $\mathbb{C}^d$ that acts*

$$F_f\left|x\right\rangle=(-1)^{f(x)}\left|x\right\rangle \tag{313}$$

for all $x\in[d]$.

Definition 8.3 (k-wise twirl). *Let $k,d\in\mathbb{N}$ and $\mathcal{F}$ be a set of all functions $f:[d]\to\{0,1\}$. We define the PF k-wise twirl $\mathcal{M}_{PF}^{(t)}$ and PFC k-wise twirl $\mathcal{M}_{PFC}^{(t)}$ as follows:*

$$\mathcal{M}_{PF}^{(t)}(\cdot)\coloneqq\mathop{\mathbb{E}}_{\pi\leftarrow S_d,f\leftarrow\mathcal{F}}(P_\pi F_f)^{\otimes k}(\cdot)(P_\pi F_f)^{\dagger\otimes k}, \tag{314}$$

$$\mathcal{M}_{PFC}^{(t)}(\cdot)\coloneqq\mathop{\mathbb{E}}_{\substack{\pi\leftarrow S_d,f\leftarrow\mathcal{F},\\ C\leftarrow\nu}}(P_\pi F_f C)^{\otimes k}(\cdot)(P_\pi F_f C)^{\dagger\otimes k}. \tag{315}$$

Here, S_d is the set of all permutations over $[d]$, $\mathcal{F}$ is a set of all functions $f:[d]\to\{0,1\}$, and ν is any unitary 2-design.

The following two lemmas are shown in [MPSY24], both of which are from the straightforward computation (without Schur-Weyl duality).

Lemma 8.4 (Lemma 3.2 in [MPSY24]). *Let $k,d\in\mathbb{N}$ and ν be any unitary 2-design. Define Λ be the projection onto*

$$\mathit{span}\{\left|x_1,...,x_k\right\rangle;x_1,...,x_k\in[d]\text{ and }x_1,...,x_k\text{ are distinct.}\}. \tag{316}$$

Then, for any quantum state ρ,

$$\mathrm{Tr}[\Lambda\mathop{\mathbb{E}}_{C\leftarrow\nu}C^{\otimes k}\rho C^{\dagger\otimes k}]\geq 1-O\left(\frac{k^2}{d}\right). \tag{317}$$

Lemma 8.5 (Immediate corollary of Lemma 3.8 of [MPSY24]). *Let $\mathbf{A}$ be a d^k-dimentional register and $\mathbf{B}$ be any register. Let Λ be the projection defined in Lemma 8.4. Then, for any state $\rho_{\mathbf{AB}}$ such that $(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}})\rho_{\mathbf{AB}}(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}})=\rho_{\mathbf{AB}}$,*

$$(\mathcal{M}_{PF,\mathbf{A}}^{(k)}\otimes\mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}})=\sum_{\sigma\in S_k}\frac{\Lambda_{\mathbf{A}}}{\mathrm{Tr}[\Lambda]}R_{\sigma,\mathbf{A}}^\dagger\otimes\mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'}\otimes I_{\mathbf{B}})\rho_{\mathbf{A}'\mathbf{B}}]. \tag{318}$$

Here $\mathbf{A}'$ is a register whose size is the same as that of the register $\mathbf{A}$.

8.2 Proof

Now by using Lemma 4.7, we show the following theorem which is originally shown by invoking the Schur-Weyl duality in [MPSY24].

Theorem 8.6. *Let $k,d\in\mathbb{N}$ such that $d>\sqrt{6}k^{7/4}$. Then,*

$$\left\|\mathcal{M}_{\mathit{Haar}}^{(k)}-\mathcal{M}_{PFC}^{(k)}\right\|_\diamond\leq O\left(\frac{k}{\sqrt{d}}\right). \tag{319}$$

Proof of Theorem 8.6. Let $\mathbf{A}$ be a d^k-dimentional register and $\mathbf{B}$ be any register. It suffices to show that for any state $\rho_{\mathbf{AB}}$,

$$\left\|(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\rho_{\mathbf{AB}}) - (\mathcal{M}^{(k)}_{PFC,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}})\right\|_1 \leq O\left(\frac{k}{\sqrt{d}}\right). \tag{320}$$

