Unclonable Encryption in the Haar Random Oracle Model

James Bartusek* Eli Goldin†

Abstract

We construct unclonable encryption (UE) in the Haar random oracle model, where all parties have query access to $U, U^\dagger, U^*, U^T$ for a Haar random unitary U. Our scheme satisfies the standard notion of unclonable indistinguishability security, supports reuse of the secret key, and can encrypt arbitrary-length messages. That is, we give the first evidence that (reusable) UE, which requires computational assumptions, exists in "microcrypt", a world where one-way functions may not exist.

As one of our central technical contributions, we build on the recently introduced path recording framework to prove a natural "unitary reprogramming lemma", which may be of independent interest.

1 Introduction

Unclonable encryption (UE), introduced by Broadbent and Lord [BL20], is a central primitive of study in quantum cryptography, both due to its potential real-world impact, say, to protect against "store-now, decrypt-later" attacks, and due to a plethora of open questions that remain about its feasibility.

An unclonable encryption scheme encodes a message m into a quantum ciphertext $\rho_{k,m}$ under secret key k with the following security guarantee. For any pair of messages m_0, m_1 and $b \leftarrow \{0,1\}$, no adversary can map ρ_{k,m_b} to a state on two registers $\mathbf{A}, \mathbf{B}$ such that b can be recovered given either register along with the key k. To be precise, the standard security definition, termed "unclonable indistinguishability" by [BL20], requires that for any cloning adversary,

$$\Pr[b_A = b_B = b] \leq \frac{1}{2} + \mathsf{negl}(\lambda),$$

where b_A (resp. b_B) is the guess made given key k and register $\mathbf{A}$ (resp. $\mathbf{B}$). We note that while several works have also considered the weaker notion of "search security", which bounds the probability that the adversary can guess an entropic message, our focus in this work is on the above notion of unclonable indistinguishability.

As in plain (private-key) encryption, one can consider two main variants: "one-time" UE, where each key is only used to encrypt a single message, and "reusable" (or many-time) UE, where a single private key can be used to encrypt any number of messages. While one-time UE is plausibly an information-theoretic object, reusable UE requires computational assumptions (as it implies reusable plain private-key encryption).

*Columbia University

†New York University. Supported by an NSF graduate research fellowship.

Surprisingly, several questions remain open about the feasibility of both one-time and reusable UE, even given the recent surge of activity in the field of unclonable cryptography. In the one-time setting, [BL20] presented a candidate construction in the random oracle model, and variants of this basic scheme were later shown secure [AKL+22, AKL23]. Unfortunately, these proofs rely heavily on the random oracle, despite the fact that cryptographic assumptions are not even believed to be necessary. Indeed, information-theoretic candidates have also been proposed (e.g. [BBC+24, CLX26, BC26]), with various partial results given about their security. For instance, [BC26] proves that one-time UE exists information-theoretically with advantage bound $\widetilde{O}(1/\lambda)$.

While there has been less explicit study of the reusable variant, it is straightforward to modify the constructions of [AKL+22, AKL23] to yield reusable UE in the random oracle model. As mentioned earlier, while reusable UE *does* require computational assumptions (partially explaining the use of the random oracle), it is natural to wonder just how much cryptographic structure is required to build reusable UE. The goal of this work is to make progress on this question.

Minicrypt vs microcrypt. As the constructions of [AKL+22, AKL23] utilize a random oracle, they at the very least require the existence of one-way functions. This places (reusable) UE in the realm of "minicrypt", i.e. primitives that have (potentially heuristic) constructions from unstructured but classical forms of cryptographic hardness. The minimal form of such classical unstructured hardness is a one-way function.

However, the following question has been left unresolved: Does (reusable) UE *require* one-way functions?[1] It may be instructive to contrast this situation with what is known about *plain* (private-key) encryption and (private-key) quantum money. In fact, plain encryption can be built from pseudo-random unitaries [AQY22], and quantum money can be built from pseudo-random states [JLS18], both of which may exist even if one-way functions do not [Kre21, KQST23, KQT25].

That is, both live in the realm of "microcrypt", i.e. primitives that have (potentially heuristic) constructions from unstructured *quantum* forms of cryptographic hardness. Just as one may consider any primitive with a construction in the random oracle model to live in minicrypt, one may also consider any primitive with a construction in the *Haar* random oracle model to live in microcrypt. In this model, a random unitary U is sampled from the Haar distribution at the beginning of time, and all parties get query access to $U, U^\dagger, U^*$, and U^T. Indeed, any construction in the Haar random oracle model can be heuristically instantiated by replacing the Haar random oracle with a concrete (say, randomly sampled) quantum circuit, analogously to how random oracle constructions have heuristic instantiations from concrete cryptographic hash functions. This definition of microcrypt is robust, a series of recent works have shown that pseudo-random unitaries (and all derivatives, such as pseudo-random states, plain encryption, and quantum money) can be constructed in the Haar random oracle model [HY26, ABGL25b, ABGL25a].

Now, unclonable encryption can be seen as a natural simultaneous strengthening of both plain encryption and quantum money. Indeed, it requires both the hiding properties of plain encryption and unclonable properties of quantum money. Thus, it is natural to ask whether unclonable encryption can also be placed in microcrypt.

[1] A recent work [PRV26] has considered a similar question in the context of *search-secure* unclonable encryption. We provide a detailed comparison with their work in Section 1.4.

1.1 Results

We show that unclonable encryption is indeed a microcrypt primitive, establishing the following main theorem.

Theorem 1.1 (Informal)**.** *For any polynomial message size, there exists a reusable unclonable encryption scheme with unclonable indistinguishability in the Haar random oracle model.*

Following the techniques of [Kre21], it is then straightforward to show

Corollary 1.2. *There exists an oracle $\mathcal{O}$ relative to which*

1. *Reusable unclonable encryption with unclonable indistinguishability exists relative to $\mathcal{O}$.*
2. *$BQP^{\mathcal{O}} = QMA^{\mathcal{O}}$, and so one-way functions do not exist relative to $\mathcal{O}$.*

In fact, we exhibit a general compiler, from which our main theorem can be derived by plugging in the schemes of [AKL+22, AKL23] proven secure in the quantum random oracle model.

Theorem 1.3 (Informal)**.** *If reusable unclonable encryption exists with respect to* any *distribution over unitary oracles,*[2] *then it exists in the Haar random oracle model.*

Note that the random oracle (consisting of a random classical function) can be seen as one particular distribution over unitary oracles, and so the above theorem applies.

Along the way, we prove the following technical lemma, which may be of independent interest. Let $\mathcal{H}([N])$ be a Hilbert space spanned by $\{|i\rangle\}_{i\in[N]}$, and suppose that $S_2 \subset [N]$ is sampled at random conditioned on containing some set of fixed points S_1, where $\frac{|S_2|}{N}, \frac{|S_1|}{|S_2|} = \mathsf{negl}(\lambda)$.

Lemma 1.4 (Informal: Unitary reprogramming lemma)**.** *No adversary has better than $\mathsf{negl}(\lambda)$ advantage in distinguishing whether they are querying a "monolithic" Haar random oracle U on the entire space $\mathcal{H}([N])$ or a product U_1U_2 of two "disjoint" Haar random oracles, where U_1 is on $\mathcal{H}(S_2)$ and U_2 is on $\mathcal{H}([N] \setminus S_2)$.*

Although S_1 and S_2 are described here as subsets, the proof of this lemma is not sensitive to the basis chosen. Thus, the same lemma holds where S_1 is some fixed subspace of $\mathcal{H}([N])$ and S_2 is a random subspace containing S_1 as long as $\frac{\dim(S_2)}{N}, \frac{\dim(S_1)}{\dim(S_2)} = \mathsf{negl}(\lambda)$.

1.2 Techniques

Construction. We begin with our construction of unclonable encryption in the Haar random oracle model. Let U be the Haar random unitary, k be a classical key, and suppose that we wish to encrypt a message $m \in \{0,1\}^\ell$ (of some fixed length). To do so, the encryptor samples some randomness $r \leftarrow \{0,1\}^n$ and outputs

$$X^k U |m, r\rangle ,$$

where X^k is the operation that applies a bit flip to qubit i if $k_i = 1$. We can think of U (which is publicly-queryable) as defining a partitioning of Hilbert space into one subspace $\{U|m, r\rangle\}_r$ for each choice of m. Then, X^k defines a random "shift" of these subspaces so that they are not accessible to the cloning adversary (who does not know k). An encryption of m is thus a shifted sample from the m'th subspace.

[2] Technically, we need the scheme to satisfy a mild structural property which we call "pure" (see Definition 4.3).

Security game. Our goal is then to show that if there exists an unclonable encryption scheme in *any* oracle model (with some minor restrictions on the format of the construction), then the above scheme is secure. We do so via a strategy akin to a random self-reduction. In order to explain the reduction, we first set up some more notation.

The adversary in the unclonable encryption game is specified by a cloner C and two distinguishers A and B. The security game proceeds as follows, where all adversaries have access to a Haar random U via $U, U^\dagger, U^*, U^T$ queries.

- The encryption key k is sampled and C obtains access to an encryption oracle $\mathrm{Enc}(k, \cdot)$ which they can query any number of times to get sample encryptions under key k.
- C outputs a pair of challenge messages m_0, m_1, and receives $|\psi\rangle = X^k U |m_b, r\rangle$ for a random choice of $b \leftarrow \{0,1\}$ and $r \leftarrow \{0,1\}^n$.
- C continues to have access to $\mathrm{Enc}(k, \cdot)$, and eventually outputs a state on two registers $\mathbf{A}, \mathbf{B}$.
- Run $b_A \leftarrow \mathsf{A}(k, \mathbf{A})$ and $b_B \leftarrow \mathsf{B}(k, \mathbf{B})$.
- The adversary wins if $b = b_A = b_B$.

We refer to the operation of C in the above game as the *cloning phase*, and operations of A, B as the *distinguishing phase*.

Now, suppose we are given an unclonable encryption scheme that has been proven secure in 7some other oracle model (meaning that no adversary has better than $1/2 + \mathsf{negl}(\lambda)$ advantage). We demand that the encryption procedure for this scheme can be written as

$$E_{\widetilde{k}}^{\widetilde{U}} |m, \widetilde{r}\rangle ,$$

where $E_{\widetilde{k}}$ is some oracle-aided unitary ($\widetilde{U}$ being the oracle) and $\widetilde{r}$ is some classical random string.[3] We will exhibit a reduction showing that any adversary against our Haar random oracle scheme can be used to break this scheme.

The reduction. The main idea is to "absorb" the description of the unitary $E_{\widetilde{k}}^{\widetilde{U}}$ into U so that the reduction can essentially re-encrypt its challenge ciphertexts encrypted under $E_{\widetilde{k}}^{\widetilde{U}}$ by additionally applying $X^k U$. In particular, we will set parameters so that n (the size of the random string r in our scheme) is twice the size of $\widetilde{r}$, and consider the encryption scheme that samples $\widetilde{r}, s \in \{0,1\}^{n/2}$ and outputs

$$X^k U E_{\widetilde{k}}^{\widetilde{U}} |m, \widetilde{r}\rangle |s\rangle .$$

The reduction can then absorb the description of $E_{\widetilde{k}}^{\widetilde{U}}$ into U, giving the adversary access to $U E_{\widetilde{k}}^{\widetilde{U}}$ rather than U, which is identically distributed due to the fact that U is Haar random.

This same approach was successfully applied in [PRV26] to analyze unclonable encryption in their variant of the Haar random oracle model, where the cloner does not receive access to the Haar random unitary. In this setting, [PRV26] showed that even without X^k and r, encryptions $U |m\rangle$

[3] In fact, we also allow the encryption unitary to operate on some auxiliary 0 qubits, but still demand that the output is pure (given m and $\widetilde{r}$). That is, the scheme does not trace out any part of the encryption unitary's output.

have inverse exponential unclonable search security. However, this idea does *not* work if the cloner is allowed query access to U (as in our setting), since the reduction does not receive the description of $\widetilde{k}$ until *after* the cloning phase.

To address this inconsistency, we sample a random subset $R \subset \{0,1\}^{n/2}$ of size, say, $2^{n/4}$, and consider splitting $\mathcal{H}(\{0,1\}^{\ell+n})$ (the Hilbert space acted upon by U) into the following subspaces:[4]

$$S_2 \coloneqq \mathsf{Span}\{|m, \widetilde{r}, s\rangle\}_{s\in R}, \quad S_2^{\perp} \coloneqq \mathsf{Span}\{|m, \widetilde{r}, s\rangle\}_{s\notin R}.$$

Now, we define the unitary queried by the adversary to be the product of two unitaries U_1U_2, where U_1 applies $UE_{\widetilde{k}}^{\widetilde{U}}$ to S_2 (and acts as the identity on $S_2^{\perp}$), and U_2 applies U to $S_2^{\perp}$ (and acts as the identity on S_2). Then, whenever the adversary makes an encryption query, we sample $s \leftarrow R$ to use as the random coins. This takes care of our issue due to the following observations.

- Since all of the adversary's ciphertexts are masked by X^k, they shouldn't learn anything about R, and therefore will not be able to query inside the subspace S_2 during the cloning phase. While intuitive, establishing this formally takes some care, which we do via a sequence of hybrids in Appendix A of the full version.
- Hence, the reduction can simulate the adversary's unitary using *only* U_2 during the cloning phase, and then U_1U_2 during the distinguishing phase, once it knows $E_{\widetilde{k}}^{\widetilde{U}}$.

The unitary reprogramming lemma. While defining the adversary's unitary as $U = U_1U_2$ allows us to get the reduction to go through, we have now actually changed the distribution over oracles that the adversary sees. A key hybrid in our proof establishes that the adversary will not be able to distinguish this change in distribution.

In more detail, we abstract the setting as follows. Let $\mathcal{H}([N])$ be a Hilbert space spanned by $\{|i\rangle\}_{i\in[N]}$, and let $S_1 \subset [N]$ be some set of public fixed points. S_1 will correspond to the set of random strings s used to respond to the adversary's encryption queries, which must be known to the reduction. Suppose that we sample a subset S_2 of some fixed size uniformly at random such that $S_1 \subset S_2 \subset [N]$. This larger set corresponds to the S_2 in the reduction described above. Then, as long as $\frac{|S_2|}{N} = \mathsf{negl}(\lambda)$ and $\frac{|S_1|}{|S_2|} = \mathsf{negl}(\lambda)$, we can show that no adversary has better than $\mathsf{negl}(\lambda)$ advantage in distinguishing the following cases.

- Sample $U \leftarrow \mathsf{Haar}([N])$ and give query access to $U, U^{\dagger}, U^*, U^T$.
- Sample $U_1 \leftarrow \mathsf{Haar}(S_2)$ and $U_2 \leftarrow \mathsf{Haar}([N] \setminus S_2)$ and give query access to $(U_1U_2), (U_1U_2)^{\dagger}$, $(U_1U_2)^*, (U_1U_2)^T$.

Path recording and proof intuition for unitary reprogramming To show this, we build on the recently introduced path recording framework [MH25, SML+25]. For the purpose of exposition, we will discuss the case where adversaries only have forward access to U or U_1U_2.

In the path recording framework, oracle queries to a Haar random unitary $U \leftarrow Haar([N])$ can be efficiently simulated by making queries to the partial isometry V operating on some internal

[4]To simplify the proof, we actually use a slightly different definition of S_2, though the definition here still conveys the basic intuition.

state $|D\rangle$ where $D \subseteq [N] \times [N]$ is an injective relation (i.e. if $D = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, the y_i's are all unique). V acts as follows:

$$V |x\rangle |D\rangle \propto \sum_{y \in [N] \setminus \mathrm{Im}(D)} |y\rangle |D \cup \{(x, y)\}\rangle .$$

Generalizing this, we can simulate queries to $U_1 U_2$ by the following map V^{S_2} defined by

1. On input $|x\rangle |D_1\rangle |D_2\rangle$ for $x \in S_2$,

$$V^{S_2} |x\rangle |D_1\rangle |D_2\rangle \propto \sum_{y \in S_2 \setminus \mathrm{Im}(D_1)} |y\rangle |D_1 \cup \{(x, y)\}\rangle |D_2\rangle .$$

2. On input $|x\rangle |D_1\rangle |D_2\rangle$ for $x \notin S_2$,

$$V^{S_2} |x\rangle |D_1\rangle |D_2\rangle \propto \sum_{y \in [N] \setminus (S_2 \cup \mathrm{Im}(D_2))} |y\rangle |D_1\rangle |D_2 \cup \{(x, y)\}\rangle .$$

We then look at the purification of this process, where we begin with the state

$$\sum_{\substack{S_1 \subseteq S_2 \\ |S_2| = M_2}} |S_2\rangle$$

stored in an ancilla register, and then apply V^{S_2} controlled on this register.

It turns out that as long as only polynomially many queries are made, the state stored in this ancilla register will always be approximately determined by the register containing D_1. In particular, the internal state of the oracle will always be close to a mixture of superpositions of states of the form

$$|D_1\rangle |D_2\rangle \sum_{\substack{S_1 \cup \mathrm{Im}(D_1) \subseteq S_2 \\ |S_2| = M_2}} |S_2\rangle .$$

Here, $S_1 \cup \mathrm{Im}(D_1)$ represents the strings the adversary is able to find in S_2. In particular, these are the strings which are either contained in S_1, or returned to the adversary from queries on strings it already knew were in S_2 (and thus are stored in D_1).

Simple algebra shows that applying the purified V^{S_2} oracle to a state of this form will result in a superposition of states of this form. When $x \notin \mathrm{Im}(D_1) \cup S_1$, this process results in some negligible error corresponding to the event that x happens to lie in S_2. The fact that the same holds for inverse, transpose, and conjugate queries follows from a direct combinatorial bound.

Thus, since the S_2 register is always determined information-theoretically by the D_1 register, we can delete it with no consequences. Doing so properly will show that query access to $U_1 U_2$ as determined by the process above is indistinguishable from query access to $\widetilde{V}$ defined by

1. On input $|x\rangle |D_1\rangle |D_2\rangle$ for $x \in \mathrm{Im}(D_1) \cup S_1$,

$$\widetilde{V} |x\rangle |D_1\rangle |D_2\rangle \propto \sum_{y \in [N] \setminus (\mathrm{Im}(D_1) \cup S_1)} |y\rangle |D_1 \cup \{(x, y)\}\rangle |D_2\rangle .$$

2. On input $|x\rangle |D_1\rangle |D_2\rangle$ for $x \notin \mathrm{Im}(D_1) \cup S_1$,

$$\widetilde{V} |x\rangle |D_1\rangle |D_2\rangle \propto \sum_{y \in N \setminus (\mathrm{Im}(D_1) \cup S_1 \cup \mathrm{Im}(D_2))} |x\rangle |D_1\rangle |D_2 \cup \{(x,y)\}\rangle .$$

At this point, standard techniques can be used to show that this is equivalent to the original path recording oracle V corresponding to a single random unitary U. In particular, there is an isometry T which takes an internal state $|D\rangle$ of V and turns it into an internal state consistent with $\widetilde{V}$, and since this isometry acts only on the internal state, queries to V and $\widetilde{V}$ are indistinguishable. In slightly more detail, T will look at the relations in D and partition them between D_1 and D_2 as follows: for $(x,y) \in D$, if there is some path $(x_1,y_1),(x_2,y_2)\ldots,(x_t,y_t) \in D$ such that

1. $(x_y, x_{t+1}) = (x,y)$
2. $x_1 \in S_1$
3. $x_i = y_{i-1}$

then T will add (x,y) to D_1. Otherwise, it will add (x,y) to D_2.

1.3 Concurrent and independent work

A recent preprint [BBC26] studies the question of information-theoretic one-time secure UE for single-bit messages. They propose a construction based on Haar random unitaries and claim negligible security, improving on the inverse-polynomial security of [BC26]. The secret key in their scheme includes the description of a Haar random unitary that is applied to the message bit concatenated with a random string. Hence, their proposed construction is not efficient, and they leave open the question of information-theoretic one-time UE with efficient encryption and decryption.

1.4 Other related work

Unclonable encryption and microcrypt. To the best of our knowledge, [PRV26] is the only other work that has explicitly considered the question of whether unclonable encryption lies in microcrypt. However, their result is weaker than ours in the following respects:

- They consider *search-secure* unclonable encryption, which, as mentioned earlier, is weaker than the standard notion of unclonable indistinguishability.
- They prove that search-secure unclonable encryption exists in a non-standard variant of the Haar random oracle model where there exists an *exponentially large family* $\{U_i\}_{i\in[2^\lambda]}$ of Haar random oracles for each security parameter. Moreover, the adversary is not given access to these oracles during the cloning phase, and is only given access to $U_i, U_i^\dagger$ for a single choice of i in the distinguishing phase.
- They do not consider *reusable* security, and only allow the adversary to see a single ciphertext per key. Like us, they do allow the message size to be bigger than the key size, which means their notion is indeed computational.

We also mention that they write down a search to decision reduction for a general class of "oracular cloning games" establishing that Haar random oracles are the hardest type of oracles for such games. Conceptually, this is similar to the compiler we analyze in this work for building UE in the Haar random oracle model. However, a crucial distinction is that in their setting, the adversary does not get access to the oracle in the cloning phase, which introduces significant complications in our setting.

Cryptography in the Haar random oracle model. The works of [ABGL25b, ABGL25a] construct pseudorandom unitaries in the Haar random oracle model by interleaving queries to U by applications of X^k. Our construction of unclonable encryption is inspired by this, although it turns out that in our setting a simplified construction using only one query to U is sufficient. Moreover, our proof structure is radically different.

Unitary reprogramming. [HY26] also establishes a lemma that they call a "unitary reprogramming lemma" (a similar lemma, under the name "one-way to hiding for unitary oracles", appears in [ÇGR24]). Intuitively, their lemma states that for any oracle, if there is a subspace for which it is difficult to find a member state, then the oracle is indistinguishable from the same oracle precomposed with an arbitrary unitary acting on that subspace. This is essentially a generalization of the one-way to hiding lemma from [BBBV97]. Our reprogramming lemma is unrelated to this: we show that a Haar random unitary is indistinguishable from the direct sum of two Haar random unitaries on random subspaces, even if a large portion of the subspaces are revealed.

One of the key challenges in our work (which we use our new unitary reprogramming lemma to solve) is to show that the cloner cannot query its oracle on the subspace corresponding to encryptions under the correct key (S_2). However, since the cloner does get some information about S_2 in the form of valid ciphertexts, it may be possible for them to find member states of the relevant subspace, and thus we cannot immediately apply a unitary version of one-way to hiding. Instead, we use our unitary reprogramming oracle to isolate the information the adversary can obtain about the encryption subspace, after which we later apply one-way to hiding style techniques (see Appendix A).

More generally, our new reprogramming lemma is very similar to techniques used in reprogramming for random *permutations* in the classical setting. This is quite different from a generalization of one-way to hiding as seen in [HY26], and the two techniques can be applied in conjunction (as we do here).

