Pseudorandomness in the (Inverseless) Haar Random Oracle Model

Prabhanjan Ananth[*] UCSB

John Bostanci[†] Columbia

Aditya Gulati[‡] UCSB

Yao-Ting Lin[§] UCSB

Abstract

We study the (in)feasibility of quantum pseudorandom notions in a quantum analog of the random oracle model, where all the parties, including the adversary, have oracle access to the same Haar random unitary. In this model, we show the following:

- (Unbounded-query secure) pseudorandom unitaries (PRU) exist. Moreover, the PRU construction makes two calls to the Haar oracle.
- We consider constructions of PRUs making a single call to the Haar oracle. In this setting, we show that unbounded-query security is impossible to achieve. We complement this result by showing that bounded-query secure PRUs do exist with a single query to the Haar oracle.
- We show that multi-copy pseudorandom state generators and function-like state generators (with classical query access), making a single call to the Haar oracle, exist.

Our results have two consequences: (a) when the Haar random unitary is instantiated suitably, our results present viable approaches for building quantum pseudorandom objects without relying upon one-way functions and, (b) for the first time, we show that the key length in pseudorandom unitaries can be generically shrunk (relative to the output length). Our results are also some of the first usecases of the new "path recording" formalism for Haar random unitaries, introduced in the recent breakthrough work of Ma and Huang.

[*] prabhanjan@cs.ucsb.edu

[†] johnb@cs.columbia.edu

[‡] adityagulati@ucsb.edu

[§] yao-ting_lin@ucsb.edu

Contents

1 Introduction **3**
1.1 Our Contributions 4

2 Related Work **7**

3 Technical Overview **8**
3.1 Path Recording Formalism of Ma and Huang 8
3.2 (Unbounded) PRUs with Two Queries 9
3.3 (Unbounded) PRUs: One Parallel Query is Insufficient 11
3.4 (Bounded) PRUs with One Query: Feasibility 12
3.5 (Unbounded) Pseudorandom States with One Query 12

4 Preliminaries **13**
4.1 Notation 13
4.2 Cryptographic Primitives 14
4.3 Useful Lemmas 15

5 Ma-Huang's Path-Recording Framework **15**
5.1 Oracle Adversary 15
5.2 Relation States 16
5.3 Path-Recording Isometry (PR) 16

6 Path-Recording Framework: New Observations **17**
6.1 Definitions 17
6.2 Recording ℓ-Fold Collision-Free Paths 17
6.3 Multiset States and Operations. 21

7 Pseudorandom Unitaries with Short Keys **22**

8 Key-Stretched PRU in the Plain Model **27**

9 Bounded-Query Pseudorandom Unitaries with Short Keys **30**

10 Unbounded-Query Secure Non-Adaptive PRUs: Barriers **33**
10.1 Optimality of ℓ-Query PRUs in Section 9 33
10.2 Almost Optimality among Parallel-Query Pseudorandom Unitaries 35

11 Unbounded-Copy PRS in the iQHROM **37**

12 Adaptively Secure PRFS in the iQHROM **40**

A Omitted Proofs **49**
A.1 Omitted Proofs in Section 6 49
A.2 Omitted Proofs in Section 7 49

1 Introduction

Pseudorandomness is a powerful concept that is integral to not only cryptography but to the broader area of theoretical computer science. In the recent years, there have been an exciting line of works on designing pseudorandom primitives in the quantum world. Quantum pseudorandom primitives already have had a major impact with applications in areas including quantum gravity theory [BFV20; ABF+24], quantum machine learning [HBC+22], quantum complexity theory [Kre21; CLS24] and more importantly, in quantum cryptography [AQY22; MY22]. From a cryptographic standpoint, thanks to Kretschmer's result [Kre21] (see also [KQST23]), there is some evidence to believe that many of the recently introduced quantum pseudorandom primitives could be a weaker assumption than one-way functions. This has led to a plethora of new results that suggest that commitments [AQY22; MY22; AGQY22; Yan22; BCQ23; HMY23; BEM+23; ALY24; KT24a; BJ24], encryption schemes [AQY22; HMY23], digital signatures [MY22; BBO+24] could be based on assumptions plausibly weaker than one-way functions.

One major criticism on this line of work is the fact that all the quantum pseudorandom primitives proposed so far [JLS18; BS19; BS20; AQY22; AGQY22; BBSS23; LQS+23; ABF+24; AGKL24; MPSY24; BM24] rely upon the existence of one-way functions. In order for us to gain more confidence that the quantum pseudorandom primitives are weaker than one-way functions, it is imperative we need to look for candidate constructions that do not rely upon the existence of one-way functions.

On Pseudorandomness from Random Quantum Circuits. Indeed, [AQY22] suggest using local random circuits, that are quantum circuits with local Haar random gates, to design pseudorandom state generators (PRSGs). A pseudorandom state generator [JLS18], one of the first quantum pseudorandom primitives, is an efficient quantum circuit G that takes as input a key $k \in \{0,1\}^\lambda$ and produces an n-qubit quantum state such that the output distribution of $G(k)^{\otimes t}$, where t is a polynomial in λ, is computationally indistinguishable from t copies of an n-qubit Haar random state.

It is natural to consider random quantum circuits to build pseudorandom state generators. In fact, [AQY22] was not the only one to suggest using random quantum circuits to instantiate PRSGs. Couple of other works [BCQ23; KT24b] also suggested using random circuits in the design of quantum cryptographic primitives. Random quantum circuits are extensively studied, notably in quantum supremacy experiments [AAB+19] and in the unitary design constructions [BHH16]. In some ways, random quantum circuits share similar properties with Haar random unitaries. The seminal work of [BHH16] (see also [Haf22]) show that random circuits with polynomial (in t) depth are unitary t-designs; in other words, random circuits with sufficient depth agree with Haar random unitaries upto the t^{th} moment. Recently, [SHH24] showed that local random quantum circuits, where the local gates act on sufficiently many qubits, are close to Haar random unitaries[1], and [BHHP24] showed that states and unitaries generated by local random diagonal circuits, where local diagonal gates act alternate with Hadamard gates, also have similar properties to Haar random states and unitaries.

The PRSG candidate posited by [AQY22] roughly states that the output of polynomial-sized random quantum circuits is pseudorandom. Interestingly, this candidate does not seem to rely upon one-way functions at all. Unfortunately, they do not provide any evidence on the security of their candidate. Concretely identifying cryptographic assumptions underlying this candidate is quite challenging.

This is reminiscent of many cryptographic constructions that use real-world hash functions, which work well in practice although formally proving security of these constructions has remained elusive. To gain more confidence in such constructions, we have often resorted to proving security in idealized models, such as the random oracle model [BR93]. Although proving the security of constructions in the random oracle model does not outright guarantee the security of their implementations in the real world (indeed, there are counterexamples [CGH04]), so far, random oracles have been proven to be a useful heuristic and widely adopted in theoretical and practical cryptography [Gre20]. Studying similar idealized models in the quantum world could prove to be impactful in quantum cryptography.

[1] Concretely, in order to have the diamond norm between the random circuits and Haar random unitaries to be negligible in λ, the local gates need to act upon $\omega(\log(\lambda))$ qubits.

Our Work: Pseudorandomness in the Quantum Haar Random Oracle Model. We consider the quantum Haar random oracle model (QHROM) introduced by Chen and Movassagh [CM24] as a quantum analog of the random oracle model. In this model, all the parties have access to a Haar random unitary U and its inverse. This model is especially useful to consider for cryptographic applications that use random circuits as a building block. Since it is challenging to base certain properties of random quantum circuits on cryptographic assumptions, we can instead consider an idealized model, where the adversary has access to a Haar random oracle. Arguing security in this model would then provide insight into the security of the construction where the Haar random oracle is instantiated with random quantum circuits. Beyond random quantum circuits, other phenomena could also be modeled in this framework. As an example, Bouland, Fefferman and Vazirani [BFV20] presented a candidate construction of pseudorandom state generators in the conformal field theory. Towards proving security of this candidate, they modeled the time evolution operators as a Haar random unitary and analyzed its behavior. [CM24] also proposed a construction of succinct quantum commitments in the QHROM. Unfortunately, they were unable to prove its security and they attribute the difficulty of proving security to the lack of tools for analyzing QHROM.

Indeed, proving security in the QHROM is much more challenging than its classical counterpart which could also partially explain the reason why it took so long to establish the feasibility of pseudorandom unitaries, which are efficiently computable unitaries that are computationally indistinguishable from Haar random unitaries.

Towards making progress in this direction, we consider a relaxation of the QHROM, that we refer to as the *inverseless* QHROM (iQHROM). In this relaxation, all the parties have access to a Haar random unitary U but not its inverse. The focus of our work is to study quantum pseudorandom primitives in the iQHROM. As we will see later, proving security in the iQHROM is already quite challenging and it involves developing new techniques. Another reason to study the iQHROM is that showing feasibility results in the iQHROM would serve as a stepping stone towards investigating the feasibility in the QHROM (with inverses).

1.1 Our Contributions

We initiate a research direction on understanding the feasibility of quantum pseudorandomness using Haar random oracles. We focus on two pseudorandom primitives: namely pseudorandom state generators and pseudorandom unitaries, both first defined in [JLS18]. We briefly discuss their definitions in the iQHROM before stating our results:

- Pseudorandom state generators (PRSG) in the iQHROM: a PRSG is an efficient quantum circuit G, with oracle access to a Haar random unitary U, that takes as input a key $k \in \{0,1\}^{\lambda}$[2] and produces an n-qubit quantum state. In terms of security, we require that any query-bounded adversary[3] $\mathcal{A}$, with oracle access to U, should not be able to distinguish $G(k)^{\otimes t}$ from $|\psi\rangle^{\otimes t}$, where $|\psi\rangle$ is an n-qubit Haar random state. If t is an arbitrary polynomial then we call this *multi-copy* PRSGs and if t is fixed ahead of time (similar to state designs), we call this *bounded-copy* PRSGs.

- Pseudorandom function-like state generators (PRFS) in the iQHROM: a PRFS is a keyed polynomial-sized circuit $G^U(k,\cdot)$ that produces $2^{m(\lambda)}$ many n-qubit states $|\psi_x\rangle = G^U(k,w)$. For PRFS security, we require that any t query-bounded adversary $\mathcal{A}^U$ that can adaptively request copies of $|\psi_w\rangle$ can not distinguish between the outputs of the PRFS generator and a family of $2^{m(\lambda)}$ many i.i.d states sampled from the Haar measure. If t is an arbitrary polynomial then we call this *multi-copy* PRFSs and if t is fixed ahead of time (similar to state designs), we call this *bounded-copy* PRFSs.

- Pseudorandom unitaries (PRU) in the iQHROM: a PRU is a keyed polynomial-sized quantum circuit G_k^U that is functionally equivalent to an m-qubit unitary. In terms of security, we require that any query-bounded $\mathcal{A}$, with oracle access to $\mathcal{O}$ and U, should not be able to distinguish whether $\mathcal{O} = G_k^U$

[2] λ is the security parameter.

[3] Typically, PRSGs guarantee security only against quantum polynomial-time adversaries. In this work, similar to the setting of state designs, we allow the adversary to be computationally unbounded. However, we restrict the number of queries made by $\mathcal{A}$ to the Haar random oracle to be any polynomial in λ.

or whether $\mathcal{O} = V$, where V is a freshly sampled m-qubit Haar random unitary. If the number of adversarial calls to G_k^U is an arbitrary polynomial then we call G_k^U an *unbounded-query* secure PRU and if the number of calls is fixed ahead of time, we call it a *bounded-query* secure PRUs.

It should be emphasized at this point that in both the definitions, the adversary does have oracle access to U.[4] This is what makes the design of both these primitives challenging. This is akin to the random oracle model, where the adversary also has access to the random function.

Unbounded-query secure PRUs. Our main result is showing that pseudorandom unitaries exist in the iQHROM.

Theorem 1 (Informal)**.** *PRUs exist in the inverseless quantum Haar random oracle model.*

We remark that our construction is quite simple: if U is the n-qubit Haar unitary and if $k \in \{0,1\}^\lambda$, where $\lambda \leq n$, is the PRU key then $G_k^U = U(X^k \otimes \mathrm{id}_{n-\lambda})U$. It is important to note that G_k makes two sequential calls to U.

Implications to Pseudorandom Unitaries in the plain model. In the plain model, we can substitute the Haar random oracle with sampling a single PRU key. Instantiating the PRU in the iQHROM with this single sample of a pseudorandom unitary yields a new unitary that looks pseudorandom relative to the first sample, at the cost of only sampling $\omega(\log(\lambda))$ more bits. Plugging these independent looking unitaries into the construction of [SHH24] yields a PRU with a much larger output size, at the cost of only a small amount of additional randomness. And as a corollary of our result, we show how to stretch the output length of *any* PRU that exists in the plain model.

Theorem 2 (Informal)**.** *If any pseudorandom unitary family exists, there is a construction of pseudorandom unitaries with keys of size $O(\lambda)$ and output size $O(\lambda^c)$ for all constants c.*

The work of [GJMZ23] proved a similar result (although technically incomparable) where the resulting pseudorandom unitary was only secure against a single adversarial query, but the stretching algorithm does not require sampling any additional randomness.

We highlight that our stretched PRU only stretches *output length.* In particular, it does not shrink the key length; though the increase in output length is much larger than the increase in key length. Hence, for some output size n, one could start from PRUs for a much smaller security parameter (say, n^δ), and build a pseudorandom unitary with output length n. The question of taking a pseudorandom unitary with a fixed output length to another pseudorandom unitary with the *same* output length, but smaller key, is still an open question.

Unbounded-query secure PRUs: On the number of calls needed. It is interesting to explore if it is inherent that G_k needs to make at least two calls to U. We show that it is necessary. Informally, we show that any PRU construction making a single call to U is insecure as long as the adversary is allowed to make $\Omega\left(\frac{\lambda}{\log(\lambda)}\right)$ queries to the PRU.

Theorem 3 (Informal)**.** *Any PRU construction that only makes a single query to the Haar random oracle is insecure against adversaries making $\Omega\left(\frac{\lambda}{\log(\lambda)}\right)$ non-adaptive queries to the PRU.*

Bounded-query secure PRUs. The above negative result leads us to an intriguing question: does there exist a PRU construction that only makes a single call to the Haar random oracle and satisfies security as long as the adversary only makes an *a priori* bounded number of queries to the PRU? We answer this question below.

[4] We assume that the number of queries to U is an arbitrary polynomial.

Theorem 4 (Informal)**.** *PRUs exist in the inverseless quantum Haar random oracle model with the following properties: (a) the construction makes a single call to the Haar oracle, (b) the adversary makes at most* $O\left(\frac{\lambda}{(\log(\lambda))^{1+\varepsilon}}\right)$ *queries, for* $\varepsilon > 0$.

From our negative result (Theorem 3), we have that condition (b) in the above theorem is tight.

Negative Result: Generalization to the Parallel Query case. We already saw that at least two calls to the Haar oracle are necessary if we were to design PRUs with unbounded query security. However, our construction in Theorem 1 makes two sequential calls to the Haar random oracle. A natural question is: *are two sequential calls necessary?* We answer this question in the affirmative. In fact, we show that any number of parallel calls to the Haar random oracle is not sufficient. Concretely, we show that any PRU making arbitrary number of *parallel* calls to the Haar random oracle U (i.e. of the form, $W \cdot U^{\otimes t} \cdot V$, for some unitaries W, V and for some polynomial t) is insecure as long as the adversary is allowed to make $\Omega(\lambda)$ queries to the PRU and U.

Theorem 5 (Informal)**.** *Any PRU construction that only makes parallel queries to the Haar oracle is insecure against adversaries making* $\Omega(\lambda)$ *non-adaptive queries to the PRU.*

Pseudorandom Quantum States and Function-like States in the iQHROM. We next look at pseudorandom state generators in the iQHROM. Since PRUs imply PRSGs, we immediately get the implication that PRSGs exist in the iQHROM. The question, then, is if there are even simpler constructions of PRSGs in the iQHROM. We show the following.

Theorem 6 (Informal)**.** *PRSGs exist in the inverseless quantum Haar random oracle model with the following properties: (a) the construction makes a single call to the Haar oracle and, (b) the adversary is given an arbitrary polynomial number of copies.*

In particular, our result shows that the negative result Theorem 3 only holds for PRUs and not PRSGs and PRFSs. We note that [BFV20] proposed a much more involved construction of PRSGs in the stronger QHROM model although they did not formally prove the security of their candidate. We also extend our construction of pseudorandom states to a construction of pseudorandom *function-like* states.

Theorem 7 (Informal)**.** *PRFSs exist in the inverseless quantum Haar random oracle model, with the following properties: (a) the construction makes a single call to the Haar random oracle and, (b) the adversary is given an arbitrary polynomial number of classical queries.*

Results Summary (Informal)

1. Unbounded query secure PRUs, with two calls to the Haar random oracle, exist in iQHROM (Theorem 1)
2. Unbounded query secure PRUs exist with keys of size $O(\lambda^{1/c})$ for any constant c, if any PRU exists in the plain model (Theorem 2).
3. Unbounded query secure PRUs, with one call to the Haar random oracle, does **not** exist in iQHROM (Theorem 3)
4. Bounded query secure PRUs, with one call to the Haar random oracle, exists in iQHROM (Theorem 4)
5. Multi-copy PRSGs, with one call to the Haar random oracle, exists in iQHROM (Theorem 6)
6. Adaptively secure PRFSs, with one call to the Haar random oracle, exists in the iQHROM (Theorem 7)
7. The negative result in bullet 3 can be generalized further: unbounded query secure PRUs, with any number of parallel calls to the Haar random oracle, does **not** exist in iQHROM (Theorem 5)

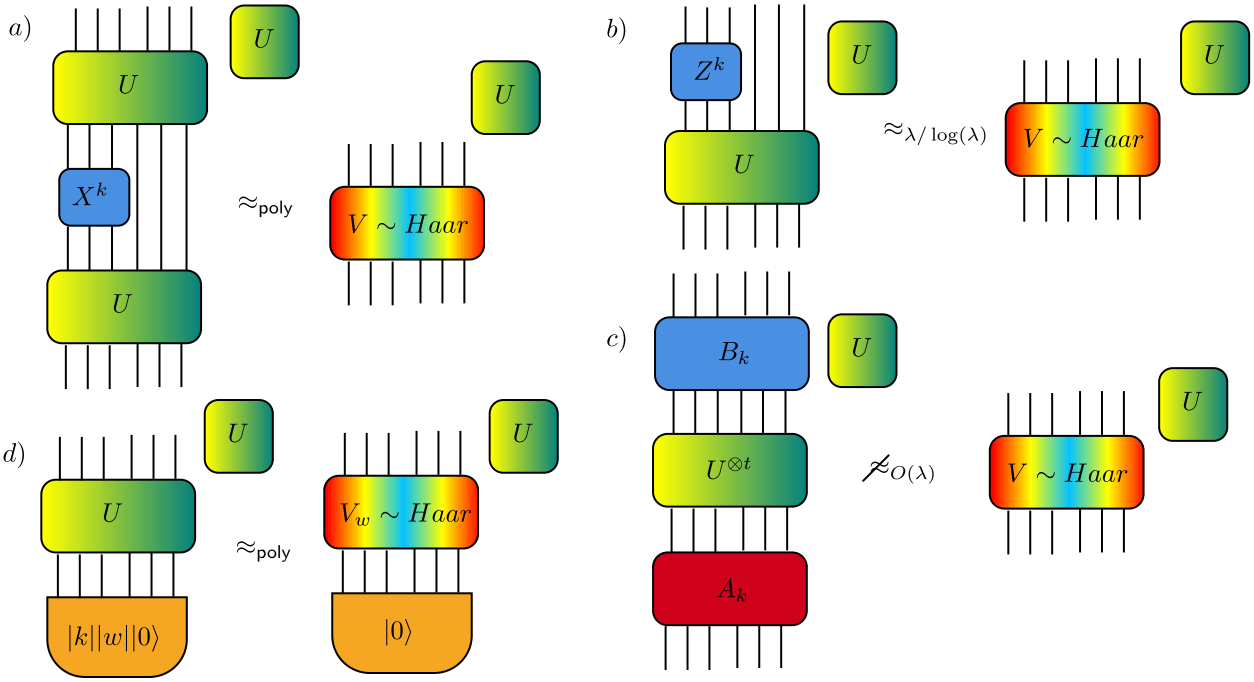

Figure 1: A summary of our results, time goes up in all diagrams. **(a)** We show that the simple UXU is indistinguishable from an independently sampled Haar random unitary for adversaries who have query access to U. **(b)** We also show that up to $\lambda/\log(\lambda)$ queries, the even simpler unitary ZU is indistinguishable from a Haar random unitary to adversaries that have query access to U. **(c)** We also show that there is no construction of $O(\lambda)$-secure pseudo-random unitaries that only make a single parallel query to the common Haar random unitary, if the adversary is given polynomial-space computation. **(d)** Finally, we show that simply calling the Haar random unitary on a uniformly random classical basis state is indistinguishable from a Haar random state to adversaries that get polynomially many queries to U, yielding both PRSGs and PRFSs

2 Related Work

Quantum Pseudorandomness. Study into quantum pseudorandomness began with the work of [JLS18], who first defined pseudorandom states and unitaries.[JLS18] presented the first construction of pseudorandom states from one-way functions. Since then, a few works [BS19; BS20; AGQY22] presented improved and simpler constructions of pseudorandom states. However, until very recently, the construction of pseudorandom unitaries have remained elusive. Recently, a few works [LQS+23; AGKL24; BM24] made progress on building pseudorandom unitaries. Specifically, they consider the security of pseudorandom unitaries on specific sets of queries.

Building on these results, [MPSY24] provided the first constructions of non-adaptively secure pseudorandom unitaries, which used the so-called PFC ensemble (which stands for "Permutation-Random Function-Clifford"). [CBB+24] simultaneously constructed pseudorandom unitaries from random permutations, but both papers rely heavily on Schur-Weyl duality and the properties of the symmetric group. Recently, [MH24] extended the compressed oracle techniques of [Zha19] to the path recording formalism for Haar random unitaries. Specifically, they show that the PFC ensemble is a pseudorandom unitary and that C†PFC is additionally inverse secure. [SHH24] showed that low-depth pseudorandom unitaries can be instantiated from concrete assumptions such as LWE.

Common Haar State Model. The common Haar random state model (CHRS) [AGL24; CCS24] is an idealized model of computation where all parties have access to a joint common state, and can be viewed as the quantum equivalent of the classical common reference string model. Both works show that in the CHRS model, some form of bounded copy pseudorandom states with short keys (and therefore quantum bit commitments) exist, while ruling out a wide range of other primitives. [AGL24] rule out quantum cryptography primitives with classical communication, and [CCS24] rule out unbounded copy pseudorandom states. While this idealized model is interesting to study and provides both efficient constructions of cryptographic primitives and black box separations, the model can be problematic to instantiate in a realistic setting. For example, instantiating the model in the real world might require a complicated multi-party computation to compute a shared quantum state, or a trusted third party who can distribute copies of the state.

Quantum Haar Random Oracle Model. The quantum Haar random oracle model was first introduced in [CM24], who provided a construction of succinct commitments. However, [CM24] was not able to analyze the security of their mode in the QHROM. [BFV20] separately consider the QHROM, using it as an idealized model of the scrambling behavior of black holes. They provide a construction of pseudorandom states, with a proof sketch. The common denominator in both the works is the lack of techniques to formally analyze security in the quantum Haar random oracle model. Finally, [Kre21] considers an idealized version of pseudorandom states, consisting of 2^λ many Haar random unitaries. They show that relative to this oracle and a PSPACE oracle, one-way functions do not exist while pseudorandom unitaries do.

3 Technical Overview

Here we provide proof sketches for the our construction of unbounded-copy secure pseudorandom unitaries in the iQHROM (Section 3.2), our negative result on an unbounded pseudorandom unitary from a single parallel query (Section 3.3), our construction of bounded-copy secure pseudorandom unitaries from a single query in the iQHROM (Section 3.4), and our simple construction of pseudorandom states in the iQHROM (Section 3.5).

3.1 Path Recording Formalism of Ma and Huang

We begin by recalling the (forward secure) characterization of Haar random unitaries, known colloquially as the path recording framework. If A, X and Y be three quantum registers, with A being the adversary's register and XY being purifying registers, then the path recording oracle $\mathsf{PR} : \mathsf{AXY} \mapsto \mathsf{AXY}$ is the following linear map:

$$\mathsf{PR} : |x\rangle_{\mathsf{A}} \otimes |R\rangle_{\mathsf{XY}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{y \in [N] \setminus \mathrm{Im}(R)} |y\rangle_{\mathsf{A}} \otimes |R \cup \{(x,y)\}\rangle \,,$$

where R is an injective relation state, which is a set of input/output pairs with the condition that the same output never appears twice in the set, and $\mathrm{Im}(R)$ is the set of outputs in the relation state. In the rest of this technical overview, we drop the normalizing factor of $\frac{1}{\sqrt{N-|R|}}$. [MH24] show that the path recording oracle is right invariant and thus indistinguishable from oracle access to a Haar random unitary. In the paper of [MH24], the authors go on to argue that the action of a uniformly random sampled permutation and binary phase function (i.e. PF) is identical to the path recording oracle *if* the inputs to the oracle are distinct. Using the properties of a 2-design, they show that any adversary (except with negligible probability) will query the PF part of the PFC oracle on distinct strings, allowing them to claim the following are all (approximately) indistinguishable from each other

$$\mathsf{PFC} \approx \mathsf{PR} \cdot \mathsf{C} \approx \mathsf{PR} \approx \mathsf{PR} \cdot \mathcal{U} \approx \mathsf{PF} \cdot \mathcal{U} = \mathcal{U} \,.$$

As the path recording framework is so important to the result of this paper, we review some of the proof. Let $\mathcal{A}$ be a t-query adversary, and let $|\mathcal{A}^{\mathsf{PR}}\rangle$ be the state of the adversary with access to PR. We can write this state as follows:

$$|\mathcal{A}^{\mathsf{PR}}\rangle = \prod_{i=1}^{t} (\mathsf{PR}_{\mathsf{AXY}} \cdot A_i) |0\rangle_{\mathsf{A}} \otimes |\{\}\rangle_{\mathsf{XY}} .$$

Expanding the definition of the path recording oracle, we get the following state:

$$|\mathcal{A}^{\mathsf{PR}}\rangle = \sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} (|y_i\rangle\langle x_i| \cdot A_i) |0\rangle_{\mathsf{A}} \otimes |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} .$$

Now consider another oracle, where instead of only being given access to the path recording oracle, the adversary is given access to an oracle that first applies a unitary $U = \sum_{x,y\in[N]} \alpha_{xy}|y\rangle\langle x|$, and then applies the path recording oracle.

$$\begin{aligned}
|\mathcal{A}^{\mathsf{PR}\cdot U}\rangle &= \sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} (|y_i\rangle\langle x_i| \cdot U \cdot A_i) |0\rangle_{\mathsf{A}} \otimes |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} \\
&= \sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(\sum_{z_i} \alpha_{z_i,x_i} |y_i\rangle\langle z_i| \cdot A_i\right) |0\rangle_{\mathsf{A}} \otimes |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} \\
&= \sum_{\substack{\vec{x},\vec{z}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} (|y_i\rangle\langle z_i| \cdot A_i) |0\rangle_{\mathsf{A}} \otimes \alpha_{z_i,x_i} |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} \\
&= \sum_{\substack{\vec{x},\vec{z}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} (|y_i\rangle\langle x_i| \cdot A_i) |0\rangle_{\mathsf{A}} \otimes \alpha_{x_i,z_i} |\{(z_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} \\
&= \sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} (|y_i\rangle\langle x_i| \cdot A_i) |0\rangle_{\mathsf{A}} \otimes U_{\mathsf{X}}^{\otimes t} |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} .
\end{aligned}$$

Here the second line is the result of expanding U, the third line is the result of aggregating all of the sums and moving the coefficient α_{z_i,x_i} to the purifying register, and the next lines the result of re-labelling $x_i \leftrightarrow z_i$ and subsequently applying the definition of U again. Thus, the state in the A register (after tracing out XY) remains un-changed after applying U. Taking U to be sampled from the Haar measure, we see that the state of an adversary with access to the path recording oracle is identical to their state if they first applied a Haar random unitary and then had the path recording oracle act, which is itself indistinguishable from a Haar random unitary (without the path recording).