Define

$$\xi_{\mathbf{AB}} \coloneqq \mathop{\mathbb{E}}_{C \leftarrow \nu} (C^{\otimes k}_{\mathbf{A}} \otimes I_{\mathbf{B}}) \rho_{\mathbf{AB}} (C^{\otimes k}_{\mathbf{A}} \otimes I_{\mathbf{B}})^\dagger, \text{ and} \tag{321}$$

$$\xi'_{\mathbf{AB}} \coloneqq \frac{(\Lambda_{\mathbf{A}} \otimes I_{\mathbf{B}}) \xi_{\mathbf{AB}} (\Lambda_{\mathbf{A}} \otimes I_{\mathbf{B}})}{\mathrm{Tr}[(\Lambda_{\mathbf{A}} \otimes I_{\mathbf{B}}) \xi_{\mathbf{AB}}]}. \tag{322}$$

From Lemmata 2.6 and 8.4, we have

$$\|\xi_{\mathbf{AB}} - \xi'_{\mathbf{AB}}\|_1 \leq O\left(\frac{k}{\sqrt{d}}\right). \tag{323}$$

Thus,

$$\begin{aligned}
&\left\|(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\rho_{\mathbf{AB}}) - (\mathcal{M}^{(k)}_{PFC,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\rho_{\mathbf{AB}})\right\|_1 && (324)\\
=&\left\|(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\xi_{\mathbf{AB}}) - (\mathcal{M}^{(k)}_{PF,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\xi_{\mathbf{AB}})\right\|_1 && (325)\\
\leq&\left\|(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\xi'_{\mathbf{AB}}) - (\mathcal{M}^{(k)}_{PF,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\xi'_{\mathbf{AB}})\right\|_1 + O\left(\frac{k}{\sqrt{d}}\right), && (326)\\
& && (327)
\end{aligned}$$

where the equality follows from the right and left invariance of the Haar measure, and the inequality follows from Equation (323) and the triangle inequality.

To conclude the proof, we show

$$\left\|(\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\xi'_{\mathbf{AB}}) - (\mathcal{M}^{(k)}_{PF,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\xi'_{\mathbf{AB}})\right\|_1 \leq O\left(\frac{k}{\sqrt{d}}\right). \tag{328}$$

Let us consider the following hybrids of matrices:

- $\xi_{0,\mathbf{AB}} \coloneqq (\mathcal{M}^{(k)}_{\mathrm{Haar},\mathbf{A}} \otimes \mathrm{id}_{\mathbf{AB}})(\xi'_{\mathbf{AB}})$.
- $\xi_{1,\mathbf{AB}} \coloneqq \sum_{\sigma \in S_k} \frac{1}{d^k} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}}) \xi'_{\mathbf{A}'\mathbf{B}}]$.
- $\xi_{2,\mathbf{AB}} \coloneqq \sum_{\sigma \in S_k} \frac{\Lambda_{\mathbf{A}}}{\mathrm{Tr}[\Lambda]} R^\dagger_{\sigma,\mathbf{A}} \otimes \mathrm{Tr}_{\mathbf{A}'}[(R_{\sigma,\mathbf{A}'} \otimes I_{\mathbf{B}}) \xi'_{\mathbf{A}'\mathbf{B}}]$.
- $\xi_{3,\mathbf{AB}} \coloneqq (\mathcal{M}^{(k)}_{PF,\mathbf{A}} \otimes \mathrm{id}_{\mathbf{B}})(\xi'_{\mathbf{AB}})$

From Lemma 4.7, we have

$$\|\xi_0 - \xi_1\|_1 \leq O(k^2/d). \tag{329}$$

Moreover, we have

$$\xi_2 = \xi_3 \tag{330}$$

from Lemma 8.5. Thus, it suffices to show $\|\xi_1 - \xi_2\|_1 \le O(k^2/d)$. Note that $\xi_{1,\mathbf{AB}}$ is invariant under the action of 2-design twirl because

$$\begin{aligned}
\mathop{\mathbb{E}}_{C\leftarrow\nu}(C_{\mathbf{A}}^{\otimes k}\otimes I_{\mathbf{B}})\xi_{1,\mathbf{AB}}(C_{\mathbf{A}}^{\otimes k}\otimes I_{\mathbf{B}})^{\dagger} &= \sum_{\sigma\in S_k}\frac{1}{d^k}\mathop{\mathbb{E}}_{C\leftarrow\nu}(C^{\otimes k}R_{\sigma}^{\dagger}C^{\dagger\otimes k})_{\mathbf{A}}\otimes\mathrm{Tr}_{\mathbf{A'}}[(R_{\sigma,\mathbf{A'}}\otimes I_{\mathbf{B}})\xi'_{\mathbf{A'B}}] && (331)\\
&= \sum_{\sigma\in S_k}\frac{1}{d^k}R_{\sigma,\mathbf{A}}^{\dagger}\otimes\mathrm{Tr}_{\mathbf{A'}}[(R_{\sigma,\mathbf{A'}}\otimes I_{\mathbf{B}})\xi'_{\mathbf{A'B}}] && (332)\\
&= \xi_{1,\mathbf{AB}}, && (333)
\end{aligned}$$