1.5 Paper structure

We begin with preliminaries in Section 2. We then prove the "unitary reprogramming lemma" described earlier in Section 3. In Section 4, we give a formal proof of Theorem 1.3. Finally, in Section 5, we conclude the argument by showing that existing constructions of unclonable encryption in the QROM can be modified to achieve many-time security with a pure construction, thus establishing our main result.

2 Preliminaries

2.1 Notation

We will use n to refer to the security parameter. For a variable X, ℓ_X will generally denote some polynomial in n where $\{0,1\}^{\ell_X(n)}$ will correspond to the domain of X. When the security parameter is clear from context, we will omit it.

X will denote Pauli X. For $k \in \{0,1\}^{\ell_k(n)}$, when the ambient space is clear from context, X^k will refer to the map $X^{k_1} \otimes \cdots \otimes X^{k_{\ell_k}} \otimes I$.

For S a set, we will define $\mathcal{H}(S)$ to be the Hilbert space with basis vectors $|s\rangle$ for $s \in S$. A register is a named Hilbert space, and will be represented by a bolded string, for example $\mathbf{A}$. For a set S, $Haar(S), HaarSt(S)$ will refer to the Haar distribution over unitaries and states respectively on $\mathcal{H}(S)$. When there is an implicit larger ambient space $\mathcal{H}(T)$ for $S \subseteq T$, $Haar(S)$ will refer to $Haar(S) \oplus I_{\mathcal{H}(T \setminus S)}$.

For a set T and a natural number M, we define $\binom{T}{M} = \{S \subseteq T : |S| = M\}$. We define $\mathcal{P}(T) = \{S \subseteq T\} = \bigcup_{i=0}^{|T|} \binom{T}{i}$ to be the powerset of T.

2.2 Oracle algorithms

Definition 2.1. *An oracle $\mathcal{O}$ is an arbitrary linear map with input registers $\mathbf{In}$ and $\mathbf{St}$ and output registers $\mathbf{Out}$ and $\mathbf{St}$ along with an initial state $|\phi_0\rangle$ in $\mathbf{St}$. An oracle algorithm $\mathcal{A}^{(\cdot)} = (\mathcal{A}_1, \ldots, \mathcal{A}_t)$ is a sequence of CPTP maps with input $\mathbf{A}, \mathbf{Out}$ and output $\mathbf{A}, \mathbf{In}$. We define the (mixed) state $\mathcal{A}^{\mathcal{O}}(|\psi_0\rangle_{\mathbf{A},\mathbf{Out},\mathbf{St}})$ to be the state*

$$\mathcal{A}^{\mathcal{O}}(|\psi_0\rangle_{A,St}) = (\mathcal{A}_t \cdot \mathcal{O} \cdot \mathcal{A}_{t-1} \cdot \mathcal{O} \cdot \mathcal{A}_{t-2} \cdots \mathcal{O} \cdot \mathcal{A}_1) \left(|\psi_0\rangle\langle\psi_0|_{\mathbf{A},\mathbf{Out}} \otimes |\phi_0\rangle\langle\phi_0|_{\mathbf{St}} \right)$$

We will also define oracle algorithms with access to multiple oracles, possibly interacting on the same internal state $\mathbf{St}$. In this case, we will arbitrarily sequence the queries made to the oracles. In particular, we define

$$\mathcal{A}^{\mathcal{O}_1,\ldots,\mathcal{O}_s}(|\psi_0\rangle) = (\mathcal{A}_t \cdots \mathcal{O}_1 \cdot \mathcal{A}_{s+1} \cdot \mathcal{O}_s \cdot \mathcal{A}_s \cdots \mathcal{O}_2 \cdot \mathcal{A}_2 \cdot \mathcal{O}_1 \cdot \mathcal{A}_1) \left(|\psi_0\rangle\langle\psi_0|_{\mathbf{A},\mathbf{Out}} \otimes |\phi_0\rangle\langle\phi_0|_{\mathbf{St}} \right)$$

For V a partial isometry, we will denote $\mathcal{A}^V = \mathcal{A}^{V(\cdot)V^\dagger}$. We will frequently denote $\vec{V} = (V, V^\dagger, V^*, V^T)$ and likewise $\mathcal{A}^{\vec{V}} = \mathcal{A}^{(V(\cdot)V^\dagger, V^\dagger(\cdot)V, V^*(\cdot)V^T, V^T(\cdot)V^*)}$.

Definition 2.2. *A unitary oracle ensemble $\mathcal{U} = \{\mathcal{U}_n\}_{n\in\mathbb{N}}$ is a family of distributions over unitaries. We will sometimes refer to unitary oracle ensembles as unitary oracles.*

Definition 2.3. *Let $\ell_u(n)$ be some polynomial. The quantum Haar random unitary model (QHROM) of length ℓ_u is the unitary oracle ensemble $\mathcal{U} = \{\mathcal{U}_n\}_{n\in\mathbb{N}}$ where $\mathcal{U}_n \coloneqq Haar(\{0,1\}^{\ell_u(n)})$.*

Definition 2.4. *Let ℓ_m, ℓ_n be some polynomials and let $\mathcal{F}_n = \{f : \{0,1\}^{\ell_m(n)} \to \{0,1\}^{\ell_n(n)}\}$. Given f in $\mathcal{F}$, define $A_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. The quantum query secure random oracle model (QROM) mapping ℓ_m to ℓ_n is the unitary oracle ensemble $\mathcal{U} = \{\mathcal{U}_n\}_{n\in\mathbb{N}}$ where $\mathcal{U}_n$ samples $f \leftarrow \mathcal{F}_n$ and outputs A_f.*

2.3 Distance metrics on quantum channels

Definition 2.5 (Diamond norm)**.** *Let Φ be a quantum channel operating on n qubits. The diamond norm of Φ is*

$$\|\Phi\|_\diamond = \sup_{|\phi\rangle} \|(\Phi \otimes I_n)(|\phi\rangle\langle\phi|)\|_1$$

The diamond distance between two quantum channels Φ_1, Φ_2 operating on n qubits is then the diamond norm of their difference

$$\|\Phi_1 - \Phi_2\|_\diamond = \sup_{|\phi\rangle} \|(\Phi_1 \otimes I_n)(|\phi\rangle\langle\phi|) - (\Phi_2 \otimes I_n)(|\phi\rangle\langle\phi|)\|_1$$

Theorem 2.6. *Let $\mathcal{A}^{(\cdot)}$ be any quantum oracle algorithm making at most t queries. Let Φ_1, Φ_2 be two quantum channels. Then*

$$\left|\Pr\left[\mathcal{A}^{\Phi_1} \to 1\right] - \Pr\left[\mathcal{A}^{\Phi_2} \to 1\right]\right| \leq t \cdot \|\Phi_1 - \Phi_2\|_\diamond$$

Definition 2.7 (Operator norm)**.** *Let V be a linear map. Then the operator norm of V is*

$$\|V\|_{op} = \sup_{|\phi\rangle} \|V|\phi\rangle\|_2$$

The operator distance between two linear operators V_1, V_2 is then the operator norm of their difference

$$\|V_1 - V_2\|_{op} = \sup_{|\phi\rangle} \|V_1|\phi\rangle - V_2|\phi\rangle\|_2$$

Proposition 2.8. *Let V_1, V_2 be two partial isometries, let Φ_1 be the operator $V_1(\cdot)V_1^\dagger$, and let Φ_2 be the operator $V_2(\cdot)V_2^\dagger$. Then*

$$\|\Phi_1 - \Phi_2\|_\diamond \leq 2\|V_1 - V_2\|_{op}$$

The proof is included in [Kre21], Lemma 9. Note that while [Kre21] proves this statement for unitaries, in fact the only fact about unitaries needed is that the absolute value of the eigenvalues of a unitary are bounded above by 1 (i.e. the operator norm is bounded by 1), and this also holds for partial isometries.

Lemma 2.9. *Let V_1, V_2, W_1, W_2 be partial isometries. Then*

$$\|V_1W_1 - V_2W_2\|_{op} \leq \|V_1 - V_2\|_{op} + \|W_1 - W_2\|_{op}$$

and

$$\|(V_1 + V_2) - (W_1 + W_2)\|_{op} \leq \|V_1 - W_1\|_{op} + \|V_2 - W_2\|_{op}$$

Proof. The first inequality follows from the following calculation (taken from [dBhdb]):

$$\begin{aligned}
&\|V_1W_1 - V_2W_2\|_{op} \\
=&\|V_1W_1 - V_2W_2 - V_2W_1 + V_2W_1\|_{op} \\
\leq&\|V_1W_1 - V_2W_1\|_{op} + \|V_2W_1 - V_2W_2\|_{op} \\
=&\|(V_1 - V_2)W_1\|_{op} + \|V_2(W_1 - W_2)\|_{op} \\
\leq&\|V_1 - V_2\|_{op}\|W_1\|_{op} + \|V_2\|_{op}\|W_1 - W_2\|_{op} \\
\leq&\|V_1 - V_2\|_{op} + \|W_1 - W_2\|_{op}
\end{aligned} \tag{1}$$

since $\|W_1\|_{op} = \|V_2\|_{op} = 1$ as they are partial isometries.

The second inequality follows immediately from the triangle inequality. □

Proposition 2.10. *Let V be any linear map, then*

$$\|V\|_{op} = \left\|V^\dagger\right\|_{op}$$

Proposition 2.11. *For all quantum states $|\phi\rangle, |\psi\rangle$,*

$$\||\phi\rangle\langle\phi| - |\psi\rangle\langle\psi|\|_2 \leq \||\phi\rangle\langle\phi| - |\psi\rangle\langle\psi|\|_1 = 2\sqrt{1 - |\langle\phi|\psi\rangle|^2}$$

2.4 Path Recording Framework

Here we present the path recording framework for simulating random unitaries defined in [MH25], along with the extension to conjugate and transpose queries from [SML+25]. In particular, we expand their definition to encompass random unitaries over subsets of $\{0,1\}^n$. These restated theorems follow from the same proofs as in [MH25].

Definition 2.12. *Given a set $S \subseteq \{0,1\}^n$, define $R_S = \mathcal{P}(\{0,1\}^{2n})$ to be the set of relations over S.*

Furthermore, define $R_S^{inj} \subseteq R_S$ to be the set of injective relations over S. Formally,

$$R_S^{inj} = \{R \subseteq \{0,1\}^{2n} : \forall (x,y) \neq (x',y') \in R, y \neq y'\}$$

We similarly define $R_{S,t} \subseteq R_S$ to be

$$R_{S,t} = \{R \in R_S : |R| \leq t\}$$

$R_{S,t}^{inj} \subseteq R_S^{inj}$ is defined similarly.

Let $D = \{(x_1,y_1),\ldots,(x_\ell,y_\ell)\} \in R_{S,t}$. We say $\mathrm{Im}(D) = \{y_1,\ldots,y_\ell\}$ and $\mathrm{Dom}(D) = \{(x_1,\ldots,x_\ell)\}$.

Definition 2.13 (Forward query path recording oracle)**.** *Let $S \subseteq \{0,1\}^n$ be any set and let $t_{max} \leq |S|$. Let V_S be the partial isometry over $\mathcal{H}(\{0,1\}^n) \otimes \mathcal{H}(R_S^{inj})$ defined as follows: for $x \in S, D \in R_{S,t_{max}-1}^{inj}$*

$$V|x\rangle|D\rangle \mapsto \frac{1}{\sqrt{|S| - |\mathrm{Im}(D)|}} \sum_{y \in S \setminus \mathrm{Im}(D)} |y\rangle|D \cup \{(x,y)\}\rangle$$

for $x \notin S, D \in R_S^{inj}$,

$$V_S|x\rangle|D\rangle \mapsto |x\rangle|D\rangle$$

Theorem 2.14. *Let $\mathbf{A}$ be an arbitrary Hilbert space, let $\mathbf{In} = \mathcal{H}(\{0,1\}^n)$ and let $\mathbf{S} = \mathcal{H}(R_S^{inj})$. Let $\mathcal{A}^{(\cdot)}$ be any t-query algorithm operating on registers $\mathbf{A}, \mathbf{In}$. Let $t \leq t_{max}$ and let $V_{S,t_{max}}$ operate on registers $\mathbf{In}, \mathbf{St}$. Then,*

$$TD\left(\mathop{\mathbb{E}}_{U \leftarrow Haar(S)}\left[\mathcal{A}^U\right], \mathcal{A}^V\right) \leq \frac{2t(t-1)}{|S|+1}$$

Theorem 2.15 (Efficient simulation over $\{0,1\}^n$ - [MH25] Appendix A)**.** *There exists an efficient algorithm* $\mathrm{Sim}(1^{t_{max}})$ *acting on registers* $\mathbf{In}, \mathbf{St}$ *such that the following holds. Let* $\mathcal{A}^{(\cdot)}$ *be any* t*-query algorithm operating on registers* $\mathbf{A}, \mathbf{In}$*, where register* $\mathbf{In}$ *is over* $\mathcal{H}(\{0,1\}^n)$*. Let* $t \leq t_{max}$ *and let* $V^{\{0,1\}^n, t_{max}}$ *operate on registers* $\mathbf{In}, \mathbf{St}$*.*

$$\mathcal{A}^{\mathrm{Sim}(1^{t_{max}})} = \mathcal{A}^{V_{\{0,1\}^n, t_{max}}}$$

Proof Sketch. The simulator will represent elements of $R^{inj}_{\{0,1\}^n, t_{max}}$ as sorted lists of pairs of elements of $\{0,1\}^n$. That is, for $D \in R^{inj}_{\{0,1\}^n, t_{max}}$, define $Rep(D) \in (\{0,1\}^{2n} \cup \{(\bot, \bot)\})^{t_{max}}$ as follows: let $(x_1, y_1), \ldots, (x_t, y_t)$ be the elements of D in sorted order.

$$Rep(D) = ((x_1, y_1), \ldots, (x_t, y_t), \underbrace{(\bot, \bot), \ldots, (\bot, \bot)}_{t_{max} - t})$$

$\mathbf{St}$ will then be a register over $\mathcal{H}((\{0,1\}^{2n} \cup \{(\bot, \bot)\})^{t_{max}})$ which will always contain an element of $R^{inj}_{S, t_{max}}$.

$\mathrm{Sim}(1^{t_{max}}) |x\rangle |D\rangle$ will then act as follows

1. Generate the state $\sum_{y \in \{0,1\}^n \setminus \mathrm{Im}(D)} |y\rangle$.
2. Perform the isometry $|x\rangle |D\rangle |y\rangle \mapsto |x\rangle |D\rangle |y\rangle |D \cup \{(x,y)\}\rangle$. This leaves the state of the simulator as
$$\sum_{y \in \{0,1\}^n \setminus \mathrm{Im}(D)} |x\rangle |D\rangle |y\rangle |D \cup \{(x,y)\}\rangle$$
3. Finally, uncompute the registers containing x and D (which is possible since these are exactly determined by $y, D \cup \{(x,y)\}$). This results in the final state
$$\sum_{y \in \{0,1\}^n \setminus \mathrm{Im}(D)} |y\rangle |D \cup \{(x,y)\}\rangle$$

□

Note that the only part of this simulator which requires knowing that the set S is $\{0,1\}^n$ is computing

$$\sum_{y \in S \setminus \mathrm{Im}(D)} |y\rangle = \sum_{y \in \{0,1\}^n \setminus \mathrm{Im}(D)} |y\rangle$$

For an arbitrary $S \subseteq \{0,1\}^n$, this state can be constructed by the following process:

1. Construct the state $\sum_{y \in \{0,1\}^n} |y\rangle$
2. Apply the measurement checking if $y \in S$
3. Apply the measurement checking if $y \notin D$

If both measurements succeed, then the residual state is exactly

$$\sum_{y \in S \setminus \mathrm{Im}(D)} |y\rangle$$

and both measurements succeed with probability $\frac{|S| - |\mathrm{Im}(D)|}{2^n}$. These measurements can further be performed using a reflection oracle for S. This leads to the following corollary

Corollary 2.16. *There exists an efficient oracle algorithm* $\mathrm{Sim}^{(\cdot)}(1^{t_{max}})$ *acting on registers* $\mathbf{In}, \mathbf{St}$ *such that the following holds. Let* $\mathcal{A}^{(\cdot)}$ *be any* t*-query algorithm operating on registers* $\mathbf{A}, \mathbf{In}$*, where register* $\mathbf{In}$ *is over* $\mathcal{H}(\{0,1\}^n)$*. Let* $S \subseteq [N]$ *and let* R_S *be reflection around* S*. Let* $t \leq t_{max}$*. Then,*

$$\mathcal{A}^{\mathrm{Sim}^{R_S}(1^{t_{max}})} = \mathcal{A}^{V_{S,t_{max}}}$$

Definition 2.17 (Inverse, conjugate, transpose capable path recording oracle [SML+25])**.** *Let* $S \subseteq \{0,1\}^n$ *be any set and let* $t_{max} \leq |S|$*. Let* $V_S^L, V_S^R, \overline{V}_S^L, \overline{V}_S^R$ *be the partial isometries over* $\mathcal{H}(\{0,1\}^n) \otimes \mathcal{H}(R_S) \otimes \mathcal{H}(R_S)$ *defined as follows: for* $x \in S$*, for* $L, R \in R_{S,t_{max}-1}$

$$V_S^L |x\rangle |L\rangle |R\rangle \mapsto \frac{1}{\sqrt{|S| - |\operatorname{Im}(L \cup R)|}} \sum_{y \in S \setminus \operatorname{Im}(L \cup R)} |y\rangle |L \cup \{(x,y)\}\rangle |R\rangle$$

$$\overline{V}_S^L |x\rangle |L\rangle |R\rangle \mapsto \frac{1}{\sqrt{|S| - |\operatorname{Im}(L \cup R)|}} \sum_{y \in S \setminus \operatorname{Im}(L \cup R)} |y\rangle |L\rangle |R \cup \{(x,y)\}\rangle$$

for $y \in S$*, for* $L, R \in R_{S,t_{max}-1}$

$$V_S^R |y\rangle |L\rangle |R\rangle \mapsto \frac{1}{\sqrt{|S| - |\operatorname{Dom}(L \cup R)|}} \sum_{x \in S \setminus \operatorname{Dom}(L \cup R)} |x\rangle |L\rangle |R \cup \{(x,y)\}\rangle$$

$$\overline{V}_S^R |y\rangle |L\rangle |R\rangle \mapsto \frac{1}{\sqrt{|S| - |\operatorname{Dom}(L \cup R)|}} \sum_{x \in S \setminus \operatorname{Dom}(L \cup R)} |x\rangle |L \cup \{(x,y)\}\rangle |R\rangle$$

for $x \notin S, (L,R) \in R_S^2$*,*

$$V_S^L |x\rangle |L\rangle |R\rangle = V_S^R |x\rangle |L\rangle |R\rangle = |x\rangle |L\rangle |R\rangle$$

Finally, define

$$V_S = V_S^L(I - V^R \cdot V^{R,\dagger}) + (I - V_S^L \cdot V_S^{L,\dagger})V_S^{R,\dagger}$$
$$\overline{V}_S = \overline{V}_S^L(I - \overline{V}_S^R \cdot \overline{V}_S^{R,\dagger}) + (I - \overline{V}_S^L \cdot \overline{V}_S^{L,\dagger})\overline{V}_S^{R,\dagger}$$

Theorem 2.18. *Let* $\mathcal{A}^{(\cdot)}$ *be any* t*-query algorithm operating on registers* AB*, where register* A *is over* $\mathcal{H}(\{0,1\}^n)$*. Let* $t \leq t_{max}$ *and let* $V_{S,t_{max}}$ *operate on registers* AR*. Define* $\vec{V}_{S,t_{max}} = (V_{S,t_{max}}, V_{S,t_{max}}^\dagger, \overline{V}_{S,t_{max}}, \overline{V}_{S,t_{max}}^\dagger)$ *Then,*

$$TD\left(\mathop{\mathbb{E}}_{U \leftarrow Haar(S)}\left[\mathcal{A}^{\vec{U}}\right], \mathcal{A}^{\vec{V}_{S,t_{max}}}\right) \leq \frac{9t(t+1)}{|S|^{1/8}}$$

Observing the efficient implementation of the inverse capable path recording oracle from [MH25], it is fortunately the case that Corollary 2.16 generalizes to the inverse setting as well. Furthermore, by applying the symmetric construction, Corollary 2.16 also applies in the case of conjugate and transpose queries.

Corollary 2.19. *There exists efficient oracle algorithms* $\mathrm{Sim}^{(\cdot)}(1^{t_{max}}), \overline{\mathrm{Sim}}^{(\cdot)}(1^{t_{max}})$ *acting on registers* $\mathbf{In}, \mathbf{St}$ *such that the following holds. Let* $\mathcal{A}^{(\cdot)}$ *be any* t*-query algorithm operating on registers* $\mathbf{A}, \mathbf{In}$*, where register* A *is over* $\mathcal{H}(\{0,1\}^n)$*. Let* $S \subseteq \{0,1\}^n$ *and let* R_S *be reflection around* S

$$R_S |x\rangle \mapsto (-1)^{\mathbb{1}[x \in S]} |x\rangle$$

Let $t \leq t_{max}$*. Define*

$$\vec{\mathrm{Sim}}^{R_S}(1^{t_{max}}) = (\mathrm{Sim}^{R_S}(1^{t_{max}}), (\mathrm{Sim}^{R_S}(1^{t_{max}}))^\dagger, \overline{\mathrm{Sim}}^{R_S}(1^{t_max}), (\overline{\mathrm{Sim}}^{R_S}(1^{t_{max}}))^\dagger)$$

then we have

$$\mathcal{A}^{\vec{\mathrm{Sim}}^{R_S}(1^{t_{max}})} = \mathcal{A}^{\vec{V}_{S,t_{max}}}$$

when clear from context, we will omit $1^{t_{max}}$*.*

3 Unitary reprogramming lemma

Lemma 3.1 (Unitary reprogramming lemma)**.** *Let* N, M_1, M_2, t *be functions such that* $\frac{M_1}{M_2} = \mathsf{negl}(n)$*,* $\frac{M_2}{N} = \mathsf{negl}(n)$*, and* $t = \mathsf{poly}(n)$*. Let* $S_1 \subseteq [N]$ *be any set of size* $|S_1| = M_1$*. Define* $\mathcal{O}$ *as follows*

1. *Sample* $S_2 \subseteq [N]$ *uniformly at random such that* $S_1 \subseteq S_2$ *and* $|S_2| = M_2$*.*
2. *Sample* U_1 *a Haar random unitary acting on* S_2*.*
3. *Sample* U_2 *a Haar random unitary acting on* $[N] \setminus S_2$*.*
4. *Let* $\mathcal{O} = U_1 U_2$*.*

Let $\mathcal{A}^{(\cdot)}$ *be any* t *query oracle algorithm (allowed to make inverse, transpose, and conjugate queries). Then*

$$\left| \Pr\left[\mathcal{A}^{\vec{\mathcal{O}}}(S_1) \to 1\right] - \Pr_{U \leftarrow Haar([N])}[\mathcal{A}^{\vec{U}}(S_1) \to 1] \right| \leq \mathsf{negl}(n)$$

We will hybrid over a series of partial isometries $\vec{V} = (V_i, V_i^\dagger, \overline{V_i}, \overline{V_i}^\dagger)$ representing forward, inverse, transpose, and conjugate queries respectively. We will frequently define operators $V_i^{L_1}$, $V_i^{R_1}, V_i^{L_2}, V_i^{R_2}, \overline{V}_i^{L_1}, \overline{V}_i^{R_1}, \overline{V}_i^{L_2}, \overline{V}_i^{R_2}$, in which case, in the style of path recording, we will implicitly set (unless otherwise stated)

$$\begin{aligned} V_i^L &= V_i^{L_1} V_i^{L_2} \\ V_i^R &= V_i^{R_1} V_i^{R_2} \\ V_i &= V_i^L \cdot (I - V_i^R \cdot V_i^{R,\dagger}) + (I - V_i^L \cdot V_i^{L,\dagger}) \cdot V_i^{R,\dagger} \\ \overline{V}_i &= \overline{V}_i^L \cdot (I - \overline{V}_i^R \cdot \overline{V}_i^{R,\dagger}) + (I - \overline{V}_i^L \cdot \overline{V}_i^{L,\dagger}) \cdot \overline{V}_i^{R,\dagger} \end{aligned} \tag{2}$$

Each of these operators will operate on a register $\mathbf{In}$ over $\mathcal{H}([N])$ and $\mathbf{St}$ over $\mathcal{H}(R_{[N]})^{\otimes 4} \otimes \mathcal{H}(\mathcal{P}([N]))$. This space is spanned by states of the form $|x\rangle |L_1\rangle |L_2\rangle |R_1\rangle |R_2\rangle |S_2\rangle$ where x is in $\{0,1\}^n$, the L_1, L_2, R_1, R_2 are relations in $R_{[N]}$, and S_2 is a subset of $[N]$.