3.2 (Unbounded) PRUs with Two Queries

The construction of unbounded-query pseudorandom unitaries in the iQHROM (with U being the Haar random oracle) is the following

$$\mathsf{PRU}_k^U = U(X^k \otimes \mathrm{id})U .$$

To show that this is a pseudorandom unitary, our goal is to show that (U, PRU_k^U) is computationally indistinguishable from (U, V), where V is sampled independently from the Haar measure, to an adversary that makes a polynomial number of queries. At a high level, we want to show that (in the purifying register), X^k allows the path recording oracle to dis-entangle calls to U and PRU_k^U, which will allow the oracle (except with negligible probability) to record the calls to the pseudorandom unitary in a separate register than calls to U, resembling an entirely distinct path recording oracle.

In order to prove this, we can extend the path recording oracle to the case when an adversary $\mathcal{A}$ gets access to two Haar random unitaries U and V and makes t queries. In this case, we can replace both Haar random unitaries with *distinct* path recording oracles PR_1 and PR_2, each with their own purifying register, $\mathsf{X}_1\mathsf{Y}_1$, and $\mathsf{X}_2\mathsf{Y}_2$. If we say $\mathcal{A}^{\mathsf{PR}_1,\mathsf{PR}_2}$ makes alternating queries to each of their oracles (with unitaries A_i and B_i before the respective oracle calls), we can express their state as follows:

$$|\mathcal{A}^{\mathsf{PR}_1,\mathsf{PR}_2}\rangle = \sum_{\substack{\vec{x},\vec{a}\in[N]^t \\ \vec{y},\vec{b}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|b_i\rangle\langle a_i| \cdot B_i|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} \otimes |\{(x_i,y_i)\}_{i\in[t]}\rangle_{\mathsf{X}_1\mathsf{Y}_1}|\{(a_i,b_i)\}_{i\in[t]}\rangle_{\mathsf{X}_2\mathsf{Y}_2}\,.$$

Similarly, we can write the state of the t-query adversary after querying U and PRU^U_k for a uniformly random k using the path recording framework as follows:

$$\begin{aligned}
&|\mathcal{A}^{\mathsf{PR},\mathsf{PRU}(\mathsf{PR})}\rangle \\
&\quad= \sum_{k\in\{0,1\}^\lambda} \sum_{\substack{\vec{x},\vec{a},\vec{c}\in[N]^t \\ (\vec{y},\vec{b},\vec{d})\in[N]^{3t}_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|d_i\rangle\langle c_i|b_i\oplus k\rangle\langle a_i| \cdot B_i|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} \otimes |\{(x_i,y_i),(a_i,b_i),(c_i,d_i)\}_{i\in[t]}\rangle_{\mathsf{XY}}|k\rangle_{\mathsf{K}} \\
&\quad= \sum_{k\in\{0,1\}^\lambda} \sum_{\substack{\vec{x},\vec{a},\in[N]^t \\ (\vec{y},\vec{b},\vec{d})\in[N]^{3t}_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|d_i\rangle\langle a_i| \cdot B_i|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} \otimes |\{(x_i,y_i),(a_i,b_i),(b_i\oplus k,d_i)\}_{i\in[t]}\rangle_{\mathsf{XY}}|k\rangle_{\mathsf{K}}\,.
\end{aligned}$$

Here the first line uses the fact that $X^k|y\rangle = |y\oplus k\rangle$, together with the expansion of the path recording oracle PR. The second line removes terms in the sum for which $\langle c_i|b_i\oplus k\rangle = 0$. Note that we also purify the key register K so that we can write the adversary's purified view as a pure state.

To show the closeness between $|\mathcal{A}^{\mathsf{PR}_1,\mathsf{PR}_2}\rangle$ and $|\mathcal{A}^{\mathsf{PR},\mathsf{PRU}(\mathsf{PR})}\rangle$ after partially tracing out their purified registers, our approach is to define two isometries $\mathsf{Split}:\mathsf{XYK}\to\mathsf{X}_1\mathsf{Y}_1\mathsf{X}_2\mathsf{Z}_2\mathsf{Y}_2\mathsf{K}$ and $\mathsf{Augment}:\mathsf{X}_1\mathsf{Y}_1\mathsf{X}_2\mathsf{Y}_2\to\mathsf{X}_1\mathsf{Y}_1\mathsf{X}_2\mathsf{Z}_2\mathsf{Y}_2\mathsf{K}$, where Z_2 is an ancilla register, such that

$$\mathsf{Split}|\mathcal{A}^{\mathsf{PR},\mathsf{PRU}(\mathsf{PR})}\rangle \approx \mathsf{Augment}|\mathcal{A}^{\mathsf{PR}_1,\mathsf{PR}_2}\rangle.$$

For intuition, we have the following *classical* interpretation of path recording oracles.

Splitting $|\mathcal{A}^{\mathsf{PR},\mathsf{PRU}(\mathsf{PR})}\rangle$. Suppose a classical algorithm $\mathcal{A}$ is given oracle access to *randomized* oracles $f:\{0,1\}^n\to\{0,1\}^n$ and $G^f_k:\{0,1\}^n\to\{0,1\}^n$. Without loss of generality, we assume that $\mathcal{A}$ alternatively asks $t=\mathsf{poly}(\lambda)$ queries to each of f and G^f_k.[5] The distribution of (f,G^f_k) is defined via the following interactive experiment involving a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. First, $\mathcal{C}$ initializes an empty relation $R=\emptyset$ and samples $k\xleftarrow{\$}\{0,1\}^n$. For odd i's, upon receiving query x_i to f, $\mathcal{C}$ samples $y_i\xleftarrow{\$}\{0,1\}^n\setminus\mathrm{Im}(R)$, adds (x_i,y_i) to R, and returns y_i to $\mathcal{A}$. For even i's, upon receiving query x_i to G^f_k, $\mathcal{C}$ samples $z_{i/2}\xleftarrow{\$}\{0,1\}^n\setminus\mathrm{Im}(R)$, adds $(x_i,z_{i/2})$ to R, samples $y_i\xleftarrow{\$}\{0,1\}^n\setminus\mathrm{Im}(R)$, adds $(z_{i/2}\oplus k,y_i)$ to R, and returns y_i to $\mathcal{A}$. Note that even if some x_i's are equal to each other, the corresponding y_i's are pairwise distinct. At the end, $\mathcal{A}$ has learned the query-answer pairs $\{(x_i,y_i)\}_{i\in[2t]}$. On the other hand, R is of size $3t$ and becomes

$$\{(x_1,y_1),(x_2,z_1),(z_1\oplus k,y_2),\ldots,(x_{2t-1},y_{2t-1}),(x_{2t},z_t),(z_t\oplus k,y_{2t})\}.$$

We crucially rely on the notion of *correlated pairs* defined as follows. Given (R,k), a pair $((u,v),(u',v'))\in R\times R$ is *k-correlated* if $v\oplus u'=k$. Note that, as long as there are only t many k-correlated pairs, we can

[5] That is the adversary makes all odd-indexed queries to f and all even-indexed queries to G^f_k.

always split odd and even queries. We say that $\mathcal{A}$ wins if there are more than t many k-correlated pairs in R.

We first show that $\mathcal{A}$'s winning probability is negligible. The idea is to defer the sampling of k until $\mathcal{A}$ is done with querying. Consider the following identically distributed experiment. First, $\mathcal{C}$ initializes an empty relation $R = \emptyset$. For odd i's, upon receiving query x_i to f, $\mathcal{C}$ samples $y_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Im}(R)$, adds (x_i, y_i) to R, and returns y_i to $\mathcal{A}$. For even i's, upon receiving query x_i to G_k^f, $\mathcal{C}$ samples $y_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Im}(R)$, adds $(\perp, y_i)$ to R, and returns y_i to $\mathcal{A}$. At the end, for $i \in [t]$, $\mathcal{C}$ samples $z_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Im}(R)$ and adds (x_{2i}, z_i) to R. Finally, $\mathcal{C}$ samples $k \xleftarrow{\$} \{0,1\}^n$ and updates $(\perp, y_{2i}) \mapsto (z_i \oplus k, y_{2i})$ for $i \in [t]$.

By a careful case analysis, we show that for *any* $(\vec{x}, \vec{y}, \vec{z})$[6] in the support, $R_k := \{(x_1, y_1), (x_2, z_1), (z_1 \oplus k, y_2), \dots, (x_{2t-1}, y_{2t-1}), (x_{2t}, z_t), (z_t \oplus k, y_{2t})\}$ has more than t many k-correlated pairs *if and only if* k is of the form $x_i \oplus y_j$ or $x_i \oplus z_j$ for some i, j. That is to say, right before $\mathcal{C}$ samples k, there are *always* at most $O(t^2) = \mathsf{poly}(\lambda)$ many "bad" keys k such that (R_k, k) has more than t many k-correlated pairs. Therefore, the winning probability of $\mathcal{A}$ is at most $O(t^2/2^\lambda) = \mathsf{negl}(\lambda)$. Suppose $\mathcal{A}$ does not win, observe that R_k has exactly t *mutually disjoint* k-correlated pairs. With the information of k, one can uniquely map R_k into $(R_k^{\mathsf{iso}}, R_k^{\mathsf{cor}})$ where $R_k^{\mathsf{iso}} := \{(x_{2i-1}, y_{2i-1})\}_{i \in [t]}$ and $R_k^{\mathsf{cor}} := \{(x_{2i}, z_i, y_{2i})\}_{i \in [t]}$.

Augmenting $|\mathcal{A}^{\mathsf{PR}_1, \mathsf{PR}_2}\rangle$. Suppose a classical algorithm $\mathcal{A}$ is given oracle access to randomized oracles $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$. Similarly, we assume that $\mathcal{A}$ alternatively asks t queries to each oracle. The distribution of (f_1, f_2) is defined via the following interactive experiment involving a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. First, $\mathcal{C}$ initializes two empty relations $R_1 = R_2 = \emptyset$. For odd i's, upon receiving query x_i to f_1, $\mathcal{C}$ samples $y_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Im}(R_1 \cup R_2)$, adds (x_i, y_i) to R_1, and returns y_i to $\mathcal{A}$. For even i's, upon receiving query x_i to f_2, $\mathcal{C}$ samples $y_i \xleftarrow{\$} \{0,1\}^n \setminus \mathrm{Im}(R_1 \cup R_2)$, adds (x_i, y_i) to R_2, and returns y_i to $\mathcal{A}$.[7] At the end, we have $R_1 = \{(x_{2i-1}, y_{2i-1})\}_{i \in [t]}$ and $R_2 = \{(x_{2i}, y_{2i})\}_{i \in [t]}$.

Now, our goal is to sample $(\{z_i\}_{i \in [t]}, k)$ conditioned on (R_1, R_2) so that the joint distribution of $(\{(x_{2i-1}, y_{2i-1})\}_{i \in [q]}$ and $\{(x_{2i}, z_i, y_{2i})\}_{i \in [t]}, k)$ is negligibly close to that of $(R_k^{\mathsf{iso}}, R_k^{\mathsf{cor}}, k)$ in the previous experiment. The following natural way turns out to work: for $i \in [t]$, sample $z_i \xleftarrow{\$} \{0,1\}^n \setminus (\mathrm{Im}(R_1 \cup R_2) \cup \bigcup_{j<i} \{z_j\})$; sample a uniformly random k conditioned on k is not of the form $x_i \oplus y_j$ or $x_i \oplus z_j$ for some i, j.

It turns out that the above classical reasoning offers a method for deriving the quantum proof in Section 7, though it involves technical subtleties. To work through these technical subtleties, we introduce a framework of working with relation states in Section 6.3. We employ the mentioned framework to construct Split and $\mathsf{Augment}$.

3.3 (Unbounded) PRUs: One Parallel Query is Insufficient

We also show that sequential queries to the Haar random oracle are required to get unbounded query secure pseudorandom unitaries. Formally, we show that for every PRU construction in the iQHROM that only makes a single parallel calls to U, there is a polynomial space adversary that breaks PRU security with $O(\lambda)$ many non-adaptive calls to the PRU and common Haar random unitary. In order to prove this, we use the quantum OR attack from [CCS24]. In particular, we show how, using the ricochet property of EPR pairs, an adversary can prepare the Choi state $|\Phi_{\mathsf{PRU}_k}\rangle$ from many copies of $|\Phi_U\rangle$.

Then, an adversary given oracle access to $\mathcal{O}$ can prepare many copies of $|\Phi_{\mathcal{O}}\rangle$ and perform swap tests with $|\Phi_{\mathsf{PRU}_k}\rangle$ to determine if they have access to one of the pseudorandom unitaries or an independently sampled Haar random unitary. Since there is a unitary that prepares $|\Phi_{\mathsf{PRU}_k}\rangle$ from many copies of $|\Phi_U\rangle$, the adversary can recover and re-use their copies of $|\Phi_U\rangle$. The proof of correctness follows a similar line as [CCS24]. We also present a tighter analysis using techniques from [AGL24] when the PRU construction queries the Haar random oracle exactly once.

[6] Here $\vec{x} := (x_1, x_2, \dots, x_{2t})$, $\vec{y} := (y_1, y_2, \dots, y_{2t})$ and $\vec{z} := (z_1, x_2, \dots, z_t)$.

[7] Notice that by definition, it is always the case that $\mathrm{Im}(R_1) \cap \mathrm{Im}(R_2) = \emptyset$ whereas it is not necessarily true for $|\mathcal{A}^{\mathsf{PR}_1, \mathsf{PR}_2}\rangle$. However, in Section 6 we prove that making such an approximation only introduces negligible error.

3.4 (Bounded) PRUs with One Query: Feasibility

In the case where the construction only makes a single query to the Haar random oracle, we present an even simpler construction of $o(\lambda/\log(\lambda))$-query secure pseudorandom unitaries. Specifically, the pseudorandom unitary is the following

$$\mathsf{PRU}_k^U = (Z^k \otimes \mathrm{id})U\,.$$

We prove that all adversaries making $o(\lambda/\log(\lambda))$ (potentially adaptive) calls to PRU and arbitrary polynomial calls to U cannot distinguish between PRU and an independently sampled Haar random unitary. To show this, begin by writing out the construction using the path recording framework to represent U. We will write the state assuming that the adversary t total queries of with ℓ queries are made to PRU_k^U (on indices $\mathbf{a} = \{a_1, \ldots, a_\ell\}$).

$$|\mathcal{A}^{\mathsf{PR},\mathsf{PRU}(\mathsf{PR})}\rangle = \sum_{k\in\{0,1\}^\lambda} \sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} (-1)^{\langle k||0^{n-\lambda}, \bigoplus_{i\in\mathbf{a}} y_i\rangle} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} \otimes |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} |k\rangle_{\mathsf{K}}\,.$$

Here the phase comes from the fact that $Z^k|y\rangle = (-1)^{\langle k,y\rangle}|y\rangle$. Then we can push both the phase, and sum over keys into the K register to the following state

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} \sum_{k\in\{0,1\}^\lambda} (-1)^{\langle k||0^{n-\lambda}, \bigoplus_{i\in\mathbf{a}} y_i\rangle} |k\rangle_{\mathsf{K}}$$

Then if we apply an isometry that appends $n-\lambda$ many 0's to the key register and then performs an n-qubit Hadamard, we get the following.

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} |\{(x_i, y_i)\}_{i\in[t]}\rangle_{\mathsf{XY}} |\bigoplus_{i\in\mathbf{a}} y_i\rangle_{\mathsf{K}}$$

Using the idea of ℓ-fold collision-freeness from [AGL24], we are able to show that if $\vec{y}$ is an ℓ-fold collision-free set, the XOR of all the $\{y_i\}_{i\in\mathbf{a}}$ will suffice to determine all $\{y_i\}_{i\in\mathbf{a}}$ from $\vec{y}$. We show that as long as $\ell = o(\lambda/\log(\lambda))$, the weight on ℓ-fold collision-free $\vec{y}$'s is overwhelming. Thus, there is an isometry that for most $\vec{y}$'s identifies $\{y_i\}_{i\in\mathbf{a}}$ from the XOR value in the key register, and extracts the elements of the set into a new relation state. Hence, outputting a state close to the following

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i| \cdot A_i\right)|0\rangle_{\mathsf{A}} |\{(x_i, y_i)\}_{i\in[t]\setminus\mathbf{a}}\rangle |\{(x_i, y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{XY}}.$$

This is exactly the state that the adversary would have after querying two independent Haar random unitaries, as desired.

3.5 (Unbounded) Pseudorandom States with One Query

We also present an extremely simple construction of pseudorandom states in the iQHROM. The pseudorandom state for key k of size λ is simply

$$|\psi_k\rangle = U|k||0^n\rangle\,.$$

In order to show that this is a pseudorandom state even against adversaries who can query U, we write out the state of the adversary who recieves t copies of the pseudorandom state as input. The state will be proportional to

$$\sum_{k=0}^{2^\lambda-1} (\mathsf{PR}|k||0\rangle)^{\otimes t}\,|k||0^n\rangle = \sum_{y_1,\ldots,y_t\in[N]^t_{\mathrm{dist}}} |y_1,\ldots,y_t\rangle \otimes \sum_{k=0}^{2^\lambda-1} |\{(k||0,y_i)\}_{i=1}^t\rangle|k||0\rangle\,.$$

Then when the adversary makes s additional calls to the Haar random unitary, they will have the following state

$$\sum_{\vec{x}\in[N]^s}\ \sum_{(\vec{y},\vec{z})\in[N]^{t+s}_{\mathrm{dist}}} \left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|A_i\right)|y_1,\ldots,y_t\rangle|0\rangle \otimes \sum_{k=0}^{2^\lambda-1} |\{(k||0,y_i)\}_{i=1}^t \cup \{(x_j,z_j)\}_{j=1}^s\rangle|k||0\rangle$$

Then, we can imagine the state that results from projecting the key register onto keys not in the support of $\vec{x}$. Since there are at most t keys, this will lead to an error of $O(t/\sqrt{2^\lambda})$. For those keys that are distinct from $\{x_j\}$, we can apply an isometry on the purifying register that extracts out the elements of the relation that have input $k||0$, to get the following state

$$\sum_{\vec{x}\in[N]^s}\ \sum_{(\vec{y},\vec{z})\in[N]^{t+s}_{\mathrm{dist}}} \left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|A_i\right)|y_1,\ldots,y_t\rangle|0\rangle \otimes |\{(0,y_i)\}_{i=1}^t\rangle|\{(x_j,z_j)\}_{j=1}^s\rangle\,.$$

Notice that for the Haar random case, y and z are sampled independently instead of being sampled to be distinct from each other. However, the probability that uniformly random $\vec{z}$ overlaps with $\vec{y}$ is on the order of $(t+s)^2/2^{n+\lambda}$. Thus, the two states are close in trace distance, and our original construction is a pseudorandom state.

4 Preliminaries

We denote the security parameter by λ. We assume that the reader is familiar with fundamentals of quantum computing, otherwise readers can refer to [NC10].

4.1 Notation

Indexing and sets We use the notation $[n]$ to refer to the set $\{1,\ldots,n\}$. For a string $x\in\{0,1\}^{n+m}$, let $x_{[1:n]}$ to denote the first n bits of x. For a finite set T, we use the binomial notation $\binom{T}{k}$ to refer to the set of all size-k subsets of T. We also use the notation $x \overset{\$}{\leftarrow} T$ to indicate that x is sampled uniformly at random from T. For $N,\ell\in\mathbb{N}$, we let $N^{\downarrow\ell}=\prod_{i=0}^{\ell-1}(N-i)$. We use $\uplus$ to denote the disjoint union of two sets.

Set products and the symmetric group We use Sym_t to refer to the symmetric group over t elements (i.e. the group of all permutations of t elements). Given a set A and $t\in\mathbb{N}$, we use the notation A^t to denote the t-fold Cartesian product of A, and the notation A^t_{dist} to denote distinct subspace of A^t, i.e. the vectors in A^t, $\vec{y}=(y_1,\ldots,y_t)$, such that for all $i\neq j$, $y_i\neq y_j$. We also define $\{\vec{x}\} := \bigcup_{i\in[t]}\{x_i\}$.

Quantum states and distances A register R is a named finite-dimensional Hilbert space. If A and B are registers, then AB denotes the tensor product of the two associated Hilbert spaces. We denote by $\mathcal{D}(\mathsf{R})$ the density matrices over register R. For $\rho_{\mathsf{AB}}\in\mathcal{D}(\mathsf{AB})$, we let $\mathrm{Tr}_{\mathsf{B}}(\rho_{\mathsf{AB}})\in\mathcal{D}(\mathsf{A})$ denote the reduced density matrix that results from taking the partial trace over B. We denote by $\mathsf{TD}(\rho,\rho')=\frac{1}{2}\|\rho-\rho'\|_1$ the trace distance between ρ and ρ', where $\|X\|_1=\mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$ is the trace norm. For two pure (and possibly subnormalized) states $|\psi\rangle$ and $|\phi\rangle$, we use $\mathsf{TD}(|\psi\rangle,|\phi\rangle)$ as a shorthand for $\mathsf{TD}(|\psi\rangle\langle\psi|,|\phi\rangle\langle\phi|)$. We also say that $A \preceq B$ if $B - A$ is a positive semi-definite matrix. For a permutation $\sigma \in \mathsf{Sym}_t$, we let $(S_\sigma)_{\mathsf{R}_1 \dots \mathsf{R}_t}$ be the nt-qubit unitary that acts on registers $\mathsf{R}_1, \dots, \mathsf{R}_t$ by permuting the registers according to σ. That is,

$$S_\sigma |x_1, \dots, x_t\rangle = |x_{\sigma(1)}, \dots, x_{\sigma(t)}\rangle \,.$$

We denote by $\mathcal{H}_n$ the Haar distribution over n-qubit states, and μ_n the Haar measure over n-qubit unitaries (i.e. the unique left and right invariant measure).

4.2 Cryptographic Primitives

In this section, we define the quantum cryptographic primitives that we reference in the rest of the paper, beginning with pseudorandom states [JLS18].

Definition 8 (Pseudorandom states)**.** *We say that a quantum polynomial-time algorithm G is a* pseudorandom state (PRS) generator *if the following holds:*

- *(Pure output) For all λ and $k \in \{0,1\}^\lambda$, the algorithm outputs*

$$G_\lambda(k) = |\psi_k\rangle\langle\psi_k| \,,$$

for some $n(\lambda)$-qubit pure state $|\psi_k\rangle$.

- *(Pseudorandomness) For all polynomials t and quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that for all λ,*

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[1 \leftarrow \mathcal{A}_\lambda(|\psi_k\rangle^{\otimes t(\lambda)}) \right] - \Pr_{|\psi\rangle \leftarrow \mathcal{H}_{n(\lambda)}} \left[1 \leftarrow \mathcal{A}_\lambda(|\psi\rangle^{\otimes t(\lambda)}) \right] \right| \le \epsilon(\lambda) \,.$$

In the iQHROM*, both G_λ and $\mathcal{A}_\lambda$ have oracle access to a family of unitaries $\{U_\lambda\}_{\lambda \in \mathbb{N}}$ sampled from the Haar measure on λ qubits.*

Pseudorandom state generators can be generalized into pseudorandom function-like states [AGQY22], which are a family of states (indexed by a parameter w) that look as if they were all sampled independently from the Haar measure.

Definition 9 (Pseudorandom function-like states)**.** *A quantum polynomial-time algorithm G is an* adaptively secure pseudorandom function-like state (APRFS) *generator if for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that for all λ,*

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[1 \leftarrow \mathcal{A}_\lambda^{\mathcal{O}_{\mathsf{PRFS}}(k,\cdot)} \right] - \Pr_{\mathcal{O}_{\mathsf{Haar}}} \left[1 \leftarrow \mathcal{A}_\lambda^{\mathcal{O}_{\mathsf{Haar}}(\cdot)} \right] \right| \le \varepsilon(\lambda),$$

where:

- *$\mathcal{O}_{\mathsf{PRFS}}(k, \cdot)$, on input $w \in \{0,1\}^{m(\lambda)}$, outputs $G_\lambda(k, w)$.*
- *$\mathcal{O}_{\mathsf{Haar}}(\cdot)$, on input $w \in \{0,1\}^{m(\lambda)}$, outputs $|\vartheta_w\rangle$, where, for every $y \in \{0,1\}^{m(\lambda)}$, $|\vartheta_y\rangle \leftarrow \mathcal{H}_{n(\lambda)}$.*

Moreover, the adversary A_λ has classical *access to $\mathcal{O}_{\mathsf{PRFS}}(k, \cdot)$ and $\mathcal{O}_{\mathsf{Haar}}(\cdot)$. That is, we can assume without loss of generality that any query made to either oracle is measured in the computational basis.*[8]

In the iQHROM*, both G_λ and $\mathcal{A}_\lambda$ have oracle access to a family of unitaries $\{U_\lambda\}_{\lambda \in \mathbb{N}}$ sampled from the Haar measure on λ qubits.*

We say that G is a $(\lambda, m(\lambda), n(\lambda))$-APRFS generator to succinctly indicate that its input length is $m(\lambda)$ and its output length is $n(\lambda)$.

