

An Operator-Norm Approach to Security with Quantum Advice

Tight(er) Bounds for Decision Games and Salting

Minki Hhan¹ Sunghyuk Jo¹ Qipeng Liu²

¹KAIST, Daejeon, Korea

minkihhan@kaist.ac.kr, josung9921@kaist.ac.kr

²UC San Diego, USA

qipengliu0@gmail.com

Abstract

Non-uniform security allows an adversary to receive bounded advice about an oracle before attempting a fresh challenge. This captures the most realistic attacks and has already been studied extensively in prior work. In this work, we introduce an operator-norm approach for non-uniform security in the quantum random oracle and random permutation models. This new approach yields a unified reduction for both search success probability and distinguishing advantage. Previously, the reduction only worked with success probability even in the decision games, yielding a worse bound.

Our framework enables tight bounds for Yao’s box, both with and without salting, and improved bounds for pseudorandom generators. We also prove an optimal generic salting theorem for decision games. By defining a property of a game, which separates the contributions of the existing queries in the offline stage and subsequent online queries, we obtain stronger bounds for specific salted constructions. These include salted permutation inversion, tight up to logarithmic factors, and salted random-function inversion, tight up to logarithmic factors and the gap already present in classical function inversion.

AI use disclosure. ChatGPT-5.6 Sol Ultra discovered a slightly worse PRG bound in a one-shot query. Subsequent conversations improved and generalized the results to the current bounds. The original proof was written in the language of operator inequalities. The authors interpreted the intermediate terms as the operational characterization of the game advantages and observed their relations. The current manuscript is entirely written by the authors based on this understanding, with assistance from ChatGPT-6 Astra in improving its presentation.

Contents

1	Introduction	3
1.1	Our Results	4
1.2	Technical Overview	5
2	Preliminaries	9
2.1	Compressed Oracle and Function Database Hierarchy	9
2.2	Permutation Analogue and Permutation Database Hierarchy	11
2.3	Uniform One-Point Reprogramming	13
3	Connecting Non-uniform Security with Bit-Fixing Security	13
3.1	Game, QROM and QRPM	13
3.2	Bit-Fixing, Quantum Auxiliary-Input, and Advantage	13
3.3	Game Operators and Their Purified Representation	15
3.4	QAI Security from Database-Size-Restricted Operator Bounds	16
4	Improving Non-uniform Security for Salting	19
4.1	Salted Database Hierarchy	20
4.2	Salting Defeats Quantum Advice	21
4.3	(γ, Δ) -Diffuse Games	23
5	Details of Applications	24
5.1	PRG Game	24
5.2	Yao's Box	26
5.3	OWF Game	27
5.4	Permutation inversion game	28
A	Missing Proofs	31
A.1	Proof for the Uniform one-point reprogramming lemma	31
A.2	Diffuse Bounds for Decision Games	33
A.3	Proof of Lemma 4.6	36
A.4	Proof of Lemma 5.2	37
A.5	Proof of Lemma 5.6	39
A.6	Proof of Lemma 5.10	40
A.7	Proof of Lemma 5.14	40
B	Database Size Increment per Query	41

1 Introduction

In modern cryptographic designs, hash functions and block ciphers form a handy toolkit for building practical and secure constructions. They are in turn analyzed in idealized models such as the random oracle model (ROM) [BR93], where we treat a hash function as a uniformly random oracle. Public permutations and block ciphers are similarly idealized in the random permutation model (RPM) and ideal cipher model (ICM). While these idealized models provide rigorous security analysis, the usefulness of these guarantees depends on how faithfully the model captures the resources available to an adversary.

Preprocessing is a particularly important resource. In practice, a relatively small collection of hash functions and block ciphers is standardized, while they are reused across many applications and over long periods of time. An adversary may therefore invest substantial computation in analyzing these standardized primitives in advance, and later make use of this preprocessing to accelerate the attack. This motivates non-uniform security models [Yao90, Unr07, CDG18] in which an online adversary receives *advice* of bounded size, occasionally called *auxiliary input*, that depends on the underlying ideal primitives. Further work established time-space tradeoffs for function inversion and pseudorandom generators [DTT10, DGK17], followed by tight bounds for permutation-based PRGs and matching attacks for Yao’s box [GGKL21]. Other work characterized how salting limits the advantage from preprocessing [DLW24].

Quantum computing adds a further resource dimension. On one hand, the quantum adversary making queries to the oracles in superposition becomes a new threat [BDF⁺11], introducing the quantum random oracle model (QROM), which allows quantum queries to the random oracles—QRPM and QICM are defined analogously. On the other hand, massive classical preprocessing can begin before a large-scale quantum computer becomes available, introducing a possibility of quantum attacks with classical preprocessing [NABT14, HXY19]. Subsequent work established stronger quantum time-space tradeoffs for function inversion and developed a framework with applications to Yao’s box and salted cryptography [CGLQ20].