We will further define notation for basis vectors D of the space $\mathcal{H}([N]) \otimes \mathcal{H}(R_{[N]})^{\otimes 4}$. These will be elements of $\mathcal{DB} = [N] \times R_{[N]}^4$. Given $D = (x, L_1, R_1, L_2, R_2)$, we will write $D_x = x, D_{L_1} = L_1, D_{R_1} = R_1, D_{L_2} = L_2, D_{R_2} = R_2$. We will define $\mathrm{Dom}(D_b) = \mathrm{Dom}(L_b) \cup \mathrm{Dom}(R_b)$ and $\mathrm{Im}(D_b) = \mathrm{Im}(L_b) \cup \mathrm{Im}(R_b)$. For ease of notation, we will write $D_{1,all} = \mathrm{Im}(D_1) \cup \mathrm{Dom}(D_1) \cup S_1$ and $D_{2,all} = \mathrm{Im}(D_2) \cup \mathrm{Dom}(D_2)$ (note the asymmetry here). We will write $D_{all} \coloneqq D_{1,all} \cup D_{2,all} \cup \{D_x\}$. We will also define $D_y^{L_1,f} = (y, L_1 \cup \{(x,y)\}, R_1, L_2, R_2)$ and $D_y^{L_1,b} = (y, L_1 \cup \{(y,x)\}, R_1, L_2, R_2)$. We define $D_y^{R_1,f}, D_y^{L_2,f}, D_y^{R_2,f}, D_y^{R_1,b}, D_y^{L_2,b}, D_y^{R_2,b}$ analogously.

For all hybrids, we will work with the initial internal state

$$|\phi_0\rangle = \frac{1}{\sqrt{\binom{N}{M_2}}} |\emptyset\rangle^{\otimes 4} \sum_{\substack{S_2 \in \mathcal{P}([N]) \\ |S_2| = M_2}} |S_2\rangle$$

We set $V_0 = U_1 U_2$ and $\vec{V_0} = (V_0, V_0^\dagger, V_0^*, V_0^T)$ for U_1, U_2 distributed as in the lemma statement. We set $V_f = U$ and $\vec{V_f} = (V_f, V_f^\dagger, V_f^*, V_f^T)$ for U a Haar random unitary over $\mathcal{H}([N])$. Our remaining hybrids are then as follows

1. In this hybrid we replace the truly random unitaries with a path recording variant. On input $|D\rangle |S_2\rangle$ such that $D_x \in S_2$, define

$$\begin{aligned}
V_1^{L_1} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus \mathrm{Im}(D_1)|}} \sum_{y \in S_2 \setminus \mathrm{Im}(D_1)} \left| D_y^{L_1,f} \right\rangle |S_2\rangle \\
V_1^{R_1} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus \mathrm{Dom}(D_1)|}} \sum_{y \in S_2 \setminus \mathrm{Dom}(D_1)} \left| D_y^{R_1,b} \right\rangle |S_2\rangle \\
\overline{V_1}^{L_1} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus \mathrm{Im}(D_1)|}} \sum_{y \in S_2 \setminus \mathrm{Im}(D_1)} \left| D_y^{R_1,f} \right\rangle |S_2\rangle \\
\overline{V_1}^{R_1} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus \mathrm{Dom}(D_1)|}} \sum_{y \in S_2 \setminus \mathrm{Dom}(D_1)} \left| D_y^{L_1,b} \right\rangle |S_2\rangle
\end{aligned} \tag{3}$$

   with $V_1^{L_2}, V_1^{R_2}, \overline{V_1}^{L_2}, \overline{V_1}^{R_2}$ acting as identity on all such states. On input $|D\rangle |S_2\rangle$ such that $D_x \in [N] \setminus S_2$, define

$$\begin{aligned}
V_1^{L_2} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup \mathrm{Im}(D_2))|}} \sum_{y \in [N] \setminus (S_2 \cup \mathrm{Im}(D_2))} \left| D_y^{L_2,f} \right\rangle |S_2\rangle \\
V_1^{R_2} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup \mathrm{Dom}(D_2))|}} \sum_{y \in [N] \setminus (S_2 \cup \mathrm{Dom}(D_2))} \left| D_y^{R_2,b} \right\rangle |S_2\rangle \\
\overline{V_1}^{L_2} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup \mathrm{Im}(D_2))|}} \sum_{y \in [N] \setminus (S_2 \cup \mathrm{Im}(D_2))} \left| D_y^{R_2,f} \right\rangle |S_2\rangle \\
\overline{V_1}^{R_2} |D\rangle |S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup \mathrm{Dom}(D_2))|}} \sum_{y \in [N] \setminus (S_2 \cup \mathrm{Dom}(D_2))} \left| D_y^{L_2,b} \right\rangle |S_2\rangle
\end{aligned} \tag{4}$$

   with $V_1^{L_1}, V_1^{R_1}, \overline{V_1}^{L_1}, \overline{V_1}^{R_1}$ acting as identity on all such states.

2. In this hybrid we adjust the domains for which new outputs of the path-recording oracle are sampled. On input $|D\rangle|S_2\rangle$ such that $D_x \in S_2$, define

$$\begin{aligned}
V_2^{L_1}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus D_{1,all}|}} \sum_{y \in S_2 \setminus D_{1,all}} \left|D_y^{L_1,f}\right\rangle |S_2\rangle \\
V_2^{R_1}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus D_{1,all}|}} \sum_{y \in S_2 \setminus D_{1,all}} \left|D_y^{R_1,b}\right\rangle |S_2\rangle \\
\overline{V_2}^{L_1}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus D_{1,all}|}} \sum_{y \in S_2 \setminus D_{1,all}} \left|D_y^{R_1,f}\right\rangle |S_2\rangle \\
\overline{V_2}^{R_1}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|S_2 \setminus D_{1,all}|}} \sum_{y \in S_2 \setminus D_{1,all}} \left|D_y^{L_1,b}\right\rangle |S_2\rangle
\end{aligned} \tag{5}$$

with $V_2^{L_2}, V_2^{R_2}, \overline{V_2}^{L_2}, \overline{V_2}^{R_2}$ acting as identity on all such states. On input $|D\rangle|S_2\rangle$ such that $D_x \in [N] \setminus S_2$, define

$$\begin{aligned}
V_2^{L_2}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup D_{all})|}} \sum_{y \in [N] \setminus (S_2 \cup D_{all})} \left|D_y^{L_2,f}\right\rangle |S_2\rangle \\
V_2^{R_2}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup D_{all})|}} \sum_{y \in [N] \setminus (S_2 \cup D_{all})} \left|D_y^{R_2,b}\right\rangle |S_2\rangle \\
\overline{V_2}^{L_2}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup D_{all})|}} \sum_{y \in [N] \setminus (S_2 \cup D_{all})} \left|D_y^{R_2,f}\right\rangle |S_2\rangle \\
\overline{V_2}^{R_2}|D\rangle|S_2\rangle &= \frac{1}{\sqrt{|[N] \setminus (S_2 \cup D_{all})|}} \sum_{y \in [N] \setminus (S_2 \cup D_{all})} \left|D_y^{L_2,b}\right\rangle |S_2\rangle
\end{aligned} \tag{6}$$

with $V_2^{L_1}, V_2^{R_1}, \overline{V_2}^{L_1}, \overline{V_2}^{R_1}$ acting as identity on all such states.

3. (a) We call a set S_2 valid if the following hold
   i. $D_{1,all} \subseteq S_2$
   ii. $D_{2,all} \cap S_2 = \emptyset$
   iii. If $D_x \notin D_{1,all}$, then $D_x \notin S_2$

   We define $Val(D) = \{S_2 \subseteq [N] : |S_2| = M_2 \text{ and } S_2 \text{ is valid for } D\}$.

   Intuitively, the first two conditions state the D_1 contains only values in S_2 and D_2 contains no values in S_2 (which would occur if D_1 and D_2 were the internal states of independent Haar random unitaries). The last condition enforces that the adversary never guesses a point in S_2 without being previously given that information (either via S_1 or given in a previous query).

   (b) Define the state

$$|ValSt_D\rangle = \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle$$

   Note that for $D \neq D'$, $|ValSt_D\rangle$ and $|ValSt_{D'}\rangle$ are orthogonal. Define the projector

$$\Pi_{good} = \sum_D |ValSt_D\rangle\langle ValSt_D|$$

(c) For all X, define $V_3^X = \Pi_{good} V_2^X \Pi_{good}$ and $\overline{V_3}^X = \Pi_{good} \overline{V_2}^X \Pi_{good}$.

4. (a) Define the following isometry $ConS$ to reconstruct the S_2 register from the rest of the state. That is,

$$ConS\,|D\rangle = \frac{1}{\sqrt{|Val(D)|}}\,|D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle$$

Note $\Pi_{good} = \mathrm{Im}(ConS)$.

(b) We will define a new set of partial isometries $W_4^{L_1}, W_4^{R_1}, \ldots$ acting only on $\mathcal{H}([N]) \otimes \mathcal{H}(R_{[N]})^{\otimes 4}$ as follows (which will implicitly define $\vec{W_4} = (W_4, W_4^\dagger, \overline{W}_4, \overline{W}_4^\dagger)$). On input $|D\rangle$ such that $D_x \in D_{1,all}$, define

$$\begin{aligned}
W_4^{L_1}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \\
W_4^{R_1}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{R_1,b} \right\rangle \\
\overline{W_4}^{L_1}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{R_1,f} \right\rangle \\
\overline{W_4}^{R_1}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,b} \right\rangle
\end{aligned} \tag{7}$$

with $W_4^{L_2}, W_4^{R_2}, \overline{W}_4^{L_2}, \overline{W}_4^{R_2}$ acting as identity on all such states. On input $|D\rangle$ such that $D_x \notin D_{1,all}$, define

$$\begin{aligned}
W_4^{L_2}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2,f} \right\rangle \\
W_4^{R_2}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{R_2,b} \right\rangle \\
\overline{W_4}^{L_2}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{R_2,f} \right\rangle \\
\overline{W_4}^{R_2}\,|D\rangle &= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2,b} \right\rangle
\end{aligned} \tag{8}$$

with $W_4^{L_1}, W_4^{R_1}, \overline{W}_4^{L_1}, \overline{W}_4^{R_1}$ acting as identity on all such states.

(c) For all X, define $V_4^X = ConS \cdot W_4^X \cdot ConS^\dagger$ and $\overline{V}_4^X = ConS \cdot \overline{W}_4^X \cdot ConS^\dagger$.

5. We set $V_5 = W_4 \otimes I$ and $\overline{V_5} = \overline{W_4} \otimes I$.

6. V_6 will correspond to a single path-recording oracle no longer split into two parts. In particular, define partial isometries $W_6^{L_1}, W_6^{R_1}, \overline{W_6}^{L_1}, \overline{W_6}^{R_1}$ acting on registers $\mathcal{H}([N]) \otimes \mathcal{H}(R_{[N]})^{\otimes 4}$

as follows

$$\begin{aligned}
W_6^{L_1}|D\rangle &\mapsto \frac{1}{\sqrt{|[N]\setminus D_{all}|}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{L_1,f}\right\rangle\\
W_6^{R_1}|D\rangle &\mapsto \frac{1}{\sqrt{|[N]\setminus D_{all}|}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{R_1,b}\right\rangle\\
\overline{W_6}^{L_1}|D\rangle &\mapsto \frac{1}{\sqrt{|[N]\setminus D_{all}|}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{R_1,f}\right\rangle\\
\overline{W_6}^{R_1}|D\rangle &\mapsto \frac{1}{\sqrt{|[N]\setminus D_{all}|}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{L_1,b}\right\rangle
\end{aligned} \tag{9}$$

We will define

$$W_6 = W_6^{L_1}(I - W_6^{R_1}\cdot W_6^{R_1,\dagger}) + (I - W_6^{L_1}\cdot W_6^{L_1,\dagger})W_6^{R_1,\dagger}$$

$$\overline{W}_6 = \overline{W}_6^{L_1}(I - \overline{W}_6^{R_1}\cdot \overline{W}_6^{R_1,\dagger}) + (I - \overline{W}_6^{L_1}\cdot \overline{W}_6^{L_1,\dagger})\overline{W}_6^{R_1,\dagger}$$

Then we will set $V_6 = W_6 \otimes I$ and $\overline{V_6} = \overline{W_6}\otimes I$.

7. V_7 will correspond to the standard path-recording oracle for a single Haar random unitary.

Before arguing about the hybrids, we will first show that each of the claimed partial isometries are actually partial isometries. This follows immediately from the following observation

Lemma 3.2. *For all $A \neq B \in \mathcal{DB}$, for all $y \in [N]\setminus(A_1\cap B_1)$,*

1. $\left\langle A_y^{L_1,f}\middle| B_y^{L_1,f}\right\rangle = 0$
2. $\left\langle A_y^{L_1,b}\middle| B_y^{L_1,b}\right\rangle = 0$
3. $\left\langle A_y^{R_1,f}\middle| B_y^{R_1,f}\right\rangle = 0$
4. $\left\langle A_y^{R_1,b}\middle| B_y^{R_1,b}\right\rangle = 0$

and for all $y \in [N]\setminus(A_2\cap B_2)$,

1. $\left\langle A_y^{L_2,f}\middle| B_y^{L_2,f}\right\rangle = 0$
2. $\left\langle A_y^{L_2,b}\middle| B_y^{L_2,b}\right\rangle = 0$
3. $\left\langle A_y^{R_2,f}\middle| B_y^{R_2,f}\right\rangle = 0$
4. $\left\langle A_y^{R_2,b}\middle| B_y^{R_2,b}\right\rangle = 0$

Proof. We will explicitly write the proof for $\left\langle A_y^{L_1,f} \middle| B_y^{L_1,f} \right\rangle = 0$, and the rest follow by the same argument.

If $(A_{L_2}, A_{R_1}, A_{R_2}) \neq (B_{L_2}, B_{R_1}, B_{L_2})$ then this is trivial. Thus, without loss of generality, we assume $(A_{L_2}, A_{R_1}, A_{R_2}) = (B_{L_2}, B_{R_1}, B_{L_2})$. We will then show that $A_{L_1} \cup \{(A_x, y)\} \neq B_{L_1} \cup \{(B_x, y)\}$.

If $A_{L_1} = B_{L_1}$, since $A_x \neq B_x$ we by definition have $A_{L_1} \cup \{(A_x, y)\} \neq B_{L_1} \cup \{(B_x, y)\}$. If $A_x = B_x$ and $A_{L_1} \neq B_{L_1}$, then again by definition we have $A_{L_1} \cup \{(A_x, y)\} \neq B_{L_1} \cup \{(A_x, y)\}$. If $|A_{L_1}| \neq |B_{L_1}|$, then the result trivially follows. In the final case, we consider $A_x \neq B_x$, $A_{L_1} \neq B_{L_1}$, and $|A_{L_1}| = |B_{L_1}|$. In this case, the only way we can have $A_{L_1} \cup \{(A_x, y)\} = B_{L_1} \cup \{(B_x, y)\}$ is if $A_{L_1} \setminus \{(B_x, y)\} = B_{L_1} \setminus \{(A_x, y)\}$.

But since $A_x \neq B_x$, this implies that $\{(B_x, y)\} \in A_{L_1}$ and $\{(A_x, y)\} \in B_{L_1}$. And so, $y \in A_1 \cap B_1$, which is a contradiction. □

To conclude the proof, we argue the formal proofs that

$$\left\| \mathcal{A}^{\vec{V_i}} - \mathcal{A}^{\vec{V_{i-1}}} \right\|_2 \leq \mathsf{negl}(n)$$

for all i. Lemma 3.1 follows immediately. As these arguments are all technically involved, we will defer them to Appendix B and provide a proof sketch of the hybrids here.

1. $\left\| \mathcal{A}^{\vec{V_1}} - \mathcal{A}^{\vec{V_0}} \right\|_2 \leq \mathsf{negl}(n)$: This follows from path recording (Theorem 2.18), although some care needs to be taken to verify that $\vec{V_1}$ is indeed the correct instantiation of the path recording oracle.

2. $\left\| \mathcal{A}^{\vec{V_2}} - \mathcal{A}^{\vec{V_1}} \right\|_2 \leq \mathsf{negl}(n)$: V_1^L and V_2^L are close in diamond distance, since V_2^L chooses y from a space which has negligibly fewer options. A similar argument holds for the other components of $\vec{V_1}, \vec{V_2}$. Since all maps here are partial isometries, this implies that $\vec{V_1}$ and $\vec{V_2}$ are close in diamond distance and so by induction the final states of the adversary when interacting with both maps will be close.

3. $\left\| \mathcal{A}^{\vec{V_3}} - \mathcal{A}^{\vec{V_2}} \right\|_2 \leq \mathsf{negl}(n)$: We will show that all maps making up $\mathcal{A}^{\vec{V_2}}$ approximately commute with Π_{good}. And so the claim follows by induction. In particular, let $|\phi\rangle \in \mathrm{Im}(\Pi_{good})$. We can observe directly that $V_2^{L_1} |\phi\rangle$ will also be in $\mathrm{Im}(\Pi_{good})$. Some more care needs to be taken to ensure that $V_2^{L_1,\dagger} |\phi\rangle$ will be close to a state in $\mathrm{Im}(\Pi_{good})$, and will follow from a direct combinatorial argument given in detail in Appendix C. Similarly, for any map A operating only in $\mathbf{In}$, $A |\phi\rangle$ will be close to a state in Π_{good}, with error corresponding to the event that the new component in register $\mathbf{In}$ lands in $S_2 \setminus D_{1,all}$. Since this is effectively a random set, the corresponding error is neglgible.

4. $\vec{V_3} = \vec{V_4}$: In particular, $\vec{W_4}$ is an exact description of the map you get when you conjugate $\vec{V_3}$ by $ConS$.

5. $\mathcal{A}^{\vec{V_5}} = \mathcal{A}^{\vec{V_4}}$: This follows immediately from the map that $\vec{V_4}$ and $\vec{V_5}$ are identical up to conjugation by the isometry $ConS$ which acts only on the internal state register.

6. $\mathcal{A}^{\vec{V}_6} = \mathcal{A}^{\vec{V}_5}$: We develop a partial isometry T acting only on the internal register such that $\vec{V}_6$ and $\vec{V}_5$ are identical up to conjugation by T. In particular, T will describe how to split a database L, R coming from $\mathcal{A}^{\vec{V}_6}$ into a database (L_1, R_1, L_2, R_2) consistent with $\mathcal{A}^{\vec{V}_5}$. The idea is that we partition all $(x, y) \in L \cup R$ into either (L_1, R_1) or (L_2, R_2). In particular, we will place (x, y) in (L_1, R_1) if and only if there is a "path" in (L, R) reaching (x, y) from a string $s \in S_2$. That is, there exists $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t) \in L \cup R$ such that

   (a) $(x_t, y_t) = (x, y)$

   (b) $x_1 \in S_1$ or $y_1 \in S_2$

   (c) $x_i = y_{i-1}$

7. $\left\|\mathcal{A}^{\vec{V}_7} - \mathcal{A}^{\vec{V}_6}\right\|_2 \leq \mathsf{negl}(n)$: This follows from the same argument as for $\left\|\mathcal{A}^{\vec{V}_2} - \mathcal{A}^{\vec{V}_1}\right\|_2 \leq \mathsf{negl}(n)$

8. $\left\|\mathcal{A}^{\vec{V}_f} - \mathcal{A}^{\vec{V}_7}\right\|_2 \leq \mathsf{negl}(n)$: This follows from path recording (Theorem 2.18).

4 Unclonable encryption compiler

Definition 4.1. *A (many-time) unclonable encryption scheme with keys of length $\ell_k(n)$ for messages of length $\ell_m(n)$ is a pair of uniform quantum algorithms* $\mathrm{Enc}, \mathrm{Dec}$ *with the following syntax*

1. $\mathrm{Enc}(1^n, k, m) \to \rho_{k,m}$ *takes as input a security parameter n, a key k, and a message m, and outputs a mixed state $\rho_{k,m}$.*

2. $\mathrm{Dec}(1^n, k, \rho) \to m$ *takes as input a security parameter n, a key k, and a quantum ciphertext ρ, and outputs a decrypted message m.*

satisfying the following properties.

1. *(Perfect) correctness: for all $n \in \mathbb{N}, m \in \{0,1\}^{\ell_m(n)}$,*

$$\Pr\left[\ \mathrm{Dec}(1^n, k, \rho_{k,m}) = m \ \ : \ \begin{array}{c} k \leftarrow \{0,1\}^{\ell_k(n)} \\ \mathrm{Enc}(1^n, k, m) \to \rho_{k,m} \end{array}\ \right] = 1.$$

2. *Security: For all (non-uniform) QPT algorithms A, B and for all (non-uniform) QPT oracle algorithms $C^{(\cdot)}$, define $GAME^n_{A,B,C}(\mathrm{Enc}, \mathrm{Dec})$ to be the following game*

   (a) *Sample $k \leftarrow \{0,1\}^{\ell_k(n)}$*

   (b) *Run $C^{\mathrm{Enc}(1^n,k,\cdot)} \to (m_0, m_1, \boldsymbol{st})$.*

   (c) *Sample $b \leftarrow \{0,1\}$*

   (d) *Set $\rho_b = \mathrm{Enc}(1^n, k, m_b)$.*

   (e) *Run $C^{\mathrm{Enc}(1^n,k,\cdot)}(\rho_b, \boldsymbol{st}) \to \sigma_{\mathbf{AB}}$. In full detail, the oracle $\mathrm{Enc}(1^n, k, \cdot)$ first measures its input register to produce a string m and then outputs $\mathrm{Enc}(1^n, k, m)$.*

   (f) *Run $A(1^n, k, \mathbf{A}) \to b_A$, $B(1^n, k, \mathbf{B}) \to b_B$.*

   (g) *Output 1 if and only if $b = b_A = b_B$.*

The unclonable encryption scheme must satisfy that for all n, QPT A, B, C,

$$\Pr\big[GAME^n_{A,B,C}(\mathrm{Enc},\mathrm{Dec}) \to 1\big] \leq \frac{1}{2} + \mathsf{negl}(n).$$

We will often omit the security parameter when it is clear from context.