[8] In [AGQY22], the authors further study a stronger security notation called *quantum-accessible adaptively secure pseudorandom function-like states (QAPRFS)*, where the adversary has *superposition* oracle access to $\mathcal{O}_{\mathsf{PRFS}}(k, \cdot)$ and $\mathcal{O}_{\mathsf{Haar}}(\cdot)$.

Pseudorandom unitaries [JLS18] are the quantum equivalent of a pseudorandom function, in that an adversary can not distinguish the PRU from a truly Haar random unitary.

Definition 10 (Pseudorandom unitaries)**.** *We say that a quantum polynomial-time algorithm G is a pseudorandom unitary if for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that for all λ,*

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[1 \leftarrow \mathcal{A}_\lambda^{G_\lambda(k)} \right] - \Pr_{\mathcal{U} \leftarrow \mu_{n(\lambda)}} \left[1 \leftarrow \mathcal{A}_\lambda^{\mathcal{U}} \right] \right| \leq \epsilon(\lambda)\,.$$

In the iQHROM, both G_λ and $\mathcal{A}_\lambda$ have oracle access to an additional family of unitaries $\{U_\lambda\}_{\lambda \in \mathbb{N}}$ sampled from the Haar measure on λ qubits.

4.3 Useful Lemmas

Here we present useful quantum lemmas that should be familiar to a reader well versed in quantum computation.

Lemma 11 (Gentle operator lemma, a special case of [Wil11, Lemma 9.4.2 & Exercise 9.4.1])**.** *Let $|\psi\rangle$ be a subnormalized state and Π a projector. Then $\mathsf{TD}(|\psi\rangle, \Pi|\psi\rangle) \leq \sqrt{1 - \|\Pi|\psi\rangle\|^2}$.*

Lemma 12. *Let $|\phi\rangle$ be a state and $|\psi\rangle$ a subnormalized state, $\||\psi\rangle\| \geq |\langle\psi|\phi\rangle|$.*

Proof. By Cauchy-Schwarz inequality, $|\langle\psi|\phi\rangle|^2 \leq \||\psi\rangle\|^2 \||\phi\rangle\|^2$. Since $\||\phi\rangle\| = 1$, we have $|\langle\psi|\phi\rangle| \leq \||\psi\rangle\|$. □

Lemma 13. *Let $\{|i\rangle\}_{i \in [N]}$ be some set of orthonormal vectors. Let $|\psi\rangle = \sum_i |i\rangle|\psi_i\rangle$ be a normalized state. Let $\{\alpha_i\}_{i \in [N]}$, be a set of non-negative real numbers with $\alpha_i \geq \beta$. Define the vector $|\phi\rangle := \sum_i \alpha_i |i\rangle|\psi_i\rangle$. Then $\langle\psi|\phi\rangle \geq \beta$.*

Proof. Notice that $\langle\psi|\phi\rangle = \sum_i \alpha_i \langle\psi_i|\psi_i\rangle$. Since $\alpha_i \geq \beta$ and $\langle\psi_i|\psi_i\rangle \geq 0$, we have $\langle\psi|\phi\rangle \geq \beta \cdot \sum_i \langle\psi_i|\psi_i\rangle$. Moreover, since $|\psi\rangle$ is normalized, we have $\langle\psi|\psi\rangle = \sum_i \langle\psi_i|\psi_i\rangle = 1$. Hence, $\langle\psi|\phi\rangle \geq \beta$. □

Lemma 14 (Ricochet property)**.** *Let $|\Omega\rangle$ be an EPR pair on registers AB and U be a unitary acting on A, then the following holds:*

$$(U \otimes \mathrm{id})|\Omega\rangle = (\mathrm{id} \otimes U^\intercal)|\Omega\rangle\,.$$

5 Ma-Huang's Path-Recording Framework

We first recall the path-recording framework by Ma and Huang [MH24]. Most of the text is copied verbatim from [MH24], but is contained here for the sake of completeness.

5.1 Oracle Adversary

We present the following definition of an oracle adversary.

Definition 15 (Oracle Adversary)**.** *An oracle adversary $\mathcal{A}$ is a quantum algorithm that makes queries to an oracle $\mathcal{O}$ that acts on the first n qubits of the adversary's space, which we call the A register. The adversary also has an m-qubit ancillary space, which we call the B register. A t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$.*

Definition 16 (Oracle Adversary's view after t queries)**.** *Given a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$, we define the adversary's view after t queries as:*

$$|\mathcal{A}^{\mathcal{O}}_t\rangle_{\mathsf{AB}} = \prod_{i=1}^{t} \left(\mathcal{O}_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}}$$

Here, $\mathcal{O}$ represents the n-qubit oracle, and $A^{(i)}_{\mathsf{AB}}$ is the unitary operation applied by the adversary between the $(i-1)^{th}$ and i^{th} oracle queries. For an arbitrary t, we denote as $|\mathcal{A}^{\mathcal{O}}\rangle_{\mathsf{AB}}$.

Generalizations. We consider generalized oracle adversaries in this work, where the adversary has access to two or more oracles. We also consider a restricted adversary who only makes selective calls.

Definition 17 (Multi-Oracle Adversary)**.** *An oracle adversary $\mathcal{A}$ is a quantum algorithm that makes queries to ℓ oracles $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ each of which acts on the first n qubits of the adversary's space, which we call the* A *register. The adversary also has an m-qubit ancillary space, which we call the* B *register. A t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$. Here, t denotes the total number of queries to all of the oracles $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$.*

Definition 18 (Multi-Oracle Adversary's view after t queries)**.** *Given a t-query multi-oracle adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$, we define the adversary's view after t queries as:*

$$|\mathcal{A}_t^{\mathcal{O}_1,\ldots,\mathcal{O}_t}\rangle_{\mathsf{AB}} = \prod_{i=1}^{t} \left(\mathcal{O}^{(i)}_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}}$$

Here, $\mathcal{O}^{(i)} \in \{\mathcal{O}_1, \ldots, \mathcal{O}_\ell\}$ represents one of the ℓ n-qubit oracles, and $A^{(i)}_{\mathsf{AB}}$ is the unitary operation applied by the adversary between the $(i-1)^{th}$ and i^{th} oracle queries. For an arbitrary t, we denote as $|\mathcal{A}^{\mathcal{O}_1,\ldots,\mathcal{O}_t}\rangle_{\mathsf{AB}}$.

When the number of queries to each of the oracles needs to be made explicit, we use the notation $(t_1, \ldots, t_\ell)$-query multi-oracle adversary. In this case, $\mathcal{A}$ makes t_i queries to the oracle $\mathcal{O}_i$

5.2 Relation States

Before we recall the definition of relation states, we first define size-t relations. A size-t relation R is represented by a multiset of t tuples $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, where $x_i \in [N], y_i \in [N]$ for all $i \in [t]$. We define $\mathrm{Im}(R) := \{y_1, \ldots, y_t\}$ and $\mathrm{Dom}(R) := \{x_1, \ldots, x_t\}$.

We define relation states below.

Definition 19 (Relation States)**.** *For $0 \le t \le N$ and a size-t relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, define the corresponding relation state to be the unit vector:*

$$|R\rangle_{\mathsf{AB}} = \alpha_R \cdot \sum_{\pi \in \mathsf{Sym}_t} S_\pi |x_1, \ldots, x_t\rangle \otimes S_\pi |y_1, \ldots, y_t\rangle,$$

where:

$$\alpha_R = \sqrt{\frac{\prod_{x,y\in[N]} \left(\sum_{i=1}^{t} \delta_{(x_i,y_i)=(x,y)}\right)!}{t!}}\,.$$

Definition 20 (Injective Relation)**.** *Let $t, N \in \mathbb{N}$. A relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ is an injective relation if $(y_1, \ldots, y_t) \in [N]^t_{\mathrm{dist}}$. The set of all injective relations consisting of exactly t pairs is denoted by $\mathfrak{R}^{\mathsf{inj}}_t$. Let $\mathfrak{R}^{\mathsf{inj}} = \cup_{j=0}^{N} \mathfrak{R}^{\mathsf{inj}}_j$.*

For an injective relation R, note that $\alpha_R = \frac{1}{\sqrt{t!}}$, where α_R is defined in Definition 19.

5.3 Path-Recording Isometry (PR)

Consider the following: for some $N \in \mathbb{N}$,

- x is an element of $[N]$,
- $R \in \mathfrak{R}^{\mathsf{inj}}$ is an injective relation, over pairs in $[N] \times [N]$, of size $|R| < N$.

The linear map PR, on registers A and E, is defined as follows:

$$\mathsf{PR}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}} |R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N - |R|}} \sum_{\substack{y \in [N], \\ y \notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}} |R \cup \{(x, y)\}\rangle_{\mathsf{E}}\,.$$

Partial Isometry [MH24] showed that PR is an isometry on some subspaces. Formally, they prove the following lemma.

Lemma 21 (Lemma 4.1 of [MH24]). *The path-recording linear map* PR*, on the registers* (A,E)*, is an isometry on the subspace spanned by the states* $|x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E}}$ *for* $x \in [N]$ *and* $R \in \mathfrak{R}^{\mathsf{inj}}$ *such that* $|R| < N$*.*

Indistinguishability Theorem. We import the following theorem from [MH24]. Informally, it states that a t-query oracle adversary cannot distinguish a Haar unitary versus a path-recording isometry.

Theorem 22 (Theorem 5 of [MH24]). *Let* $\mathcal{A}$ *be a* t*-oracle adversary. Then:*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_n}|\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|,\ \mathrm{Tr}_{\mathsf{E}}\left(|\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}}}|_{\mathsf{ABE}}\right)\right) \le \frac{2t(t-1)}{N+1}$$

We have the following simple corollary.

Corollary 23. *Let* $\mathcal{A}$ *be a* t*-oracle adversary. Then:*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}_1,\mathcal{O}_2\leftarrow\mu_n}|\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}\rangle\langle\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}|,\ \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1},\mathsf{PR}_{\mathsf{AE}_2}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1},\mathsf{PR}_{\mathsf{AE}_2}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)\right) \le \frac{4t(t-1)}{N+1}$$

6 Path-Recording Framework: New Observations

We discuss new observations about the path-recording framework in this section. Before that, we state some definitions related to sets whose prefixes are all distinct.

6.1 Definitions

Definition 24 (Strong ℓ-fold λ-prefix collision-free sets). *Let* $n, \lambda \in \mathbb{N}$ *with* $\lambda \le n$*. Let* $\mathcal{S}$ *be a set with elements from* $\{0,1\}^n$*. We say that* $\mathcal{S}$ *is* strong ℓ-fold λ-prefix collision-free *if the following holds: for all two* i*-sized subsets* S_1, S_2*, for any* $i \le \ell$*, it holds that* $\bigoplus_{x\in S_1} x_{[1:\lambda]} = \bigoplus_{y\in S_2} y_{[1:\lambda]}$ *if and only if* $S_1 = S_2$*. We denote* $\mathfrak{S}_n^{\mathsf{cf}(\ell,\lambda)}$ *to be the set of all strong* ℓ*-fold* λ*-prefix collision-free sets.*

Lemma 25. *Let* $S \in \mathfrak{S}_n^{\mathsf{cf}(\ell,\lambda)}$*, where* $\mathfrak{S}_n^{\mathsf{cf}(\ell,\lambda)}$ *is as defined in Definition 24. Define the following:*

$$\mathsf{CF}_{\ell,\lambda}(S) = \{y \in \{0,1\}^n | S \cup \{y\} \text{ is strong } \ell\text{-fold } \lambda\text{-prefix collision-free}\}$$

then

$$|\mathsf{CF}_{\ell,\lambda}(S)| \ge 2^n - \ell|S|^{2\ell}2^{n-\lambda}.$$

The proof of Lemma 25 can be found in Appendix A.1.

Definition 26 (Prefix Collision-Free Relations). *Let* $t, n, \lambda \in \mathbb{N}$ *with* $\lambda \le n$*. A relation* $R = \{(x_1,y_1),\ldots,(x_t,y_t)\}$ *is strong* ℓ*-fold* λ*-prefix collision-free if* $\{y_1,\ldots,y_t\} \in \mathfrak{S}_n^{\mathsf{cf}(\ell,\lambda)}$*. We denote* $\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$ *to be the set of all strong* ℓ*-fold* λ*-prefix collision-free relations.*

Note that $\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$ is a subset of $\mathfrak{R}^{\mathsf{inj}}$.

6.2 Recording ℓ-Fold Collision-Free Paths

We define a variant of the path-recording linear map below. Later we show the indistinguishability of this variant from the original path-recording map.

Prefix ℓ-fold Collision-Free Path Recording Linear Maps. Consider the following: for some $n, \lambda, \ell \in \mathbb{N}$ such that $\lambda \leq n$,

- x is an element of $\{0,1\}^n$,
- $R_1, R_2 \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$ are strong ℓ-fold λ-prefix collision-free relation, over pairs in $\{0,1\}^n \times \{0,1\}^n$, such that of $R_1 \cup R_2 \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$, $R_1 \cap R_2 = \emptyset$ and $|R_1 \cup R_2| < 2^n$.

We define two prefix collision-free path linear maps, on registers A and $\mathsf{E} := (\mathsf{E}_1, \mathsf{E}_2)$, as follows:

$$\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2} \mapsto \frac{1}{\sqrt{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))|}} \sum_{y \in \mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))} |y\rangle_{\mathsf{A}}|R_1 \cup \{(x,y)\}\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2},$$

$$\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2} \mapsto \frac{1}{\sqrt{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))|}} \sum_{y \in \mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))} |y\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2 \cup \{(x,y)\}\rangle_{\mathsf{E}_2}$$

Intuitively, these prefix collision-free path recording oracles are similar to the original path recording oracle, except that they only output y that are prefix collision-free with respect to the relation, instead of outputting y that are distinct from the image of the relation. We will show that most y that are distinct are also prefix collision-free (for a suitably large prefix), which will imply that the prefix collision-free path recording oracle acts similarly to the original path recording oracle.

Indistinguishability. We prove the following theorem:

Theorem 27. *Let $\mathcal{A}$ be a t-oracle adversary. Then:*

$$\mathsf{TD}(\rho, \sigma) \leq O\left(\frac{\sqrt{\ell} t^{\ell+1}}{2^{\lambda/2}}\right),$$

where:

$$\rho = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)$$

$$\sigma = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)$$

Proof. Without loss of generality, assume $\mathcal{A} = (A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$. We start by defining the following hybrids.
Hybrid_1: Output

$$\mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right).$$

$\mathsf{Hybrid}_{2.j}$, for $j \in \{0, \ldots, t\}$: Let

$$|\psi_j\rangle = \prod_{i=j+1}^{t}\left(\mathcal{O}^{(i)}_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right)\prod_{i=1}^{j}\left(\tilde{\mathcal{O}}^{(i)}_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}},$$

with $\mathcal{O}^{(i)}_{\mathsf{A}} \in \{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}\}$ and $\tilde{\mathcal{O}}^{(i)}_{\mathsf{A}} \in \{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}\}$. Output

$$\mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\psi_j\rangle\langle\psi_j|\right).$$

Hybrid_3: Output

$$\mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right).$$

Note that for $|\psi_0\rangle = |\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}, \mathsf{PR}_{\mathsf{AE}_2}}\rangle$ and $|\psi_t\rangle = |\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle$. Hence, Hybrid_1 is identical to $\mathsf{Hybrid}_{2.0}$ and Hybrid_3 is identical to $\mathsf{Hybrid}_{2.t}$.

Lemma 28. *The trace distance between the output of* $\mathsf{Hybrid}_{2.(j-1)}$ *and* $\mathsf{Hybrid}_{2.(j)}$*, for* $j \in [t]$*, is* $\frac{\sqrt{\ell}(j-1)^{\ell}}{2^{\lambda/2}}$*.*

Proof of Lemma 28. Since taking partial trace cannot increase the trace distance, we instead find the trace distance between $|\psi_{j-1}\rangle$ and $|\psi_j\rangle$. Recall that

$$|\psi_{j-1}\rangle = \prod_{i=j}^{t} \left(\mathcal{O}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) \prod_{i=1}^{j-1} \left(\tilde{\mathcal{O}}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}},$$

and

$$|\psi_j\rangle = \prod_{i=j+1}^{t} \left(\mathcal{O}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) \prod_{i=1}^{j} \left(\tilde{\mathcal{O}}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}.$$

Since applying the same channel cannot increase the trace distance, we only need to calculate the trace distance between

$$|\phi_{j-1}\rangle := \mathcal{O}_{\mathsf{A}}^{(j)} \cdot A_{\mathsf{AB}}^{(j)} \prod_{i=1}^{j-1} \left(\tilde{\mathcal{O}}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}},$$

and

$$|\phi_j\rangle := \prod_{i=1}^{j} \left(\tilde{\mathcal{O}}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}.$$

Note that the trace distance between pure states $|\phi_{j-1}\rangle$ and $|\phi_j\rangle$ is $\sqrt{1-|\langle\phi_{j-1}|\phi_j\rangle|^2}$. Notice that

$$|\phi_{j-1}\rangle = \mathcal{O}_{\mathsf{A}}^{(j)} |\theta_j\rangle,$$

and

$$|\phi_j\rangle := \tilde{\mathcal{O}}_{\mathsf{A}}^{(j)} |\theta_j\rangle,$$

for

$$|\theta_j\rangle := A_{\mathsf{AB}}^{(j)} \prod_{i=1}^{j-1} \left(\tilde{\mathcal{O}}_{\mathsf{A}}^{(i)} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}.$$

Hence, $\langle\phi_{j-1}|\phi_j\rangle = \langle\theta_j| \left(\mathcal{O}_{\mathsf{A}}^{(j)}\right)^{\dagger} \tilde{\mathcal{O}}_{\mathsf{A}}^{(j)} |\theta_j\rangle$ and we will look at the behavior of $\left(\mathcal{O}_{\mathsf{A}}^{(j)}\right)^{\dagger} \tilde{\mathcal{O}}_{\mathsf{A}}^{(j)}$. We assume $\mathcal{O}_{\mathsf{A}}^{(j)} = \mathsf{PR}_{\mathsf{AE}_1}$ and $\tilde{\mathcal{O}}_{\mathsf{A}}^{(j)} = \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)}$, the other case works by symmetry.
Notice that if

- x is an element of $\{0,1\}^n$,
- $R_1, R_2 \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$ are strong ℓ-fold λ-prefix collision-free relations, over pairs in $\{0,1\}^n \times \{0,1\}^n$, such that of $R_1 \cup R_2 \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$, $R_1 \cap R_2 = \emptyset$ and $|R_1 \cup R_2| < 2^n$.

$$\begin{aligned}\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)} :\ & |x\rangle_{\mathsf{A}} |R_1\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2} \\ \mapsto\ & \frac{1}{\sqrt{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))|}} \sum_{y \in \mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))} |y\rangle_{\mathsf{A}} |R_1 \cup \{(x,y)\}\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2},\end{aligned}$$

and

$$\mathsf{PR}_{\mathsf{AE}_1} : |x\rangle_{\mathsf{A}} |R_1\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2} \mapsto \frac{1}{\sqrt{N - |R_1|}} \sum_{\substack{y \in [N], \\ y \notin \mathrm{Im}(R_1)}} |y\rangle_{\mathsf{A}} |R_1 \cup \{(x,y)\}\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2},$$

Since $\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2)) \subseteq [N] \setminus \mathrm{Im}(R_1)$,

$$(\mathsf{PR}_{\mathsf{AE}_1})^{\dagger}\, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)} \left(|x\rangle_{\mathsf{A}} |R_1\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2}\right) = \sqrt{\frac{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1 \cup R_2))|}{N - |R_1|}} |x\rangle_{\mathsf{A}} |R_1\rangle_{\mathsf{E}_1} |R_2\rangle_{\mathsf{E}_2}.$$

Hence,

$$(\mathsf{PR}_{\mathsf{AE}_1})^\dagger\, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)} = \sum_{\substack{x,R_1,R_2\\ R_1,R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}\\ R_1\cap R_2=\{\}\\ R_1\cup R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}}} \sqrt{\frac{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1\cup R_2))|}{N-|R_1|}}\,|x\rangle\langle x|_{\mathsf{A}} \otimes |R_1\rangle\langle R_1|_{\mathsf{E}_1}\otimes |R_2\rangle\langle R_2|_{\mathsf{E}_2}.$$

By Lemma 25,

$$\sqrt{\frac{|\mathsf{CF}_{\ell,\lambda}(\mathrm{Im}(R_1\cup R_2))|}{N-|R_1|}} \geq \sqrt{\frac{2^n-\ell|\mathrm{Im}(R_1\cup R_2)|^{2\ell}2^{n-\lambda}}{2^n}} \geq \sqrt{1-\frac{\ell|\mathrm{Im}(R_1\cup R_2)|^{2\ell}}{2^\lambda}}.$$

Hence, we can write

$$(\mathsf{PR}_{\mathsf{AE}_1})^\dagger\, \mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)} \succeq I_{\mathsf{A}} \otimes \left(\bigoplus_{i=1}^{2^{n/2}} \sum_{\substack{R_1,R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}\\ R_1\cap R_2=\{\}\\ R_1\cup R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}\\ |R_1\cup R_2|=i}} \sqrt{1-\frac{\ell i^{2\ell}}{2^\lambda}}|R_1\rangle\langle R_1|_{\mathsf{E}_1}\otimes |R_2\rangle\langle R_2|_{\mathsf{E}_2} \right).$$

Note that since $|\theta_j\rangle$ is formed by $j-1$ total queries to $\tilde{\mathcal{O}}_{\mathsf{A}}$,

$$|\theta_j\rangle \in \mathsf{span}\{|x\rangle_{\mathsf{AB}}|R_1\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2} : x\in\{0,1\}^{n+m}, R_1,R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)},$$
$$R_1\cap R_2=\emptyset, R_1\cup R_2\in\mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}, |R_1\cup R_2|=j-1\}.$$

Hence,

$$|\langle\phi_{j-1}|\phi_j\rangle|^2 = \left|\langle\theta_j|\left(\mathcal{O}_{\mathsf{A}}^{(j)}\right)^\dagger \tilde{\mathcal{O}}_{\mathsf{A}}^{(j)}|\theta_j\rangle\right|^2 \geq 1-\frac{\ell(j-1)^{2\ell}}{2^\lambda}.$$

The trace distance between $|\phi_{j-1}\rangle$ and $|\phi_j\rangle$ is $\sqrt{1-|\langle\phi_{j-1}|\phi_j\rangle|^2} \leq \frac{\sqrt{\ell}(j-1)^\ell}{2^{\lambda/2}}$. This completes the proof of Lemma 28. □

By Lemma 28, the total trace distance between Hybrid_1 and Hybrid_3 is $\sum_{j=1}^t \frac{\sqrt{\ell}(j-1)^\ell}{2^{\lambda/2}} \leq \frac{\sqrt{\ell}t^{\ell+1}}{2^{\lambda/2}}$. This completes the proof of Theorem 27. □

Applying triangle inequality on Theorem 27 and Corollary 23, we have the following corollary.

Corollary 29. *Let $\mathcal{A}$ be a t-oracle adversary. Then:*

$$\mathsf{TD}(\rho,\sigma) \leq O\left(\frac{\sqrt{\ell}t^{\ell+1}}{2^{\lambda/2}}\right) + \frac{4t(t-1)}{N+1},$$

where:

$$\rho = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)},\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_2)}}\rangle\langle\mathcal{A}_t^{\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_1)},\mathsf{pcf}_{\ell,\lambda}\mathsf{PR}_{\mathsf{AE}}^{(\mathsf{E}_2)}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)$$

$$\sigma = \mathop{\mathbb{E}}_{\mathcal{O}_1,\mathcal{O}_2\leftarrow\mu_n} |\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}\rangle\langle\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}|$$

We also look at a special case of ℓ-fold collision-free path recording where $\ell=1$ and $\lambda=n$, which we call the collision-free path recording oracle. We define these as follows:

Collision-Free Path Recording Linear Maps. Consider the following: for some $n \in \mathbb{N}$,

- x is an element of $\{0,1\}^n$,
- $R_1, R_2 \in \mathfrak{R}^{\mathsf{inj}}$ are injective relations, over pairs in $\{0,1\}^n \times \{0,1\}^n$, such that of $R_1 \cup R_2 \in \mathfrak{R}^{\mathsf{inj}}$, $R_1 \cap R_2 = \emptyset$ and $|R_1 \cup R_2| < 2^n$.

We define two collision-free path linear maps, on registers A and $\mathsf{E} = (\mathsf{E}_1, \mathsf{E}_2)$, as follows:

$$\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2} \mapsto \frac{1}{\sqrt{N - |\mathrm{Im}(R_1 \cup R_2)|}} \sum_{y \in [N] \setminus \mathrm{Im}(R_1 \cup R_2))} |y\rangle_{\mathsf{A}}|R_1 \cup \{(x,y)\}\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2},$$

$$\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2\rangle_{\mathsf{E}_2} \mapsto \frac{1}{\sqrt{N - |\mathrm{Im}(R_1 \cup R_2)|}} \sum_{y \in [N] \setminus \mathrm{Im}(R_1 \cup R_2)} |y\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1}|R_2 \cup \{(x,y)\}\rangle_{\mathsf{E}_2}$$

We highlight that the difference between this oracle and two independent path recording oracles is that the two collision-free path recording oracles are aware not only of their own relation, but also the image of the other relation. Setting $\ell = 1$, $\lambda = n$ for Corollary 29, we get the following corollary.