where we have used the fact $U^{\otimes k}R_{\sigma}U^{\dagger\otimes k} = R_{\sigma}$ for any $\sigma\in S_k$ and $U\in\mathbb{U}(d)$ in the second equality. This and Lemma 8.4 imply

$$\mathrm{Tr}[(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}})\xi_{1,\mathbf{AB}}] \ge 1 - O\left(\frac{k^2}{d}\right). \tag{334}$$

Thus, we have

$$\begin{aligned}
\|\xi_{1,\mathbf{AB}} - \xi_{2,\mathbf{AB}}\|_1 &\le \|(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}})\xi_{1,\mathbf{AB}}(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}}) - \xi_{2,\mathbf{AB}}\|_1 + O\left(\frac{k}{\sqrt{d}}\right) && (335)\\
&= \left\|\left(\frac{\mathrm{Tr}[\Lambda]}{d^k} - 1\right)\xi_{2,\mathbf{AB}}\right\|_1 + O\left(\frac{k}{\sqrt{d}}\right) && (336)\\
&= O\left(\frac{k^2}{d}\right) + O\left(\frac{k}{\sqrt{d}}\right) && (337)\\
&\le O\left(\frac{k}{\sqrt{d}}\right), && (338)
\end{aligned}$$

where we have used

- Equation (334) and Lemma 2.6 in the first inequality and
- $\mathrm{Tr}[\Lambda] = d(d-1)\cdots(d-k+1)$ and $(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}})\xi_{1,\mathbf{AB}}(\Lambda_{\mathbf{A}}\otimes I_{\mathbf{B}}) = \xi_{2,\mathbf{AB}}$ in the second equality.

Therefore, Equation (328) follows from Equations (329), (330) and (338), which concludes the proof. □

Acknowledgments. SY thanks Benoît Collins for lecturing about Weingarten calculus. SY also thanks Tomoyuki Morimae for helpful discussions and for helping him to write the introduction.

References

[ABGL24] Prabhanjan Ananth, Jhon Bostanci, Aditya Gulati, and Yao-Ting Lin. Pseudorandomness in the (inverseless) haar random oracle model. *arXiv preprint arXiv:2410.19320*, 2024. (Cited on page 5, 6, 7.)

[ABKM22] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the even-mansour cipher. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 458–487. Springer, 2022. (Cited on page 3, 5, 8, 33, 34, 39.)

[ACQ22] Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. Quantum algorithmic measurement. *Nature communications*, 13(1):887, 2022. (Cited on page 18.)

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. Cryptography in the common haar state model: Feasibility results and separations. *arXiv preprint arXiv:2407.07908*, 2024. (Cited on page 3, 6.)

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 237–265, November 2022. (Cited on page 3, 14, 31.)

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 788–817, May 2020. (Cited on page 5.)

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236, August 2022. (Cited on page 3, 14.)

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. In *ITCS 2023*, pages 24:1–24:21. LIPIcs, January 2023. (Cited on page 3.)

[BFM19] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 329–349. 2019. (Cited on page 3.)

[BFV20] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the ads/cft duality. In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2020. (Cited on page 3, 4, 6.)

[BGTW24] Adam Bouland, Tudor Giurgica-Tiron, and John Wright. The state hidden subgroup problem and an efficient algorithm for locating unentanglement. *arXiv preprint arXiv:2410.12706*, 2024. (Cited on page 6.)

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states. *arXiv preprint arXiv:2410.08073*, 2024. (Cited on page 7.)

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993. (Cited on page 3.)

[CCS24] Boyang Chen, Andrea Coladangelo, and Or Sattath. The power of a single haar random state: constructing and separating quantum pseudorandomness. *arXiv preprint arXiv:2404.03295*, 2024. (Cited on page 3, 5.)

[CM17] Benoît Collins and Sho Matsumoto. Weingarten calculus via orthogonality relations: new applications. *arXiv preprint arXiv:1701.04493*, 2017. (Cited on page 15, 18.)

[CM24] Lijie Chen and Ramis Movassagh. Quantum merkle trees. *Quantum*, 8:1380, June 2024. (Cited on page 3, 4, 6.)