Definition 4.2. *Let $\mathcal{U} = \{\mathcal{U}_n\}_{n\in\mathbb{N}}$ be a unitary oracle. An unclonable encryption scheme relative to $\mathcal{U}$ is a pair of quantum oracle algorithms $\mathrm{Enc}^{\vec{U}}, \mathrm{Dec}^{\vec{U}}$ with the following syntax*

1. *$\mathrm{Enc}^{\vec{U}}(1^n, k, m) \to \rho_{k,m}$: takes as input a security parameter n, a key k, and a message m, and outputs a mixed state $\rho_{k,m}$.*
2. *$\mathrm{Dec}^{\vec{U}}(1^n, k, \rho) \to m$ takes as input a security parameter n, a key k, and a quantum ciphertext ρ, and outputs a decrypted message m.*

satisfying the following notions of security.

1. *(Perfect) correctness: for all n, $m \in \{0,1\}^{\ell_m(n)}$,*

$$\Pr\left[\mathrm{Dec}^{\vec{U}}(1^n, k, \rho_{k,m}) = m \;:\; \begin{array}{c} U \leftarrow \mathcal{U}_n \\ k \leftarrow \{0,1\}^{\ell_k(n)} \\ \mathrm{Enc}^{\vec{U}}(1^n, k, m) \to \rho_{k,m} \end{array}\right] = 1$$

2. *Security: For oracle algorithms $A^{\vec{U}}, B^{\vec{U}}, C^{\vec{U},(\cdot)}$, define $GAME^n_{A,B,C}(\mathrm{Enc},\mathrm{Dec})$ to be the following game*
   (a) *Sample $U \leftarrow \mathcal{U}_n$.*
   (b) *Sample $k \leftarrow \{0,1\}^{\ell_k(n)}$*
   (c) *Run $C^{\vec{U},\mathrm{Enc}^{\vec{U}}(1^n,k,\cdot)} \to (m_0, m_1, \boldsymbol{st})$.*
   (d) *Sample $b \leftarrow \{0,1\}$*
   (e) *Set $\rho_b = \mathrm{Enc}^{\vec{U}}(1^n, k, m_b)$.*
   (f) *Run $C^{\vec{U},\mathrm{Enc}^{\vec{U}}(1^n,k,\cdot)}(\rho_b, \boldsymbol{st}) \to \sigma_{\mathbf{AB}}$.*
   (g) *Run $A^{\vec{U}}(1^n, k, \mathbf{A}) \to b_A$, $B^{\vec{U}}(1^n, k, \mathbf{B}) \to b_B$.*
   (h) *Output 1 if and only if $b = b_A = b_B$.*

   Security requires that for all polynomials t, for all oracle adversaries $A^{(\cdot)}, B^{(\cdot)}, C^{(\cdot)}$ making at most t oracle queries,

$$\Pr\big[GAME^n_{A,B,C}(\mathrm{Enc},\mathrm{Dec}) \to 1\big] \leq \frac{1}{2} + \mathsf{negl}(n)$$

Definition 4.3. *We will call a candidate unclonable encryption scheme $(\mathrm{Enc},\mathrm{Dec})$ pure if the encryption algorithm Enc is of the following form:*

1. *On input a key k and a message m.*

2. *Sample* $r \leftarrow \{0,1\}^{\ell_r(n)}$.

3. *Output* $E_k \left|m, r, 0\right\rangle$ *where* E_k *is some efficient unitary.*

We will call $E = \{E_k\}$ *the purification of* Enc.

We will call an oracle unclonable encryption scheme $(\mathrm{Enc}^{\vec{U}}, \mathrm{Dec}^{\vec{U}})$ *pure if the same definition holds for some oracularly efficient unitary* $E_k^{\vec{U}}$.

Note that if a (secure) scheme is pure, then without loss of generality we may assume that $\mathrm{Dec}(1^n, k, \rho)$ *is the map which applies* E_k^{-1} *to* ρ *and then measures the first register in the standard basis.*

For $r \in \{0,1\}^{\ell_r}$*, we will denote* $\mathrm{Enc}(k, m; r) = E_k \left|m, r, 0\right\rangle$.

Theorem 4.4. *Let* ℓ_r, ℓ_k *be any polynomials in* n*, and let* $\mathcal{V}$ *be any unitary oracle model. Let* $(\widetilde{\mathrm{Enc}}^{\vec{V}}, \widetilde{\mathrm{Dec}}^{\vec{V}})$ *be any pure unclonable encryption scheme relative to* $\mathcal{V}$ *operating on message space* $\{0,1\}^{\ell_m}$*, key space* $\{0,1\}^{\ell_{\tilde{k}}(n)}$*, randomness space* $\{0,1\}^{\ell_{\tilde{r}}(n)}$*, and using* $\ell_a(n)$ *ancilla qubits. Let* $\mathcal{U}$ *be the QHROM of length* $\ell_m + \ell_{\tilde{r}} + \ell_a + \ell_r$*. Then the following encryption scheme is a (pure) unclonable encryption scheme relative to* $\mathcal{U}$ *with keys in* $\{0,1\}^{\ell_k}$.

1. $\mathrm{Enc}^{\vec{U}}(1^n, k, m)$*:*

   (a) *Sample* $r_1 \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$*,* $r_2 \leftarrow \{0,1\}^{\ell_r}$

   (b) *Output* $X^k U \left|m, r_1, 0^{\ell_a(n)}, r_2\right\rangle$.

2. $\mathrm{Dec}^{\vec{U}}(1^n, k, \rho)$*: computes* $\sigma = U^\dagger X^k \rho X^k U$*, then measures the first register.*

Proof. Correctness follows by observation.

To prove security, we will define the following reduction. Let $C^{\vec{U}, \mathrm{Enc}^{\vec{U}}}, A^{\vec{U}}, B^{\vec{U}}$ be any attacker against Enc making at most t queries to the encryption oracle. We will define an attacker $\widetilde{C}^{\vec{V}, \mathrm{Enc}^{\vec{V}}}, \widetilde{A}^{\vec{V}}, \widetilde{B}^{\vec{V}}$ against $\widetilde{\mathrm{Enc}}$.

In particular, let $\widetilde{E}^{\vec{V}}$ be the purification of $\widetilde{\mathrm{Enc}}^{\vec{V}}$. Let $\widetilde{\mathcal{CT}} = \{0,1\}^{\ell_m} \times \{0,1\}^{\ell_{\tilde{r}}} \times \{0,1\}^{\ell_{\tilde{a}}}$ and let $\mathcal{CT} = \widetilde{\mathcal{CT}} \times \{0,1\}^{\ell_r}$. Note that $\mathcal{H}(\widetilde{\mathcal{CT}}), \mathcal{H}(\mathcal{CT})$ are the ciphertext spaces of Enc and $\widetilde{\mathrm{Enc}}$ respectively. Let $d = \frac{1}{2}\min(\ell_k, \ell_r)$.

We will define $\widetilde{C}^{\vec{V}, \widetilde{\mathrm{Enc}}^{\vec{V}}(\tilde{k}, \cdot)}$ as follows

1. Sample $R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$.[5] Write $R = \{r_1, \ldots, r_t\}$ in some arbitrary order.

2. Set $S_1 = \{(x, r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$

3. Sample $S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - |S_1|}$

4. Set $S_2 = S_1 \cup S'$

5. Sample $U_1 \leftarrow Haar(S_2)$

6. Sample $U_2 \leftarrow Haar(\mathcal{CT} \setminus S_2)$

[5] Recall this means to sample a uniformly random subset of $\{0,1\}^{\ell_r}$ of size t.

7. Sample $k \leftarrow \mathcal{CT}$
8. Define $\mathcal{O}(m)$ as follows
   (a) On the ith query, set $r = r_i$.
   (b) Output $X^k U_1(\widetilde{\text{Enc}}^{\vec{V}}(\widetilde{k}, m) \otimes |r\rangle)$
9. Run $C^{\vec{U_2},\mathcal{O}} \to (m_0, m_1, \mathbf{st})$
10. Output challenge m_0, m_1, receive ciphertext $|\phi\rangle$
11. Set $|\psi\rangle = X^k U_1(|\phi\rangle \otimes |r_t\rangle)$
12. Run $C^{\vec{U_2},\mathcal{O}}(|\psi\rangle, \mathbf{st}) \to \sigma_{\mathbf{AB}}$
13. Output $\widetilde{\mathbf{A}} = (k, R, U_1, U_2, \mathbf{A})$
14. Output $\widetilde{\mathbf{B}} = (k, R, U_1, U_2, \mathbf{B})$

We will then define $\widetilde{A}^{\vec{V}}(\widetilde{k}, \widetilde{\mathbf{A}})$ as follows

1. Parse $\widetilde{\mathbf{A}} = (k, R, U_1, U_2, \mathbf{A})$
2. Let $c_R\widetilde{E}_{\widetilde{k}}^{\vec{V}}$ be the unitary $\widetilde{E}_{\widetilde{k}}^{\vec{V}}$ controlled on the following register containing a string in R. Formally,
$$c_R\widetilde{E}_{\widetilde{k}}^{\vec{V}} := \widetilde{E}_{\widetilde{k}}^{\vec{V}} \otimes \sum_{r \in R} |r\rangle\langle r| + I \otimes \left(I - \sum_{r \in R} |r\rangle\langle r|\right)$$
3. Set $U_1' = U_1 \cdot c\widetilde{E}_k^{\vec{V}}$
4. Set $U = U_1' U_2$
5. Run $A^{\vec{U}}(k, \mathbf{A}) \to b_A$

$\widetilde{B}^{\vec{V}}(k, \widetilde{\mathbf{B}})$ will be defined symmetrically.
The proof of security then follows by applying a sequence of hybrids described in Figures 1 to 3. In particular, we will show that for each i, $|\Pr[G_i \to 1] - \Pr[G_{i-1} \to 1]| \leq \mathsf{negl}(n)$.

Lemma 4.5. $G_1 \equiv G_2$

Proof. The two games are equivalent other than the fact that in G_2, the values $r_1, \ldots, r_t$ are sampled in the beginning instead of when they are used. But the time when they are sampled does not affect the overall distribution of the game, and so the claim follows. □

Lemma 4.6. $|\Pr[G_3 \to 1] - \Pr[G_2 \to 1]| \leq \mathsf{negl}(n)$

G_1:
$k \leftarrow \{0,1\}^{\ell_k}$
$U \leftarrow Haar(\mathcal{CT})$
$C^{\vec{U},\mathcal{O}} \rightarrow (m_0, m_1, \mathbf{st})$
$b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$C^{\vec{U},\mathcal{O}}(|\phi_b\rangle, \mathbf{st}) \rightarrow \sigma_{\mathbf{AB}}$
$A^{\vec{U}}(k, \mathbf{A}) \rightarrow b_A$
$B^{\vec{U}}(k, \mathbf{B}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow \{0,1\}^{\ell_r}$
Output $\text{Enc}^{\vec{U}}(k, m; r_{orig}, r)$

Hybrid 1: The security game for unclonable encryption

G_2:
$k \leftarrow \{0,1\}^{\ell_k}$
$R : \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
$t = 1$
$U \leftarrow Haar(\mathcal{CT})$
$C^{\vec{U},\mathcal{O}} \rightarrow (m_0, m_1, \mathbf{st})$
$b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$C^{\vec{U},\mathcal{O}}(|\phi_b\rangle, \mathbf{st}) \rightarrow \sigma_{\mathbf{AB}}$
$A^{\vec{U}}(k, \mathbf{A}) \rightarrow b_A$
$B^{\vec{U}}(k, \mathbf{B}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$t \leftarrow t + 1$
Output $\text{Enc}^{\vec{U}}(k, m; r_{orig}, r)$

Hybrid 2: We sample the randomness used for encryption at the beginning of the game.

Figure 1: The hybrid games used in the proof of Theorem 4.4.

G_3:
$k \leftarrow \{0,1\}^{\ell_k}$
$R : \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
$t = 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - |S_1|}$
$S_2 \leftarrow S_1 \cup S'$
$U_1 \leftarrow Haar(S_2)$
$U_2 \leftarrow Haar(\mathcal{CT} \setminus S_2)$
$U \leftarrow U_1 U_2$
$C^{\vec{U},\mathcal{O}} \rightarrow (m_0, m_1, \mathbf{st})$
$b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$C^{\vec{U},\mathcal{O}}(|\phi_b\rangle, \mathbf{st}) \rightarrow \sigma_{\mathbf{AB}}$
$A^{\vec{U}}(k, \mathbf{A}) \rightarrow b_A$
$B^{\vec{U}}(k, \mathbf{B}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$t \leftarrow t + 1$
Output $\mathrm{Enc}^{\vec{U}}(k, m; r_{orig}, r)$

Hybrid 3: We split the Haar random unitary U into two random unitaries: U_1 acting on a superset of the encryption randomness and U_2 acting on the orthogonal space.

G_4:
$k \leftarrow \{0,1\}^{\ell_k}$
$R : \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
$t = 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - |S_1|}$
$S_2 \leftarrow S_1 \cup S'$
$U_1 \leftarrow Haar(S_2)$
$U_2 \leftarrow Haar(\mathcal{CT} \setminus S_2)$
$U \leftarrow U_1 U_2$
$C^{\vec{U}_2,\mathcal{O}} \rightarrow (m_0, m_1, \mathbf{st})$
$b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$C^{\vec{U}_2,\mathcal{O}}(|\phi_b\rangle, \mathbf{st}) \rightarrow \sigma_{\mathbf{AB}}$
$A^{\vec{U}}(k, \mathbf{A}) \rightarrow b_A$
$B^{\vec{U}}(k, \mathbf{B}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$t \leftarrow t + 1$
Output $X^k U_1 \left|m, r_{orig}, 0^{\ell_a}, r\right\rangle$

Hybrid 4: We rewrite encryption as $X^k U_1 |b, r\rangle$, and we replace C's oracle access to U with oracle access to U_2.

Figure 2: The hybrid games used in the proof of Theorem 4.4.

G_5:
$k \leftarrow \{0,1\}^{\ell_k}$
$R : \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
$t = 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \left(\frac{|\mathcal{CT}|}{2^d} - |S_1|\right)$
$S_2 \leftarrow S_1 \cup S'$
$\widetilde{k} \leftarrow \{0,1\}^n$
$V \leftarrow \widetilde{\mathcal{V}}_n$
$U_1 \leftarrow Haar(S_2)$
$U_1' \leftarrow U_1' \cdot c_R \widetilde{E}_{\widetilde{k}}^{\vec{V}}$
$U_2 \leftarrow Haar(\mathcal{CT} \setminus S_2)$
$U \leftarrow U_1' U_2$
$C^{\vec{U},\mathcal{O}}(|\phi_b\rangle, \mathbf{st}) \rightarrow (m_0, m_1, \mathbf{st})$
$b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$C^{\vec{U}_2,\mathcal{O}}(|\phi_b\rangle) \rightarrow \sigma_{\mathbf{AB}}$
$A^{\vec{U}}(k, \mathbf{A}) \rightarrow b_A$
$B^{\vec{U}}(k, \mathbf{B}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$t \leftarrow t + 1$
Output $X^k U_1' \left|m, r_{orig}, 0^{\ell_a}, r\right\rangle$

Hybrid 5: We sample V, and then set U_1 to first apply $\widetilde{E}_k^{\vec{V}}$.

G_6:
$V \leftarrow \mathcal{V}_n$
$\widetilde{C}^{\vec{V},\widetilde{\mathrm{Enc}}^{\vec{V}}(\widetilde{k},\cdot)} \rightarrow (m_0, m_1, \mathbf{st})$ $b \leftarrow \{0,1\}$
$|\phi_b\rangle \leftarrow \mathcal{O}(m_b)$
$\widetilde{C}^{\vec{V},\widetilde{\mathrm{Enc}}^{\vec{V}}(\widetilde{k},\cdot)}(|\phi_b\rangle, \mathbf{st}) \rightarrow \widetilde{\sigma}_{\mathbf{AB}}$
$\widetilde{A}^{\widetilde{V}}(k, \widetilde{\mathbf{A}}) \rightarrow b_A$
$\widetilde{B}^{\widetilde{V}}(k, \widetilde{\mathbf{B}}) \rightarrow b_B$
Output 1 if and only if $b = b_A = b_B$

Hybrid 6: The security game for the secure scheme under $\widetilde{\mathcal{V}}$.

Figure 3: The hybrid games used in the proof of Theorem 4.4.

Proof. This follows immediately from our "unitary reprogramming lemma" Lemma 3.1 by setting S_1 to be S_1 from G_3, $N = |\mathcal{CT}|$ $M_2 = \frac{|\mathcal{CT}|}{2^d}$, $M_2 = |S_1| = t \cdot |\widetilde{\mathcal{CT}}|$. It is clear that

$$\frac{M_1}{M_2} = \frac{|\widetilde{\mathcal{CT}}|}{\frac{|\mathcal{CT}|}{2^d}} = \frac{\frac{|\mathcal{CT}|}{2^{\ell_r}}}{\frac{|\mathcal{CT}|}{2^d}} = 2^{d-\ell_r} \leq 2^{-\ell_r/2} = \mathsf{negl}(n)$$

and

$$\frac{M_2}{N} = \frac{|\mathcal{CT}| \cdot 2^{-d}}{|\mathcal{CT}|} = 2^{-d} = \mathsf{negl}(n)$$

Furthermore, the only information used in the game about U_1, U_2 is the values in R, which is less information than contained in S_1. And so the lemma applies. □

Lemma 4.7. $|\Pr[G_4 \to 1] - \Pr[G_3 \to 1]| \leq \mathsf{negl}(n)$

This claim is significantly more complicated, and so the proof is deferred to Appendix A. The intuition is that $\widetilde{C}$ cannot query U on any state with more than negligible support on S_2. In particular, the only information about S_2 which is revealed to $\widetilde{C}$ are ciphertext outputs, which are of the form $X^k |\psi\rangle$ for some $|\psi\rangle$ in the support of S_2. Since only one sample of these is provided, these look like strings of the form $k \oplus s$ for some $s \in S_2$, and given many samples of strings of this form it should be difficult to find a single string in S_2. Some care needs to be taken to ensure that these facts hold with unitary queries to U, and the key idea to handle this is the fact that unitary queries to U_1 can be simulated efficiently using a reflection oracle around states with support in S_2. We then reduce to a Grover's search bound on the ability to find $s \in S_2$ given all strings of the form $s \oplus k$ as well as a reflection oracle around S_2.

Lemma 4.8. $G_5 \equiv G_4$

Proof. This follows immediately from unitary invariance. In particular, $c_R \widetilde{E}_{\widetilde{k}}^{\vec{V}}$ is the identity on all basis states not ending with a string in R, and so in particular is identity on all states with support in $\mathcal{CT} \setminus S_1 \supseteq \mathcal{CT} \setminus S_2$, just as U_1 is. □

Lemma 4.9. $G_6 \equiv G_5$

Proof. This follows from the definitions of $\widetilde{A}, \widetilde{B}, \widetilde{C}$. □

□

5 Unclonable encryption in the QROM

Here, we observe that (reusable) unclonable encryption in the quantum random oracle model readily follows from prior work [AKL+22, AKL23].

Theorem 5.1. *For any message length $\ell_m = \mathsf{poly}(n)$, there exists a pure many-time unclonable encryption scheme in the QROM.*

Proof. Prior work [BL20, AKL+22, AKL23] has established that the following is a one-time unclonable encryption scheme, where F is a random oracle, $k \leftarrow \{0,1\}^n$, and $m \in \{0,1\}^{\ell_m}$.

- $\mathrm{Enc}^F(1^n, k, m)$:

- Sample $x \leftarrow \{0,1\}^n$
- Output $E_k |m\rangle |x\rangle = |m \oplus F(x)\rangle H^k |x\rangle$

To complete the proof, we demonstrate a compiler that takes any pure one-time unclonable encryption scheme in the QROM and outputs a pure many-time unclonable encryption scheme in the QROM. Let $(\mathrm{Enc}^F, \mathrm{Dec}^F)$ be a one-time scheme, with encryption unitary E_k and randomness space $\mathcal{R}$. The many-time scheme is the following.

- $\widetilde{\mathrm{Enc}}^F(1^n, k, m)$:
  - Sample $s \leftarrow \{0,1\}^n$.
  - Sample $r \leftarrow \mathcal{R}$.
  - Output $\widetilde{E}_k |m\rangle |r\rangle |s\rangle = (E_{F(k,s)} |m\rangle |r\rangle) |s\rangle$.
- $\widetilde{\mathrm{Dec}}^F(1^n, k, \rho)$: Parse ρ as $\rho' \otimes |s\rangle\langle s|$ and output $\mathrm{Dec}^F(1^n, F(k,s), \rho')$.

The many-time security of $(\widetilde{\mathrm{Enc}}^F, \widetilde{\mathrm{Dec}}^F)$ reduces in a standard way to the one-time security of $(\mathrm{Enc}^F, \mathrm{Dec}^F)$ by re-sampling $F(k,\cdot)$ at the point s sampled when generating the challenge ciphertext.

□

The main result of this paper follows as a direct corollary of Theorem 5.1 and Theorem 4.4.

Corollary 5.2. *Let n be the security parameter. For any message length $\ell_m = \mathsf{poly}(n)$, there exists reusable unclonable encryption with n-bit keys in the Haar random oracle model (QHROM).*

References

[ABGL25a] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. Pseudorandom unitaries in the haar random oracle model. In *Advances in Cryptology – CRYPTO 2025: 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2025, Proceedings, Part II*, page 301–333, Berlin, Heidelberg, 2025. Springer-Verlag.

[ABGL25b] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. Pseudorandomness in the (inverseless) haar random oracle model. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 138–166, Cham, 2025. Springer Nature Switzerland.

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024*, pages 226–254, Cham, 2024. Springer Nature Switzerland.

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 212–241, Cham, 2022. Springer Nature Switzerland.

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, page 66–98, Berlin, Heidelberg, 2023. Springer-Verlag.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 208–236, Cham, 2022. Springer Nature Switzerland.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[BBC+24] Pierre Botteron, Anne Broadbent, Eric Culf, Ion Nechita, Clément Pellegrini, and Denis Rochette. Towards Unconditional Uncloneable Encryption. 10 2024.

[BBC26] Archishna Bhattacharyya, Anne Broadbent, and Eric Culf. The uncloneable bit exists, 2026.