Corollary 30. *Let $\mathcal{A}$ be a t-oracle adversary. Then:*

$$\mathsf{TD}(\rho, \sigma) \leq O\left(\frac{t^2}{\sqrt{N}}\right),$$

where:

$$\rho = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}},\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}},\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)$$

$$\sigma = \mathop{\mathbb{E}}_{\mathcal{O}_1,\mathcal{O}_2 \leftarrow \mu_n} |\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}\rangle\langle\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2}|$$

6.3 Multiset States and Operations.

We define a generalization of relation states as multiset states below and define some general isometric operations on these states:

Definition 31 (Multiset States)**.** *For $0 \leq t \leq N$ and a size-t multiset $S = \{a_1, \ldots, a_t\}$, define the corresponding multiset state to be the unit vector:*

$$|S\rangle_{\mathsf{A}} = \alpha_S \cdot \sum_{\pi \in \mathsf{Sym}_t} S_\pi |a_1, \ldots, a_t\rangle$$

where:

$$\alpha_S = \sqrt{\frac{\prod_{a \in [N]} \left(\sum_{i=1}^{t} \delta_{a_i = a}\right)!}{t!}}$$

Note that when the elements of the multiset are tuples of size 2, it becomes a relation state.

Next, we define some isometric operations on these multiset states that give us a framework to work with these states. We define the three operations as:

- $\mathsf{Partition}$: For any key $k \in \{0,1\}^*$, there exists a unique partition of any multiset S into S_1^k, S_2^k with $S_1^k \uplus S_2^k = S$,[9] then we define
$$V^{\mathsf{part}} : |S\rangle|k\rangle \mapsto |S_1^k\rangle|S_2^k\rangle|k\rangle.$$

[9] Without loss of generality, we can always assume an order between S_1^k, S_2^k.

- Apply: For any key $k \in \{0,1\}^*$, there exists an injective function $f(\cdot,\cdot)$ on the elements of any multiset S. Define $f(S,k) := \{f(a,k) : a \in S\}$. Then we define

$$V^{\mathsf{func},f} : |S\rangle|k\rangle \mapsto |f(S,k)\rangle|k\rangle.$$

- Pair: For any key $k \in \{0,1\}^*$, and any two multisets S_1 and S_2 with $|S_1| = |S_2|$, there exists a unique relation $R^k_{S_1,S_2}$ such that $\mathrm{Dom}(R^k_{S_1,S_2}) = S_1$ and $\mathrm{Im}(R^k_{S_1,S_2}) = S_2$. Then we define

$$V^{\mathsf{pair}} : |S_1\rangle|S_2\rangle|k\rangle \mapsto |R^k_{S_1,S_2}\rangle|k\rangle.$$

Note that since all the above operations are reversible on the range of these operations, they are all isometries.

7 Pseudorandom Unitaries with Short Keys

In this section, we present a construction of pseudorandom unitaries with keys of length n, which is secure against adversaries making any $\mathsf{poly}(n)$ many queries in the iQHROM. The construction simply involves (1) applying U, (2) applying a short random Pauli X string, and (3) applying U again.

Theorem 32. *For $k \in \{0,1\}^n$, define $G^U_k := UX^kU$, where U is an n-qubit unitary. Then $\{G^U_k\}_{k\in\{0,1\}^n}$ is a PRU in iQHROM, where U is the Haar oracle. Formally, for any t-query two-oracle adversary $\mathcal{A}$, for any polynomial t in n, we have:*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ k\leftarrow\{0,1\}^n}}\left[|\mathcal{A}_t^{G^U_k,U}\rangle\langle\mathcal{A}_t^{G^U_k,U}|\right], \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ V\leftarrow\mu_n}}\left[|\mathcal{A}_t^{V,U}\rangle\langle\mathcal{A}_t^{V,U}|\right]\right) \le \mathsf{negl}(n).$$

Proof. Without loss of generality, assume that $\mathcal{A}$ queries the first oracle on indices $\mathbf{a} = \{a_1,\ldots,a_\ell\} \subseteq [t]$ and the second oracle on indices $\mathbf{b} = [t] \setminus \{a_1,\ldots,a_\ell\}$. Consider the following hybrids.

Hybrid_1: Output $\rho_1 = \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ k\leftarrow\{0,1\}^n}}\left[|\mathcal{A}_t^{G^U_k,U}\rangle\langle\mathcal{A}_t^{G^U_k,U}|\right]$.

Hybrid_2: Output $\rho_2 = \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^n}\left[\mathrm{Tr}_{\mathsf{E}_1}\left(|\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}X^k\mathsf{PR}_{\mathsf{AE}_1},\mathsf{PR}_{\mathsf{AE}_1}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}_{\mathsf{AE}_1}X^k\mathsf{PR}_{\mathsf{AE}_1},\mathsf{PR}_{\mathsf{AE}_1}}|_{\mathsf{ABE}_1}\right)\right]$.

Hybrid_3: Output $\rho_3 = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2}\left(|\mathcal{A}_t^{\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}},\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}},\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2}\right)$.

Hybrid_4: Output $\rho_4 = \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ V\leftarrow\mu_n}}\left[|\mathcal{A}_t^{V,U}\rangle\langle\mathcal{A}_t^{V,U}|\right]$.

Claim 33. $\mathsf{TD}(\rho_1,\rho_2) \le \frac{4(t+\ell)(t+\ell-1)}{N+1}$.

Proof. Follows from Theorem 22. □

Claim 34. $\mathsf{TD}(\rho_3,\rho_4) \le O\left(\frac{(t+\ell)^2}{\sqrt{N}}\right)$.

Proof. Follows from Corollary 30. □

Hence, the only thing left to prove is that ρ_2 is close to ρ_3.

Claim 35. $\mathsf{TD}(\rho_2,\rho_3) \le 2\sqrt{\frac{t^2+t\ell}{N}}$.

Proof. We start by noticing that $\rho_2 = \mathrm{Tr}_{\mathsf{E_1K}}\left(|\psi_2\rangle\langle\psi_2|_{\mathsf{ABE_1K}}\right)$, where

$$|\psi_2\rangle_{\mathsf{ABE_1K}} = \sum_{k\in\{0,1\}^n} \frac{1}{2^{n/2}} |\mathcal{A}_t^{\mathsf{PR_{AE_1}}X^k\mathsf{PR_{AE_1}},\mathsf{PR_{AE_1}}}\rangle_{\mathsf{ABE_1}}|k\rangle_{\mathsf{K}}.$$

Similarly, $\rho_3 = \mathrm{Tr}_{\mathsf{E_1E_2}}\left(|\psi_3\rangle\langle\psi_3|_{\mathsf{ABE_1E_2}}\right)$, where

$$|\psi_3\rangle_{\mathsf{ABE_1E_2}} = |\mathcal{A}_t^{\mathsf{PR_{AE}^{(E_1)}},\mathsf{PR_{AE}^{(E_2)}}}\rangle_{\mathsf{ABE_1E_2}}.$$

We start by expanding $|\psi_3\rangle$ using the definition of $\mathsf{PR_{AE}^{(E_1)}}$ and $\mathsf{PR_{AE}^{(E_2)}}$,

$$|\psi_3\rangle_{\mathsf{ABE_1E_2}} = \frac{1}{\sqrt{N^{\downarrow t}}} \sum_{\substack{(x_1,\dots,x_t)\in[N]^t\\(y_1,\dots,y_t)\in[N]^t_{\mathrm{dist}}}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}} |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E_1}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_2}}.$$

We use $\vec{x} = (x_1,\dots,x_t)$, $\vec{y} = (y_1,\dots,y_t)$, and $|\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} = \frac{1}{\sqrt{N^{\downarrow t}}}\prod_{i=1}^t \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}$. Hence,

$$|\psi_3\rangle_{\mathsf{ABE_1E_2}} = \sum_{\substack{\vec{x}\in[N]^t\\\vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E_1}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_2}}.$$

Similarly, to expand $|\psi_2\rangle$, we notice that for any $k\in\{0,1\}^n$, $\mathsf{PR_{AE_1}}X^k\mathsf{PR_{AE_1}}$ behaves as follows:

$$\mathsf{PR_{AE_1}}X^k\mathsf{PR_{AE_1}}|x_i\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E_1}} = \frac{1}{\sqrt{(N-|R|)^{\downarrow 2}}} \sum_{\substack{z_i\in[N]\setminus\mathrm{Im}(R)\\y_i\in[N]\setminus(\mathrm{Im}(R)\cup\{z_i\})}} |y_i\rangle_{\mathsf{A}}|R\uplus\{(x_i,z_i),(z_i\oplus k,y_i)\}\rangle_{\mathsf{E_1}}.$$

Using identity functions, we can write the above as:

$$\mathsf{PR_{AE_1}}X^k\mathsf{PR_{AE_1}}|x_i\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E_1}} = \frac{1}{\sqrt{(N-|R|)^{\downarrow 2}}} \sum_{z_i,y_i\in[N]} \prod_{w\in\mathrm{Im}(R)} \left(\delta_{z_i\neq w}\delta_{y_i\neq w}\right)\delta_{z_i\neq y_i}|y_i\rangle_{\mathsf{A}}|R\uplus\{(x_i,z_i),(z_i\oplus k,y_i)\}\rangle_{\mathsf{E_1}}.$$

Hence, we expand $|\psi_2\rangle$ as

$$\begin{aligned}|\psi_2\rangle_{\mathsf{ABE_1K}} = \frac{1}{\sqrt{N\cdot N^{\downarrow(t+\ell)}}} \sum_{\substack{k\in\{0,1\}^n\\x_1,\dots,x_t\in[N]\\y_1,\dots,y_t\in[N]\\z_{a_1},\dots,z_{a_\ell}\in[N]}} \prod_{i=1}^{t}\left(\prod_{j=i}^{t}\delta_{y_i\neq y_j}\prod_{j=1}^{\ell}\delta_{y_i\neq z_{a_j}}\right)\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot A^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\\ \otimes|\{(x_i,z_i)\}_{i\in\mathbf{a}}\uplus\{(z_i\oplus k,y_i)\}_{i\in\mathbf{a}}\uplus\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|k\rangle_{\mathsf{K}}.\end{aligned}$$

We use $\vec{x} = (x_1,\dots,x_t)$, $\vec{y} = (y_1,\dots,y_t)$ and $\vec{z} = (z_{a_1},\dots,z_{a_\ell})$ and expand $|\psi_2\rangle$ as

$$\begin{aligned}&|\psi_2\rangle_{\mathsf{ABE_1K}} =\\ &\sum_{\vec{x}\in[N]^t\vec{y}\in[N]^t_{\mathrm{dist}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}}\otimes\frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}}\sum_{\substack{k\in\{0,1\}^n\\\vec{z}\in([N]\setminus\{\vec{y}\})^{\ell}_{\mathrm{dist}}}} |\{(x_i,z_i)\}_{i\in\mathbf{a}}\uplus\{(z_i\oplus k,y_i)\}_{i\in\mathbf{a}}\uplus\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|k\rangle_{\mathsf{K}}.\end{aligned}$$

We prove ρ_2 is close to ρ_3 by showing that there exists a projector $\Pi^{\mathrm{good}}_{\mathsf{E_1K}}$, and two isometries $V^2_{\mathsf{E_1K}}$ and $V^3_{\mathsf{E_1E_2}}$ such that $V^2_{\mathsf{E_1K}}\Pi^{\mathrm{good}}_{\mathsf{E_1K}}|\psi_2\rangle_{\mathsf{ABE_1K}}$ is close to $V^3_{\mathsf{E_1E_2}}|\psi_3\rangle_{\mathsf{ABE_1E_2}}$. To define $\Pi^{\mathrm{good}}_{\mathsf{E_1K}}$, we start by defining $\mathrm{CorX}(R,k)$ as a set of pairs in R that are correlated by k. Formally,

$$\mathrm{CorX}(R,k) := \{((u,v),(u',v'))\in R\times R : v\oplus u' = k\}.$$

Next, we define the set of good keys for a given relation R as

$$\mathsf{Good}(R,\ell) := \{k : |\mathrm{CorX}(R,k)| = \ell\}.$$

Hence, we define $\Pi^{\mathrm{good}}_{\mathsf{E_1K}}$ as

$$\Pi^{\mathrm{good}}_{\mathsf{E_1K}} := \sum_{R}\left(|R\rangle\langle R|_{\mathsf{E_1}} \otimes \sum_{k\in\mathsf{Good}(R,\ell)} |k\rangle\langle k|_{\mathsf{K}}\right).$$

Next, we study the effect of $\Pi^{\mathrm{good}}_{\mathsf{E_1K}}$ on relations of the form $\{(x_i,z_i)\}_{i\in\mathbf{a}} \uplus \{(z_i \oplus k, y_i)\}_{i\in\mathbf{a}} \uplus \{(x_i,y_i)\}_{i\in\mathbf{b}}$. We use the following notation: $(\{\vec{x}\}\oplus\{\vec{y}\}) \cup (\{\vec{x}\}\oplus\{\vec{z}\}) = \left(\{x_i \oplus y_j\}_{\substack{i\in[t]\\ j\in[t]}} \cup \{x_i \oplus z_j\}_{\substack{i\in[t]\\ j\in\mathbf{a}}}\right)$.

Claim 36. *Let* $\vec{x}\in[N]^t$, $\vec{y}\in[N]^t_{\mathrm{dist}}$ *and* $\vec{z}\in([N]\setminus\{\vec{y}\})^{\ell}_{\mathrm{dist}}$, *then*

$$\Pi^{\mathrm{good}}_{\mathsf{E_1K}} \sum_{k\in\{0,1\}^n} |\{(x_i,z_i)\}_{i\in\mathbf{a}} \uplus \{(z_i\oplus k, y_i)\}_{i\in\mathbf{a}} \uplus \{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|k\rangle_{\mathsf{K}} = \sum_{k\in\{0,1\}^n\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |\{(x_i,z_i)\}_{i\in\mathbf{a}} \uplus \{(z_i\oplus k, y_i)\}_{i\in\mathbf{a}} \uplus \{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|k\rangle_{\mathsf{K}}.$$

The proof of Claim 36 is deferred to Appendix A.2. We define $|\widetilde{\psi_2}\rangle := \Pi^{\mathrm{good}}_{\mathsf{E_1K}}|\psi_2\rangle$. Then by Claim 36,

$$|\widetilde{\psi_2}\rangle = \sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^{\ell}_{\mathrm{dist}}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |\{(x_i,z_i)\}_{i\in\mathbf{a}} \uplus \{(z_i\oplus k, y_i)\}_{i\in\mathbf{a}} \uplus \{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|k\rangle_{\mathsf{K}}.$$

Next we define the isometry $V^2_{\mathsf{E_1K}}$ on $|\widetilde{\psi_2}\rangle$ as the following procedure:

1. We define the following partition (indexed by a key k) of any relation $R = \{(u_i,v_i)\}_i$ as $R^k_2 = \{(u,v) : \exists(u',v')\in R, v\oplus u' = k\}$, and $R^k_1 = R\setminus R^k_2$. Then applying $V^{\mathsf{part}}{}_{\mathsf{E_1K}}$ isometry for the above partition $|\widetilde{\psi_2}\rangle$ gives us

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^{\ell}_{\mathrm{dist}}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |\{(z_i\oplus k, y_i)\}_{i\in\mathbf{a}} \uplus \{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|\{(x_i,z_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E_2}}|k\rangle_{\mathsf{K}}.$$

2. We define the following partition (indexed by a key k and a relation R') of any relation $R = \{(u_i,v_i)\}_i$ as $R^k_2 = \{(u,v) : \exists(u',v')\in R', u\oplus v' = k\}$, and $R^k_1 = R\setminus R^k_2$. Then applying $V^{\mathsf{part}}{}_{\mathsf{E_1E_2K}}$ isometry gives us

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^{\ell}_{\mathrm{dist}}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E_1}}|\{(x_i,z_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E_2}}|\{(z_i\oplus k, y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E_3}}|k\rangle_{\mathsf{K}}.$$

3. We define the following pairing (indexed by a key k) of two relations $R_1 = \{(u_i^1, v_i^1)\}_i$ and $R_2 = \{(u_i^2, v_i^2)\}_i$ as $R^k_{R_1,R_2} = \{(u_i^1, v_i^1, u_{i'}^2, v_{i'}^2) : (u_i^1, v_i^1) \in R_1, (u_{i'}^2, v_{i'}^2) \in R_2, v_i^1 \oplus u_{i'}^2 = k\}$. Then applying ${V^{\mathsf{pair}}}_{\mathsf{E}_2\mathsf{E}_3\mathsf{K}}$ isometry gives us

$$\sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^\ell_{\mathrm{dist}}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1} |\{(x_i,z_i,z_i\oplus k,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_2} |k\rangle_{\mathsf{K}}.$$

4. We define the following injection (indexed by a key k) $f_k : (x_i, z_i, z_i \oplus k, y_i) \mapsto (x_i, z_i, y_i)$. Then applying ${V^{\mathsf{func},f_k}}_{\mathsf{E}_2\mathsf{K}}$ isometry gives us

$$\sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^\ell_{\mathrm{dist}}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1} |\{(x_i,z_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_2} \otimes \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Now, we further expand the register E_2 according to the definition of multiset states:

$$\sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\vec{z}\in([N]\setminus\{\vec{y}\})^\ell_{\mathrm{dist}}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1} \otimes \left(\frac{1}{\sqrt{\ell!}} \sum_{\pi\in\mathsf{Sym}_\ell} S_\pi|x_{a_1},\dots,x_{a_\ell}\rangle \otimes S_\pi|z_{a_1},\dots,z_{a_\ell}\rangle \otimes S_\pi|y_{a_1},\dots,y_{a_\ell}\rangle\right)_{\mathsf{E}_2} \otimes \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Notice that we can sample $\{\vec{z}\}$ first and then assign an order[10]. Hence, the state looks like

$$\sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} \sum_{\sigma\in\mathsf{Sym}_\ell} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1} \otimes \left(\frac{1}{\sqrt{\ell!}} \sum_{\pi\in\mathsf{Sym}_\ell} S_\pi|x_{a_1},\dots,x_{a_\ell}\rangle \otimes S_\pi S_\sigma|z_{a_1},\dots,z_{a_\ell}\rangle \otimes S_\pi|y_{a_1},\dots,y_{a_\ell}\rangle\right)_{\mathsf{E}_2} \otimes \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

By switching the order of σ and π and setting $\sigma \leftarrow \pi^{-1}\sigma$, we can disentangle $\vec{z}$,

$$\sum_{\substack{\vec{x}\in[N]^t \\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{1}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1} \otimes \left(\frac{1}{\sqrt{\ell!}} \sum_{\pi\in\mathsf{Sym}_\ell} S_\pi|x_{a_1},\dots,x_{a_\ell}\rangle \otimes S_\pi|y_{a_1},\dots,y_{a_\ell}\rangle\right)_{\mathsf{E}_2} \otimes \left(\sum_{\sigma\in\mathsf{Sym}_\ell} S_\sigma|z_{a_1},\dots,z_{a_\ell}\rangle\right)_{\mathsf{E}_3} \otimes \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

[10] Consider $\{\vec{z}\}$ to have a canonical order and we look at all possible permutations of this order.

Using the multiset state notation:

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \frac{\sqrt{\ell!}}{\sqrt{N\cdot(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_1}\otimes$$

$$|\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_2}|\{z_i\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_3} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Re-arranging and setting $|\Psi_2\rangle := V^2_{\mathsf{E}_1\mathsf{K}}\Pi^{\mathrm{good}}_{\mathsf{E}_1\mathsf{K}}|\psi_2\rangle_{\mathsf{ABE}_1\mathsf{K}}$, then

$$|\Psi_2\rangle = \sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}\otimes$$

$$\sqrt{\frac{\ell!}{(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{z_i\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_3}\frac{1}{\sqrt{N}}\otimes \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Recall that $|\psi_3\rangle$ is defined as

$$|\psi_3\rangle_{\mathsf{ABE}_1\mathsf{E}_2} = \sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}}|\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}.$$

Next we define the isometry $V^3_{\mathsf{E}_1\mathsf{E}_2}$ on $|\psi_3\rangle$ as the following procedure:

1. Controlled on the y_i's in registers $\mathsf{E}_1\mathsf{E}_2$, we create a superposition over all ℓ-sized sets disjoint from y_i's to get

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \quad\otimes\quad |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2} \quad\otimes\quad \sqrt{\frac{\ell!}{(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{z_i\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_3}.$$

2. Finally, controlled on $\mathsf{E}_1\mathsf{E}_2\mathsf{E}_3$, we create a superposition over all keys not in $(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})$,

$$\sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2} \otimes \sqrt{\frac{\ell!}{(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{z_i\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_3}$$

$$\otimes\frac{1}{\sqrt{N-|\,(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})\,|}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Hence, let $|\Psi_3\rangle := V^3_{\mathsf{E}_1\mathsf{E}_2}|\psi_3\rangle_{\mathsf{ABE}_1\mathsf{E}_2}$. Then

$$|\Psi_3\rangle = \sum_{\substack{\vec{x}\in[N]^t\\ \vec{y}\in[N]^t_{\mathrm{dist}}}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2} \otimes \sqrt{\frac{\ell!}{(N-t)^{\downarrow\ell}}} \sum_{\{\vec{z}\}\in\binom{[N]\setminus\{\vec{y}\}}{\ell}} |\{z_i\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_3}$$

$$\otimes\frac{1}{\sqrt{N-|\,(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})\,|}} \sum_{k\in[N]\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})} |k\rangle_{\mathsf{K}}.$$

Note that by a simple counting argument, for all $(\vec{x}, \vec{y}, \vec{z})$,

$$\sqrt{\frac{N - |(\{\vec{x}\} \oplus \{\vec{y}\}) \cup (\{\vec{x}\} \oplus \{\vec{z}\})|}{N}} \geq \sqrt{\frac{N - (t^2 + t\ell)}{N}}. \tag{1}$$

Applying Lemma 13,

$$\langle \Psi_2 | \Psi_3 \rangle \geq \sqrt{\frac{N - (t^2 + t\ell)}{N}}.$$

Hence, by Lemma 12, we get

$$\| |\widetilde{\psi}_2\rangle \|^2 = \| |\Psi_2\rangle \|^2 \geq 1 - \frac{t^2 + t\ell}{N}.$$

Finally, by Lemma 11, we get

$$\mathsf{TD}(|\psi_2\rangle, |\widetilde{\psi}_2\rangle) \leq \sqrt{\frac{t^2 + t\ell}{N}}.$$

Hence, combining the above bounds, $\mathsf{TD}(\rho_2, \rho_3) \leq 2\sqrt{\frac{t^2+t\ell}{N}}$. □

Combining the above three claims, we complete the proof of Theorem 32. □

In the above proof, we assume the size of the Pauli X to be equal to the size of U, but we can generalize the above proof to hold as long as the size of the Pauli X is $\omega(\log \lambda)$.

Corollary 37. *For any $f(\lambda) = \omega(\log \lambda)$, $k \in \{0,1\}^{f(\lambda)}$, define $G_k^U = U(X^k \otimes I_{n-f(\lambda)})U$, where U is an n-qubit unitary. Then $\{G_k^U\}_{k \in \{0,1\}^{f(\lambda)}}$ is a PRU in* iQHROM*, where U is the Haar oracle. Formally, for any t-query two-oracle adversary $\mathcal{A}$, for any polynomial t in λ, we have:*

$$\mathsf{TD}\left(\underset{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^{f(\lambda)}}}{\mathbb{E}} \left[|\mathcal{A}_t^{G_k^U, U}\rangle\langle \mathcal{A}_t^{G_k^U, U}| \right], \underset{\substack{U \leftarrow \mu_n \\ V \leftarrow \mu_n}}{\mathbb{E}} \left[|\mathcal{A}_t^{V,U}\rangle\langle \mathcal{A}_t^{V,U}| \right] \right) \leq \mathsf{negl}(\lambda).$$

Proof sketch. The proof above goes exactly the same except that the bound in Equation (1) changes to

$$\sqrt{\frac{2^{f(\lambda)} - |(\{\vec{x}\} \oplus \{\vec{y}\}) \cup (\{\vec{x}\} \oplus \{\vec{z}\})|}{2^{f(\lambda)}}} \geq \sqrt{\frac{2^{f(\lambda)} - (t^2 + t\ell)}{2^{f(\lambda)}}},$$

since $f(\lambda) = \omega(\log \lambda)$, the above is still lower-bounded by $1 - \mathsf{negl}(\lambda)$. Hence, the construction is secure. □

8 Key-Stretched PRU in the Plain Model

In this section, applying our result from Section 7 to a pseudorandom unitary in the plain model, we show that we can stretch the output length of *any* PRU, relative to its key size.

As an immediate consequence of Corollary 37, we can actually get arbitrary polynomial-stretch PRU in the *plain* model. At a high level, the idea is to sample a single PRU key, and use this to computationally instantiate a Haar random oracle. Then use the construction of PRUs with short keys in the Haar oracle model to get more PRUs while only using $O(\log^{1+\epsilon} \lambda)$ more bits of randomness (for any constant ϵ, although we will set this to be $\log^2 \lambda$ in the remainder of this section).

Plugging these seemingly fresh pseudorandom unitaries into the construction of [SHH24], we can stretch the output size of the pseudorandom unitary. For a graphical depiction of the construction, see Figure 2.