[CMN22] Benoit Collins, Sho Matsumoto, and Jonathan Novak. The weingarten calculus. *arXiv preprint arXiv:2109.14890*, 2022. (Cited on page 15.)

[CMS12] Benoit Collins, Sho Matsumoto, and Nadia Saad. Integration of invariant matrices and application to statistics. *arXiv preprint arXiv:1205.0956*, 2012. (Cited on page 17, 18.)

[CŚ06] Benoît Collins and Piotr Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264(3):773–795, 2006. (Cited on page 5, 15, 16.)

[DKS12] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even-Mansour scheme revisited. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 336–354, April 2012. (Cited on page 3, 4.)

[DLS22] Frédéric Dupuis, Philippe Lamontagne, and Louis Salvail. Fiat-shamir for proofs lacks a proof even in the presence of shared entanglement. Cryptology ePrint Archive, Paper 2022/435, 2022. (Cited on page 3.)

[EAŻ05] Joseph Emerson, Robert Alicki, and Karol Życzkowski. Scalable noise estimation with random unitary operators. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(10):S347, 2005. (Cited on page 45.)

[EM97] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. *Journal of cryptology*, 10:151–161, 1997. (Cited on page 3, 4.)

[ES15] Edward Eaton and Fang Song. Making existential-unforgeable signatures strongly unforgeable in the quantum random-oracle model. In *10th Conference on the Theory of Quantum Computation, Communication and Cryptography*, page 147, 2015. (Cited on page 5.)

[Gao15] Jingliang Gao. Quantum union bounds for sequential projective measurements. *Physical Review A*, 92(5):052331, 2015. (Cited on page 12.)

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 637–667, December 2021. (Cited on page 5.)

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013. (Cited on page 13.)

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th FOCS*, pages 230–235. IEEE Computer Society Press, October / November 1989. (Cited on page 3.)

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152, August 2018. (Cited on page 3, 13.)

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586, April / May 2018. (Cited on page 5.)

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. In *2012 international symposium on information theory and its applications*, pages 312–316. IEEE, 2012. (Cited on page 5.)

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *55th ACM STOC*, pages 1589–1602. ACM Press, June 2023. (Cited on page 3.)

[Kre21] W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021. (Cited on page 3, 11, 12.)

[KT24] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In *56th ACM STOC*, pages 968–978. ACM Press, June 2024. (Cited on page 3.)

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. In *56th ACM STOC*, pages 979–990. ACM Press, June 2024. (Cited on page 3.)

[Mec19] Elizabeth S. Meckes. *The Random Matrix Theory of the Classical Compact Groups*. Cambridge University Press, 2019. (Cited on page 11.)

[Mel24] Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner's tutorial. *Quantum*, 8:1340, 2024. (Cited on page 11, 13.)

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. *arXiv preprint arXiv:2410.10116*, 2024. (Cited on page 3, 6, 7.)

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. *arXiv preprint arXiv:2404.12647*, 2024. (Cited on page 5, 7, 8, 47, 48.)

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295, August 2022. (Cited on page 3.)

[MY24] Tomoyuki Morimae and Takashi Yamakawa. Quantum advantage from one-way functions. LNCS, pages 359–392, August 2024. (Cited on page 3.)

[MYY24] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. Quantum unpredictability. *arXiv preprint arXiv:2405.04072*, 2024. (Cited on page 3.)

[MZ24] Saachi Mutreja and Mark Zhandry. Quantum state group actions. *arXiv preprint arXiv:2410.08547*, 2024. (Cited on page 6.)

[OV22] Ryan O'Donnell and Ramgopal Venkateswaran. The quantum union bound made easy. In *Symposium on Simplicity in Algorithms (SOSA)*, pages 314–320. SIAM, 2022. (Cited on page 12.)

[Qia24] Luowen Qian. Unconditionally secure quantum commitments with preprocessing. LNCS, pages 38–58, August 2024. (Cited on page 3.)

[Sim96] Daniel R. Simon. Anonymous communication and anonymous cash. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 61–73, August 1996. (Cited on page 5.)

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551, April / May 2018. (Cited on page 5.)

[Unr14a] Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 1–18, August 2014. (Cited on page 5.)

[Unr14b] Dominique Unruh. Revocable quantum timed-release encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 129–146, May 2014. (Cited on page 5.)

[Wat18] John Watrous. *The theory of quantum information*. Cambridge university press, 2018. (Cited on page 12.)

[Win99] Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999. (Cited on page 12.)