[BC26] Archishna Bhattacharyya and Eric Culf. Uncloneable encryption from decoupling. *Nature Physics*, 2026. published online 4 Feb 2026.

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable Quantum Encryption via Oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[ÇGR24] Alper Çakan, Vipul Goyal, and Justin Raizes. How to delete without a trace: Certified deniability in a quantum world. Cryptology ePrint Archive, Paper 2024/1832, 2024.

[CLX26] Andrea Coladangelo, Qipeng Liu, and Ziyi Xie. The Curious Case of "XOR Repetition" of Monogamy-Of-Entanglement Games. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 41:1–41:20, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[dBhdb] Niel de Beaudrap (https://quantumcomputing.stackexchange.com/users/124/niel-de beaudrap). Is the diamond norm subadditive under composition? Quantum Computing Stack Exchange. URL:https://quantumcomputing.stackexchange.com/questions/7043/is-the-diamond-norm-subadditive-under-composition (version: August 18, 2019).

[DH08] Catalin Dohotaru and Peter Høyer. Exact quantum lower bound for grover's problem. *Quantum Inf. Comput.*, 9:533–540, 2008.

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[HY26] Minki Hhan and Shogo Yamada. Pseudorandom function-like states from common haar unitary. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Theory of Cryptography*, pages 134–165, Cham, 2026. Springer Nature Switzerland.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 126–152, Cham, 2018. Springer International Publishing.

[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*, STOC 2023, page 1589–1602, New York, NY, USA, 2023. Association for Computing Machinery.

[KQT25] William Kretschmer, Luowen Qian, and Avishay Tal. Quantum-computable one-way functions without one-way functions. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 189–200, New York, NY, USA, 2025. Association for Computing Machinery.

[Kre21] William Kretschmer. Quantum Pseudorandomness and Classical Complexity. *Leibniz Int. Proc. Inf.*, 197:2:1–2:20, 2021.

[MH25] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 806–809, New York, NY, USA, 2025. Association for Computing Machinery.

[PRV26] Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan. Cloning Games, Black Holes and Cryptography. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 109:1–109:21, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[SML+25] Thomas Schuster, Fermi Ma, Alex Lombardi, Fernando Brandao, and Hsin-Yuan Huang. Strong random unitaries and fast scrambling, 2025.

A Proof of Lemma 4.7

The goal of this section will be to prove the following.

Lemma A.1 (Lemma 4.7 restated)**.** $|\Pr[G_3 \to 1] - \Pr[G_4 \to 1]| \leq \mathsf{negl}(n)$*, where* G_2, G_3 *are as described in Figures 1 and 2.*

To do this, it suffices to show that C will never make a query to its first oracle that has weight on the support of S_2. In particular, the claim will immediately follow from the following lemma

Lemma A.2. *Let* $C^{(\cdot)}$ *be any oracle algorithm making at most* $t \leq \mathsf{poly}(n)$ *queries. Let* $\ell_m, \ell_k, \ell_{\widetilde{k}}, \ell_r, \ell_{\widetilde{r}}, \ell_a, \mathcal{CT}, \widetilde{\mathcal{CT}}$ *be as in Theorem 4.4 and its proof. Consider the following game* $FindSEnc(C)$

1. $k \leftarrow \{0,1\}^{\ell_k}$
2. $R = \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
3. $S_1 \leftarrow \{(x, r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
4. $S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - |S_1|}$
5. $S_2 \leftarrow S_1 \cup S'$
6. $U_1 \leftarrow Haar(S_2)$
7. $U_2 \leftarrow Haar(\mathcal{CT} \setminus S_2)$
8. $U \leftarrow U_1 U_2$
9. $C^{\vec{U},\mathcal{O}} \to s$
10. C *wins if* $s \in S_2$

where $\mathcal{O}(m)$ *is the oracle which on the* i*th query responds with*

1. *Sample* $r_{orig} \leftarrow \{0,1\}^{\ell_{\widetilde{r}}}$
2. *Output* $X^k U_1 \left|m, r_{orig}, 0^{\ell_a}, r_i\right\rangle$

Then

$$\Pr[FindSEnc(C) \to 1] \leq \mathsf{negl}(n)$$

We will prove the lemma by reducing to the information-theoretic lower bound on unstructured search.

Theorem A.3 (Grover's search lower bound [DH08])**.** *Let* $N \in \mathbb{N}$ *and for* $k \in [N]$*, let* $\delta_k := R_{\{k\}}$*. Let* $\mathcal{A}^{(\cdot)}$ *be any QPT oracle algorithm making at most* T *queries such that*

$$\Pr_{k\leftarrow[N]}\left[\mathcal{A}^{\delta_k} \to k\right] \geq p$$

Then

$$T \geq \frac{\sqrt{N}}{2}\left(1 + \sqrt{p} - \sqrt{1-p} - \frac{2}{\sqrt{N}}\right)$$

We will rely on the following useful concentration bound.

Lemma A.4 (Sampling Chernoff bound (Section 5 of [Hoe63]))**.** *Let $N, M \in \mathbb{N}$, $\delta > 0$, and let $S \subseteq [N]$ be any subset. Then*

$$\Pr_{S' \leftarrow \binom{[N]}{M}}\left[|S \cap S'| \geq (1+\delta)\frac{M \cdot |S|}{N}\right] \leq e^{-\frac{\delta^2 \cdot M \cdot |S|}{3N}}$$

Our search problem is of a slightly different flavor than standard unstructured search. In particular, to prove Lemma A.2, we will reduce to the information-theoretic hardness of the following task: for a random set S, given access to a reflection oracle for S as well as a classical description of the set $\{s \oplus k : s \in S\}$ for a random k, the goal is to output a single value $s \in S$.

Lemma A.5. *Let $\ell_n(n), \ell_k(n), M(n)$ be functions. Define $N = 2^{\ell_n}$. Let $C^{(\cdot)}$ be any oracle algorithm making at most t queries. Given a set $S \subseteq \mathcal{P}(\{0,1\}^{\ell_n})$ and a value $k \in \{0,1\}^{\ell_k}$, define $S \oplus k = \{s \oplus (k||0^{\ell_n - \ell_k}) : s \in S\}$. Consider the following game $FindSXOR(C)$*

1. *Sample $S \leftarrow \binom{[N]}{M}$*
2. *Sample $k \leftarrow \{0,1\}^{\ell_k}$*
3. *Run $C^{R_S}(S \oplus k) \rightarrow s$*
4. *Output 1 if $s \in S$*

Then $\Pr[C \text{ wins}] \leq \frac{9t^2M^3}{2^{3\ell_n - 2\ell_k}} - 2^{\ell_n - \ell_k} \cdot e^{-\frac{4 \cdot M}{3 \cdot 2^{\ell_n - \ell_k}}}$

Proof. We begin by defining the following notation. For $x \in \{0,1\}^{\ell_n}$, define $x_{\leq \ell_k}$ to be the first ℓ_k bits of x, and define $x_{>\ell_k}$ to be the last $\ell_n - \ell_k$ bits of x. For $k \in \{0,1\}^{\ell_k}$, we will for simplicity write $x \oplus k \coloneqq x \oplus (k||0^{\ell_n - \ell_k})$.

For $S \subseteq \{0,1\}^{\ell_n}, v \in \{0,1\}^{\ell_n - \ell_k}$, define $S_v = \{x \in S : x_{>\ell_k} = v\}$.

We then reduce to the lower bound for Grover's search Theorem A.3. In particular, for a random $k \in \{0,1\}^{\ell_n}$, given quantum query access to $\delta_k \coloneqq R_{\{k\}}$, we give an algorithm $\mathcal{A}^{\delta_k}$ to find k

1. Sample $S' \leftarrow \binom{[N]}{M}$
2. If there exists some $v \in \{0,1\}^{\ell_n - \ell_k}$ such that $|S_v| \geq \frac{2M}{2^{\ell_n - \ell_k}}$, output $\perp$.
3. Define $\mathcal{O}|s\rangle$ to be the coherent version of the following process
   (a) For each $s' \in S'$ such that $s'_{>\ell_k} = s_{>\ell_k}$, run $\delta_k(s \oplus s')$. If the result is 1, output 1.
   (b) If the result is 0 for all such s', output 0.

   Formally,

$$\begin{aligned}\mathcal{O} &\coloneqq I - 2 \sum_{\substack{s' \in S' \\ s'_{>\ell_k} = s_{>\ell_k}}} |s' \oplus k\rangle\langle s' \oplus k| \\ &= \prod_{\substack{s' \in S' \\ s'_{>\ell_k} = s_{>\ell_k}}} X^{s'} \delta_k X^{s'}\end{aligned} \tag{10}$$

4. Run $C^{\mathcal{O}}(S') \to s$

5. Pick a random $s' \in S'$, output $s - s'$

Clearly, this algorithm makes at most $t \cdot \frac{M}{2^{\ell_n - \ell_k}}$ queries.

Note that for each $v \in \{0,1\}^{\ell_n - \ell_k}$, by Lemma A.4 we have that

$$\Pr\left[|S_v| \geq \frac{2M}{2^{\ell_n - \ell_k}}\right] \leq e^{-\frac{4 \cdot M}{3 \cdot 2^{\ell_n - \ell_k}}}$$

Define

$$\gamma := 2^{\ell_n - \ell_k} \cdot e^{-\frac{4 \cdot M}{3 \cdot 2^{\ell_n - \ell_k}}}$$

by union bound, the algorithm passes step 2 with probability

$$\geq 1 - \gamma$$

Thus, it only remains to lower bound its success probability.

Define $S := S' \oplus k = \{s' \oplus k : s' \in S'\}$. Note that S is also a uniformly random set, and from the perspective of C, S' is identically distributed to $S \oplus k$. It is not hard to see that $\mathcal{O}$ exactly implements R_S.

If C succeeds with probability ϵ in its own game, then by union bound, with probability $\epsilon - \gamma$, in step 4 $\mathcal{A}^{\delta_k}$ produces some $s \in S = S' \oplus k$. But note that if $s \in S$, then there exists exactly one point $s' \in S'$ such that $s \oplus s' = k$. And so $\mathcal{A}^{\delta_k}$ succeeds with probability $\frac{1}{M} \cdot (\epsilon - \gamma)$.

And so we have an algorithm for unstructured search succeeding with probability $\frac{\epsilon - \gamma}{M}$ and making at most $\frac{t \cdot M}{2^{\ell_n - \ell_k}}$ queries.

Set $p := \frac{\epsilon - \gamma}{M}$

By Theorem A.3, we have

$$\begin{aligned}
\frac{t \cdot M}{2^{\ell_n - \ell_k}} &\geq \frac{\sqrt{N}}{2}\left(1 + \sqrt{p} - \sqrt{1-p} - \frac{2}{\sqrt{N}}\right) \\
&= \frac{\sqrt{N}}{2}\left((1 - \sqrt{1-p}) + \sqrt{p}\right) - 1 \\
&\geq \frac{\sqrt{Np}}{2} - 1 \\
&\geq \frac{\sqrt{\frac{N(\epsilon-\gamma)}{M}}}{3}
\end{aligned} \tag{11}$$

And so

$$\epsilon \leq \frac{9t^2M^3}{2^{3\ell_n - 2\ell_k}} - \gamma$$

□

Corollary A.6. *Let $\ell_n(n), \ell_k(n)$ be any polynomials such that $\ell_k < \ell_n$. Let $\ell_M(n)$ be any polynomial satisfying $\ell_M \geq \ell_n - \frac{\ell_k}{2}$ and $\ell_n - \ell_M \geq n^c$ for some $c > 0$. Define $N = 2^{\ell_n}$, $M(n) = 2^{\ell_M}$. Let $C^{(\cdot)}$ be any oracle algorithm making at most $t = \mathsf{poly}(n)$ queries. Given a set $S \subseteq \mathcal{P}(\{0,1\}^{\ell_n})$ and a value $k \in \{0,1\}^{\ell_k}$, define $S \oplus k = \{s \oplus (k||0^{\ell_n - \ell_k}) : s \in S\}$. Consider the game FindSXOR(C) as in Lemma A.5. Then* $\Pr[C \text{ wins}] \leq \mathsf{negl}(n)$

Proof. Note that $2(\ell_n - \ell_M) \leq \ell_k$, and so since increasing the length of the key only decreases C's advantage, we can assume without loss of generality that $\ell_k = 2(\ell_n - \ell_M)$.

Observe that $\ell_n - \ell_k = \ell_n - 2\ell_n + 2\ell_M = 2\ell_M - \ell_n$.

Plugging in Lemma A.5, we get

$$\begin{aligned}
\Pr[C \text{ wins}] &\leq \frac{9t^2M^3}{2^{3\ell_n - 2\ell_k}} - 2^{\ell_n - \ell_k} \cdot e^{-\frac{4 \cdot M}{3 \cdot 2^{\ell_n - \ell_k}}} \\
&\leq \frac{9t^2 2^{3\ell_M}}{2^{\ell_n + 2\ell_M}} - \exp\left(\ln(2)(2\ell_M - \ell_n) - \frac{4 \cdot 2^{\ell_M}}{3 \cdot 2^{2\ell_M - \ell_n}}\right) \\
&= 9t^2 \cdot 2^{\ell_M - \ell_n} - \exp\left(\ln(2)(2\ell_M - \ell_n) - \frac{4}{3} \cdot 2^{\ell_n - \ell_M}\right) \qquad (12) \\
&\leq \mathsf{poly}(n) \cdot 2^{-n^c} - \exp\left(\mathsf{poly}(n) - \frac{4}{3} \cdot 2^{n^c}\right) \\
&\leq \mathsf{negl}(n)
\end{aligned}$$

□

Finally, before we begin the proof of Lemma A.2, we will cite an important fact about random unitaries.

Lemma A.7 (Modified Lemma 4.1 from [AGKL24])**.** *Let S be a set. Let $n, s, t \in \mathbb{N}$ and $\vec{x} = (x_1, \ldots, x_s) \in S^s$ such that $\vec{x}$ has no repeating coordinates. Let*

$$\rho \coloneqq \mathop{\mathbb{E}}_{U \leftarrow Haar(S)} \left[\bigotimes_{j=1}^{s} \left(U \left|0\right\rangle\!\left\langle 0\right| U^\dagger \right)^{\otimes t} \right]$$

and let

$$\sigma \coloneqq \bigotimes_{j=1}^{t} \mathop{\mathbb{E}}_{\left|\phi_j\right\rangle \leftarrow Haar(S)} \left[\left|\phi_j\right\rangle\!\left\langle \phi_j\right|^{\otimes t} \right]$$

Then

$$TD(\rho, \sigma) \leq \frac{s^2 t}{|S|}$$

Remark A.8. Lemma 4.1 from [AGKL24] defined the set S as explicitly $\{0,1\}^n$, but the same proof applies.

We will now proceed to the proof of Lemma A.2.

Proof. Given an adversary C for $FindSEnc$, we will come up with an adversary D for $FindSXOR$ (with $N = |\mathcal{CT}|$ and $M = \frac{|\mathcal{CT}|}{2^d} - t$) such that

$$|\Pr[FindSEnc(C) \to 1] - \Pr[FindSXOR(D) \to 1]| \leq \mathsf{negl}(n)$$

Lemma A.2 will then follow immediately from Lemma A.5.

Let $\vec{\mathrm{Sim}}^{R_S}$ be the simulator from Corollary 2.19 with $t_{max} = t$. $D^{R_S}(S \oplus k)$ will simulate $C^{\vec{U}, \mathcal{O}}$ as follows

1. D^{R_S} will replace all queries to $\vec{U}$ with queries to $\vec{\mathrm{Sim}}^{R_S}$

2. $D^{R_S}(S \oplus k)$ will replace all queries to $\mathcal{O}$ with the following oracle, which we will name $\mathrm{Sim}_{\mathrm{Enc}}(m)$:
   (a) Sample $r \leftarrow S \oplus k$
   (b) Output r
3. At the end, $D^{R_S}(S \oplus k)$ will output the same value as $C^{\vec{\mathrm{Sim}}^{R_S}}$

To show

$$|\Pr[FindSEnc(C) \to 1] - \Pr[FindSXOR(D) \to 1]| \leq \mathsf{negl}(n)$$

we will proceed through a sequence of hybrids $H_0, \ldots, H_f$ with $H_0 = FindSEnc(C)$ and $H_f = FindSXOR(D)$. The hybrids are defined in Figures 4 to 6.

Claim 1. $|\Pr[H_1 \to 1] - \Pr[H_0 \to 1]| \leq \mathsf{negl}(n)$

Proof. Note that conditioned on R containing no duplicates in H_0, H_0 and H_1 are identically distributed. But the probability that R contains a duplicate is

$$\leq \frac{t^2}{2^{\ell_r}} = \mathsf{negl}(n)$$

by the union bound. □

Claim 2. $|\Pr[H_2 \to 1] - \Pr[H_1 \to 1]| \leq \mathsf{negl}(n)$

Proof. This follows immediately from Lemma A.7 setting $S = S_2$ and $s = t$ since

$$\frac{t^2}{|S_2|} \leq \frac{\mathsf{poly}(n)}{\frac{|\mathcal{CT}|}{2^d} - t \cdot |\widetilde{\mathcal{CT}}|} = \mathsf{negl}(n)$$

□

Claim 3. $H_3 \equiv H_2$

Proof. Observe that in H_2, each $(m, r_{orig}, 0^{\ell_a}, r_i)$ is unique since each r_i is distinct. Thus, H_3 is the same as H_2, but we simply sample each $|\phi_s\rangle$ later. This makes no difference to the games output probability. □

Claim 4. $H_4 \equiv H_3$

Proof. Note that the mixed state corresponding to $|\phi\rangle \leftarrow HaarSt(S_2)$ is exactly the maximally mixed state. This is the same density matrix one would obtain from sampling a random string from S_2. And so since only one copy of $|\phi\rangle$ is ever used, replacing it with a random string has no effect on the hybrid. □

Claim 5. $|\Pr[H_5 \to 1] - \Pr[H_4 \to 1]| \leq \mathsf{negl}(n)$

Proof. This follows immediately from Corollary 2.19. □

Claim 6. $|\Pr[H_6 \to 1] - \Pr[H_5 \to 1]| \leq \mathsf{negl}(n)$

$H_0 = FindSEnc(C)$:
$k \leftarrow \{0,1\}^{\ell_n}$
$R = \{r_i\}_{i\in[t]} \leftarrow \{0,1\}^{\ell_r}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - |S_1|}$
$S_2 \leftarrow S_1 \cup S'$
$U_1 \leftarrow Haar(S_2)$
$U_2 \leftarrow Haar(\{0,1\}^n \setminus S_2)$
$C^{\vec{U}_2,\mathcal{O}} \to s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$i \leftarrow i+1$
Output $X^k U_1 |m, r_{orig}, 0, r_i\rangle$

Hybrid 0: The game $FindSEnc(C)$.

H_1:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - t\cdot|\widetilde{\mathcal{CT}}|}$
$S_2 \leftarrow S_1 \cup S'$
$U_1 \leftarrow Haar(S_2)$
$U_2 \leftarrow Haar(\{0,1\}^n \setminus S_2)$
$C^{\vec{U}_2,\mathcal{O}} \to s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$i \leftarrow i+1$
Output $X^k U_1 |m, r_{orig}, 0, r_i\rangle$

Hybrid 1: Here we guarantee that there are no collisions in R.

Figure 4: The hybrid games used in the proof of Lemma A.2.

Proof. It is sufficient to bound the probability that given access to $R_{S_2}, \mathcal{O}$ as in H_5, you can output something in S_1.

Note that the probability that in H_5, $\mathcal{O}$ ever outputs something in S_1 is bounded by

$$t \cdot \frac{|S_1|}{|S_2|} = \mathsf{poly}(n) \cdot \frac{2^d \cdot |\widetilde{\mathcal{CT}}|}{|\mathcal{CT}|} \leq 2^{d-\ell_r} \leq \mathsf{negl}(n)$$

Thus, the problem reduces to unstructured search. We want to bound the probability that given polynomial queries to R_{S_2}. This is clearly bounded by the probability that given polynomial queries to R_{S_1}, you can find something in S_1. But this is negligible by optimality of Grover's. □

Claim 7. $H_f \equiv H_6$

Proof. These are identical games by observation. □

We then conclude the proof of the lemma by applying apply Corollary A.6. In particular, we set $S = S$, $\ell_n = \ell_m + \ell_a + \ell_{\tilde{r}} + \ell_r = |\mathcal{CT}|$, $\ell_k = \ell_k$, $\ell_M = \ell_n - d$. We then observe that $d = \frac{1}{2}\min(\ell_k, \ell_r)$, $\ell_M \geq \ell_n - \frac{\ell_k}{2}$ and $\ell_n - \ell_M = d \geq n^c$ for some $c > 0$, and so Corollary A.6 gives us $\Pr[H_f \to 1] \leq \mathsf{negl}(n)$.

The hybrids then imply that $\Pr[H_1 \to 1] \leq \mathsf{negl}(n)$, and so we are done. □

H_2:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \left(\frac{|\mathcal{CT}|}{2^d} \overset{\mathcal{CT}}{-t \cdot |\widetilde{\mathcal{CT}}|}\right)$
$S_2 \leftarrow S_1 \cup S'$
$\{|\phi_s\rangle\}_{s \in S_1} \leftarrow HaarSt(S)$
$U_2 \leftarrow Haar(\{0,1\}^n \setminus S_2)$
$C^{\vec{U}_2, \mathcal{O}} \rightarrow s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$r_{orig} \leftarrow \{0,1\}^{\ell_{\tilde{r}}}$
$r \leftarrow r_i$
$i \leftarrow i + 1$
Output $X^k \left|\phi_{m, r_{orig}, 0^{\ell_a}, r}\right\rangle$

Hybrid 2: Instead of sampling $U_1 \leftarrow Haar(S_2)$, we sample each $|\phi_s\rangle = U_1 |s\rangle$ from $HaarSt(S_2)$.

H_3:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \left(\frac{|\mathcal{CT}|}{2^d} \overset{\mathcal{CT}}{-t \cdot |\widetilde{\mathcal{CT}}|}\right)$
$S_2 \leftarrow S_1 \cup S'$
$U_2 \leftarrow Haar(\{0,1\}^n \setminus S_2)$
$C^{\vec{U}_2, \mathcal{O}} \rightarrow s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$|\phi\rangle \leftarrow HaarSt(S_2)$
Output $X^k |\phi\rangle$

Hybrid 3: Instead of sampling $|\phi_s\rangle$ at the beginning, we sample it live when it is needed.

Figure 5: The hybrid games used in the proof of Lemma A.2.

H_4:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \left(\frac{|\mathcal{CT}|}{2^d} \overset{\mathcal{CT}}{-t \cdot |\widetilde{\mathcal{CT}}|}\right)$
$S_2 \leftarrow S_1 \cup S'$
$U_1 \leftarrow Haar(S_2)$
$U_2 \leftarrow Haar(\{0,1\}^n \setminus S_2)$
$C^{\vec{U}_2, \mathcal{O}} \rightarrow s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$s \leftarrow S_2$
Output $s \oplus k$

Hybrid 4: Instead of sampling $|\phi_s\rangle$ as a Haar random state, we sample it as a random element of S.