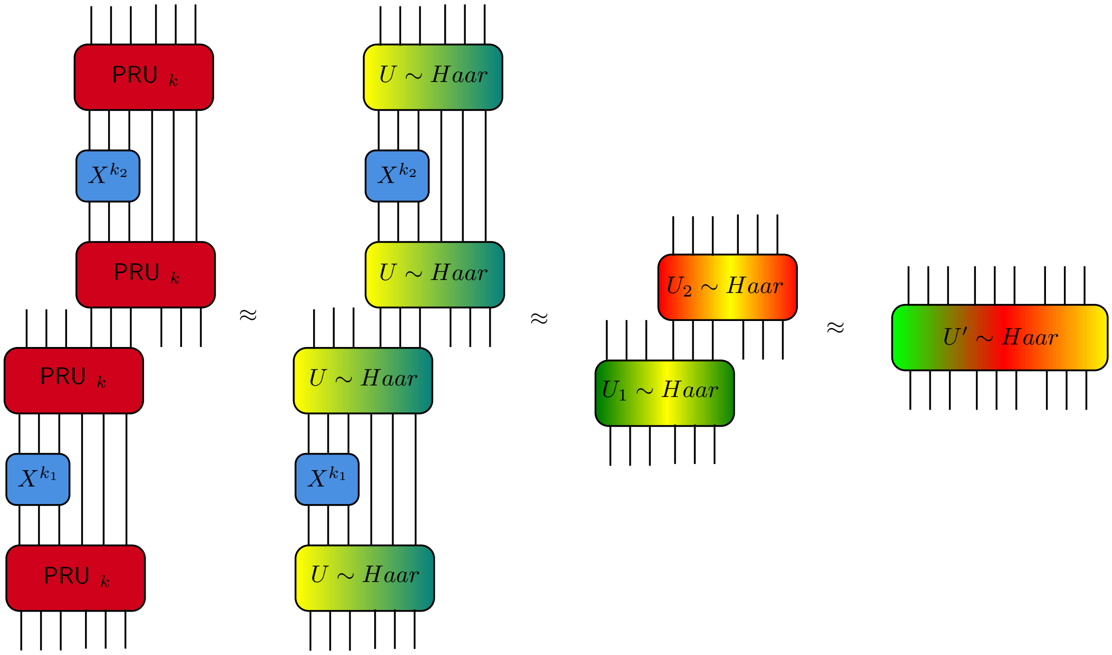

Figure 2: Implementation of key-stretched PRU from any PRU. Going from left to right, the first approximation uses the definition of the PRU, the next one uses Theorem 1, and the final one uses the result from [SHH24].

We recall the main lemma of [SHH24].

Lemma 38 (Gluing two random unitaries [SHH24])**.** *Let* $\mathsf{A}, \mathsf{B}, \mathsf{C}$ *be three disjoint subsystems. Consider a random unitary given by* $V_{\mathsf{ABC}} = U_{\mathsf{AB}} U'_{\mathsf{BC}}$*, where* U *and* U' *are drawn from* ϵ_1 *and* ϵ_2*-approximate* k*-designs, respectively. Then* V_{ABC} *is an* ϵ*-approximate* k *design, with*

$$1 + \epsilon \leq (1 + \epsilon_1)(1 + \epsilon_2) \left(1 + \frac{5k^2}{2^{|\mathsf{B}|}}\right) .$$

As long as the number of qubits in B *satisfies* $|\mathsf{B}| \geq \log(5k^2)$.

Theorem 39 (Stretching a PRU)**.** *Let* $\{\mathsf{PRU}_{\lambda,k}\}_{\lambda \in \mathbb{N}, k \in \{0,1\}^\lambda}$ *be a PRU family with keys of size* λ*, where* U_k *acts on* $t(\lambda)$ *many qubits. Then there exists a pseudorandom unitary family* $\{\mathsf{SPRU}_k\}_{\lambda \in \mathbb{N}, k \in \{0,1\}^{\lambda + 2\log^2(\lambda)}}$ *(*S *for stretched) with keys of size* $\lambda + 2\log^2(\lambda)$ *that acts on* $2t(\lambda) - \log^2(\lambda)$ *qubits.*

Proof. Let $\{\mathsf{PRU}_k\}_k$ be a family of pseudorandom unitaries for a fixed security parameter λ. Let $\mathcal{A}^{(\cdot)}$ be a quantum polynomial time adversary that makes queries to an oracle and outputs either $\top$ or $\bot$. We first define $\mathsf{SPRU}_{k,k_1,k_2}$ as follows. Let ABC be three quantum registers, with A, C being $t(\lambda) - \log^2(\lambda)$ and B being $\log^2(\lambda)$. Then for a key k of size λ and keys k_1, k_2 of size $\log^2(\lambda)$,

$$\mathsf{SPRU}_{k,k_1,k_2} = (\mathsf{PRU}_k)_{\mathsf{BC}} X^{k_2}_{\mathsf{BC}} (\mathsf{PRU}_k)_{\mathsf{BC}} (\mathsf{PRU}_k)_{\mathsf{AB}} X^{k_1}_{\mathsf{AB}} (\mathsf{PRU}_k)_{\mathsf{AB}} .$$

We claim the following holds

$$\left| \Pr_{\substack{k \xleftarrow{\$} \{0,1\}^\lambda \\ k_1, k_2 \xleftarrow{\$} \{0,1\}^{\log^2(\lambda)}}} \left[\top \leftarrow \mathcal{A}^{\mathsf{SPRU}_{k,k_1,k_2}}\right] - \Pr_{\substack{U \leftarrow \mu_{t(\lambda)} \\ k_1, k_2 \xleftarrow{\$} \{0,1\}^{\log^2(\lambda)}}} \left[\top \leftarrow \mathcal{A}^{U_{\mathsf{BC}} X^{k_2}_{\mathsf{BC}} U_{\mathsf{BC}} U_{\mathsf{AB}} X^{k_1}_{\mathsf{AB}} U_{\mathsf{AB}}}\right] \right| \leq \mathsf{negl}(\lambda) .$$

This holds by the pseudorandomness of the original PRU. If, for the sake of contradiction, there exists an adversary that has a non-negligible advantage above, then the adversary can be turned into an adversary for PRU_k and U just by simulating SPRU by sampling the additional keys.

Then, we have the following

$$\left| \Pr_{\substack{U \leftarrow \mu_{t(\lambda)} \\ k_1,k_2 \xleftarrow{\$} \{0,1\}^{\log^2(\lambda)}}} \left[\top \leftarrow \mathcal{A}^{U_{\mathsf{BC}} X_{\mathsf{BC}}^{k_2} U_{\mathsf{BC}} U_{\mathsf{AB}} X_{\mathsf{AB}}^{k_1} U_{\mathsf{AB}}} \right] - \Pr_{\substack{U,V \leftarrow \mu_{t(\lambda)} \\ k_1 \xleftarrow{\$} \{0,1\}^{\log^2(\lambda)}}} \left[\top \leftarrow \mathcal{A}^{V_{\mathsf{BC}} U_{\mathsf{AB}} X_{\mathsf{AB}}^{k_1} U_{\mathsf{AB}}} \right] \right| \leq \mathsf{negl}(\lambda)\,.$$

This holds because of the construction of Corollary 37. In particular, we proved that UX^kU is indistinguishable from an independently sampled Haar random unitary V, even to adversaries who also get query access to U.

Again by Corollary 37, $UX^{k_1}U$ is indistinguishable from a Haar random unitary, so the following holds

$$\left| \Pr_{\substack{U,V \leftarrow \mu_{t(\lambda)} \\ k_1 \xleftarrow{\$} \{0,1\}^{\log^2(\lambda)}}} \left[\top \leftarrow \mathcal{A}^{V_{\mathsf{BC}} U_{\mathsf{AB}} X_{\mathsf{AB}}^{k_1} U_{\mathsf{AB}}} \right] - \Pr_{U,V \leftarrow \mu_{t(\lambda)}} \left[\top \leftarrow \mathcal{A}^{V_{\mathsf{BC}} U_{\mathsf{AB}}} \right] \right| \leq \mathsf{negl}(\lambda)\,.$$

Then we apply Lemma 38 with $k = 2^{\log^{1.5}(\lambda)}$, and $|B| = \log^2(\lambda)$. Since Haar random unitaries are exact k-designs for all k, $\epsilon_1 = \epsilon_2 = 0$, and we get that $V_{\mathsf{BC}} U_{\mathsf{AB}}$ is an ε-approximate k-design, where

$$\varepsilon(\lambda) = \frac{5 \cdot 2^{2 \log^{1.5}(\lambda)}}{2^{\log^2(\lambda)}} = \mathsf{negl}(\lambda)\,.$$

Finally, it is known that δ-approximate q-designs are PRUs if $\delta = \mathsf{negl}(\lambda)$ and $q = \lambda^{\omega(1)}$ (see e.g., [AMR20; Kre21; MPSY24] or [SHH24, Lemma 5]).

Since $k = 2^{\log^{1.5}(\lambda)} = \lambda^{\omega(1)}$, for any adversary that makes only a polynomial number of queries, the following holds

$$\left| \Pr_{U,V \leftarrow \mu_{t(\lambda)}} \left[\top \leftarrow \mathcal{A}^{V_{\mathsf{BC}} U_{\mathsf{AB}}} \right] - \Pr_{U \leftarrow \mu_{2t(\lambda) - \log^2(\lambda)}} \left[\top \leftarrow \mathcal{A}^{U_{\mathsf{ABC}}} \right] \right| \leq \mathsf{negl}(\lambda)\,.$$

Thus, by the triangle inequality, the original construction of $\mathsf{SPRU}_{k,k_1,k_2}$ is indistinguishable from a large Haar random unitary on $2t(\lambda) - \log^2(\lambda)$ qubits. □

We can repeat this reduction $O(\log(\lambda))$ many times (since the size of the pseudorandom unitary doubles every time we apply it) to get the following lemma.

Corollary 40 (Pseudorandom unitaries with small keys from any pseudorandom unitary)**.** *Let $\{\mathsf{PRU}_{\lambda,k}\}_{\lambda,k}$ be a family of pseudorandom unitaries that has keys of length λ and acts on $t(\lambda)$ qubits. Then for every constant c, there exists a pseudorandom unitary family such that*

1. *The key length of the family is $\lambda + 2c\log^3(\lambda)$.*
2. *The pseudorandom unitary acts on $\lambda^c \left(t(\lambda) - \log^2(\lambda)\right) + \log^2(\lambda)$ many qubits.*

Proof. Applying the reduction recursively $c\log(\lambda)$ many times, we add $2\log^2(\lambda)$ many bits to the key each time, and double (minus $\log^2(\lambda)$) the output length of the pseudorandom unitary. Hence, after doing this n times, the output length becomes

$$2^n t(\lambda) - 2^{n-1} \log^2 \lambda - 2^{n-2} \log^2 \lambda - \ldots - 2^0 \log^2 \lambda\,.$$

Hence, the final output length is

$$2^n \left(t(\lambda) - \log^2 \lambda\right) + \log^2 \lambda \,.$$

Thus, for $n = c\log(\lambda)$, we get the desired key length and output length for the pseudorandom unitary. Additionally note that doing this requires running the original pseudorandom unitary $2^{c\log(\lambda)} = \lambda^c$ times, but since this is a polynomial the entire construction runs in polynomial time. □

Rescaling so that $\lambda + 2c\log^3(\lambda) = \lambda'$, we see that for every choice of c, there is a pseudorandom unitary whose output length is roughly λ^c, for keys of length λ. We also note that our construction did not require any extra conditions on the pseudorandom unitary family, simply that any construction is a pseudorandom unitary.

Applying a brickwork, instead of staircase, layout, we can take any pseudorandom unitary family in depth d, and output a pseudorandom unitary family in depth $4d+2$ that has arbitrarily small keys.

Corollary 41 (Low depth pseudorandom unitaries with short keys)**.** *Let $\{\mathsf{PRU}_{\lambda,k}\}_{\lambda,k}$ be a family of pseudorandom unitaries with keys of length λ, such that every PRU_k is depth at most $d(\lambda)$ and acts on $t(\lambda)$ qubits. Then for every constant c, there is a pseudorandom unitary family with keys of length $O(\lambda)$, output length $\lambda^c t(\lambda)$, and depth $4d(\lambda)+2$.*

Proof. We apply Theorem 32 to the brickwork architecture shown in Figure 3, we get a pseudorandom unitary whose depth is $4d(\lambda)+2$, and at a cost of sampling $c\log^3\lambda$ additional bits of randomness, whose output length is scaled up by a factor of λ^c. □

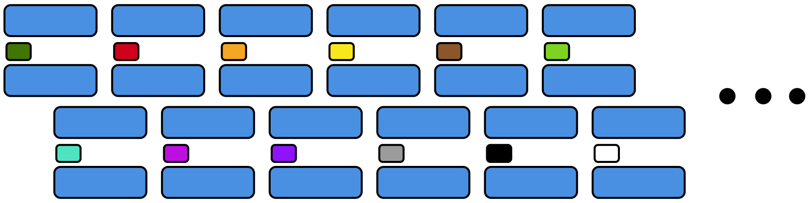

Figure 3: Implementation of low depth, short key pseudorandom unitaries from any pseudorandom unitary family. Long blue boxes are a single sample of the original pseudorandom unitary family, and short colored boxes are additional $\omega(\log(\lambda))$ sized Pauli X strings.

We note that if one-way functions exist (as in [SHH24], which assumes the subexponential hardness of LWE), then this key shrinkage can be achieved by first shrinking the keys used in the pseudorandom function construction, however our reduction applies to *all* pseudorandom unitary families, even those that do not arise from a classical pseudorandom function.

9 Bounded-Query Pseudorandom Unitaries with Short Keys

Now, we present an even simpler construction of $O(\lambda/\log(\lambda)^{1+\epsilon})$-query secure pseudorandom unitaries with keys of length λ in the iQHROM that only makes *a single query* to the common Haar random unitary.

Theorem 42. *For $k \in \{0,1\}^\lambda$, define $G_k^U = (Z^k \otimes I)U$, where U is an n-qubit unitary such that $\lambda \leq n$. Then $\{G_k^U\}_{k\in\{0,1\}^\lambda}$ is an ℓ-query secure pseudorandom unitary for $\ell = O(\lambda/\log(\lambda)^{1+\epsilon})$ for all $\epsilon > 0$ in* iQHROM*, where U is the Haar oracle. Formally, for any $(\ell, t-\ell)$-query two-oracle adversary $\mathcal{A}$, for any t polynomial in n, we have:*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ k\leftarrow\{0,1\}^\lambda}}\left[|\mathcal{A}_t^{G_k^U,U}\rangle\!\langle\mathcal{A}_t^{G_k^U,U}|\right], \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n\\ V\leftarrow\mu_n}}\left[|\mathcal{A}_t^{V,U}\rangle\!\langle\mathcal{A}_t^{V,U}|\right]\right) \leq \mathsf{negl}(\lambda).$$

Note that $\mathcal{A}$ makes ℓ queries to G_k^U (or V) and $t-\ell$ queries to U.

Proof of Theorem 42. Consider the following hybrids.

Hybrid_1: Output $\rho_1 = \underset{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^\lambda}}{\mathbb{E}} \left[|\mathcal{A}_t^{G_k^U, U}\rangle\langle\mathcal{A}_t^{G_k^U, U}| \right]$.

Hybrid_2: Output

$$\rho_2 := \underset{k \leftarrow \{0,1\}^\lambda}{\mathbb{E}} \left[\mathrm{Tr}_{\mathsf{E}_1} \left(|\mathcal{A}_t^{Z^k \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}}\rangle\langle\mathcal{A}_t^{Z^k \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}}|_{\mathsf{ABE}_1} \right) \right].$$

Claim 43. $\mathsf{TD}(\rho_1, \rho_2) \leq O\left(\frac{\sqrt{\ell} t^{\ell+1}}{2^{\lambda/2}}\right) + \frac{4t(t-1)}{N+1}$.

Proof. Follows from Corollary 29. □

Hybrid_3: Output

$$\rho_3 := \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2} \left(|\mathcal{A}_t^{\mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2} \right).$$

Claim 44. $\rho_2 = \rho_3$.

Proof. We note that

$$\rho_2 = \mathrm{Tr}_{\mathsf{E}_1\mathsf{K}} \left[\left(\frac{1}{\sqrt{2^\lambda}} \sum_k |k\rangle_{\mathsf{K}} |\mathcal{A}_t^{Z^k \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}}\rangle_{\mathsf{ABE}_1} \right) \left(\frac{1}{\sqrt{2^\lambda}} \sum_{k'} \langle k'|_{\mathsf{K}} \langle\mathcal{A}_t^{Z^{k'} \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}}|_{\mathsf{ABE}_1} \right) \right]$$

and

$$\rho_3 = \mathrm{Tr}_{\mathsf{E}_1\mathsf{E}_2} \left(|\mathcal{A}_t^{\mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle\langle\mathcal{A}_t^{\mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}|_{\mathsf{ABE}_1\mathsf{E}_2} \right).$$

We show this by showing that there exists an isometry on the register $\mathsf{E}_1\mathsf{K}$ that maps

$$|\psi_1\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_k |k\rangle_{\mathsf{K}} |\mathcal{A}_t^{Z^k \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}_1}}\rangle_{\mathsf{ABE}_1}$$

to

$$|\psi_2\rangle = |\mathcal{A}_t^{\mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}, \mathsf{pcf}_{\ell,n} \mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}}\rangle_{\mathsf{ABE}_1\mathsf{E}_2}.$$

Without loss of generality, assume $\mathcal{A}$ queries the first oracle on $\mathbf{a} = \{a_1, \ldots, a_\ell\}$ indices and the second oracle on $\mathbf{b} = [t] \setminus \{a_1, \ldots, a_\ell\}$ indices. Hence we expand $|\psi_2\rangle$ using the definition of $\mathsf{pcf}_{\ell,n}\mathsf{PR}^{(\mathsf{E}_1)}_{\mathsf{AE}}$ and $\mathsf{pcf}_{\ell,n}\mathsf{PR}^{(\mathsf{E}_2)}_{\mathsf{AE}}$,

$$|\psi_2\rangle = \sum_{\substack{x_1,\ldots,x_t \in [N] \\ y_1 \in \mathsf{CF}_{\ell,\lambda}(\{\}) \\ y_2 \in \mathsf{CF}_{\ell,\lambda}(\{y_1\}) \\ \vdots \\ y_t \in \mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{t-1}\})}} \prod_{i=1}^t \frac{1}{\sqrt{|\mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{i-1}\})|}} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \otimes |\{(x_i, y_i)\}_{i \in \mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i, y_i)\}_{i \in \mathbf{b}}\rangle_{\mathsf{E}_2}.$$

For conciseness, we use the subnormalized vector $|\phi_{\vec{x},\vec{y}}\rangle$ to denote

$$|\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} := \prod_{i=1}^{t} \frac{1}{\sqrt{|\mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{i-1}\})|}} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}.$$

Hence,

$$|\psi_2\rangle = \sum_{\substack{x_1,\ldots,x_t\in[N] \\ y_1\in\mathsf{CF}_{\ell,\lambda}(\{\}) \\ y_2\in\mathsf{CF}_{\ell,\lambda}(\{y_1\}) \\ \vdots \\ y_t\in\mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{t-1}\})}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}}|\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}.$$

Similarly, we can we expand $|\psi_1\rangle$ as

$$|\psi_1\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{\substack{k\in\{0,1\}^\lambda \\ x_1,\ldots,x_t\in[N] \\ y_1\in\mathsf{CF}_{\ell,\lambda}(\{\}) \\ y_2\in\mathsf{CF}_{\ell,\lambda}(\{y_1\}) \\ \vdots \\ y_t\in\mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{t-1}\})}} \prod_{i=1}^{\ell}(-1)^{\langle y_{a_i},k||0\rangle}|\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}}|\{(x_i,y_i)\}_{i\in[t]}\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}.$$

Moving the sum over k to the purification, we get

$$|\psi_1\rangle = \sum_{\substack{x_1,\ldots,x_t\in[N] \\ y_1\in\mathsf{CF}_{\ell,\lambda}(\{\}) \\ y_2\in\mathsf{CF}_{\ell,\lambda}(\{y_1\}) \\ \vdots \\ y_t\in\mathsf{CF}_{\ell,\lambda}(\{y_1,\ldots,y_{t-1}\})}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}}|\{(x_i,y_i)\}_{i\in[t]}\rangle_{\mathsf{E}_1} \otimes \frac{1}{\sqrt{2^\lambda}}\sum_{k\in\{0,1\}^\lambda}(-1)^{\langle\oplus_{i=1}^{\ell}y_{a_i},k||0\rangle}|k\rangle_{\mathsf{K}}.$$

Next, we show that there exists an isometry W such that for all $\{(x_i,y_i)\}_{i\in[t]} \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$,

$$\begin{aligned} &W|\{(x_i,y_i)\}_{i\in[t]}\rangle_{\mathsf{E}_1} \otimes \frac{1}{\sqrt{2^\lambda}}\sum_{k\in\{0,1\}^\lambda}(-1)^{\langle\oplus_{i=1}^{\ell}y_{a_i},k||0\rangle}|k\rangle_{\mathsf{K}} \\ &= |\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}. \end{aligned}$$

We describe W as the following procedure. We start by applying Hadamard on K to get

$$|\{(x_i,y_i)\}_{i\in[t]}\rangle_{\mathsf{E}_1}|\oplus_{i=1}^{\ell}y_{a_i}[1:\lambda]\rangle_{\mathsf{K}}.$$

Next, using $\oplus_{i=1}^{\ell}y_{a_i}[1:\lambda]$ as the key we can define a partition of $\{(x_i,y_i)\}_{i\in[t]}$ the XOR of ℓ-sized subset of y's is $|\oplus_{i=1}^{\ell}y_{a_i}[1:\lambda]\rangle$. Since $\{(x_i,y_i)\}_{i\in[t]} \in \mathfrak{R}^{\mathsf{cf}(\ell,\lambda)}$, there is a unique partition with this property, namely $\{y_i\}_{i\in\mathbf{a}}$ and $\{(x_i,y_i)\}_{i\in\mathbf{b}}$. Hence, applying V^{part}, we get the state as

$$|\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}|\oplus_{i=1}^{\ell}y_{a_i}[1:\lambda]\rangle_{\mathsf{K}}.$$

Next, we XOR the bits y's from E_1 with K to get $|0\rangle_{\mathsf{K}}$,tracing out $|0\rangle_{\mathsf{K}}$, we get

$$|\{(x_i,y_i)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1}|\{(x_i,y_i)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}.$$

Hence, W maps $|\psi_1\rangle$ to $|\psi_2\rangle$, and $\rho_2 = \rho_3$. □

Hybrid_4: Output $\rho_4 = \underset{\substack{U \leftarrow \mu_n \\ V \leftarrow \mu_n}}{\mathbb{E}} \left[|\mathcal{A}_t^{V,U}\rangle\langle\mathcal{A}_t^{V,U}| \right]$.

Claim 45. $\mathsf{TD}(\rho_3, \rho_4) \leq O\left(\frac{\sqrt{\ell} t^{\ell+1}}{2^{\lambda/2}}\right) + \frac{4t(t-1)}{N+1}$

Proof. Follows from Corollary 29. □

This completes the proof of Theorem 42. □

10 Unbounded-Query Secure Non-Adaptive PRUs: Barriers

Here we show that the construction of $o(\lambda/\log(\lambda))$-copy secure PRUs are almost tight for constructions that make arbitrary depth-1 calls to the PRU. The main observation is that we can apply the quantum OR technique from [CCS24] to the Choi states of any PRU that only makes non-adaptive calls. In particular, consider the following:

Lemma 46. *Let U be a unitary and C^U be any algorithm that makes t non-adaptive calls to U. Then there is an algorithm that prepares $|\Phi_{C^U}\rangle$ given t-copies of $|\Phi_U\rangle$, where $|\Phi_U\rangle$ is the Choi state of U.*

Proof. We can assume without loss of generality that C^U applies a unitary A, then $U^{\otimes t}$, and then another unitary B. Thus, we can prepare the Choi state $|\Phi_{C^U}\rangle$ as follows:

$$\begin{aligned}
(\mathrm{id} \otimes B)(A^\intercal \otimes \mathrm{id})|\Phi_U\rangle^{\otimes t} &= (\mathrm{id} \otimes B)(A^\intercal \otimes \mathrm{id})|\Phi_{U^{\otimes t}}\rangle \\
&= (\mathrm{id} \otimes B)(A^\intercal \otimes \mathrm{id})(\mathrm{id} \otimes U^{\otimes t})|\Omega\rangle \\
&= (\mathrm{id} \otimes B)(\mathrm{id} \otimes U^{\otimes t})(A^\intercal \otimes \mathrm{id})|\Omega\rangle \\
&= (\mathrm{id} \otimes B)(\mathrm{id} \otimes U^{\otimes t})(\mathrm{id} \otimes A)|\Omega\rangle \\
&= |\Phi_{BU^{\otimes t}A}\rangle \\
&= |\Phi_{C^U}\rangle .
\end{aligned}$$

Here the first line uses the definition of the Choi state. Then we use the fact that $U^{\otimes t}$ and $A^\intercal$ act on different registers and therefore commute with each other. Finally, we use the ricochet property of EPR pairs, and the definition of the Choi state and C^U. □

10.1 Optimality of ℓ-Query PRUs in Section 9

We argue that the construction presented in Section 9 is optimal in terms of its query bound. That is, we show that for any ℓ-query PRU, where the algorithm makes a *single* query to the Haar random oracle, it has to be the case that $\ell = O(\lambda/\log(\lambda)^{1+\varepsilon})$, where $\varepsilon > 0$. Our proof is inspired by the dimension counting argument from [AGQY22; AGL24].

Theorem 47. *Let $\{G_k^U\}_{k \in \{0,1\}^\lambda}$ be a set of oracle algorithms, where G_k runs in polynomial time. Moreover, for every $k \in \{0,1\}^\lambda$, there exists efficiently implementable unitaries A_k and B_k such that $G_k = B_k U A_k$.*

Then, $\{G_k^U\}_{k \in \{0,1\}^\lambda}$ is not an ℓ-query PRU for $\ell = \omega(\lambda/\log(\lambda))$ in iQHROM, where U is the Haar unitary.

Proof. Before we describe the distinguisher that violates the security of G_k^U, we first state some observations.