The bit-fixing (BF) model is one of the methods to deal with the preprocessing lower bound. In this model, the adversary presamples or fixes parts of the oracles instead of receiving the advice [Unr07, CDGS18]. The preprocessing security is then bounded by the bit-fixing security. Guo, Li, Liu, and Zhang developed a quantum version of bit-fixing [GLLZ21] based on the implicit ideas in [CGLQ20]. These ideas lead to the tight non-uniform security of function inversion and more in the QROM given *classical* advice.

More generally, a quantum adversary may store a quantum state as the outcome of preprocessing, which we refer to as quantum auxiliary input (QAI). Early lower bounds for inversion with quantum advice were established for random permutations [HXY19] and random functions [CLQ20]. The most conservative model is therefore the quantum idealized model with quantum advice, for example QAI-QROM and QAI-QICM. The security in the presence of QAI is much more difficult to show. One difficulty is that quantum advice cannot generally be copied, and using it may disturb the state, complicating arguments based on reuse or rewinding. Beyond these proof-technical obstacles, quantum advice can be intrinsically more powerful than classical advice: exponential separations are known for certain games in the QROM [Liu23], and a separation between BQP/qpoly and BQP/poly is known relative to classically accessible classical oracles [LLPY24]. Related work on quantum versus classical proofs established a classical-oracle separation of QMA and QCMA under a quantum pseudorandomness conjecture [LMY25], followed by an unconditional classical-oracle separation [BHNZ26].

The reduction between QAI security and the quantum version of BF security has been established in [CGLQ20, Liu23]. There are two versions of these reductions with multiplicative loss and additive loss, which are used for the search problems and decision problems, respectively. The multiplicative version is relatively tight and yields the tight OWF security of random oracles and permutations in the corresponding QAI models [Liu23, ABC⁺26]. More precisely, they obtain a security bound $O((ST + T^2)/N)$, where N is the domain size of the function or permutation (assuming a codomain of size at least N in the function case), S is the number of advice qubits, and T is the number of online quantum queries.

The tightness of the additive version (as well as the non-uniform security for many decision games) is unclear. For example, the proven PRG advantage is about $O((T^2/N)^{1/2} + (ST/N)^{1/3})$ while there are known attacks with the advantage $\Omega(T^2/N + (S/N)^{1/2})$ where the first term is due to quantum search and the

second term is from [DTT10].¹ Ignoring constant factors, obtaining an advantage bound on the order of 2^{-128} from the previous result requires $n \approx 640$ when $S = T = 2^{128}$, compared with $n \approx 384$ for the corresponding OWF bound.

Another open question concerns preprocessing security with salting. The generic phenomenon called the salting-defeat-preprocessing [CDGS18] is shown in the QAI setting as well. However, for the size of the salting space K , these generic theorems incur a loss of S/K for many search games [DLW24] and $(ST/K)^{1/3}$ for all decision games [Liu23]. In many security games, the desired security would be tighter; for example, the OWF security with an $O(ST/KN)$ term is known in AI-ROM [DGK17, CDGS18]. A similar quantum result is only in the AI-QROM setting with loose bounds of $O(ST^2/KN)$ [HXY19]. With the previous results, salting is known to defeat preprocessing only with a very lengthy salt, e.g., $K = 2^{640}$ against $S = T = 2^{128}$ to have 2^{-128} PRG advantage.

1.1 Our Results

In this paper, we systematically study the idealized model in the QAI setting. We present a new route towards understanding non-uniform security with quantum advice in the idealized models. We present a new method based on the operator norm of a quantum algorithm, and connect it to the bit-fixing model [CGLQ20, GLLZ21].

To state our results, let S be the number of advice qubits, T denote the number of online queries, and P the number of offline queries in the bit-fixing model. Let N and M denote the oracle domain and range sizes, respectively.

Our first result is the unified reduction between QAI security and the quantum bit-fixing security. Previously, the bound connected the success probabilities in both the QAI setting and the BF setting. Our new result directly applies to the advantages in both cases—for decision games, the advantage is defined as the absolute difference between the success probability and $1/2$. This improves the additive bound of [Liu23, Theorem 6.1] and [GLLZ21, Theorem 1].

Theorem 1.1 (QAI security to BF security, informal). *Fix any game G . Let $\delta(S, T)$ be the maximum advantage that a quantum algorithm with S -qubit auxiliary input and T quantum queries can achieve. Let $\nu(P, T)$ be the maximum advantage in the P -BF model with at most T quantum queries. Then we have*

$$\delta(S, T) \leq \sqrt{2} \cdot \nu(Sr, T),$$

where $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$. Here T_{Sample} and T_{Verify} are the numbers of queries made by the sampler and verifier in G , respectively.

This theorem alone improves the QAI-QROM security of Yao’s box problem from $\tilde{O}(\sqrt[19]{S^5 T/N})$ in [CGLQ20]² to $O(\sqrt{ST/N})$. For PRG security, we prove the bound $O(\sqrt{ST/N} + T^2/N)$. The previous best bound was $O(\sqrt[3]{ST/N} + \sqrt{T^2/N})$ [Liu23]. The improvement of the first term is due to the improved reduction. For the second term, we observe that the PRG security in the quantum P -bit-fixing model can be improved from $O(\sqrt{(P+T^2)/N})$ to $O(\sqrt{P/N} + T^2/N)$ using the polynomial method [BBC+98]. All comparisons can be found in Table 1.