H_5:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S_1 \leftarrow \{(x,r) : r \in R, x \in \widetilde{\mathcal{CT}}\}$
$S' \leftarrow \left(\frac{|\mathcal{CT}|}{2^d} \overset{\mathcal{CT}}{-t \cdot |\widetilde{\mathcal{CT}}|}\right)$
$S_2 \leftarrow S_1 \cup S'$
$C^{\vec{\mathrm{Sim}}^{R_{S_2}}(t_{max}), \mathcal{O}} \rightarrow s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$s \leftarrow S_2$
Output $s \oplus k$

Hybrid 5: We replace $\vec{U}_2$ with $\vec{\mathrm{Sim}}^{R_{S_2}}$.

Figure 6: The hybrid games used in the proof of Lemma A.2.

H_6:
$k \leftarrow \{0,1\}^{\ell_n}$
$R \leftarrow \binom{\{0,1\}^{\ell_r}}{t}$
$i \leftarrow 1$
$S \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - t \cdot |\widetilde{\mathcal{CT}}|}$
$C^{\vec{\mathrm{Sim}}^{R_S}(t_{max}),\mathcal{O}} \rightarrow s$ Output 1 if and only if $s \in S$

$\mathcal{O}(m)$:
$s \leftarrow S$
Output $s \oplus k$

Hybrid 6: We no longer include S_1 inside of S_2.

$H_f = FindSXOR(D)$:
$S \leftarrow \binom{\mathcal{CT}}{\frac{|\mathcal{CT}|}{2^d} - t \cdot |\widetilde{\mathcal{CT}}|}$
$D^{R_S}(S \oplus k) \rightarrow s$ Output 1 if and only if $s \in S$

The final hybrid: $FindSXOR$.

Figure 7: The hybrid games used in the proof of Lemma A.2.

B Proof of hybrids for Lemma 3.1

We provide the formal proofs that

$$\left\| \mathcal{A}^{\vec{V_i}} - \mathcal{A}^{\vec{V_{i-1}}} \right\|_2 \leq \mathsf{negl}(n)$$

for all i.

Lemma B.1.

$$\left\| \mathcal{A}^{\vec{V_1}} - \mathcal{A}^{\vec{V_0}} \right\|_2 \leq \mathsf{negl}(n)$$

Proof. While this seems like it should immediately follow from Theorem 2.18, in fact there is a slight mismatch in terms of how the operators are defined.

In particular, we can write $\mathcal{H}([N]) \otimes \mathcal{H}(R_{[N]})^{\otimes 4} \otimes \mathcal{H}(\mathcal{P}([N])) = A_1 \oplus A_2$ for some subspaces A_1, A_2 defined as follows. A_1 will be spanned by states of the form $|D\rangle |S_2\rangle$ where $D_x \in S_2$, and A_2 will be spanned by states of the form $|D\rangle |S_2\rangle$ where $D_x \notin S_2$.

For any X, we can write $V_1^X = V_{1,1}^X + V_{1,2}^X$ where $V_{1,1}^X$ is a partial isometry on A_1 and $V_{1,2}^X$ is a partial isometry on A_2.

Then, the proper path-recording oracle for U_1 is

$$PR_1 = (V_{1,1}^{L_1} \cdot (I_{A_1} - V_{1,1}^{R_1} \cdot V_{1,1}^{R_1,\dagger}) + (I_{A_1} - V_{1,1}^{L_1} \cdot V_{1,1}^{L_1,\dagger}) V_{1,1}^{R_1}) + I_{A_2}$$

$$\overline{PR}_1 = (\overline{V}_1^{L_1} \cdot (I_{A_1} - \overline{V}_1^{R_1} \cdot \overline{V}_1^{R_1,\dagger}) + (I_{A_1} - \overline{V}_1^{L_1} \cdot \overline{V}_1^{L_1,\dagger}) \overline{V}_1^{R_1}) + I_{A_2}$$

Similarly, the proper path-recording oracle for U_2 is

$$PR_2 = I_{A_1} + (V_{1,2}^{L_2} \cdot (I_{A_2} - V_{1,2}^{R_2} \cdot V_{1,2}^{R_2,\dagger}) + (I_{A_2} - V_{1,2}^{L_2} \cdot V_{1,2}^{L_2,\dagger}) V_{1,2}^{R_2})$$

$$\overline{PR}_2 = I_{A_1} + (\overline{V}_1^{L_2} \cdot (I_{A_2} - \overline{V}_1^{R_2} \cdot \overline{V}_1^{R_2,\dagger}) + (I_{A_2} - \overline{V}_1^{L_2} \cdot \overline{V}_1^{L_2,\dagger}) \overline{V}_1^{R_2})$$

Theorem 2.18 tells us that

$$\left\|\mathcal{A}^{(PR_1PR_2,PR_2^\dagger PR_1^\dagger,\overline{PR}_1\overline{PR}_2,\overline{PR}_1^\dagger\overline{PR}_2^\dagger)} - \mathcal{A}^{\vec{V_0}}\right\|_2^2 \leq \mathsf{negl}(n)$$

We will show that in fact $V_1 = PR_1PR_2$ and so Theorem 2.18 applies directly. We make the following simple observations

1. $V_1^{L_1} = V_{1,1}^{L_1} + I_{A_2}$
2. $V_1^{R_1} = V_{1,1}^{R_1} + I_{A_2}$
3. $V_1^{L_2} = I_{A_1} + V_{1,1}^{R_1}$
4. $V_1^{R_2} = I_{A_1} + V_{1,1}^{R_2}$

We can then compute

$$\begin{aligned}
&V_1^{L_1}V_1^{L_2}(I - V_1^{R_1}V_1^{R_2}V_1^{R_2,\dagger}V_1^{R_1,\dagger}) \\
&= (V_{1,1}^{L_1} + V_{1,2}^{L_2})(I_{A_1} + I_{A_2} - (V_{1,1}^{R_1} + V_{1,2}^{R_2})(V_{1,1}^{R_1,\dagger} + V_{1,2}^{R_2,\dagger})) \\
&= V_{1,1}^{L_1}(I_{A_1} - V_{1,1}^{R_1} \cdot V_{1,1}^{R_1,\dagger}) + V_{1,2}^{L_2}(I_{A_2} - V_{1,2}^{R_2} \cdot V_{1,2}^{R_2,\dagger})
\end{aligned} \tag{13}$$

and so

$$\begin{aligned}
&V_1 \\
=&V_1^{L_1}V_1^{L_2}(I - V_1^{R_1}V_1^{R_2}V_1^{R_2,\dagger}V_1^{R_1,\dagger}) + (I - V_1^{L_1}V_1^{L_2}V_1^{L_2,\dagger}V_1^{L_1,\dagger})V_1^{R_2,\dagger}V_1^{R_1,\dagger} \\
=&V_{1,1}^{L_1}(I_{A_1} - V_{1,1}^{R_1} \cdot V_{1,1}^{R_1,\dagger}) + V_{1,2}^{L_2}(I_{A_2} - V_{1,2}^{R_2} \cdot V_{1,2}^{R_2,\dagger}) \\
&+ (I_{A_1} - V_{1,1}^{L_1} \cdot V_{1,1}^{L_1,\dagger})V_{1,1}^{R_1,\dagger} + (I_{A_2} - V_{1,2}^{L_2} \cdot V_{1,2}^{L_2,\dagger})V_{1,2}^{R_2,\dagger} \\
=&V_{1,1}^{L_1}(I_{A_1} - V_{1,1}^{R_1} \cdot V_{1,1}^{R_1,\dagger}) + (I_{A_1} - V_{1,1}^{L_1} \cdot V_{1,1}^{L_1,\dagger})V_{1,1}^{R_1,\dagger} \\
&+ V_{1,2}^{L_2}(I_{A_2} - V_{1,2}^{R_2} \cdot V_{1,2}^{R_2,\dagger}) + (I_{A_2} - V_{1,2}^{L_2} \cdot V_{1,2}^{L_2,\dagger})V_{1,2}^{R_2,\dagger} \\
=&(V_{1,1}^{L_1}(I_{A_1} - V_{1,1}^{R_1} \cdot V_{1,1}^{R_1,\dagger}) + (I_{A_1} - V_{1,1}^{L_1} \cdot V_{1,1}^{L_1,\dagger})V_{1,1}^{R_1,\dagger} + I_{A_2}) \\
&\cdot (I_{A_1} + V_{1,2}^{L_2}(I_{A_2} - V_{1,2}^{R_2} \cdot V_{1,2}^{R_2,\dagger}) + (I_{A_2} - V_{1,2}^{L_2} \cdot V_{1,2}^{L_2,\dagger})V_{1,2}^{R_2,\dagger}) \\
=&PR_1 \cdot PR_2
\end{aligned} \tag{14}$$

□

Lemma B.2.

$$\left\|\mathcal{A}^{\vec{V_2}} - \mathcal{A}^{\vec{V_1}}\right\|_2 \leq \mathsf{negl}(n)$$

Proof. We will show that $\left\|V_2^{L_1} - V_1^{L_1}\right\|_{op} \leq \mathsf{negl}(n)$. The same will hold for all other components of $V_2, \overline{V_2}$ by a symmetric argument. And so by Propositions 2.8 and 2.10 and lemma 2.9 we get that $\|V_2 - V_1\|_\diamond \leq \mathsf{negl}(n)$ (and similarly for the other components of $\vec{V_2}$). Applying Theorem 2.6 gives the full lemma.

To begin, let $D \in \mathcal{DB}$. Let $A, B \subseteq [N] \setminus D_{1,all}$ be arbitrary subsets. Then

$$\begin{aligned}
&\left(\frac{1}{\sqrt{|A|}}\sum_{y\in A}\left\langle D_y^{L_1,f}\right|\right)\left(\frac{1}{\sqrt{|B|}}\sum_{y\in B}\left|D_y^{L_1,f}\right\rangle\right) \\
&\qquad = \frac{1}{\sqrt{|A|\cdot|B|}}\sum_{y\in A\cap B}\left\langle D_y^{L_1,f}\middle|D_y^{L_1,f}\right\rangle \\
&\qquad\qquad = \frac{|A\cap B|}{\sqrt{|A|\cdot|B|}} \\
&\qquad\qquad \geq \frac{|A\cap B|}{\sqrt{|A\cap B|\cdot|A\cup B|}} \\
&\qquad\qquad = \sqrt{\frac{|A\cap B|}{|A\cup B|}}
\end{aligned} \tag{15}$$

For all D, S_2 such that $D_x \notin S_2$, it is clear that

$$\langle D, S_2|\, V_2^{L_1,\dagger} V_1^{L_1}\, |D, S_2\rangle = \langle D, S_2|D, S_2\rangle = 1$$

For all D, S_2 such that $D_x \in S_2$, we have

$$\begin{aligned}
&\langle D, S_2|\, V_2^{L_1,\dagger} V_1^{L_1}\, |D, S_2\rangle \\
&= \left(\frac{1}{\sqrt{|S_2\setminus D_{1,all}|}}\sum_{y\in S_2\setminus D_{1,all}}\left\langle D_y^{L_1,f}, S_2\right|\right)\left(\frac{1}{\sqrt{|S_2\setminus \mathrm{Im}(D_1)|}}\sum_{y\in S_2\setminus \mathrm{Im}(D_1)}\left|D_y^{L_1,f}, S_2\right\rangle\right) \\
&\geq \sqrt{\frac{|(S_2\setminus D_{1,all})\cap(S_2\setminus \mathrm{Im}(D_1))|}{|(S_2\setminus D_{1,all})\cup(S_2\setminus \mathrm{Im}(D_1))|}} \\
&\geq \sqrt{\frac{|S_2|-2t}{|S_2|}} \\
&= \sqrt{\frac{M_2-2t}{M_2}}
\end{aligned} \tag{16}$$

But note that by Lemma 3.2 we have that for all $(D, S_2) \neq (D', S_2')$, $V_2^{L_1}\,|D, S_2\rangle$ and $V_1^{L_1}\,|D', S_2'\rangle$ are orthogonal. And so for all

$$|\phi\rangle = \sum_{D\in\mathcal{DB}, S_2\in\mathcal{P}([N])} \alpha_{D,S_2}\,|D, S_2\rangle\,,$$

we have

$$\begin{aligned}
&\langle\phi|\, V_2^{L_1,\dagger} V_1^{L_1} \,|\phi\rangle \\
&= \sum_{D\in\mathcal{DB}, S_2\in\mathcal{P}([N])} |\alpha_{D,S_2}|^2 \,\langle D, S_2|\, V_2^{L_2,\dagger} V_1^{L_1} \,|D, S_2\rangle \\
&\geq \sum_{D\in\mathcal{DB}, S_2\in\mathcal{P}([N])} |\alpha_{D,S_2}|^2 \sqrt{\frac{M_2-2t}{M_2}} \qquad (17)\\
&= \sqrt{\frac{M_2-2t}{M_2}} \\
&\geq 1-\mathsf{negl}(n)
\end{aligned}$$

and so by Proposition 2.11 we are done. □

Before proving the next hybrid, we will make a few crucial observations.

Lemma B.3. *Let $D \in \mathcal{DB}$ such that $D_x \in D_{1,all}$. Then for all $y \in [N] \setminus D_{1,all}$,*

$$Val(D) \cap \{S_2 : y \in S_2\} = Val(D_y^{L_1,f}) = Val(D_y^{R_1,f}) = Val(D_y^{L_1,b}) = Val(D_y^{R_1,b})$$

Proof. We will only show $Val(D) \cap \{S_2 : y \in S_2\} = Val(D_y^{L_1,f})$, and the rest will follow by symmetric arguments.

$\subseteq$: Let $S_2 \in Val(D)$ and $y \in S_2$. We show

1. $(D_y^{L_1,f})_1 \subseteq S_2$: Note that $(D_y^{L_1,f})_1 = D_{1,all} \cup \{(D_x, y)\}$. We know $D_x \in D_{1,all} \subseteq S_2$ and $y \in S_2$, so $(D_y^{L_1,f})_1 \subseteq S_2$
2. $(D_y^{L_1,f})_2 \cap S_2 = \emptyset$: $(D_y^{L_1,f})_2 = D_{2,all}$ and $D_{2,all} \cap S_2 = \emptyset$
3. If $(D_y^{L_1,f})_x \notin (D_y^{L_1,f})_1$, then $(D_y^{L_1,f})_x \notin S_2$: $(D_y^{L_1,f})_x = y \in (D_y^{L_1,f})_1$, so this holds vacuously.

and so $S_2 \in Val(D_y^{L_1,f})$.

$\supseteq$: Let $S_2 \in Val(D_y^{L_1,f})$. We show

1. $D_{1,all} \subseteq S_2$: Follows from $D_{1,all} \subseteq (D_y^{L_1,f})_1 \subseteq S_2$
2. $D_{2,all} \cap S_2 = \emptyset$: Follows from $D_{2,all} \subseteq (D_y^{L_1,f})_2$ and $(D_y^{L_1,f})_2 \cap S_2 = \emptyset$
3. If $D_x \notin D_{1,all}$, then $D_x \notin S_2$: We know $D_x \in (D_y^{L_1,f})_2$ so this holds vacuously.
4. $y \in S_2$: $y \in D_{1,all} \cup \{(D_x, y)\} = (D_y^{L_1,f})_1 \subseteq S_2$.

and so $S_2 \in Val(D) \cap \{S_2 : y \in S_2\}$. □

Lemma B.4. *Let $D \in \mathcal{DB}$ such that $D_x \notin D_{1,all}$. Then for all $y \in [N] \setminus D_{all}$,*

$$Val(D) \cap \{S_2 : y \notin S_2\} = Val(D_y^{L_2,f}) = Val(D_y^{R_2,f}) = Val(D_y^{L_2,b}) = Val(D_y^{R_2,b})$$

Proof. We will only show $Val(D) \cap \{S_2 : y \notin S_2\} = Val(D_y^{L_2,f})$, and the rest will follow by symmetric arguments.

$\subseteq$: Let $S_2 \in Val(D)$ and $y \notin S_2$. We show

1. $(D_y^{L_2,f})_1 \subseteq S_2$: This follows from $(D_y^{L_2,f})_1 = D_{1,all} \subseteq S_2$.

2. $(D_y^{L_2,f})_2 \cap S_2 = \emptyset$: We know $(D_y^{L_1,f})_2 = D_{2,all} \cup \{(D_x, y)\}$. $y \notin S_2$ by assumption. Since S_2 is valid and $D_x \notin D_{1,all}$, $D_x \notin S_2$ and $D_{2,all} \cap S_2 = \emptyset$.

3. If $(D_y^{L_2,f})_x \notin (D_y^{L_2,f})_1$, then $(D_y^{L_2,f})_x \notin S_2$: $(D_y^{L_2,f})_x = y \notin S_2$.

and so $S_2 \in Val(D_y^{L_2,f})$.

$\supseteq$: Let $S_2 \in Val(D_y^{L_2,f})$. We show

1. $D_{1,all} \subseteq S_2$: Follows from $D_{1,all} = (D_y^{L_2,f})_1 \subseteq S_2$

2. $D_{2,all} \cap S_2 = \emptyset$: Follows from $D_{2,all} \subseteq (D_y^{L_1,f})_2$ and $(D_y^{L_1,f})_2 \cap S_2 = \emptyset$.

3. If $D_x \notin D_{1,all}$, then $D_x \notin S_2$: We know $D_x \in D_{1,all}$ so this holds vacuously.

4. $y \notin S_2$: $y \in D_{2,all} \cup \{(D_x, y)\} = (D_y^{L_1,f})_2$. But $(D_y^{L_1,f})_2 \cap S_2 = \emptyset$, so $y \notin S_2$.

and so $S_2 \in Val(D) \cap \{S_2 : y \in S_2\}$. □

Lemma B.5.

$$\left\| \mathcal{A}^{\vec{V}_3} - \mathcal{A}^{\vec{V}_2} \right\|_2 \leq \mathsf{negl}(n)$$

The proof of this lemma is involved and is thus deferred to Appendix D. In particular, the error in this reduction stems from the fact that for a state in Π_{good}, $V_2^{L_1,\dagger}$ may map it to a state slightly outside of Π_{good}. We then bound this overlap by a combinatorial argument given in Appendix C.

Lemma B.6. *$V_4 = V_3$ and $\overline{V}_4 = \overline{V}_3$.*

Proof. This follows from directly reasoning about the partial isometries. As an example, we will show $V_4^{L_1} = V_3^{L_1}$ and $V_4^{L_2} = V_3^{L_2}$, and the other cases will be analogous.

To show this, it is sufficient to show that they behave the same on $|ValSt_D\rangle$ for all databases D, since $\mathrm{Im}(\Pi_{good}) = \mathrm{Im}(ConS)$.

Consider the case $D_x \in D_{1,all}$. Then

$$\begin{aligned}
&V_4^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_1} \cdot ConS^\dagger \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_1} |D\rangle \\
&= ConS \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \\
&= \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \sum_{y \in [N] \setminus D_{all}} \frac{1}{\sqrt{|Val(D_y^{L_1,f})|}} \left| D_y^{L_1,f} \right\rangle \sum_{S_2 \in Val(D_y^{L_1,f})} |S_2\rangle
\end{aligned} \tag{18}$$

We can then compute the normalization factor by

$$\begin{aligned}
&|Val(D_y^{L_1,f})| \cdot |[N] \setminus D_{all}| \\
&= \binom{N - |D_{all}| - 1}{M_2 - |D_{1,all}| - 1} \cdot (N - |D_{all}|) \\
&= \frac{(N - |D_{all}| - 1)!(N - |D_{all}|)}{(M_2 - |D_{1,all}| - 1)!(N - |D_{all}| - M_2 + |D_{1,all}|)!} \\
&= \frac{(N - |D_{all}|)!(M_2 - |D_{1,all}|)}{(M_2 - |D_{1,all}|)!(N - |D_{all}| - M_2 + |D_{1,all}|)!} \\
&= \binom{N - |D_{all}|}{M_2 - |D_{1,all}|} \cdot (M_2 - |D_{1,all}|)
\end{aligned} \tag{19}$$

and so

$$\begin{aligned}
&V_4^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= \frac{1}{\sqrt{\binom{N-|D_{all}|}{M_2-|D_{1,all}|}(M_2 - |D_{1,all}|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \sum_{S_2 \in Val(D_y^{L_1,f})} |S_2\rangle
\end{aligned} \tag{20}$$

This let's us compute

$$\begin{aligned}
&V_3^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= \frac{1}{\sqrt{Val(D)}} \sum_{S_2 \in Val(D)} \frac{1}{\sqrt{|S_2 \setminus D_{1,all}|}} \sum_{y \in S_2 \setminus D_{1,all}} \left| D_y^{L_1,f} \right\rangle |S_2\rangle \\
&= \frac{1}{\sqrt{\binom{N-|D_{all}|}{M_2-|D_{1,all}|}}} \frac{1}{\sqrt{M_2 - |D_{1,all}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \sum_{\substack{S_2 \in Val(D) \\ y \in S_2}} |S_2\rangle \\
&= V_4^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle
\end{aligned} \tag{21}$$

On the other side, when $D_x \in D_{1,all}$

$$\begin{aligned}
&V_4^{L_2} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_2} \cdot ConS^\dagger \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_2} |D\rangle \\
&= ConS |D\rangle \\
&= \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= V_3^{L_2} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle
\end{aligned} \tag{22}$$

For $D_x \notin D_{1,all}$, we similarly have

$$\begin{aligned}
&V_4^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_1} \cdot ConS^\dagger \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_1} |D\rangle \\
&= ConS |D\rangle \\
&= \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= V_3^{L_1} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle
\end{aligned} \tag{23}$$

Thus, it remains to show

$$V_3^{L_2} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle = V_4^{L_2} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle$$

We compute

$$\begin{aligned}
&V_4^{L_2} \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\
&= ConS \cdot W_4^{L_2} |D\rangle \\
&= ConS \frac{1}{\sqrt{[N] \setminus D_{all}}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2, f} \right\rangle \\
&= \sum_{y \in [N] \setminus D_{all}} \frac{1}{\sqrt{|Val(D_y^{L_2,f})| \cdot (N - |D_{all}|)}} \left| D_y^{L_2, f} \right\rangle \sum_{S_2 \in Val(D_y^{L_2,f})} |S_2\rangle \\
&= \frac{1}{\sqrt{\binom{N-|D_{all}|-1}{M_2-|D_{1,all}|}(N - |D_{all}|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2, f} \right\rangle \sum_{S_2 \in Val(D_y^{L_2,f})} |S_2\rangle
\end{aligned} \tag{24}$$

On the other hand,

$$
\begin{aligned}
&V_3^{L_2}\frac{1}{\sqrt{|Val(D)|}}|D\rangle\sum_{S_2\in Val(D)}|S_2\rangle\\
&=\frac{1}{\sqrt{\binom{N-|D_{all}|}{M_2-|D_{1,all}|}}}\sum_{S_2\in Val(D)}\frac{1}{\sqrt{N-|S_2\cup D_{all}|}}\left|D_y^{L_2,f}\right\rangle\sum_{y\in N\setminus(S_2\cup D_{all})}|S_2\rangle\\
&=\frac{1}{\sqrt{\binom{N-|D_{all}|}{M_2-|D_{1,all}|}(N-M_2-|D_{all}|+|D_{1,all}|)}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{L_2,f}\right\rangle\sum_{\substack{S_2\in Val(D)\\ y\notin S_2}}|S_2\rangle\\
&=\frac{1}{\sqrt{\binom{N-|D_{all}|}{M_2-|D_{1,all}|}(N-M_2-|D_{all}|+|D_{1,all}|)}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{L_2,f}\right\rangle\sum_{S_2\in Val(D_y^{L_2,f})}|S_2\rangle\\
&=\frac{1}{\sqrt{\binom{N-|D_{all}|-1}{M_2-|D_{1,all}|}(N-|D_{all}|)}}\sum_{y\in[N]\setminus D_{all}}\left|D_y^{L_2,f}\right\rangle\sum_{S_2\in Val(D_y^{L_2,f})}|S_2\rangle\\
&=V_4^{L_2}\frac{1}{\sqrt{|Val(D)|}}|D\rangle\sum_{S_2\in Val(D)}|S_2\rangle
\end{aligned}
\tag{25}
$$

where the second to last equality comes from Lemma B.4. □

Lemma B.7. $\mathcal{A}^{\vec{V_5}}=\mathcal{A}^{\vec{V_4}}$

Proof. This follows immediately from the fact that $\vec{V_5}$ and $\vec{V_4}$ are identical up to an isometry on register St. □

Lemma B.8. $\mathcal{A}^{\vec{V_6}}=\mathcal{A}^{\vec{V_5}}$

Proof. To show this, we will define a partial isometry T acting on $\mathcal{H}(R_{[N]})^{\otimes 4}$ such that $(I\otimes T)W_6=W_4(I\otimes T)$.