Observations. From Lemma 46, note that $|\Phi_{G_k^U}\rangle = (A_k^\intercal \otimes B_k)|\Phi_U\rangle$. We define $\rho_0^{(t,\ell)}$ below.

$$\begin{aligned}
\rho_0^{(t,\ell)} &= \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda \\ U\leftarrow\mu_n}} \left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes |\Phi_{G_k^U}\rangle\langle\Phi_{G_k^U}|^{\otimes \ell}\right] \\
&= \mathop{\mathbb{E}}_{\substack{k\leftarrow\{0,1\}^\lambda \\ U\leftarrow\mu_n}} \left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes \left((A_k^\intercal \otimes B_k)\,|\Phi_U\rangle\langle\Phi_U|\,((A_k^\intercal)^\dagger \otimes (B_k)^\dagger)\right)^{\otimes \ell}\right] \\
&= \mathop{\mathbb{E}}_{k\leftarrow\{0,1\}^\lambda} \left[\left(\mathrm{id} \otimes (A_k^\intercal \otimes B_k)^{\otimes \ell}\right) \mathop{\mathbb{E}}_{U\leftarrow\mu_n}\left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes |\Phi_U\rangle\langle\Phi_U|^{\otimes \ell}\right] \left(\left(\mathrm{id} \otimes (A_k^\intercal \otimes B_k)^\dagger\right)^{\otimes \ell}\right)\right].
\end{aligned}$$

We determine $\mathsf{rank}\left(\rho_0^{(t,\ell)}\right)$. In order to do that, note that, from [Har23],[11] the following holds:

$$\mathsf{rank}\left(\mathop{\mathbb{E}}_{U\leftarrow\mu_n}\left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes |\Phi_U\rangle\langle\Phi_U|^{\otimes \ell}\right]\right) = \dim(\Pi_{\mathsf{Sym}}^{(t+\ell),2m}),$$

where $\Pi_{\mathsf{Sym}}^{(t+\ell),2m}$ is the projector onto the symmetric subspace spanned by $(t+\ell)$-copy m-qubit states. Thus, we have the following:

$$\mathsf{rank}\left(\rho_0^{(t,\ell)}\right) \leq 2^\lambda \cdot \binom{2^{2m}+\ell+t-1}{\ell+t}.$$

We define another state $\rho_1^{(t,\ell)}$ as

$$\rho_1^{(t,\ell)} = \mathop{\mathbb{E}}_{\substack{U\leftarrow\mu_n \\ V\leftarrow\mu_n}}\left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes |\Phi_V\rangle\langle\Phi_V|^{\otimes \ell}\right].$$

We determine $\mathsf{rank}\left(\rho_1^{(t,\ell)}\right)$ and have

$$\mathsf{rank}\left(\rho_1^{(t,\ell)}\right) = \binom{2^{2m}+\ell-1}{\ell} \cdot \binom{2^{2m}+t-1}{t}.$$

Finally, we use the following fact to upper bound $\frac{\mathrm{rank}(\rho_0^{(t,\ell)})}{\mathrm{rank}(\rho_1^{(t,\ell)})}$.

Claim 48 ([AGL24]). *Suppose $\ell = \omega(\lambda/\log(\lambda))$, $t = \lambda^3$. Then:*

$$\frac{2^\lambda \cdot \binom{2^{2m}+\ell+t-1}{\ell+t}}{\binom{2^{2m}+\ell-1}{\ell} \cdot \binom{2^{2m}+t-1}{t}} \leq \frac{1}{2^\lambda}$$

Using the above claim, we have (for the parameters stated in the claim) that $\frac{\mathrm{rank}(\rho_0^{(t,\ell)})}{\mathrm{rank}(\rho_1^{(t,\ell)})} \leq \frac{1}{2^\lambda}$.

Distinguisher. Let Π be the projector that projects onto the eigenspace of $\rho_0^{(t,\ell)}$. The distinguisher $\mathcal{A}$, with oracle access to the Haar random unitary U and another unitary W (which is either the unitary design that depends on U or a Haar random unitary that is independently sampled), does the following:

- $\mathcal{A}$ creates t copies of $|\Phi_U\rangle\langle\Phi_U|$ by making t queries to U.

[11] Specifically, [Har23] gives a closed form expression for $\sigma_0 = \mathop{\mathbb{E}}_{U\leftarrow\mu_n}\left[|\Phi_U\rangle\langle\Phi_U|^{\otimes t} \otimes |\Phi_U\rangle\langle\Phi_U|^{\otimes \ell}\right]$ (see equation (23) in [Har23]) and also, $\sigma_1 = \mathop{\mathbb{E}}_{U\leftarrow\mu_n}\left[U^{\otimes(t+\ell)}|0^{2m}\rangle\langle 0^{2m}|U^{\otimes(t+\ell)}\right]$ (see equation (22) in [Har23]). From the closed form expressions, it follows that $\mathsf{rank}(\sigma_0) = \mathsf{rank}(\sigma_1)$. But σ_1 is precisely, the normalized projector on the symmetric subspace $\Pi_{\mathsf{Sym}}^{(t+\ell),2m}$.

- $\mathcal{A}$ creates ℓ copies of $|\Phi_W\rangle\!\langle\Phi_W|$ by making ℓ queries to W.
- It then measures $|\Phi_U\rangle\!\langle\Phi_U|^{\otimes t} \otimes |\Phi_W\rangle\!\langle\Phi_W|^{\otimes \ell}$ using the measurement basis $\{\Pi, \mathrm{id} - \Pi\}$.
- If the measurement succeeds, output 1. Otherwise, output 0.

Let us consider the following cases.

Case 1. $W = G_k^U$: In this case, the probability that the distinguisher always outputs 1.

Case 2. $W = V$**, where** V **is an i.i.d Haar random unitary**: We have the following:

$$\begin{aligned}
\mathrm{Tr}\left(\Pi\rho_1^{\ell,t}\right) &\leq \frac{\mathrm{Tr}(\Pi)}{\mathrm{rank}(\rho_1^{(\ell,t)})} \\
&= \frac{\mathrm{rank}(\rho_0^{(\ell,t)})}{\mathrm{rank}(\rho_1^{(\ell,t)})} \\
&\leq \frac{1}{2^\lambda} \text{ (Claim 48)}
\end{aligned}$$

□

10.2 Almost Optimality among Parallel-Query Pseudorandom Unitaries

In the previous section, we showed that a PRU construction that makes only a single call to the Haar random unitary cannot be more secure than our construction. Here we show that PRU constructions that make arbitrarily many queries in *parallel* cannot be much more secure than our construction.

We begin as in [CCS24], showing that many copies of the Choi state of a Haar random unitary are far from the Choi state of any fixed unitary with high probability. To prove this, we follow the proof of Lemma 5.4 from [CCS24], with a slight modification to handle Choi states of Haar random unitaries.

Lemma 49 (Lemma 5.4 from [CCS24])**.** *Let $|\psi_0\rangle$ be a 2^n-dimensional state, then*

$$\Pr_{|\psi\rangle \leftarrow \mathcal{H}_n}\left[|\langle\psi|\psi_0\rangle|^2 \geq \frac{1}{2}\right] \leq 8\exp\left(\frac{-2^n}{600}\right).$$

We prove a slightly modified version of the lemma as it pertains to Choi states.

Lemma 50. *Let U_0 be a $2^n \times 2^n$ unitary matrix, then the following holds*

$$\Pr_{U \leftarrow \mu_n}\left[|\langle\Phi_U|\Phi_{U_0}\rangle|^2 \geq \frac{1}{2}\right] \leq 2\exp\left(\frac{-2^n}{96}\right).$$

Proof. Our goal is to apply Levy's lemma to the squared inner product of the Choi states. First, consider the following function of two unitaries:

$$f_1(U) = \mathrm{Re}\left(\langle\Omega|UU_0^\dagger|\Omega\rangle\right).$$

Then the following holds

$$\begin{aligned}
|f_1(U) - f_1(V)| &= \left|\mathrm{Re}\left(\langle\Omega|UU_0^\dagger|\Omega\rangle\right) - \mathrm{Re}\left(\langle\Omega|VU_0^\dagger|\Omega\rangle\right)\right| \\
&\leq \left|\langle\Omega|(U-V)U_0^\dagger|\Omega\rangle\right| \\
&= \left|\frac{1}{2^n}\mathrm{Tr}\Big[(U-V)U_0^\dagger\Big]\right| \\
&\leq \frac{1}{2^n}\|U-V\|_F\|U_0\|_F
\end{aligned}$$

$$= \|U - V\|_F \, .$$

The same inequalities apply for $f_2(U) = \mathrm{Im}\left(\langle\Omega|UU_0^\dagger|\Omega\rangle\right)$. Applying Levy's lemma, we have the following:

$$\Pr_{U \leftarrow \mu_n}\left[f_1(U) \geq 1/2\right] \leq \exp\left(-\frac{2^n}{96}\right) .$$

The same holds for f_2. Thus by a union bound, we have that

$$\begin{aligned}\Pr_{U \leftarrow \mathcal{H}_n}\left[|\langle\Phi_U|\Phi_{U_0}\rangle|^2 \geq \frac{1}{2}\right] &= \Pr_{U \leftarrow \mu_n}\left[f_1^2(U) + f_2^2(U) \geq \frac{1}{2}\right] \\ &\leq \Pr_{U \leftarrow \mu_n}\left[f_1(U) \geq \frac{1}{2}\right] + \Pr_{U \leftarrow \mu_n}\left[f_2(U) \geq \frac{1}{2}\right] \\ &\leq 2\exp\left(-\frac{2^n}{96}\right) ,\end{aligned}$$

as desired. This completes the proof of the lemma. □

The final technical tool we need for this section is the quantum OR lemma.

Lemma 51 (Quantum OR lemma [WB24; HLM17])**.** *Let $\Pi_1, \ldots, \Pi_m$ be a collection of projectors, and let $\epsilon \leq \frac{1}{2}$ and δ. Let ρ be a state with the promise that either there exists Π_i such that $\mathrm{Tr}[\Pi_i\rho] \geq 1 - \epsilon$ (case 1), or for all i, $\mathrm{Tr}[\Pi_i\rho] \leq \delta$ (case 2). Then there is a polynomial space quantum algorithm A such that*

1. *In case 1, A accepts with probability at least $(1-\epsilon)^2/4.5$.*
2. *In case 2, A accepts with probability at most $2m\delta$.*

A only requires black box access to the projector valued measurements $\{\Pi_i, \mathrm{id} - \Pi_i\}$ and $O(\log m)$ additional space.

Using these results, we can prove that no construction of PRU in the iQHROM can only make a single parallel query to the common Haar random unitary.

Theorem 52 (Tightness of PRU)**.** *For any construction of PRU making non-adaptive calls to the Haar random oracle, with output size equal to λ, there exists an adversary that breaks its security by making $O(\lambda)$ non-adaptive queries to the PRU and $p(\lambda)$ non-adaptive queries to the Haar random oracle for some polynomial p.*

Proof. We construct an adversary against any PRU that makes non-adaptive queries using the quantum OR attack from [CCS24]. Assume that the PRU construct on key k first calls unitary A_k, then calls the Haar random unitary $U^{\otimes t}$, and finally runs B_k. We describe the k^{th} measurement that we use as input to the quantum OR algorithm. Starting from $O(t\lambda)$ copies of $|\Phi_U\rangle$ and $O(\lambda)$ copies of $|\Phi_{\mathcal{O}}\rangle$, for every key k, the adversary performs the algorithm described by Lemma 46 on $(|\Phi_U\rangle^{\otimes t})^{\otimes O(\lambda)}$ to get $O(\lambda)$ copies of $|\Phi_{U_k}\rangle$, the Choi state corresponding to the PRU with key k. Then the measurement performs a SWAP test with all $O(\lambda)$ copies of $|\Phi_{\mathcal{O}}\rangle$. Finally, the measurement uncomputes the computation. Formally, the k'th measurement operator Π_k has the following description, where the registers AB contain copies of the Choi state $|\Phi_U\rangle$ and the registers CD contain copies of the Choi state $|\Phi_{\mathcal{O}}\rangle$.

$$\Pi_k = \left(\left((A_k^* \otimes B_k^\dagger)_{\mathsf{AB}} \otimes \mathrm{id}_{\mathsf{BC}}\right)(\Pi^{\mathrm{sym}}_{\mathsf{ABCD}})\left((A_k^\intercal \otimes B_k)_{\mathsf{AB}} \otimes \mathrm{id}_{\mathsf{BC}}\right)\right)^{\otimes O(\lambda)} .$$

Here A^* is the complex conjugate of A, as opposed to $A^\dagger$, which is the conjugate transpose. From Lemma 46, when the oracle $\mathcal{O}$ is equal to U_k for some k, there is a choice (namely the one corresponding to k) of measurement that accepts with probability 1. Thus, in Lemma 51, we can set $\epsilon = 0$.

Furthermore, from Lemma 50 if the oracle is a Haar random unitary, then with probability $1-2\exp\left(-\frac{d}{96}\right)$, the Choi states have less than $1/2$ squared fidelity. The probability that the swap test succeeds on all $O(\lambda)$ copies of the state is thus upper bounded by $\left(\frac{3}{4}\right)^{O(\lambda)}$. Setting the number of copies of the state to be $c\lambda$ for any constant such that $(3/4)^c < 1/2$, we can apply a union bound over all 2^λ measurements to get that the probability that the quantum OR accepts for a Haar random state is negligible in λ. Applying Lemma 51, we see that our adversary breaks PRU security with constant probability. □

11 Unbounded-Copy PRS in the iQHROM

In this section the main result is a simple construction of pseudorandom states in the iQHROM. The construction of a PRS generator G, with oracle access to an $n(\lambda)$-qubit Haar random unitary U for $n \geq \lambda$, is as follows: on input $k \in \{0,1\}^\lambda$, output $U|k||0^{n-\lambda}\rangle$. We note that this result is probably provable using the lower bound on unstructured search. However, as a warm-up for the next section, we present a nice argument using the path-recording framework.

Theorem 53. *G is a multi-copy secure PRS generator in the* iQHROM*. Formally, an adversary that receives t copies of a state that is either the output of G on a random $k \in \{0,1\}^\lambda$ or a Haar random state that is independent of U and makes s adaptive queries to U has distinguishing advantage at most $O\left(\sqrt{\frac{s}{2^\lambda}} + \frac{(t+s)^2}{\sqrt{2^n}}\right)$.*

Proof. Fix n, λ, t, s and let $N := 2^n$ for the rest of the proof. We complete by hybrid arguments.

Hybrid 1: The challenger samples a uniformly random $k \in \{0,1\}^\lambda$ and sends t copies of $U|k||0^{n-\lambda}\rangle$ to the adversary, where U is the Haar random oracle. Then, the adversary makes s queries to U.

Hybrid 2: Using the path-recording framework, we can write the initial state of an adversary that receives t copies of $\mathsf{PR}|k||0^{n-\lambda}\rangle$ for a uniformly random $k \in \{0,1\}^\lambda$ as follows

$$\frac{1}{\sqrt{2^\lambda}} \sum_{k \in \{0,1\}^\lambda} \left(\bigotimes_{i=1}^{t} \mathsf{PR}|k||0^{n-\lambda}\rangle_{\mathsf{C_i}} \right) |k\rangle_{\mathsf{K}} = \sqrt{\frac{1}{2^\lambda N^{\downarrow t}}} \sum_{\substack{k \in \{0,1\}^\lambda, \\ (y_1,\ldots,y_t) \in [N]^t_{\mathrm{dist}}}} |y_1,\ldots,y_t\rangle_{\mathsf{C_1 \ldots C_t}} |\{(k||0^{n-\lambda}, y_i)\}_{i=1}^t\rangle_{\mathsf{E}} |k\rangle_{\mathsf{K}}.$$

Then we can write the state of any adversary that given registers $(\mathsf{C_1},\ldots,\mathsf{C_t})$ and makes s many queries to PR as follows

$$|\psi_{\mathrm{real}}\rangle_{\mathsf{ABEK}} := \\ \sqrt{\frac{1}{2^\lambda N^{\downarrow t+s}}} \sum_{\substack{k \in \{0,1\}^\lambda, \\ (x_1,\ldots,x_s) \in [N]^s, \\ (y_1,\ldots,y_t,z_1,\ldots,z_s) \in [N]^{t+s}_{\mathrm{dist}}}} \left(\prod_{i=1}^{s} |z_i\rangle\langle x_i|_{\mathsf{A}} A^{(i)}_{\mathsf{AB}} \right) |\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}} |\{(k||0^{n-\lambda}, y_i)\}_{i=1}^t \cup \{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}} |k\rangle_{\mathsf{K}},$$

where $|\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}} := |y_1,\ldots,y_t\rangle_{\mathsf{C_1 \ldots C_t}} |0\rangle_{\mathsf{B'}}$ for some ancilla register $\mathsf{B'}$. From Theorem 22, the trace distance between $\mathrm{Tr}_{\mathsf{EK}}(|\psi_{\mathrm{real}}\rangle\langle\psi_{\mathrm{real}}|_{\mathsf{ABEK}})$ and the adversary's density matrix in Hybrid 1 is $O\left((t+s)^2/2^n\right)$.

Here the key fact is that the z_j and y_i are distinct from each other, because the path-recording oracle only appends z_j that are not already in the image of the relation. We can then apply an isometry on the purifying register that takes all elements of the relation state that have k as the input and puts them in a new set. To do so, we say that a pair (R, k) of an injective relation R of size $t+s$ and a key k is *good* if and only if

$$|\{y \in \mathrm{Im}(R) : \ (k||0^n, y) \in R\}| = t.$$

We define the projection Π_{good} onto the the subspace spanned by $\{|R\rangle|k\rangle : (R,k) \text{ is good}\}$. Explicitly,

$$\Pi_{\text{good}} := \sum_{(R,k) \text{ is good}} |R\rangle\langle R|_{\mathsf{E}} \otimes |k\rangle\langle k|_{\mathsf{K}}.$$

Hybrid 3: Now, consider applying Π_{good} on $|\psi_{\text{real}}\rangle_{\mathsf{ABEK}}$. Observe that $|\{(k||0^{n-\lambda}, y_i)\}_{i=1}^t \cup \{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}}|k\rangle_{\mathsf{K}}$ vanishes if and only if $k \in \{\vec{x}\}$, where $\{\vec{x}\} := \bigcup_{i=1}^s \{x_i\}$. Therefore, we get the following subnormalized state

$$\sqrt{\frac{1}{2^\lambda N^{\downarrow t+s}}} \sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\ (y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\text{dist}},\\ k\notin\{\vec{x}\}}} \left(\prod_{i=1}^s |z_i\rangle\langle x_i|_{\mathsf{A}} A^{(i)}_{\mathsf{AB}}\right) |\psi_{\text{Init}}(\vec{y})\rangle_{\mathsf{AB}} |\{(k||0^{n-\lambda}, y_i)\}_{i=1}^t \cup \{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}}|k\rangle_{\mathsf{K}}.$$

Then applying the partition isometry, we obtain

$$\sqrt{\frac{1}{2^\lambda N^{\downarrow t+s}}} \sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\ (y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\text{dist}},\\ k\notin\{\vec{x}\}}} \left(\prod_{i=1}^s |z_i\rangle\langle x_i|_{\mathsf{A}} A^{(i)}_{\mathsf{AB}}\right) |\psi_{\text{Init}}(\vec{y})\rangle_{\mathsf{AB}} |\{(k||0^{n-\lambda}, y_i)\}_{i=1}^t\rangle_{\mathsf{E}_1} |\{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}}.$$

Then we apply an isometry to uncompute k in register E_1, controlled by register K, and obtain the subnormalized state $|\psi_{\text{good}}\rangle_{\mathsf{ABE_1E_2K}}$:

$$\sqrt{\frac{1}{2^\lambda N^{\downarrow t+s}}} \sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\ (y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\text{dist}},\\ k\notin\{\vec{x}\}}} \left(\prod_{i=1}^s |z_i\rangle\langle x_i|_{\mathsf{A}} A^{(i)}_{\mathsf{AB}}\right) |\psi_{\text{Init}}(\vec{y})\rangle_{\mathsf{AB}} |\{(0^n, y_i)\}_{i=1}^t\rangle_{\mathsf{E}_1} |\{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}}. \quad (2)$$

The trace distance between $\mathrm{Tr}_{\mathsf{EK}}(|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|)$ in Hybrid 2 and $\mathrm{Tr}_{\mathsf{E_1E_2K}}(|\psi_{\text{good}}\rangle\langle\psi_{\text{good}}|)$ in Hybrid 3 satisfies

$$\begin{aligned}
&\mathsf{TD}(\mathrm{Tr}_{\mathsf{EK}}(|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|_{\mathsf{ABEK}}), \mathrm{Tr}_{\mathsf{E_1E_2K}}(|\psi_{\text{good}}\rangle\langle\psi_{\text{good}}|_{\mathsf{ABE_1E_2K}}))\\
=&\mathsf{TD}(\mathrm{Tr}_{\mathsf{EK}}(|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|_{\mathsf{ABEK}}), \mathrm{Tr}_{\mathsf{EK}}(\Pi_{\text{good}}|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|_{\mathsf{ABEK}}\Pi_{\text{good}}))\\
\le&\mathsf{TD}(|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|_{\mathsf{ABEK}}, \Pi_{\text{good}}|\psi_{\text{real}}\rangle\langle\psi_{\text{real}}|_{\mathsf{ABEK}}\Pi_{\text{good}})\\
\le&\sqrt{1 - \|\Pi_{\text{good}}|\psi_{\text{real}}\rangle_{\mathsf{ABEK}}\|^2}\\
=&\sqrt{1 - \||\psi_{\text{good}}\rangle_{\mathsf{ABE_1E_2K}}\|^2},
\end{aligned} \quad (3)$$

where the last inequality follows from Lemma 11. Looking ahead, instead of bounding $\||\psi_{\text{good}}\rangle\|$ directly, we will show that the inner product between $|\psi_{\text{good}}\rangle$ and some normalized state is negligibly close to 1. Hence, we can conclude that $\||\psi_{\text{good}}\rangle\|$ is also negligibly close to 1 from Lemma 12.

For readability, we define Hybrid 6 to Hybrid 4 in reverse order.

Hybrid 6: Next, we can examine the state of an adversary who got copies of an independently sampled Haar random state, which we can model as getting copies of $V|0\rangle$ for an independently sampled unitary V.

Hybrid 5: Similar to Hybrid 2, using the path-recording framework, we replace (U, V) with $(\mathsf{PR}_1, \mathsf{PR}_2)$ and define the normalized state

$$|\psi^{\mathsf{PR}_1,\mathsf{PR}_2}_{\text{ideal}}\rangle_{\mathsf{ABE_1E_2}} := \sqrt{\frac{1}{N^{\downarrow t}N^{\downarrow s}}} \sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\ (y_1,\dots,y_t)\in[N]^t_{\text{dist}},\\ (z_1,\dots,z_s)\in[N]^s_{\text{dist}}}} \left(\prod_{i=1}^s |z_i\rangle\langle x_i|_{\mathsf{A}} A^{(i)}_{\mathsf{AB}}\right) |\psi_{\text{Init}}(\vec{y})\rangle_{\mathsf{AB}} |\{(0^n, y_i)\}_{i=1}^t\rangle_{\mathsf{E}_1} |\{(x_j, z_j)\}_{j=1}^s\rangle_{\mathsf{E}_2}.$$

From Theorem 22, the trace distance between $\mathrm{Tr}_{\mathsf{E_1E_2}}(|\psi^{\mathsf{PR_1,PR_2}}_{\mathrm{ideal}}\rangle\langle\psi^{\mathsf{PR_1,PR_2}}_{\mathrm{ideal}}|)$ in Hybrid 5 and the adversary's density matrix in Hybrid 6 is $O((t^2+s^2)/2^n)$.

Hybrid 4: We replace $(\mathsf{PR_1},\mathsf{PR_2})$ with $(\mathsf{pcf}_{1,n}\mathsf{PR}^{(\mathsf{E_1})},\mathsf{pcf}_{1,n}\mathsf{PR}^{(\mathsf{E_2})})$ as defined in Section 6.2 and define the normalized state

$$|\psi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle_{\mathsf{ABE_1E_2}} := \sqrt{\frac{1}{N^{\downarrow t+s}}}\sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\(y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\mathrm{dist}}}}\left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|_{\mathsf{A}}A^{(i)}_{\mathsf{AB}}\right)|\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}}|\{(0^n,y_i)\}_{i=1}^t\rangle_{\mathsf{E_1}}|\{(x_j,z_j)\}_{j=1}^s\rangle_{\mathsf{E_2}}.$$

We apply an isometry to append $\frac{1}{\sqrt{2^\lambda-|\{\vec{x}\}|}}\sum_{k\notin\{\vec{x}\}}|k\rangle_{\mathsf{K}}$ on the above state, controlled by register E, and result in the normalized state

$$\begin{aligned}|\phi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle_{\mathsf{ABE_1E_2K}} := \sqrt{\frac{1}{N^{\downarrow t+s}}}&\sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\(y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\mathrm{dist}}}}\left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|_{\mathsf{A}}A^{(i)}_{\mathsf{AB}}\right)|\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}}\\&\otimes|\{(0^n,y_i)\}_{i=1}^t\rangle_{\mathsf{E_1}}|\{(x_j,z_j)\}_{j=1}^s\rangle_{\mathsf{E_2}}\frac{1}{\sqrt{2^\lambda-|\{\vec{x}\}|}}\sum_{k\notin\{\vec{x}\}}|k\rangle_{\mathsf{K}}.\end{aligned} \tag{4}$$

By Theorem 27, the trace distance between $|\psi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle$ in Hybrid 4 and $|\psi^{\mathsf{PR_1,PR_2}}_{\mathrm{ideal}}\rangle$ in Hybrid 5 is $O((t+s)^2/\sqrt{2^n})$.