In particular, let $L,R\in R_{[N]}$. We will define (L_1',R_1',L_2',R_2') such that

$$T\,|L\rangle\,|R\rangle\,|\emptyset\rangle\,|\emptyset\rangle=\left|L_1'\right\rangle\left|R_1'\right\rangle\left|L_2'\right\rangle\left|R_2'\right\rangle$$

We will define $Reachable(L,R)$ to be the set of $x\in[N]$ such that there exists a "path" connecting x to S_1 in L and R. Formally, we build $Reachable(L,R)$ as follows

1. $S_1\subseteq Reachable(L,R)$
2. If there exists $y\in Reachable(L,R)$ such that $(x,y)\in L\cup R$ or $(y,x)\in L\cup R$, then $x\in Reachable(L,R)$.

We then define

$$
\begin{aligned}
L_1'&=\{(x,y)\in L: x\in Reachable(L,R)\}\\
R_1'&=\{(x,y)\in R: x\in Reachable(L,R)\}\\
L_2'&=\{(x,y)\in L: x\notin Reachable(L,R)\}\\
R_2'&=\{(x,y)\in R: x\notin Reachable(L,R)\}
\end{aligned}
$$

We will then show that $(I \otimes T)W_6 = W_4(I \otimes T)$. In particular, we will show $(I \otimes T)W_6^{L_1} = W_4^{L_1}(I \otimes T)$ and $(I \otimes T)W_6^{L_2} = W_4^{L_2}(I \otimes T)$, and the same will hold for other variants by an analogous argument.

Let $L, R \in R_{[N]}$, $x \in [N]$. Define $DB = \mathrm{Im}(L) \cup \mathrm{Dom}(L) \cup \mathrm{Im}(R) \cup \mathrm{Dom}(R)$.

We will show that $(I \otimes T)W_6^{L_1} = W_4^{L}(I \otimes T)$. The other cases will follow analogously, and so together we will get $(I \otimes T)W_6 = W_4(I \otimes T)$

We will consider the case where $x \in \mathit{Reachable}(L, R)$ and $x \notin \mathit{Reachable}(L, R)$ separately.

If $x \in \mathit{Reachable}(L, R)$,

$$\begin{aligned}
&(I \otimes T)W_6^{L_1} |x\rangle |L\rangle |R\rangle \\
&= T\frac{1}{\sqrt{N - |DB|}} \sum_{y \in [N] \setminus DB} |y\rangle |L \cup \{(x, y)\}\rangle |R\rangle \\
&= \frac{1}{\sqrt{N - |DB|}} \sum_{y \in [N] \setminus DB} |y\rangle \left|L_1' \cup \{(x, y)\}\right\rangle \left|R_1'\right\rangle \left|L_2'\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L_1} |x\rangle \left|L_1'\right\rangle \left|R_1'\right\rangle \left|L_2'\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L_1} W_4^{L_2} |x\rangle \left|L_1'\right\rangle \left|R_1'\right\rangle \left|L_2'\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L_1} W_4^{L_2} (I \otimes T) |x\rangle |L\rangle |R\rangle \\
&= W_4^{L} (I \otimes T) |x\rangle |L\rangle |R\rangle
\end{aligned} \tag{26}$$

Here the key observation is that since $x \in \mathit{Reachable}(L, R)$, (x, y) will appear in the L_1' register after applying T. Furthermore, since $x \in \mathit{Reachable}(L, R)$, if we define $D = (x, L_1', R_1', L_2', R_2')$, $D_x \in D_{1,all}$ and so $W_4^{L_2} |D\rangle = |D\rangle$.

If $x \notin \mathit{Reachable}(L, R)$,

$$\begin{aligned}
&(I \otimes T)W_6^{L_1} |x\rangle |L\rangle |R\rangle \\
&= T\frac{1}{\sqrt{N - |DB|}} \sum_{y \in [N] \setminus DB} |y\rangle |L \cup \{(x, y)\}\rangle |R\rangle \\
&= \frac{1}{\sqrt{N - |DB|}} \sum_{y \in [N] \setminus DB} |y\rangle \left|L_1'\right\rangle \left|R_1'\right\rangle \left|L_2' \cup \{(x, y)\}\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L_2} |x\rangle \left|L_1'\right\rangle \left|R_1'\right\rangle \left|L_2'\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L_2} W_4^{L_1} |x\rangle \left|L_1'\right\rangle \left|R_1'\right\rangle \left|L_2'\right\rangle \left|R_2'\right\rangle \\
&= W_4^{L} (I \otimes T) |x\rangle |L\rangle |R\rangle
\end{aligned} \tag{27}$$

Here the key observation is that since $x \notin \mathit{Reachable}(L, R)$, and since $y \notin DB$ is definitely not in $\mathit{Reachable}(L, R)$, (x, y) will appear in the L_2' register after applying T. Furthermore, if we define $D = (x, L_1', R_1', L_2', R_2')$, we have $x \notin D_{1,all}$, and so $W_4^{L_1} |D\rangle = |D\rangle$. □

Lemma B.9. $\left\| \mathcal{A}^{\vec{V_7}} - \mathcal{A}^{\vec{V_6}} \right\|_2^2 \leq \mathsf{negl}(n)$

Proof. This follows from the exact same techniques as Lemma B.2. □

Lemma B.10. $\left\| \mathcal{A}^{\vec{V_f}} - \mathcal{A}^{\vec{V_7}} \right\|_2^2 \leq \mathsf{negl}(n)$

Proof. This follows from Theorem 2.18. □

C Combinatorial Lemma

We make use of the following combinatorial lemma in the proof of Lemma B.5. We would like to acknowledge that the proof sketch for this lemma was derived by Chat-GPT.

Lemma C.1. *Let P be any set of size $|P| = N$ and let $2 \leq M \leq N/2$. Define $\mathcal{S} = \{S \subseteq P : |S| = M\}$. Let $\vec{a} : \mathcal{S} \to \mathbb{C}$ be such that*

$$\sum_{S \in \mathcal{S}} \alpha_S = 0$$
$$\|\vec{\alpha}\|_2 = 1$$

Then,

$$\sum_{y \in P} \left| \sum_{S \in \mathcal{S} : y \in S} a_S \right|^2 \leq \binom{N-2}{M-1}$$

Proof. We first define an $N \times \binom{N}{M}$ matrix B with rows indexed by P and columns indexed by $\mathcal{S}$ as follows:

$$B_{y,S} = \begin{cases} 1 & y \in S \\ 0 & y \notin S \end{cases}$$

For ease of notation, let $\vec{1}_P, \vec{1}_{\mathcal{S}}$ be the all-ones vectors indexed by P and $\mathcal{S}$ respectively. Let $\mathbf{1}_{P \times P}$ be the all-ones matrix with rows and columns both indexed by P.

Let $\vec{a} : \mathcal{S} \to \mathbb{C}$ be such that $\|\vec{a}\|_2 = 1$ and $\|\vec{a}\|_1 = 0$. Observe that

$$\begin{aligned} \|B \cdot \vec{a}\|_2^2 &= \sum_{y \in P} \left| \sum_{S \in \mathcal{S}} B_{y,S} \cdot a_S \right|^2 \\ &= \sum_{y \in P} \left| \sum_{S \in \mathcal{S} : y \in S} a_S \right|^2 \end{aligned}$$

and so it suffices to show $\|B\vec{a}\|_2^2 \leq \binom{N-2}{M-1}$. But note that $\|B\vec{a}\|_2^2 = \vec{a}^\dagger B^\dagger B \vec{a}$. In order to bound this value, we will compute the eigenvalues of $B^\dagger B = B^T B$.

Note that the non-zero eigenvalues of $B^T B$ are the squared singular values of B or B^T, and so the non-zero eigenvalues of $B^T B$ are the same as the non-zero eigenvalues of BB^T. We can write BB^T as follows

$$\begin{aligned} (BB^T)_{x,y} &= \sum_{S \in \mathcal{S}} Ind[x \in S] \cdot Ind[y \in S] \\ &= |\{S : \{x, y\} \subseteq S\}| = \begin{cases} \binom{N-1}{M-1} & \text{if } x = y \\ \binom{N-2}{M-2} & \text{if } x \neq y \end{cases} \end{aligned} \tag{28}$$

Then

$$BB^T = \binom{N-2}{M-2} \mathbf{1}_{P \times P} + \left(\binom{N-1}{M-1} - \binom{N-2}{M-2} \right) I = \binom{N-2}{M-2} \mathbf{1}_{P \times P} + \binom{N-2}{M-1} I \tag{29}$$

Now, we can explicitly compute the spectrum of BB^T. For each $x \in P$,

$$(BB^T\vec{1})_x = \binom{N-1}{M-1} + (N-1)\binom{N-2}{M-2}$$

and so $\vec{1}$ is an eigenvector with eigenvalue

$$\begin{aligned}\lambda_1 &= \binom{N-1}{M-1} + (N-1)\binom{N-2}{M-2} \\ &= \frac{(N-1)!}{(M-1)!(N-M)!} + \frac{(N-1)(N-2)!}{(M-2)!(N-M)!} \\ &= \frac{(N-1)!}{(M-1)!(N-M)!} + \frac{(M-1)(N-1)!}{(M-1)!(N-M)!} \\ &= M\frac{(N-1)!}{(M-1)!(N-M)!} = M\binom{N-1}{M-1}\end{aligned} \tag{30}$$

. Furthermore, consider any vector $\vec{v}$ such that $\vec{v} \cdot \vec{1} = 0$. Then $\mathbf{1}\vec{v} = \vec{0}$ and so

$$BB^T\vec{v} = \left(\binom{N-2}{M-2}\mathbf{1} + \binom{N-2}{M-1}I\right)\vec{v} = \binom{N-2}{M-1}\vec{v}$$

Therefore, BB^T is a full rank matrix with eigenvalues $M\binom{N-1}{M-1}$ with multiplicity 1 and $\binom{N-2}{M-1}$ with multiplicity $N-1$. Similarly, B^TB has eigenvalues $M\binom{N-1}{M-1}$ with multiplicity 1, $\binom{N-2}{M-1}$ with multiplicity $N-1$, and 0 with multiplicity $\binom{N}{M} - N$.

To complete the argument, we will show that the all-ones vector $\vec{1}_{\mathcal{S}}$ is an eigenvector of B^TB with eigenvalue $M\binom{N-1}{M-1}$.

$$\begin{aligned}(B\vec{1})_S &= \sum_{y\in P} Ind[y \in S] = |\{S : y \in S\}| = \binom{N-1}{M-1} \\ (B^TB\vec{1})_y &= \sum_{S\in\mathcal{S}} Ind[y \in S](B\vec{1})_S = M\binom{N-1}{M-1} \\ B^TB\vec{1} &= M \cdot \binom{N-1}{M-1}\vec{1}\end{aligned} \tag{31}$$

Thus, since the largest eigenvalue of B^TB has multiplicity 1 and is spanned by $\vec{1}_{\mathcal{S}}$, and since we know $\vec{a} \cdot \vec{1}_{\mathcal{S}} = 0$, we must have that $\vec{a}^\dagger B^TB\vec{a}$ is bounded by the second largest eigenvalue of B^TB, which is $\binom{N-2}{M-1}$.

In detail, let $\vec{v}_1, \ldots, \vec{v}_{\binom{N}{M}}$ be any basis with $\vec{v}_1 = \vec{1}$, $(\vec{v}_2, \ldots, \vec{v}_N)$ orthogonal eigenvectors for the eigenvalue $\binom{N-2}{M-1}$, and $(\vec{v}_{N+1}, \ldots, \vec{v}_{\binom{N}{M}})$ a basis for the kernel of B^TB. Then, $\vec{a} = \sum_i a_i\vec{v}_1$, with $a_i = 0$ since $\vec{a} \cdot \vec{1}_{\mathcal{S}} = 0$. And so

$$\begin{aligned}\vec{a}^\dagger B^TB\vec{a} &= \sum_{i,j} a_i^* a_j \vec{v}_i B^TB\vec{v}_j \\ &= \sum_{i\neq 0} |a_i|^2\lambda_i \leq \binom{N-2}{M-1}\sum_i |a_i|^2 \\ &\leq \binom{N-2}{M-1}\end{aligned} \tag{32}$$

□

D Proof of Lemma B.5

Lemma D.1 (Lemma B.5 restated)**.**

$$\left\|\mathcal{A}^{\vec{V}_3} - \mathcal{A}^{\vec{V}_2}\right\|_2 \leq \mathsf{negl}(n)$$

We will show that Π_{good} almost commutes with all operations used in $\mathcal{A}^{\vec{V}_2}$. In particular, we will show that

$$\left\|\Pi_{good} V_2^{L_1} - V_2^{L_1}\Pi_{good}\right\|_{op} \leq \mathsf{negl}(n)$$

and similar statements hold for all components of $V_2, \overline{V_2}$. We will also show that for all unitaries A acting only on an internal register $\mathbf{A}$ and register $\mathbf{In}$, $\left\|(A_{\mathbf{A},\mathbf{In}} \otimes I_{\mathbf{St}}(I_{\mathbf{A}} \otimes \Pi_{good}) - (I_{\mathbf{A}} \otimes \Pi_{good})(A_{\mathbf{A},\mathbf{In}\otimes I_{\mathbf{St}})}\right\|_{op} \leq \mathsf{negl}(n)$. Note that $|\phi_0\rangle \in \mathrm{Im}(\Pi_{good})$. By Propositions 2.8 and 2.10 and lemma 2.9 we get that $\|\Pi_{good} V_2 \Pi_{good} - V_2\Pi_{good}\|_{op} \leq \mathsf{negl}(n)$ and the same holds for $V_2^\dagger, \overline{V_2}, \overline{V_2}^\dagger$ as well as A as described prior.

Thus, there exist maps $W_1, \ldots, W_{2t}$ such that

$$\mathcal{A}^{\vec{V}_2} = W_{2t} \cdots W_3 \cdot W_2 \cdot W_1 |0\rangle |\phi_0\rangle$$

and for each i, $\|\Pi_{good} W_i \Pi_{good} - W_i \Pi_{good}\|_\diamond \leq \mathsf{negl}(n)$.

Thus, if $\approx$ denotes that the two states are negligibly close in trace distance, we have by induction

$$\begin{aligned}
&\mathcal{A}^{\vec{V}_2} = W_{2t} \cdots W_3 \cdot W_2 \cdot W_1 |0\rangle |\phi_0\rangle \\
&= W_{2t} \cdots W_3 \cdot W_2 \cdot W_1 \cdot (I \otimes \Pi_{good}) |0\rangle |\phi_0\rangle \\
&\approx W_{2t} \cdots W_3 \cdot W_2 \cdot (I \otimes \Pi_{good}) \cdot W_1 \cdot (I \otimes \Pi_{good}) |0\rangle |\phi_0\rangle \\
&\approx W_{2t} \cdots W_3 \cdot (I \otimes \Pi_{good}) \cdot W_2 \cdot (I \otimes \Pi_{good}) \cdot W_1 \cdot (I \otimes \Pi_{good}) |0\rangle |\phi_0\rangle \\
&\approx W_{2t} \cdot (I \otimes \Pi_{good}) \cdots W_3 \cdot (I \otimes \Pi_{good}) \cdot W_2 \cdot (I \otimes \Pi_{good}) \cdot W_1 \cdot (I \otimes \Pi_{good}) |0\rangle |\phi_0\rangle \\
&= \mathcal{A}^{\vec{V}_3}
\end{aligned} \tag{33}$$

In order to show that Π_{good} approximately commutes with $\vec{V}_2$, we will show that it approximately commutes with all components of $\vec{V}_2$. We will only show the cases of $V_2^{L_1}$ and $V_2^{L_2}$, and all other cases will follow by symmetric arguments.

Lemma D.2. $\left\|\Pi_{good} V_2^{L_1} - V_2^{L_1}\Pi_{good}\right\|_{op} \leq \mathsf{negl}(n)$

Proof. It turns out that $\Pi_{good} V_2^{L_1} \Pi_{good} = V_2^{L_1}\Pi_{good}$. To show this, let $|\phi\rangle = \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle$ be a basis state of Π_{good}. We will show that $V_2^{L_1} |\phi\rangle \in \mathrm{Im}(\Pi_{good})$.

If $D_x \notin D_1$, then for all $S_2 \in Val(D)$, $D_x \notin S_2$. And so,

$$\begin{aligned} & V_2^{L_1} |\phi\rangle \\ &= \frac{1}{\sqrt{|Val(D)|}} \sum_{S_2 \in Val(D)} V_2^{L_1}(|D\rangle |S_2\rangle) \\ &= \frac{1}{\sqrt{|Val(D)|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\ &= |\phi\rangle \end{aligned} \tag{34}$$

which is clearly in $\mathrm{Im}(\Pi_{good})$.

If $D_x \in D_1$, then for all $S_2 \in Val(D)$, $D_1 \subseteq S_2$ and so $D_x \in S_2$. Observe that for all $S_2 \in Val(D)$, for all $y \in S_2 \setminus D_1$, $y \neq D_x$ (since $D_x \in D_1$) and $y \notin D_2$ (since $D_2 \cap S_2 = \emptyset$). Thus, for all $y \in S_2 \setminus D_1$, $y \in [N] \setminus D_{all}$.

$$\begin{aligned} & V_2^{L_1} |\phi\rangle \\ &= \frac{1}{\sqrt{|Val(D)|}} \sum_{S_2 \in Val(D)} V_2^{L_1}(|D\rangle |S_2\rangle) \\ &= \frac{1}{\sqrt{|Val(D)|}} \sum_{S_2 \in Val(D)} \frac{1}{\sqrt{|S_2 \setminus D_1|}} \sum_{y \in S_2 \setminus D_1} \left| D_y^{L_1, f} \right\rangle |S_2\rangle \\ &= \frac{1}{\sqrt{|Val(D)| \cdot (M_2 - |D_1|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1, f} \right\rangle \sum_{\substack{S_2 \in Val(D) \\ y \in S_2}} |S_2\rangle \\ &= \frac{1}{\sqrt{|Val(D)| \cdot (M_2 - |D_1|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1, f} \right\rangle \sum_{S_2 \in Val(D_y^{L_1, f})} |S_2\rangle \end{aligned} \tag{35}$$

where the last line follows from Lemma B.3. But note that this is a superposition of basis states for $\mathrm{Im}(\Pi_{good})$, and so is clearly also in $\mathrm{Im}(\Pi_{good})$.

It thus follows that $\Pi_{good} V_2^{L_1} \Pi_{good} = V_2^{L_1} \Pi_{good}$.

And so, it remains to show

$$\left\| \Pi_{good} V_2^{L_1} \Pi_{good} - \Pi_{good} V_2^{L_1} \right\|_{op} \leq \mathsf{negl}(n)$$

Observe

$$\begin{aligned} & \left\| \Pi_{good} V_2^{L_1} (I - \Pi_{good}) \right\|_{op} \\ &= \left\| \Pi_{good} V_2^{L_1} - \Pi_{good} V_2^{L_1} \Pi_{good} \right\|_{op} \\ &= \left\| \Pi_{good} V_2^{L_1} \Pi_{good} - \Pi_{good} V_2^{L_1} \right\|_{op} \end{aligned} \tag{36}$$

and so it is sufficient to bound

$$\begin{aligned} & \sup_{|\langle\phi|\phi\rangle|^2 \leq 1} \left\| \Pi_{good} V_2^{L_1} (I - \Pi_{good}) |\phi\rangle \right\|_2^2 \\ &= \sup_{\substack{|\phi\rangle \in \mathrm{Im}(I - \Pi_{good}) \\ |\langle\phi|\phi\rangle|^2 \leq 1}} \left\| \Pi_{good} V_2^{L_1} |\phi\rangle \right\|_2^2 \end{aligned} \tag{37}$$

We can define a spanning set for $\mathrm{Im}(I - \Pi_{good})$ consisting of two types of states

1. States of type 1 will be states with an "invalid" S_2. These will be states of the form

$$|\phi_1\rangle = |D\rangle |S_2\rangle$$

for some $D \in \mathcal{DB}$, $S_2 \notin Val(D)$.

2. States of type 2 will be states with a valid S_2 register, but which are orthogonal from the uniform superposition over valid registers. These will be states of the form

$$|\phi_2\rangle = |D\rangle \sum_{S_2 \in Val(D)} \alpha_{S_2} |S_2\rangle$$

for some $\vec{\alpha} : \mathcal{P}([N]) \to \mathbb{C}$ satisfying

$$\sum_{S_2 \in Val(D)} \alpha_{S_2} = \|\vec{\alpha}\|_1 = 0$$

$$\sum_{S_2 \in Val(D)} \alpha_{S_2}^2 = \|\vec{\alpha}\|_2^2 = 1$$

We then make the following observations

1. States of type 1 are mapped by $V_2^{L_1}$ into states of type 1. In particular, let $D \in \mathcal{DB}, S_2 \notin Val(D)$, and $|\phi_1\rangle = |D\rangle |S_2\rangle$. Then if $D_x \in S_2$

$$\begin{aligned} & V_2^{L_1} |\phi\rangle \\ &= V_2^{L_1} |D\rangle |S_2\rangle \\ &= \left|D_y^{L_1,f}\right\rangle |S_2\rangle \end{aligned} \tag{38}$$

which is also a state of type 1, since $Val(D_y^{L_1,f}) \subseteq Val(D)$ by Lemma B.3. If $D_x \notin S_2$, then $V_2^{L_1} |\phi\rangle = |\phi\rangle$ which is also a state of type 1.

This implies that for all states $|\phi_1\rangle$ of type 1, $\left\|\Pi_{good} V_2^{L_1} |\phi_1\rangle\right\|_2^2 = 0$.

2. Let $D \in \mathcal{DB}$, $S_2 \in Val(D)$. Define

$$\Pi_{good}^D = \sum_{y \in [N] \setminus D_{all}} \left|ValSt_{D_y^{L_1,f}}\right\rangle\left\langle ValSt_{D_y^{L_1,f}}\right|$$

Then

$$\Pi_{good} |D\rangle |S_2\rangle = \Pi_{good}^D |D\rangle |S_2\rangle$$

and for any $D \neq D'$, by Lemma 3.2,

$$\Pi_{good}^{D'} \Pi_{good}^D = 0$$

3. Let $A \neq B \in \mathcal{DB}$ and $\vec{\alpha}, \vec{\beta}$ be such that

$$|\phi_A\rangle = |A\rangle \sum_{S_2 \in Val(A)} \alpha_{S_2} |S_2\rangle$$

$$|\phi_B\rangle = |B\rangle \sum_{S_2 \in Val(B)} \beta_{S_2} |S_2\rangle$$

are states of type 2. Then

$$\begin{aligned}
&\left\| \Pi_{good} V_2^{L_1} (|\phi_A\rangle + |\phi_B\rangle) \right\|_2^2 \\
=&\left\| \Pi^A_{good} V_2^{L_1} |\phi_A\rangle + \Pi^B_{good} V_2^{L_1} |\phi_B\rangle \right\|_2^2 \\
=&| \langle \phi_A | V_2^{L_1,\dagger} \Pi^A_{good} V_2^{L_1} |\phi_A\rangle + \langle \phi_A | V_2^{L_1,\dagger} \Pi^A_{good} \Pi^B_{good} V_2^{L_1} |\phi_B\rangle \\
&+ \langle \phi_B | V_2^{L_1,\dagger} \Pi^B_{good} \Pi^A_{good} V_2^{L_1} |\phi_A\rangle + \langle \phi_B | V_2^{L_1,\dagger} \Pi^B_{good} V_2^{L_1} |\phi_B\rangle | \\
=&| \langle \phi_A | V_2^{L_1,\dagger} \Pi^A_{good} V_2^{L_1} |\phi_A\rangle + \langle \phi_B | V_2^{L_1,\dagger} \Pi^B_{good} V_2^{L_1} |\phi_B\rangle | \\
=&\left\| \Pi^A_{good} V_2^{L_1} |\phi_A\rangle \right\|_2^2 + \left\| \Pi^B_{good} V_2^{L_1} |\phi_B\rangle \right\|_2^2 \\
=&\left\| \Pi_{good} V_2^{L_1} |\phi_A\rangle \right\|_2^2 + \left\| \Pi_{good} V_2^{L_1} |\phi_B\rangle \right\|_2^2
\end{aligned} \tag{39}$$

4. For any state of type 2, $\left\| V_2^{L_1} |\phi_2\rangle \right\|^2 \leq \mathsf{negl}(n)$. In particular, let $D \in \mathcal{DB}$, and $\vec{\alpha}$ satisfying the requirements for states of type 2. Let

$$|\phi_2\rangle = |D\rangle \sum_{S_2 \in Val(D)} \alpha_{S_2} |S_2\rangle$$

. We will split this up into two cases.

(a) Consider the case when $D_x \in D_1$. Then,

$$\begin{aligned}
&V_2^{L_1} |\phi_2\rangle \\
=&\sum_{S_2 \in Val(D)} \alpha_{S_2} V_2^{L_1} (|D\rangle |S_2\rangle) \\
=&\sum_{S_2 \in Val(D)} \frac{1}{\sqrt{|S_2 \setminus D_1|}} \alpha_{S_2} \sum_{y \in S_2 \setminus D_1} \left| D_y^{L_1,f} \right\rangle |S_2\rangle \\
=&\frac{1}{\sqrt{M_2 - |D_1|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \sum_{\substack{S_2 \in Val(D) \\ y \in S_2}} \alpha_{S_2} |S_2\rangle \\
=&\frac{1}{\sqrt{M_2 - |D_1|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_1,f} \right\rangle \sum_{S_2 \in Val(D_y^{L_1,f})} \alpha_{S_2} |S_2\rangle
\end{aligned} \tag{40}$$

where the last line follows from Lemma B.3.
Observe that for all $y \in [N] \setminus D_{all}$, since $D_x \in D_1$, $|Val(D_y^{L_1,f})| = \binom{N - |D_{all}| - 1}{M_2 - |D_1| - 1}$.

We can then compute

$$\begin{aligned}
&\left\|\Pi_{good} V_2^{L_1} |\phi_2\rangle\right\|_2^2 \\
=&\left\|\Pi_{good}^D V_2^{L_1} |\phi_2\rangle\right\|_2^2 \\
=&\sum_{y\in[N]\setminus D_{all}} \left|\left\langle ValSt_{D_y^{L_1,f}} \right| V_2^{L_1} |\phi_2\rangle\right|^2 \\
=&\sum_{y\in[N]\setminus D_{all}} \left|\frac{1}{\sqrt{|Val(D_y^{L_1,f})|\cdot(M_2-|D_1|)}} \sum_{S_2\in Val(D_y^{L_1,f})} |S_2\rangle\right|^2 \\
=&\frac{1}{(M_2-|D_1|)\cdot\binom{N-|D_{all}|-1}{M_2-|D_1|-1}} \sum_{y\in[N]\setminus D_{all}} \left|\sum_{\substack{S_2\in Val(D)\\ y\in S_2}} \alpha_{S_2}\right|^2 \\
=&\frac{1}{(M_2-|D_1|)\cdot\binom{N-|D_{all}|-1}{M_2-|D_1|-1}} \sum_{y\in[N]\setminus D_{all}} \left|\sum_{\substack{S_2\subseteq[N]\setminus D_{all}\\ |S_2|=M_2-|D_1|\\ y\in S_2}} \alpha_{S_2\cup D_1}\right|^2
\end{aligned} \tag{41}$$

So setting $P = [N] \setminus D_{all}$ and $M = M_2 - |D_1|$ in Lemma C.1, we get

$$\begin{aligned}
&\left\|\Pi_{good} V_2^{L_1} |\phi_2\rangle\right\|_2^2 \\
\leq&\frac{\binom{N-|D_{all}|-2}{M_2-|D_1|-1}}{(M_2-|D_1|)\cdot\binom{N-|D_{all}|-1}{M_2-|D_1|-1}} \\
\leq&\mathsf{negl}(n)
\end{aligned} \tag{42}$$

(b) Now, consider the case where $D_x \notin D_1$. Then for all $S_2 \in Val(D)$, we know $D_x \notin S_2$. Thus, we get

$$\begin{aligned}
&V_2^{L_1} |\phi_2\rangle \\
=&\sum_{S_2\in Val(D)} \alpha_{S_2} V_2^{L_1}(|D\rangle |S_2\rangle) \\
=&|D\rangle \sum_{S_2\in Val(D)} \alpha_{S_2} |S_2\rangle \\
=&|\phi_2\rangle
\end{aligned} \tag{43}$$

which is in $\mathrm{Im}(I - \Pi_{good})$.

Finally, we can write $|\phi\rangle \in \mathrm{Im}(I - \Pi_{good})$ as a superposition of states of types 1 and 2 where, for each database D, D appears at most once as a state of type 1 or type 2. In particular, for all

databases $D \in \mathcal{DB}$ and subsets $S_2 \in \mathcal{P}([N])$, there exist constants $b_{D,S_2}, a_D, \alpha_{D,S_2}$ such that

$$|\phi\rangle = \sum_{D \in \mathcal{DB}} \left(|D\rangle \left(\sum_{S_2 \notin Val(D)} b_{D,S_2} |S_2\rangle + a_D \sum_{S_2 \in Val(D)} \alpha_{D,S_2} |S_2\rangle \right) \right)$$

$$\sum_D |a_D|^2 + \sum_{D,S_2} |b_{D,S_2}|^2 = 1$$

and for all D,

$$\sum_{S_2 \in Val(D)} |\alpha_{D,S_2}|^2 = 1$$

$$\sum_{S_2 \in Val(D)} \alpha_{D,S_2} = 0$$

Then by our first observation,

$$\begin{aligned} & \left\| \Pi_{good} V_2^{L_1} |\phi\rangle \right\|_2^2 \\ =& \left\| \Pi_{good} V_2^{L_1} \left(\sum_{D \in \mathcal{DB}} |D\rangle \left(\sum_{S_2 \notin Val(D)} b_{D,S_2} |S_2\rangle + a_D \sum_{S_2 \in Val(D)} \alpha_{D,S_2} |S_2\rangle \right) \right) \right\|_2^2 \\ =& \left\| \Pi_{good} V_2^{L_1} \left(\sum_{D \in \mathcal{DB}} a_D |D\rangle \sum_{S_2 \in Val(D)} \alpha_{D,S_2} |S_2\rangle \right) \right\|_2^2 \end{aligned} \tag{44}$$

And by our third and fourth observations,

$$\begin{aligned} & \left\| \Pi_{good} V_2^{L_1} |\phi\rangle \right\|_2^2 \\ =& \sum_{D \in \mathcal{DB}} \left\| a_D \Pi_{good} V_2^{L_1} |D\rangle \sum_{S_2 \in Val(D) \alpha_{D,S_2} |S_2\rangle} \right\|_2^2 \\ \leq& \left(\sum_{D \in \mathcal{DB}} |a_D|^2 \right) \cdot \mathsf{negl}(n) \\ =& \mathsf{negl}(n) \end{aligned} \tag{45}$$

□

Lemma D.3. $\left\| \Pi_{good} V_2^{L_2} - V_2^{L_2} \Pi_{good} \right\|_{op} \leq \mathsf{negl}(n)$

Proof. The proof of this will mostly follow the same argument as the previous lemma. There are only two portions of the proof which differ. In particular, we need to separately argue that

$$\Pi_{good} V_2^{L_2} \Pi_{good} = V_2^{L_2} \Pi_{good}$$

and that for $|\phi_2\rangle$ a state of type 2,

$$\left\| V_2^{L_2} |\phi_2\rangle \right\|_2^2 \leq \mathsf{negl}(n)$$

Let us first show $\Pi_{good} V_2^{L_2} \Pi_{good} = V_2^{L_2} \Pi_{good}$. Let $|\phi\rangle = \frac{1}{\sqrt{M_2}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle$ be a basis state of Π_{good}. We will show that $V_2^{L_2} |\phi\rangle \in \mathrm{Im}(\Pi_{good})$.

If $D_x \in D_1$, then for all $S_2 \in Val(D)$, $D_x \in S_2$. And so,

$$\begin{aligned} & V_2^{L_2} |\phi\rangle \\ =& \frac{1}{\sqrt{M_2 - |D_1|}} \sum_{S_2 \in Val(D)} V_2^{L_2}(|D\rangle |S_2\rangle) \\ =& \frac{1}{\sqrt{M_2 - |D_1|}} |D\rangle \sum_{S_2 \in Val(D)} |S_2\rangle \\ =& |\phi\rangle \end{aligned} \tag{46}$$

which is clearly in $\mathrm{Im}(\Pi_{good})$.

If $D_x \notin D_1$, then for all $S_2 \in Val(D)$, $D_x \in S_2$. Observe that for all $S_2 \in Val(D)$, for all $y \in [N] \setminus (S_2 \cup D_{all})$, $y \neq D_x$ and $y \notin D_2$ (since $D_2 \cup \{D_x\} \subseteq D_{all}$). Thus, for all $y \in [N] \setminus D_{all}$, $y \in [N] \setminus (S_2 \cup D_{all})$.

$$\begin{aligned} & V_2^{L_2} |\phi\rangle \\ =& \frac{1}{\sqrt{M_2}} \sum_{S_2 \in Val(D)} V_2^{L_2}(|D\rangle |S_2\rangle) \\ =& \frac{1}{\sqrt{M_2}} \sum_{S_2 \in Val(D)} \frac{1}{\sqrt{|[N] \setminus (S_2 \cup D_{all})|}} \sum_{y \in [N] \setminus (S_2 \cup D_{all})} \left| D_y^{L_2, f} \right\rangle |S_2\rangle \\ =& \frac{1}{\sqrt{M_2 \cdot (N - M_2 - |D_2 \cup \{D_x\}|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2, f} \right\rangle \sum_{\substack{S_2 \in Val(D) \\ y \notin S_2}} |S_2\rangle \\ =& \frac{1}{\sqrt{M_2 \cdot (N - M_2 - |D_2 \cup \{D_x\}|)}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2} \right\rangle \sum_{S_2 \in Val(D_y^{L_2, f})} |S_2\rangle \end{aligned} \tag{47}$$

where the last line follows from Lemma B.4. But note that this is a superposition of basis states for $\mathrm{Im}(\Pi_{good})$, and so is clearly also in $\mathrm{Im}(\Pi_{good})$.

It thus follows that $\Pi_{good} V_2^{L_2} \Pi_{good} = V_2^{L_2} \Pi_{good}$.

And so it remains to show that for $|\phi_2\rangle$ a state of type 2,

$$\left\| V_2^{L_2} |\phi_2\rangle \right\|_2^2 \leq \mathsf{negl}(n)$$

We will write

$$|\phi_2\rangle = |D\rangle \sum_{S_2 \in Val(D)} \alpha_{S_2} |S_2\rangle$$

Just as in the previous lemma, we split into two cases

1. If $D_x \in D_1$, then for all $S_2 \in Val(D)$, we know $D_x \in S_2$. And so we get

$$V_2^{L_2} |\phi_2\rangle = |\phi_2\rangle \tag{48}$$

2. If $D_x \notin D_1$, then

$$\begin{aligned}
&V_2^{L_2} |\phi_2\rangle \\
=&\sum_{S_2 \in Val(D)} \alpha_{S_2} V_2^{L_2}(|D\rangle |S_2\rangle) \\
=&\sum_{S_2 \in Val(D)} \frac{1}{\sqrt{|[N] \setminus D_{all}|}} \alpha_{S_2} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2,f} \right\rangle |S_2\rangle \\
=&\frac{1}{\sqrt{N - M_2 - |D_2 \cup \{D_x\}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2,f} \right\rangle \sum_{\substack{S_2 \in Val(D) \\ y \notin S_2}} \alpha_{S_2} |S_2\rangle \\
=&\frac{1}{\sqrt{N - M_2 - |D_2 \cup \{D_x\}|}} \sum_{y \in [N] \setminus D_{all}} \left| D_y^{L_2,f} \right\rangle \sum_{S_2 \in Val(D_y^{L_2,f})} \alpha_{S_2} |S_2\rangle
\end{aligned} \tag{49}$$

where the last line follows from Lemma B.4. Observe that for all $y \in [N] \setminus D_{all}$,

$$|Val(D_y^{L_2,f})| = \binom{N - |D_{all}| - 1}{M_2 - |D_1|}$$

Analogously to the $V_2^{L_1}$ case, we have

$$\begin{aligned}
&\left\| \Pi_{good} V_2^{L_2} |\phi_2\rangle \right\|_2^2 \\
=&\frac{1}{(N - M_2 - |D_2 \cup \{D_x\}|) \cdot \binom{N-|D_{all}|-1}{M_2-|D_1|}} \sum_{y \in [N] \setminus D_{all}} \left| \sum_{\substack{S_2 \in Val(D) \\ y \notin S_2}} \alpha_{S_2} \right|^2 \\
=&\frac{1}{(N - M_2 - |D_2 \cup \{D_x\}|) \cdot \binom{N-|D_{all}|-1}{M_2-|D_1|}} \sum_{y \in [N] \setminus D_{all}} \left| \sum_{\substack{S_2 \in Val(D) \\ y \in S_2}} \alpha_{S_2} \right|^2 \\
=&\frac{1}{(N - M_2 - |D_2 \cup \{D_x\}|) \cdot \binom{N-|D_{all}|-1}{M_2-|D_1|}} \sum_{y \in [N] \setminus D_{all}} \left| \sum_{\substack{S_2 \subseteq [N] \setminus D_{all} \\ |S_2| = M_2 - |D_1| \\ y \in S_2}} \alpha_{S_2 \cup D_1} \right|^2
\end{aligned} \tag{50}$$

where the second equality comes from the fact that $\sum_{S_2 \in Val(D)} \alpha_{S_2} = 0$. So setting $P =$

$[N] \setminus D_{all}$ and $M = M_2 - |D_1|$ in Lemma C.1, we get

$$\begin{aligned}
&\left\| \Pi_{good} V_2^{L_1} |\phi_2\rangle \right\|_2^2 \\
\leq &\frac{\binom{N-|D_{all}|-2}{M_2-|D_1|-1}}{(N - M_2 - |D_2 \cup \{D_x\}|) \cdot \binom{N-|D_{all}|-1}{M_2-|D_1|}} \\
\leq &\mathsf{negl}(n)
\end{aligned} \tag{51}$$

□

We will conclude the argument by showing that unitaries A which do not touch register **St** approximately commute with Π_{good}.

Lemma D.4. *Let A be a unitary acting on $\mathbf{A}, \mathbf{In}$. Then*

$$\left\| (A_{\mathbf{A},\mathbf{In}} \otimes I_{\mathbf{St}}(I_{\mathbf{A}} \otimes \Pi_{good}) - (I_{\mathbf{A}} \otimes \Pi_{good})(A_{\mathbf{A},\mathbf{In}\otimes I_{\mathbf{St}}}) \right\|_{op} \leq \mathsf{negl}(n)$$

Proof. We will define a different projector $\widetilde{\Pi}_{good}$ which is close to Π_{good} in operator norm and exactly commutes with all such unitaries A. In particular, define $\widetilde{Val}(D)$ to be the same as $Val(D)$ except for the condition on D_x. That is, $\widetilde{Val}(D) = \{S_2 : D_1 \subseteq S_2, D_2 \cap S_2 = \emptyset\}$. Similarly, we define

$$\left|\widetilde{ValSt}_D\right\rangle = \frac{1}{\sqrt{|\widetilde{Val}(D)|}} |D\rangle \sum_{S_2 \in \widetilde{Val}(D)} |S_2\rangle$$

Define $\widetilde{\Pi}_{good} = \sum_D \left|\widetilde{ValSt}_D\right\rangle\!\left\langle\widetilde{ValSt}_D\right|$.

We will separately show

$$\left\| \Pi_{good} \widetilde{\Pi}_{good} - \Pi_{good} \right\|_{op} \leq \mathsf{negl}(n)$$

$$\left\| \widetilde{\Pi}_{good} \Pi_{good} - \Pi_{good} \right\|_{op} \leq \mathsf{negl}(n)$$

By Proposition 2.11, it is sufficient to show that for all unit vectors $|\phi\rangle$,

$$|\langle\phi| \widetilde{\Pi}_{good} \Pi_{good} \widetilde{\Pi}_{good} |\phi\rangle|^2 \geq 1 - \mathsf{negl}(n)$$

$$|\langle\phi| \Pi_{good} \widetilde{\Pi}_{good} \Pi_{good} |\phi\rangle|^2 \geq 1 - \mathsf{negl}(n)$$

That is, for all unit vectors $|\phi\rangle \in \mathrm{Im}(\Pi_{good})$,

$$\left\| \widetilde{\Pi}_{good} |\phi\rangle \right\|_2^2 \geq 1 - \mathsf{negl}(n)$$

and for all unit vectors $|\psi\rangle \in \mathrm{Im}(\widetilde{\Pi}_{good})$,

$$\| \Pi_{good} |\phi\rangle \|_2^2 \geq 1 - \mathsf{negl}(n)$$

Note that $|\widetilde{Val}(D)| = \binom{N-|D_1|-|D_2|}{M_2-|D_1|}$. Meanwhile, $|Val(D)| \geq \binom{N-|D_1|-|D_2|-1}{M_2-|D_1|}$

And so we observe

$$\begin{aligned}
&\left\langle \widetilde{ValSt}_D \middle| ValSt_D \right\rangle \\
=&\frac{|Val(D) \cap \widetilde{Val}(D)|}{\sqrt{|Val(D)| \cdot |\widetilde{Val}(D)|}} \\
\geq&\frac{|Val(D)|}{|\widetilde{Val}(D)|} \\
\geq&\frac{\binom{N-|D_1|-|D_2|-1}{M_2-|D_1|}}{\binom{N-|D_1|-|D_2|}{M_2-|D_1|}} \\
=&\frac{(N-|D_1|-|D_2|-1)!(M_2-|D_1|)!(N-M_2-|D_2|)!}{(N-|D_1|-|D_2|)!(M_2-|D_1|)!(N-M_2-|D_2|-1)!} \\
=&\frac{N-M_2-|D_2|}{N-|D_1|-|D_2|} \\
\geq&\frac{N-M_2-2t}{N} \\
\geq&1-\mathsf{negl}(n)
\end{aligned} \tag{52}$$

and for $D \neq D'$,

$$\left\langle \widetilde{ValSt}_D \middle| ValSt_D \right\rangle = 0$$

1. Let $|\phi\rangle = \sum_D \alpha_D |ValSt_D\rangle$ be a unit vector in $\mathrm{Im}(\Pi_{good})$. Define

$$\left|\widetilde{\phi}\right\rangle = \sum_D \alpha_D \left|\widetilde{ValSt}_D\right\rangle$$

   Then

$$\begin{aligned}
&\left\langle \widetilde{\phi} \middle| \phi \right\rangle \\
=&\sum_D |\alpha_D|^2 (1-\mathsf{negl}(n)) \\
\geq&1-\mathsf{negl}(n)
\end{aligned} \tag{53}$$

   Thus, since $\left|\widetilde{\phi}\right\rangle \in \mathrm{Im}(\widetilde{\Pi}_{good})$,

$$\left\| \widetilde{\Pi_{good}} |\phi\rangle \right\|_2^2 \geq 1-\mathsf{negl}(n)$$

2. A symmetric argument gives that for all $|\psi\rangle \in \mathrm{Im}(\widetilde{\Pi}_{good})$,

$$\|\Pi_{good} |\psi\rangle\|_2^2 \geq 1-\mathsf{negl}(n)$$

Thus, $\left\| \Pi_{good} - \widetilde{\Pi}_{good} \right\|_{op} \leq \mathsf{negl}(n)$.

But it is clear that for any unitary A,

$$(A_{\mathbf{A},\mathbf{In}} \otimes I_{\mathbf{St}}) \cdot (I_{\mathbf{A}} \otimes \widetilde{\Pi}_{good}) = (I_{\mathbf{A}} \otimes \widetilde{\Pi}_{good}) \cdot (A_{\mathbf{A},\mathbf{In}} \otimes I_{St}).$$

And so by Lemma 2.9, where $\approx$ means negligibly close in operator distance, we have

$$A\Pi_{good} \approx A\widetilde{\Pi}_{good} = \widetilde{\Pi}_{good}A \approx \Pi_{good}A \tag{54}$$

□