Finally, we show that the inner product between the sub-normalized state $|\psi_{\mathrm{good}}\rangle$ in Hybrid 3 (Equation (2)) and the normalized state $|\phi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle$ in Hybrid 4 (Equation (4)) is negligibly close to 1. Notice that

$$\begin{aligned}|\phi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle_{\mathsf{ABE_1E_2K}} := \sqrt{\frac{1}{N^{\downarrow t+s}}}&\sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\(y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\mathrm{dist}}}}\left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|_{\mathsf{A}}A^{(i)}_{\mathsf{AB}}\right)|\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}}\\&\otimes|\{(0^n,y_i)\}_{i=1}^t\rangle_{\mathsf{E_1}}|\{(x_j,z_j)\}_{j=1}^s\rangle_{\mathsf{E_2}}\frac{1}{\sqrt{2^\lambda-|\{\vec{x}\}|}}\sum_{k\notin\{\vec{x}\}}|k\rangle_{\mathsf{K}},\end{aligned}$$

and

$$\begin{aligned}|\psi_{\mathrm{good}}\rangle_{\mathsf{ABE_1E_2K}} := \sqrt{\frac{1}{N^{\downarrow t+s}}}&\sum_{\substack{(x_1,\dots,x_s)\in[N]^s,\\(y_1,\dots,y_t,z_1,\dots,z_s)\in[N]^{t+s}_{\mathrm{dist}}}}\sqrt{\frac{2^\lambda-|\{\vec{x}\}|}{2^\lambda}}\left(\prod_{i=1}^{s}|z_i\rangle\langle x_i|_{\mathsf{A}}A^{(i)}_{\mathsf{AB}}\right)|\psi_{\mathrm{Init}}(\vec{y})\rangle_{\mathsf{AB}}\\&\otimes|\{(0^n,y_i)\}_{i=1}^t\rangle_{\mathsf{E_1}}|\{(x_j,z_j)\}_{j=1}^s\rangle_{\mathsf{E_2}}\frac{1}{\sqrt{2^\lambda-|\{\vec{x}\}|}}\sum_{k\notin\{\vec{x}\}}|k\rangle_{\mathsf{K}}.\end{aligned}$$

Since for all $(x_1,\dots,x_s)\in[N]^s$,

$$\sqrt{\frac{2^\lambda-|\{\vec{x}\}|}{2^\lambda}}\geq\sqrt{\frac{2^\lambda-s}{2^\lambda}}.$$

Hence, by Lemma 13, the inner product between $|\psi_{\mathrm{good}}\rangle$ and $|\phi^{\mathsf{cfPR_1,cfPR_2}}_{\mathrm{ideal}}\rangle$ is $\sqrt{1-\frac{s}{2^\lambda}}$ and the trace distance between $\mathrm{Tr}_{\mathsf{EK}}(|\psi_{\mathrm{real}}\rangle\langle\psi_{\mathrm{real}}|)$ in Hybrid 2 and $\mathrm{Tr}_{\mathsf{E_1E_2K}}(|\psi_{\mathrm{good}}\rangle\langle\psi_{\mathrm{good}}|))$ in Hybrid 3 (Equation (3)) is $O(\sqrt{s/2^\lambda})$.

Collecting the bounds, the trace distance between the adversary's density matrix in Hybrid 1 and that in Hybrid 6 is upper bounded by $O\left(\sqrt{\frac{s}{2^\lambda}}+\frac{(t+s)^2}{\sqrt{2^n}}\right)$ as desired. □

12 Adaptively Secure PRFS in the iQHROM

In this section, we extend the construction of PRS to PRFS. Our construction of a PRFS generator with key length λ, input length $m = m(\lambda)$, and output length $n = n(\lambda)$ such that $n \geq \lambda + m$ is intuitive and simple. Given oracle access to an n-qubit Haar random oracle U, on input $w \in \{0,1\}^m$ and key $k \in \{0,1\}^\lambda$, the PRFS generator G outputs $U|k||w||0^{n-\lambda-m}\rangle$. Namely,

$$\mathcal{O}_{\mathsf{PRFS}}(k,\cdot) : |w\rangle|0^n\rangle \mapsto |w\rangle \otimes U|k||w||0^{n-\lambda-m}\rangle.$$

We will prove that G is secure against any adversary that makes arbitrary polynomial adaptive quantum queries to U and arbitrary polynomial adaptive *classical* queries to $\mathcal{O}$, where $\mathcal{O}$ is either the PRFS construction $\mathcal{O}_{\mathsf{PRFS}}$ or a Haar random state generator $\mathcal{O}_{\mathsf{Haar}}$ defined in Definition 9.

Theorem 54. *G is an APRFS generator in the* iQHROM *if n and m satisfy $n \geq \lambda + m$. Formally, for any $t \in \mathbb{N}$ and adversary that makes t adaptive quantum queries to U and t adaptive classical queries to $\mathcal{O}$, the distinguishing advantage of $\mathcal{A}$ is at most $O\left(\frac{t^2}{2^{n-m}} + \frac{t^2}{\sqrt{2^n}} + \sqrt{\frac{t}{2^\lambda}}\right)$.*

Proof. Fix $\lambda, m, n, t \in \mathbb{N}$ and let $M := 2^m$ and $N := 2^n$. We assume that $\mathcal{A}$ alternatively makes queries to U and $\mathcal{O}$. That is, the adversary makes all odd-indexed queries to U and all even-indexed queries to $\mathcal{O}$. This is without loss of generality, as we can pad dummy queries and will later prove that the asymptotic bound remains unchanged.

From Definition 9, we need to show that classical query access to $\mathcal{O}_{\mathsf{PRFS}}(k,\cdot)$ is indistinguishable from classical query access to $\mathcal{O}_{\mathsf{Haar}}$. Here $\mathcal{O}_{\mathsf{Haar}}(\cdot)$, on input $x \in \{0,1\}^{m(\lambda)}$, outputs $|\vartheta_x\rangle$, where, for every $w \in \{0,1\}^{m(\lambda)}$, $|\vartheta_w\rangle := U_w|0^n\rangle$ and $\{U_w\}_{w\in\{0,1\}^m}$ is a set of i.i.d. n-qubit Haar unitaries. Notice that by the unitary invariance of the Haar measure, we can equivalently define $|\vartheta_w\rangle := U_w|\overline{w}\rangle$, where $\overline{w} := 0^\lambda||w||0^{n-\lambda-m}$.

To model that adversary $\mathcal{A}$ makes classical queries, we introduce the transcript register $\mathsf{Q} = (\mathsf{Q}_1, \ldots, \mathsf{Q}_t)$ where Q_i stores $\mathcal{A}$'s i-th classical query. We allow $\mathcal{A}$ to send the input register A, but then register A is immediately measured in the computational basis. Moreover, the adversary $\mathcal{A}$ does not have access to register Q. By the deferred measurement principle, equivalently, we can assume that right after $\mathcal{A}$ makes a classical query, the content in A is copied to Q. At the end, register Q is measured in the computational basis. Further note that whenever $\mathcal{A}$ queries on an input, the oracle appends an n-qubit answer register D to the system. See Figure 4 for an exposition.[12]

For ease of notation, going forward we define

$$\mathcal{O}_{\mathsf{PRFS}}(k,\cdot) : |w\rangle_{\mathsf{A}} \mapsto |w\rangle_{\mathsf{A}} \otimes U|k||w||0^{n-\lambda-m}\rangle_{\mathsf{D}},$$

and

$$\mathcal{O}_{\mathsf{Haar}} : |w\rangle_{\mathsf{A}} \mapsto |w\rangle_{\mathsf{A}} \otimes U_w|\overline{w}\rangle_{\mathsf{D}}.$$

Here for the i-th query, the register appended is called D_i and is appended to the system.
We refer to the experiment as Ideal if $\mathcal{O} = \mathcal{O}_{\mathsf{Haar}}$ and as Real if $\mathcal{O} = \mathcal{O}_{\mathsf{PRFS}}$, respectively.

We complete the proof by hybrid arguments.

- Ideal: The adversary gets access to the Quantum Haar Random Oracle U and $\mathcal{O}_{\mathsf{Haar}}$.

- $\mathsf{Hybrid\ 1}$: The adversary gets access to a path recording isometry $\mathsf{PR}_{\mathsf{ABE}_1}$ and $\mathcal{O}_{\mathsf{Haar}}$.

Lemma 55. $\left|\Pr_{\mathsf{Hybrid\ 1}}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1},\mathcal{O}_{\mathsf{Haar}}}] - \Pr_{\mathsf{Ideal}}[1 \leftarrow \mathcal{A}^{U,\mathcal{O}_{\mathsf{Haar}}}]\right| = O\left(\frac{t^2}{2^n}\right).$

[12] Register A contains the first m qubits of $\mathcal{A}$, register B contains the $(m+1)$-th qubit to the n-th qubit of $\mathcal{A}$, and register C contains all the other qubits of $\mathcal{A}$. Recall that $\mathcal{O}$ is an isometry with an input length m and an output length $m+n$. Hence, the number of $\mathcal{A}$'s qubits increases by n after the i-th query to $\mathcal{O}$ for all $i \in [t]$, and the next internal unitary A_{2i-1} is defined over the extended space. Although this is not reflected in Figure 4, it should not cause confusion.

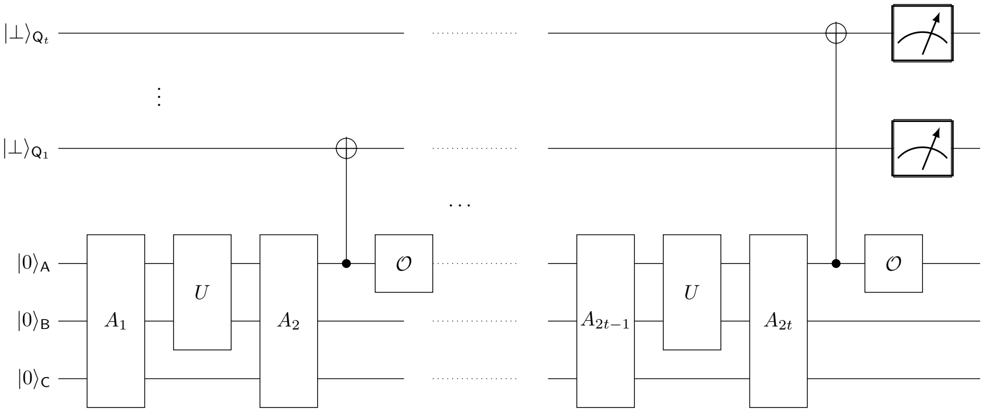

Figure 4: Modeling classical queries to $\mathcal{O}$.

Proof of Lemma 55. This is true by Theorem 22. □

Before defining $\mathsf{Hybrid}\ 2.i$, we define the path-recording isometries indexed by $w \in \{0,1\}^m$,

$$\mathsf{PR}^w_{\mathsf{DE}_2^w} : |x\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w'\in\{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} \mapsto \frac{1}{\sqrt{N - |R_2^w|}} \sum_{z\in[N]\setminus \mathrm{Im}(R_2^w)} |z\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1}|R_2^w \cup (\overline{x}, z)\rangle_{\mathsf{E}_2^w} \bigotimes_{\substack{w'\in\{0,1\}^m \\ w'\neq w}} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}}.$$ [13]

Hence, for $i \in \{0,1\}^m$, we define $\mathcal{O}_{\mathsf{Hyb2}.i}$ as

$$\mathcal{O}_{\mathsf{Hyb2}.i} : |w\rangle_A|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w'\in\{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} \mapsto \begin{cases} |w\rangle_{\mathsf{A}}\mathsf{PR}^w_{\mathsf{DE}_2^w}|w\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w'\in\{0,1\}^m}|R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} & \text{, if } w \le i \\ |w\rangle_{\mathsf{A}}|\vartheta_w\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w'\in\{0,1\}^m}|R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} & \text{, otherwise,} \end{cases}$$

where, for every $w \in \{0,1\}^{m(\lambda)}$, $|\vartheta_w\rangle = U_w|\overline{w}\rangle$ and U_w is an i.i.d. n-qubit Haar unitary.

- $\mathsf{Hybrid}\ 2.i$ for $0 \le i \le M$: The adversary gets access to a path recording isometry $\mathsf{PR}_{\mathsf{ABE}_1}$ and $\mathcal{O}_{\mathsf{Hyb2}.i}$. We assume that the initial state is

$$|0\rangle_{\mathsf{ABC}}|\bot,\ldots,\bot\rangle_{\mathsf{Q}}|\{\}\rangle_{\mathsf{E}_1} \bigotimes_{w\in\{0,1\}^m} |\{\}\rangle_{\mathsf{E}_2^w},$$

where registers $\mathsf{E}_1, \mathsf{E}_2$ are purifying registers.

Lemma 56. $\Pr_{\mathsf{Hybrid}\ 2.0}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb2.0}}}] = \Pr_{\mathsf{Hybrid}\ 1}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Haar}}}]$.

Proof of Lemma 56. Note that $\mathcal{O}_{\mathsf{Hyb2.0}}$ and $\mathcal{O}_{\mathsf{Haar}}$ are identically distributed. Hence the above lemma holds. □

Lemma 57. *For all* $0 \le i < M$, $\left|\Pr_{\mathsf{Hybrid}\ 2.i}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb2}.i}}] - \Pr_{\mathsf{Hybrid}\ 2.i+1}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb2}.i+1}}]\right| = O\left(\frac{t^2}{2^n}\right)$.

Proof of Lemma 57. Let there is an adversary $\mathcal{A}$ such that

$$\left|\Pr_{\mathsf{Hybrid}\ 2.i}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb2}.i}}] - \Pr_{\mathsf{Hybrid}\ 2.i+1}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb2}.i+1}}]\right| = \varepsilon,$$

[13] Here we assume that each E_2^w to be of the size $2n2^n$, with the first $|R_2^{w'}|$ qubits to hold $R_2^{w'}$ and the rest $2n2^n - |R_2^{w'}|$ to be $\bot$. Whenever we add something to $R_2^{w'}$, we update the number of $\bot$ such that the total size of E_2^w remains $2n2^n$.

for some $\varepsilon \in [0,1]$. We give the following (information-theoretic) reduction $\mathcal{R}$ given access to an oracle $\mathcal{P}$ that is either an n-qubit Haar random oracle U or a path-recoding oracle PR such that

$$\left|\Pr\left[1 \leftarrow \mathcal{R}^{\mathsf{PR},\mathcal{A}}\right] - \Pr\left[1 \leftarrow \mathcal{R}^{U,\mathcal{A}}\right]\right| = \varepsilon.$$

First, $\mathcal{R}$ initializes Q, E_1 and E_2^w for all $w \in \{0,1\}^m, w \neq i+1$. Next, $\mathcal{R}$ samples i.i.d. n-qubit Haar random unitaries U_w for $i+2 \leq w \leq M$.

- Whenever $\mathcal{A}$ queries $\mathsf{PR}_{\mathsf{ABE}_1}$, $\mathcal{R}$ locally simulates an independent path-recording oracle to respond to $\mathcal{A}$'s quantum queries to PR using E_1.
- To respond to $\mathcal{A}$'s classical queries, the reduction $\mathcal{R}$ locally simulates $\mathsf{PR}^w_{\mathsf{AE}_2^w}$ for $1 \leq w \leq i$, embeds $\mathcal{P}$ as the $(i+1)$-th oracle, and returns with $U_w|\overline{w}\rangle$, for $i+2 \leq w \leq M$.

By the above, $\mathcal{R}$ perfectly simulates $\mathcal{A}$, hence

$$\left|\Pr\left[1 \leftarrow \mathcal{R}^{\mathsf{PR},\mathcal{A}}\right] - \Pr\left[1 \leftarrow \mathcal{R}^{U,\mathcal{A}}\right]\right| = \varepsilon.$$

By Theorem 22, it holds that $\varepsilon = O\left(\frac{t^2}{2^n}\right)$. Hence, $\left|\Pr_{\mathsf{Hybrid}\ 2.i}[1 \leftarrow \mathcal{A}^{\mathsf{PR},\mathcal{O}_{\mathsf{Hyb2}.i}}] - \Pr_{\mathsf{Hybrid}\ 2.i+1}[1 \leftarrow \mathcal{A}^{\mathsf{PR},\mathcal{O}_{\mathsf{Hyb2}.i+1}}]\right| = O\left(\frac{t^2}{2^n}\right)$ as desired. □

Before defining Hybrid 3, we define

$$\mathcal{O}_{\mathsf{Hyb3}} : |w\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} \mapsto |w\rangle_{\mathsf{A}}\mathsf{PR}^w_{\mathsf{DE}_2^w}|w\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}}.$$

- Hybrid 3: The adversary gets access to a path recording isometry $\mathsf{PR}_{\mathsf{ABE}_1}$ and $\mathcal{O}_{\mathsf{Hyb3}}$.

Lemma 58. $\Pr_{\mathsf{Hybrid}\ 3}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1},\mathcal{O}_{\mathsf{Hyb3}}}] = \Pr_{\mathsf{Hybrid}\ 2.M}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1},\mathcal{O}_{\mathsf{Hyb2}.M}}]$.

Proof of Lemma 58. Note that $\mathcal{O}_{\mathsf{Hyb2}.M}$ and $\mathcal{O}_{\mathsf{Hyb3}}$ are identical. Hence the above lemma holds. □

Before defining Hybrid 4, we define oracles cfPR and $\mathcal{O}_{\mathsf{Hyb4}}$ that maintain the "global" injectivity of all purifying registers:

$$\mathsf{cfPR}|x\rangle_{\mathsf{AB}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} :=$$

$$\frac{1}{\sqrt{N - \left|\mathrm{Im}\left(R_1 \cup \bigcup_{w' \in \{0,1\}^m} R_2^{w'}\right)\right|}} \sum_{\substack{y \in [N]: \\ y \notin \mathrm{Im}\left(R_1 \cup \bigcup_{w' \in \{0,1\}^m} R_2^{w'}\right)}} |y\rangle_{\mathsf{AB}} \otimes |R_1 \cup \{(x,y)\}\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}}$$

and

$$\mathcal{O}_{\mathsf{Hyb4}}|w\rangle_{\mathsf{A}}|R_1\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}} :=$$

$$\frac{1}{\sqrt{N - \left|\mathrm{Im}\left(R_1 \cup \bigcup_{w' \in \{0,1\}^m} R_2^{w'}\right)\right|}} \sum_{\substack{y \in [N]: \\ y \notin \mathrm{Im}\left(R_1 \cup \bigcup_{w' \in \{0,1\}^m} R_2^{w'}\right)}} |w\rangle_{\mathsf{A}}|y\rangle_{\mathsf{D}}|R_1\rangle_{\mathsf{E}_1}|R_2^w \cup (\overline{w}, y)\rangle_{\mathsf{E}_2^w} \bigotimes_{\substack{w' \in \{0,1\}^m \\ w' \neq w}} |R_2^{w'}\rangle_{\mathsf{E}_2^{w'}}.$$

- Hybrid 4: The adversary gets access to a path recording isometry cfPR and $\mathcal{O}_{\mathsf{Hyb4}}$.

Lemma 59. $\left|\Pr_{\mathsf{Hybrid}\ 4}[1 \leftarrow \mathcal{A}^{\mathsf{cfPR}_{\mathsf{ABE}_1},\mathcal{O}_{\mathsf{Hyb4}}}] - \Pr_{\mathsf{Hybrid}\ 3}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1},\mathcal{O}_{\mathsf{Hyb3}}}]\right| = O\left(\frac{t^2}{\sqrt{2^n}}\right)$.

Proof of Lemma 59. By a similar hybrid as in Theorem 27 and calculation of inner product as in Lemma 28, we have $\left|\Pr_{\mathsf{Hybrid}\ 4}[1 \leftarrow \mathcal{A}^{\mathsf{cfPR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb4}}}] - \Pr_{\mathsf{Hybrid}\ 3}[1 \leftarrow \mathcal{A}^{\mathsf{PR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb3}}}]\right| = O\left(\frac{t^2}{\sqrt{2^n}}\right)$. □

For ease of notation, we assume that A_{2i+1} maps ABCD_i to ABC where C is updated to be increased by the size of D_i.

Hence, the final state in Hybrid 4 is

$$|\mathcal{A}_{t,t}^{\mathsf{cfPR}, \mathcal{O}_{\mathsf{Hyb4}}}\rangle := \sum_{\substack{\vec{x} \in [N]^t, \vec{w} \in [M]^t, \\ (y_1, \ldots, y_t, z_1, \ldots, z_t) \in [N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}} \left(\prod_{i=1}^{t} |w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i} |y_i\rangle\langle x_i|_{\mathsf{AB}} A_{2i-1} \right) |0\rangle_{\mathsf{ABC}}$$
$$\otimes |\vec{w}\rangle_{\mathsf{Q}} |\{(x_j, y_j)\}_{j \in [t]}\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |\{(\overline{w}_i, z_i) : w_i = w'\}\rangle_{\mathsf{E}_2^{w'}}. \quad (5)$$

Finally, Hybrid 5 is the same as Real except that U is replaced with PR.

- Hybrid 5: $\mathcal{A}$ makes t quantum queries to $\mathsf{PR}_{\mathsf{ABE}}$ and t classical queries to $\mathcal{O}_{\mathsf{Hyb5}}$ defined as follows.
  - Initial state: $|0\rangle_{\mathsf{ABC}} |\bot, \ldots, \bot\rangle_{\mathsf{Q}} |\{\}\rangle_{\mathsf{E}} \otimes \frac{1}{\sqrt{2^\lambda}} \sum_{k \in \{0,1\}^\lambda} |k\rangle_{\mathsf{K}}$.
  - Oracle $\mathsf{PR}_{\mathsf{ABE}}$:
  $$|x\rangle_{\mathsf{AB}} |R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N - |\mathrm{Im}(R)|}} \sum_{\substack{y \in [N]: \\ y \notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{AB}} |R \cup \{(x, y)\}\rangle_{\mathsf{E}}.$$
  - Oracle $\mathcal{O}_{\mathsf{Hyb5}}$:
  $$|w\rangle_{\mathsf{A}} |R\rangle_{\mathsf{E}} |k\rangle_{\mathsf{K}} \mapsto |w\rangle_{\mathsf{A}} \otimes \frac{1}{\sqrt{N - |\mathrm{Im}(R)|}} \sum_{\substack{z \in [N]: \\ z \notin \mathrm{Im}(R)}} |z\rangle_{\mathsf{D}_i} |R \cup \{(k||w||0^{n-\lambda-m}, z)\}\rangle_{\mathsf{E}} |k\rangle_{\mathsf{K}}.$$

Hence, the final state in Hybrid 5 is

$$|\mathcal{A}_{t,t}^{\mathsf{PR}, \mathcal{O}_{\mathsf{Hyb5}}}\rangle = \sum_{\substack{k \in \{0,1\}^\lambda, \\ \vec{x} \in [N]^t, \vec{w} \in [M]^t, \\ (y_1, \ldots, y_t, z_1, \ldots, z_t) \in [N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{2^\lambda \cdot N^{\downarrow 2t}}} \left(\prod_{i=1}^{t} |w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i} |y_i\rangle\langle x_i|_{\mathsf{AB}} A_{2i-1} \right) |0\rangle_{\mathsf{ABC}}$$
$$\otimes |\vec{w}\rangle_{\mathsf{Q}} |\{(x_j, y_j), (k||w_j||0^{n-\lambda-m}, z_j)\}_{j \in [t]}\rangle_{\mathsf{E}} |k\rangle_{\mathsf{K}}. \quad (6)$$

Lemma 60. $\left|\Pr_{\mathsf{Hybrid}\ 5}[1 \leftarrow \mathcal{A}^{\mathsf{PR}, \mathcal{O}_{\mathsf{Hyb5}}}] - \Pr_{\mathsf{Hybrid}\ 4}[1 \leftarrow \mathcal{A}^{\mathsf{cfPR}_{\mathsf{ABE}_1}, \mathcal{O}_{\mathsf{Hyb4}}}]\right| = O\left(\sqrt{\frac{t}{2^\lambda}}\right)$.

Proof of Lemma 60. The structure of the proof is similar to that of Theorem 53. We will show that $|\mathcal{A}_{t,t}^{\mathsf{cfPR}, \mathcal{O}_{\mathsf{Hyb4}}}\rangle$ (Equation (5)) and $|\mathcal{A}_{t,t}^{\mathsf{PR}, \mathcal{O}_{\mathsf{Hyb5}}}\rangle$ (Equation (6)) are negligibly close after partially tracing out their purifying registers. Specifically, we will define a projector Π^{good} and isometries V^{part}, $V^{\mathsf{func},\oplus}$, V^{split} and W^{AppK} such that

$$W^{\mathsf{AppK}} |\mathcal{A}_{t,t}^{\mathsf{cfPR}, \mathcal{O}_{\mathsf{Hyb4}}}\rangle \approx V^{\mathsf{split}} \cdot V^{\mathsf{func},\oplus} \cdot V^{\mathsf{part}} \cdot \Pi^{\mathsf{good}} |\mathcal{A}_{t,t}^{\mathsf{PR}, \mathcal{O}_{\mathsf{Hyb5}}}\rangle.$$

We say that a pair of an injective relation and a key $(R, k) \in \mathfrak{R}^{\mathsf{inj}}_{2t} \times \{0,1\}^\lambda$ is *good* if

$$|\{(x, y) \in R : x_{[1:\lambda]} = k\}| = t,$$

where $x_{[1:\lambda]}$ denotes the first λ bits of $x \in \{0,1\}^n$. For any good (R,k), we denote $R_k := \{(x,y) \in R : x_{[1:\lambda]} = k\}$. Define the projector $\Pi^{\mathsf{good}}_{\mathsf{EK}}$ onto the subspace spanned by $\{|R\rangle_{\mathsf{E}}|k\rangle_{\mathsf{K}}\}$ for all good (R,k). Then we have

$$\Pi^{\mathsf{good}}|\mathcal{A}_{t,t}^{\mathsf{PR},\mathcal{O}_{\mathsf{Hyb5}}}\rangle = \sum_{\substack{\vec{x}\in[N]^t,\vec{w}\in[M]^t,\\ (y_1,\ldots,y_t,z_1,\ldots,z_t)\in[N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}}\left(\prod_{i=1}^{t}|w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} A_{2i}|y_i\rangle\langle x_i|_{\mathsf{AB}}A_{2i-1}\right)|0\rangle_{\mathsf{ABC}}|\vec{w}\rangle_{\mathsf{Q}} \otimes \frac{1}{\sqrt{2^\lambda}}\sum_{k\notin\{\vec{x}_{[1:\lambda]}\}}|\{(x_j,y_j),(k||w_j||0^{n-\lambda-m},z_j)\}_{j\in[t]}\rangle_{\mathsf{E}}|k\rangle_{\mathsf{K}}, \quad (7)$$

where $\{\vec{x}_{[1:\lambda]}\}$ denotes the union of the first λ bits of all coordinates of $\vec{x}$, i.e., $\{\vec{x}_{[1:\lambda]}\} := \bigcup_{i\in[t]}\{(x_i)_{[1:\lambda]}\} \subseteq \{0,1\}^\lambda$ for any $\vec{x} = (x_1,\ldots,x_t) \in [N]^t$.

By Lemmas 11 and 13, it is sufficient to show the closeness between Equation (5) and Equation (7) up to isometries. First, we define the following partial isometry on all good (R,k)

$$V^{\mathsf{part}} : |R\rangle_{\mathsf{E}}|k\rangle_{\mathsf{K}} \mapsto |R\setminus R_k\rangle_{\mathsf{E}_1}|R_k\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}}.$$

Then applying V^{part} on Equation (7), we have

$$V^{\mathsf{part}}\Pi^{\mathsf{good}}|\mathcal{A}_{t,t}^{\mathsf{PR},\mathcal{O}_{\mathsf{Hyb5}}}\rangle = \sum_{\substack{\vec{x}\in[N]^t,\vec{w}\in[M]^t,\\ (y_1,\ldots,y_t,z_1,\ldots,z_t)\in[N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}}\left(\prod_{i=1}^{t}|w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i}|y_i\rangle\langle x_i|_{\mathsf{AB}}A_{2i-1}\right)|0\rangle_{\mathsf{ABC}}|\vec{w}\rangle_{\mathsf{Q}} \otimes \frac{1}{\sqrt{2^\lambda}}\sum_{k\notin\{\vec{x}_{[1:\lambda]}\}}|\{(x_j,y_j)\}_{j\in[t]}\rangle_{\mathsf{E}_1} \otimes |\{(k||w_\ell||0^{n-\lambda-m},z_\ell)\}_{\ell\in[t]}\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}}. \quad (8)$$

Next, define a partial isometry isometry $V^{\mathsf{func},\oplus}$ on all $\vec{w} \in [M]^t, \vec{z} \in [N]^t_{\mathrm{dist}}$ and $k \in \{0,1\}^\lambda$ such that

$$V^{\mathsf{func},\oplus} : |\{(k||w_\ell||0^{n-\lambda-m},z_\ell)\}_{\ell\in[t]}\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}} \mapsto |\{(\overline{w_\ell},z_\ell)\}_{\ell\in[t]}\rangle_{\mathsf{E}_2}|k\rangle_{\mathsf{K}}.$$

Applying $V^{\mathsf{func},\oplus}$ to Equation (8) to uncompute k from each $k||w_\ell||0^{n-\lambda-m}$ on register E_2, we have

$$V^{\mathsf{func},\oplus}V^{\mathsf{part}}\Pi^{\mathsf{good}}|\mathcal{A}_{t,t}^{\mathsf{PR},\mathcal{O}_{\mathsf{Hyb5}}}\rangle = \sum_{\substack{\vec{x}\in[N]^t,\vec{w}\in[M]^t,\\ (y_1,\ldots,y_t,z_1,\ldots,z_t)\in[N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}}\left(\prod_{i=1}^{t}|w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i}|y_i\rangle\langle x_i|_{\mathsf{AB}}A_{2i-1}\right)|0\rangle_{\mathsf{ABC}} \otimes |\vec{w}\rangle_{\mathsf{Q}}|\{(x_j,y_j)\}_{j\in[t]}\rangle_{\mathsf{E}_1}|\{(\overline{w_\ell},z_\ell)\}_{\ell\in[t]}\rangle_{\mathsf{E}_2} \otimes \frac{1}{\sqrt{2^\lambda}}\sum_{k\notin\{\vec{x}_{[1:\lambda]}\}}|k\rangle_{\mathsf{K}}. \quad (9)$$

Define a partial isometry V^{split} defined on all $\vec{w} \in [M]^t$ and $\vec{z} \in [N]^t_{\mathrm{dist}}$ such that

$$V^{\mathsf{split}} : |\{(\overline{w_i},z_i)\}_{i\in[t]}\rangle_{\mathsf{E}_2} \mapsto \bigotimes_{w'\in\{0,1\}^m}|\{(\overline{w}_i,z_i) : w_i = w'\}\rangle_{\mathsf{E}_2^{w'}}.$$

Applying V^{split} to Equation (9), we have the following subnormalized state $|\psi_5\rangle$,

$$|\psi_5\rangle = \sum_{\substack{\vec{x}\in[N]^t,\vec{w}\in[M]^t,\\ (y_1,\ldots,y_t,z_1,\ldots,z_t)\in[N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}}\left(\prod_{i=1}^{t}|w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i}|y_i\rangle\langle x_i|_{\mathsf{AB}}A_{2i-1}\right)|0\rangle_{\mathsf{ABC}}$$

$$\otimes |\vec{w}\rangle_{\mathsf{Q}} |\{(x_j, y_j)\}_{j \in [t]}\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |\{(\overline{w}_i, z_i) : w_i = w'\}\rangle_{\mathsf{E}_2^{w'}} \otimes \frac{1}{\sqrt{2^\lambda}} \sum_{k \notin \{\vec{x}_{[1:\lambda]}\}} |k\rangle_{\mathsf{K}}. \quad (10)$$

Now, we define the following isometry

$$W^{\mathsf{AppK}} : |R\rangle_{\mathsf{E}_1} \mapsto |R\rangle_{\mathsf{E}_1} \otimes \frac{1}{\sqrt{2^\lambda - |\{\vec{x}_{[1:\lambda]}\}|}} \sum_{\substack{k \in \{0,1\}^\lambda : \\ k \notin \{\vec{x}_{[1:\lambda]}\}}} |k\rangle_{\mathsf{K}}.$$

Applying W^{AppK} to Equation (5), we get $|\psi_4\rangle$ as

$$|\psi_4\rangle = \sum_{\substack{\vec{x} \in [N]^t, \vec{w} \in [M]^t, \\ (y_1, \ldots, y_t, z_1, \ldots, z_t) \in [N]^{2t}_{\mathrm{dist}}}} \frac{1}{\sqrt{N^{\downarrow 2t}}} \left(\prod_{i=1}^{t} |w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i} |y_i\rangle\langle x_i|_{\mathsf{AB}} A_{2i-1} \right) |0\rangle_{\mathsf{ABC}}$$
$$\otimes |\vec{w}\rangle_{\mathsf{Q}} |\{(x_j, y_j)\}_{j \in [t]}\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |\{(\overline{w}_i, z_i) : w_i = w'\}\rangle_{\mathsf{E}_2^{w'}} \otimes \frac{1}{\sqrt{2^\lambda - |\{\vec{x}_{[1:\lambda]}\}|}} \sum_{k \notin \{\vec{x}_{[1:\lambda]}\}} |k\rangle_{\mathsf{K}}. \quad (11)$$

Notice that

$$|\psi_5\rangle = \sum_{\substack{\vec{x} \in [N]^t, \vec{w} \in [M]^t, \\ (y_1, \ldots, y_t, z_1, \ldots, z_t) \in [N]^{2t}_{\mathrm{dist}}}} \sqrt{\frac{2^\lambda - |\{\vec{x}_{[1:\lambda]}\}|}{2^\lambda}} \frac{1}{\sqrt{N^{\downarrow 2t}}} \left(\prod_{i=1}^{t} |w_i\rangle\langle w_i|_{\mathsf{A}} \otimes |z_i\rangle_{\mathsf{D}_i} \cdot A_{2i} |y_i\rangle\langle x_i|_{\mathsf{AB}} A_{2i-1} \right) |0\rangle_{\mathsf{ABC}}$$
$$\otimes |\vec{w}\rangle_{\mathsf{Q}} |\{(x_j, y_j)\}_{j \in [t]}\rangle_{\mathsf{E}_1} \bigotimes_{w' \in \{0,1\}^m} |\{(\overline{w}_i, z_i) : w_i = w'\}\rangle_{\mathsf{E}_2^{w'}} \otimes \frac{1}{\sqrt{2^\lambda - |\{\vec{x}_{[1:\lambda]}\}|}} \sum_{k \notin \{\vec{x}_{[1:\lambda]}\}} |k\rangle_{\mathsf{K}}. \quad (12)$$

Since for all $\vec{x} \in [N]^t$,

$$\sqrt{\frac{2^\lambda - |\{\vec{x}_{[1:\lambda]}\}|}{2^\lambda}} \geq \sqrt{\frac{2^\lambda - t}{2^\lambda}},$$

by Lemma 13, the inner product between $|\psi_4\rangle$ and $|\psi_5\rangle$ is at most $\sqrt{1 - t/2^\lambda}$. Hence the required trace distance is at most $O\left(\sqrt{\frac{t}{2^\lambda}}\right)$. □

- Real: The adversary gets access to the Quantum Haar Random Oracle U and $\mathcal{O}_{\mathsf{PRFS}}$.

Lemma 61. $\left|\Pr_{\mathsf{Hybrid}\,5}[1 \leftarrow \mathcal{A}^{\mathsf{PR}, \mathcal{O}_{\mathsf{Hyb5}}}] - \Pr_{\mathsf{Real}}[1 \leftarrow \mathcal{A}^{U, \mathcal{O}_{\mathsf{PRFS}}}]\right| = O\left(\frac{t^2}{2^n}\right)$.

Proof of Lemma 61. This is true by Theorem 22. □

Collecting the probabilities, the distinguishing advantage of $\mathcal{A}$ is at most $O\left(\frac{t^2}{2^{n-m}} + \frac{t^2}{\sqrt{2^n}} + \sqrt{\frac{t}{2^\lambda}}\right)$ as desired. This completes the proof of Theorem 54. □

Acknowledgements

This work is supported by the National Science Foundation under Grant No. 2329938 and Grant No. 2341004. JB is supported by Henry Yuen's AFORS (award FA9550-21-1-036) and NSF CAREER (award CCF2144219). This work was done in part when JB was visiting the Simons Institute for the Theory of Computing, supported by NSF QLCI Grant No. 2016245.

References

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (2019), pp. 505–510 (cit. on p. 3).

[ABF+24] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh V. Vazirani, Chenyi Zhang, and Zixin Zhou. "Quantum Pseudoentanglement". In: *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA*. Ed. by Venkatesan Guruswami. Vol. 287. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, 2:1–2:21. DOI: 10.4230/LIPICS.ITCS.2024.2. URL: https://doi.org/10.4230/LIPIcs.ITCS.2024.2 (cit. on p. 3).

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. "Pseudorandom isometries". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2024, pp. 226–254 (cit. on pp. 3, 7).

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. *Cryptography in the Common Haar State Model: Feasibility Results and Separations*. Cryptology ePrint Archive, Paper 2024/1043. *To appear in TCC 2024*. 2024. URL: https://eprint.iacr.org/2024/1043 (cit. on pp. 8, 11, 12, 33, 34).

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. "Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications". In: *Theory of Cryptography Conference*. Springer. 2022, pp. 237–265 (cit. on pp. 3, 7, 14, 33).

[ALY24] Prabhanjan Ananth, Yao-Ting Lin, and Henry Yuen. "Pseudorandom strings from pseudorandom quantum states". In: *ITCS*. 2024 (cit. on p. 3).

[AMR20] Gorjan Alagic, Christian Majenz, and Alexander Russell. "Efficient simulation of random states and random unitaries". In: *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III 39*. Springer. 2020, pp. 759–787 (cit. on p. 29).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from Pseudorandom Quantum States." In: *CRYPTO*. 2022 (cit. on p. 3).

[BBO+24] Mohammed Barhoush, Amit Behera, Lior Ozer, Louis Salvail, and Or Sattath. *Signatures From Pseudorandom States via ⊥-PRFs*. 2024. arXiv: 2311.00847 [cs.CR]. URL: https://arxiv.org/abs/2311.00847 (cit. on p. 3).

[BBSS23] Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. "Pseudorandomness with Proof of Destruction and Applications". In: *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part IV*. Ed. by Guy N. Rothblum and Hoeteck Wee. Vol. 14372. Lecture Notes in Computer Science. Springer, 2023, pp. 125–154. DOI: 10.1007/978-3-031-48624-1_5. URL: https://doi.org/10.1007/978-3-031-48624-1%5C_5 (cit. on p. 3).

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. "On the Computational Hardness Needed for Quantum Cryptography". In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023*. Schloss Dagstuhl-Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing. 2023, p. 24 (cit. on p. 3).

[BEM+23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. "Unitary complexity and the uhlmann transformation problem". In: *arXiv preprint arXiv:2306.13073* (2023) (cit. on p. 3).

[BFV20] Adam Bouland, Bill Fefferman, and Umesh V. Vazirani. “Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)”. In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*. Ed. by Thomas Vidick. Vol. 151. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 63:1–63:2. DOI: 10.4230/LIPIcs.ITCS.2020.63 (cit. on pp. 3, 4, 6, 8).

[BHH16] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. “Local random quantum circuits are approximate polynomial-designs”. In: *Communications in Mathematical Physics* 346 (2016), pp. 397–434 (cit. on p. 3).

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. “Efficient Quantum Pseudorandomness from Hamiltonian Phase States”. In: *arXiv preprint arXiv:2410.08073* (2024) (cit. on p. 3).

[BJ24] Rishabh Batra and Rahul Jain. “Commitments are equivalent to one-way state generators”. In: *FOCS 2024 (to appear)* (2024). URL: https://arxiv.org/abs/2404.03220 (cit. on p. 3).

[BM24] Zvika Brakerski and Nir Magrafta. “Real-Valued Somewhat-Pseudorandom Unitaries”. In: *TCC 2024 (to appear)* (2024). URL: https://arxiv.org/abs/2403.16704 (cit. on pp. 3, 7).

[BR93] Mihir Bellare and Phillip Rogaway. “Random oracles are practical: A paradigm for designing efficient protocols”. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security*. 1993, pp. 62–73 (cit. on p. 3).

[BS19] Zvika Brakerski and Omri Shmueli. “(Pseudo) Random Quantum States with Binary Phase”. In: *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. Lecture Notes in Computer Science. Springer, 2019, pp. 229–250. DOI: 10.1007/978-3-030-36030-6_10 (cit. on pp. 3, 7).

[BS20] Zvika Brakerski and Omri Shmueli. “Scalable Pseudorandom Quantum States”. In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 417–440. DOI: 10.1007/978-3-030-56880-1_15 (cit. on pp. 3, 7).

[CBB+24] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. “Efficient unitary designs and pseudorandom unitaries from permutations”. In: *arXiv preprint arXiv:2404.16751* (2024) (cit. on p. 7).

[CCS24] Boyang Chen, Andrea Coladangelo, and Or Sattath. “The power of a single Haar random state: constructing and separating quantum pseudorandomness”. In: *arXiv preprint arXiv:2404.03295* (2024) (cit. on pp. 8, 11, 33, 35, 36).

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. “The random oracle methodology, revisited”. In: *Journal of the ACM (JACM)* 51.4 (2004), pp. 557–594 (cit. on p. 3).

[CLS24] Nai-Hui Chia, Daniel Liang, and Fang Song. “Quantum State Learning Implies Circuit Lower Bounds”. In: *arXiv preprint arXiv:2405.10242* (2024) (cit. on p. 3).

[CM24] Lijie Chen and Ramis Movassagh. “Quantum merkle trees”. In: *Quantum* 8 (2024), p. 1380 (cit. on pp. 4, 8).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. “Commitments to quantum states”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1579–1588 (cit. on p. 5).

[Gre20] Matthew Green. *What is the random oracle model and why should you care?* https://blog.cryptographyengineering.com/2020/01/05/what-is-the-random-oracle-model-and-why-should-you-care-part-5/. 2020 (cit. on p. 3).

[Haf22] Jonas Haferkamp. “Random quantum circuits are approximate unitary t-designs in depth $O\left(nt^{5+o(1)}\right)$”. In: *Quantum* 6 (2022), p. 795 (cit. on p. 3).

[Har23] Aram W Harrow. “Approximate orthogonality of permutation operators, with application to quantum information”. In: *Letters in Mathematical Physics* 114.1 (2023), p. 1 (cit. on p. 34).

[HBC+22] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, et al. “Quantum advantage in learning from experiments”. In: *Science* 376.6598 (2022), pp. 1182–1186 (cit. on p. 3).

[HLM17] Aram W Harrow, Cedric Yen-Yu Lin, and Ashley Montanaro. “Sequential measurements, disturbance and property testing”. In: *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM. 2017, pp. 1598–1611 (cit. on p. 36).

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. *A Note on Output Length of One-Way State Generators*. 2023. arXiv: 2312.16025 [quant-ph] (cit. on p. 3).

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. “Pseudorandom Quantum States”. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5 (cit. on pp. 3, 4, 7, 14, 15).

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. “Quantum cryptography in algorithmica”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1589–1602 (cit. on p. 3).

[Kre21] William Kretschmer. “Quantum Pseudorandomness and Classical Complexity”. In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*. Ed. by Min-Hsiu Hsieh. Vol. 197. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 2:1–2:20. DOI: 10.4230/LIPIcs.TQC.2021.2 (cit. on pp. 3, 8, 29).

[KT24a] Dakshita Khurana and Kabir Tomer. “Commitments from quantum one-wayness”. In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. 2024, pp. 968–978 (cit. on p. 3).

[KT24b] Dakshita Khurana and Kabir Tomer. *Founding Quantum Cryptography on Quantum Advantage, or, Towards Cryptography from #P-Hardness*. Cryptology ePrint Archive, Paper 2024/1490. 2024. URL: https://eprint.iacr.org/2024/1490 (cit. on p. 3).

[LQS+23] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. “Quantum pseudorandom scramblers”. In: *TCC 2024 (to appear)* (2023). URL: https://arxiv.org/abs/2309.08941 (cit. on pp. 3, 7).

[MH24] Fermi Ma and Hsin-Yuan Huang. *How to Construct Random Unitaries*. 2024. arXiv: 2410.10116 [quant-ph]. URL: https://arxiv.org/abs/2410.10116 (cit. on pp. 7, 8, 15, 17).

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. “Pseudorandom unitaries with non-adaptive security”. In: *FOCS 2024 (to appear)* (2024). URL: https://arxiv.org/abs/2402.14803 (cit. on pp. 3, 7, 29).

[MY22] Tomoyuki Morimae and Takashi Yamakawa. “Quantum commitments and signatures without one-way functions”. In: *Annual International Cryptology Conference*. Springer. 2022, pp. 269–295 (cit. on p. 3).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667 (cit. on p. 13).

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. “Random unitaries in extremely low depth”. In: *arXiv preprint arXiv:2407.07754* (2024) (cit. on pp. 3, 5, 7, 27–30).

[WB24] Adam Bene Watts and John Bostanci. “Quantum Event Learning and Gentle Random Measurements”. In: *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik. 2024 (cit. on p. 36).

[Wil11] Mark M Wilde. “From classical to quantum Shannon theory”. In: *arXiv preprint arXiv:1106.1445* (2011) (cit. on p. 15).

[Yan22] Jun Yan. “General properties of quantum bit commitments”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2022, pp. 628–657 (cit. on p. 3).

[Zha19] Mark Zhandry. “How to record quantum queries, and applications to quantum indifferentiability”. In: *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*. Springer. 2019, pp. 239–268 (cit. on p. 7).

A Omitted Proofs

A.1 Omitted Proofs in Section 6

Proof of Lemma 25. The total number of constraints imposed by i-fold collision-freeness is $\binom{|S|}{i}\binom{|S|}{i-1}$. Each constraint removes at most $2^{n-\lambda}$ elements from $\mathsf{CF}_{\ell,\lambda}(S)$. Hence the total number of elements not in $\mathsf{CF}_{\ell,\lambda}(S)$ is less than

$$2^{n-\lambda}\cdot\left(\sum_{i=1}^{\ell}\binom{|S|}{i}\binom{|S|}{i-1}\right)\le 2^{n-\lambda}\cdot\left(\sum_{i=1}^{\ell}\left(\frac{e|S|}{i}\right)^{2i}\right)$$
$$\le 2^{n-\lambda}\cdot\left(\sum_{i=1}^{\ell}\left(\frac{e|S|}{\ell}\right)^{2\ell}\right)\le 2^{n-\lambda}\cdot\ell|S|^{2\ell}.$$

□

A.2 Omitted Proofs in Section 7

Proof of Claim 36. Fix $\vec{x}\in[N]^t$, $\vec{y}\in[N]^t_{\text{dist}}$ and $\vec{z}\in([N]\setminus\{\vec{y}\})^\ell_{\text{dist}}$. Let for any $k\in\{0,1\}^n$,

$$R_k:=\{(x_i,z_i)\}_{i\in\mathbf{a}}\uplus\{(z_i\oplus k,y_i)\}_{i\in\mathbf{a}}\uplus\{(x_i,y_i)\}_{i\in\mathbf{b}}.$$

Then, we want to show that

$$\sum_{k\in\{0,1\}^n}\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}=\sum_{k\in\{0,1\}^n\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}$$

We show this in 3 parts,

1. If $k\in\{\vec{x}\}\oplus\{\vec{y}\}$, then $\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}=0$.
2. If $k\in\{\vec{x}\}\oplus\{\vec{z}\}$, then $\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}=0$.
3. If $k\in\{0,1\}^n\setminus(\{\vec{x}\}\oplus\{\vec{y}\})\cup(\{\vec{x}\}\oplus\{\vec{z}\})$, then $\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}=|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}$.

Claim 62. *If $k\in\{\vec{x}\}\oplus\{\vec{y}\}$, then $\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}}|R_k\rangle_{\mathsf{E}_1}|k\rangle_{\mathsf{K}}=0$.*

Proof. Let $k=y_{j_1}\oplus x_{j_2}$ for some $j_1,j_2\in[t]$, then we can divide this into the following cases:

- Let $j_1, j_2 \in \mathbf{a}$, then

  $$\{((x_i, z_i), (z_i \oplus k, y_i))\}_{i\in\mathbf{a}} \cup \{((z_{j_1} \oplus k, y_{j_1}), (x_{j_2}, z_{j_2}))\} \subseteq \mathrm{CorX}(R_k, k),$$

  hence $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.
- Let $j_1 \in \mathbf{a}, j_2 \in \mathbf{b}$, then

  $$\{((x_i, z_i), (z_i \oplus k, y_i))\}_{i\in\mathbf{a}} \cup \{((z_{j_1} \oplus k, y_{j_1}), (x_{j_2}, y_{j_2}))\} \subseteq \mathrm{CorX}(R_k, k),$$

  hence $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.
- Let $j_1 \in \mathbf{a}, j_2 \in \mathbf{b}$, then symmetric to the above case $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.
- Let $j_1, j_2 \in \mathbf{b}$, then

  $$\{((x_i, z_i), (z_i \oplus k, y_i))\}_{i\in\mathbf{a}} \cup \{((x_{j_1}, y_{j_1}), (x_{j_2}, y_{j_2}))\} \subseteq \mathrm{CorX}(R_k, k),$$

  hence $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.

□

Claim 63. *If $k \in \{\vec{x}\} \oplus \{\vec{z}\}$, then $\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}} |R_k\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}} = 0$.*

Proof. Let $k = z_{j_1} \oplus x_{j_2}$ for some $j_2 \in [t], j_1 \in \mathbf{a}$, then we can divide this into the following cases:

- Let $j_1, j_2 \in \mathbf{a}$, then

  $$\{((x_i, z_i), (z_i \oplus k, y_i))\}_{i\in\mathbf{a}} \cup \{((x_{j_1}, z_{j_1}), (x_{j_2}, z_{j_2}))\} \subseteq \mathrm{CorX}(R_k, k),$$

  hence $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.
- Let $j_1 \in \mathbf{a}, j_2 \in \mathbf{b}$, then

  $$\{((x_i, z_i), (z_i \oplus k, y_i))\}_{i\in\mathbf{a}} \cup \{((x_{j_1} \oplus k, z_{j_1}), (x_{j_2}, y_{j_2}))\} \subseteq \mathrm{CorX}(R_k, k),$$

  hence $|\mathrm{CorX}(R_k, k)| \geq \ell + 1$.

□

Claim 64. *If $k \in \{0,1\}^n \setminus (\{\vec{x}\} \oplus \{\vec{y}\}) \cup (\{\vec{x}\} \oplus \{\vec{z}\})$, then*

$$\Pi^{\text{good}}_{\mathsf{E}_1\mathsf{K}} |R_k\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}} = |R_k\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}.$$

Proof. We complete the proof by a case analysis. For any $(p_0, p_1) \in R_k \times R_k$, there are 9 cases depending on the sets which p_0 and p_1 respectively belong to (see Table 1).

$p_1 \in$ p_0 $\in$	$\{(x_j, z_j)\}_{j\in\mathbf{a}}$	$\{(z_j \oplus k, y_j)\}_{j\in\mathbf{a}}$	$\{(x_j, y_j)\}_{j\in\mathbf{b}}$
$\{(x_i, z_i)\}_{i\in\mathbf{a}}$	$E_1 := \{z_i\}_{i\in\mathbf{a}} \oplus \{x_j\}_{j\in\mathbf{a}}$	$E_2 := \{z_i\}_{i\in\mathbf{a}} \oplus \{z_j \oplus k\}_{j\in\mathbf{a}}$	$E_3 := \{z_i\}_{i\in\mathbf{a}} \oplus \{x_j\}_{j\in\mathbf{b}}$
$\{(z_i \oplus k, y_i)\}_{i\in\mathbf{a}}$	$E_4 := \{y_i\}_{i\in\mathbf{a}} \oplus \{x_j\}_{j\in\mathbf{a}}$	$E_5 := \{y_i\}_{i\in\mathbf{a}} \oplus \{z_j \oplus k\}_{j\in\mathbf{a}}$	$E_6 := \{y_i\}_{i\in\mathbf{a}} \oplus \{x_j\}_{j\in\mathbf{b}}$
$\{(x_i, y_i)\}_{i\in\mathbf{b}}$	$E_7 := \{y_i\}_{i\in\mathbf{b}} \oplus \{x_j\}_{j\in\mathbf{a}}$	$E_8 := \{y_i\}_{i\in\mathbf{b}} \oplus \{z_j \oplus k\}_{j\in\mathbf{a}}$	$E_9 := \{y_i\}_{i\in\mathbf{b}} \oplus \{x_j\}_{j\in\mathbf{b}}$

Table 1: Cases analysis for (p_0, p_1).

We will show that $|E_2| = \ell$ and $|E_i| = 0$ for $i \neq 2$.

- Since $\vec{z}$ has pairwise distinct coordinates, $z_i \oplus (z_j \oplus k) = k$ if and only if $i = j$. Hence, $|E_2| = |\mathbf{a}| = \ell$.
- Since $k \notin \{\vec{x}\} \oplus \{\vec{y}\}$, then $E_4 = E_6 = E_7 = E_9 = \{\}$.
- Since $k \notin \{\vec{x}\} \oplus \{\vec{z}\}$, then $E_1 = E_3 = \{\}$.
- Since for any $i \in [t], j \in \mathbf{a}$, $y_i \neq z_j$, $y_i \oplus z_j \oplus k \neq k$, hence $E_2 = E_5 = \{\}$.

As a result, we have $|\mathrm{CorX}(R_k, k)| = \sum_{i=1}^{9} |E_i| = \ell$. □

Combining the above claims completes the proof of Claim 36. □