Salting. Throughout the presentation below, we use the same conventions for S , T , N , M , and P . We let K denote the size of the salt space.

Let $\nu_G(T)$ and $\varepsilon_G(T)$ denote the base game’s, i.e., without salting, uniform search success and decision advantage, respectively. Existing works [CGLQ20, GLLZ21] have established bit-fixing bounds for salted games. In the QROM, they show $O(\nu_G(T) + P/K)$ for search games and $O(\varepsilon_G(T) + \sqrt{P/K})$ for decision games. Using these bit-fixing bounds, [Liu23, Theorem 7.5] obtained QAI bounds of $O(\nu_G(T) + Sr/K)$ for search games and $O(\varepsilon_G(T) + (Sr/K)^{1/3})$ for decision games, where $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$.

¹The preprocessing inversion algorithm [Hel80] can be used to attack PRGs with the advantage $\min(ST/N, (S^2 T/N^2)^{1/3})$. This does not change the discussion about the parameters here. This observation was suggested by ChatGPT 6 Astra.

²This can be further improved to $O(\sqrt[3]{ST/N})$ by [Liu23, Theorem 6.1], but was never explicitly written up.

Decision Game	Known Bound	Ours
PRG	$O\left(\sqrt[3]{\frac{ST}{N}} + \sqrt{\frac{T^2}{N}}\right)$	$O\left(\sqrt{\frac{ST}{N}} + \frac{T^2}{N}\right)$
Yao's box	$\tilde{O}\left(\sqrt[19]{\frac{S^5 T}{N}}\right)$ or $O\left(\sqrt[3]{\frac{ST}{N}}\right)$	$O\left(\sqrt{\frac{ST}{N}}\right)$

Table 1: We assume $T \geq 1$ in this table. PRG bound is from [Liu23, Theorem 1.2]. Yao's box bound is from [CGLQ20, Theorem 1.4] and can be improved by [Liu23, Theorem 6.1].

Our generic salting theorem (Theorem 4.2) recovers the search bound up to constant factors and improves the salt-dependent term in the decision bound from $(Sr/K)^{1/3}$ to $\sqrt{Sr/K}$. We obtain this refinement by combining the salting analysis of [CGLQ20] with our novel operator-norm-based approach.

Theorem 1.2 (Salting for decision games, informal). *Fix a decision game $\mathcal{G}$ in the QROM or quantum random permutation model (QRPM) with uniform T -query advantage at most $\varepsilon_{\mathcal{G}}(T)$. Let $\mathcal{G}_S$ be its salted version with K independent oracle instances and a uniformly random challenge salt. Then the maximum advantage of a quantum adversary with S -qubit auxiliary input and at most T online queries satisfies*

$$\varepsilon_{\mathcal{G}_S}^{\text{QAI}}(S, T) = O\left(\varepsilon_{\mathcal{G}}(T) + \sqrt{\frac{Sr}{K}}\right),$$

where $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$, and T_{Sample} and T_{Verify} are the numbers of queries made by the sampler and verifier, respectively.

The square-root term is optimal for general decision games. Indeed, the one-bit Yao game ($N = 1$) has zero uniform advantage, and its salted version is Yao's box on K bits. The attack of [GGKL21, Theorem 1.3] achieves $\Omega(\sqrt{S(T+1)/K})$, matching this term since $r = 2(T+1)$.

As already noticed by [CDGS18], the salting-defeat-preprocessing gives a worse bound than the direct application of bit-fixing to the salted games. Thus, we individually work on different games and obtain refined bounds for various games, in both the QROM and QRPM. All comparisons and results can be found in Table 2.

Our unsalted and salted Yao's-box bounds are tight up to constant factors, matching the classical attack of [GGKL21, Theorem 1.3] with domain sizes N and KN , respectively. Our salted permutation-inversion bound is tight up to logarithmic factors, by choosing between Grover search and Hellman's attack with preprocessing distributed across salts [Hel80, ABC⁺26].

For salted random-function OWFs and $T \geq 1$, our bound matches the attacks (See e.g., [HXY19, Table 1]) up to logarithmic factors whenever $ST^2 \leq K \min\{N, M\}$. It also matches Grover search whenever $S \leq KT$, since the uniform term then dominates.

1.2 Technical Overview

In this section, we will go over the main ideas used to obtain these results.

Purified game operators and database hierarchies. We start by expressing the adversary's advantage through an operator. Let $\mathcal{G}$ be a game which can be either a search or a decision game with oracle space $\mathcal{F}$ which can be either a set of functions or a set of permutations. Fix a quantum adversary $\mathcal{A}$ who receives S -qubit advice and makes T quantum queries to the oracle $H \in \mathcal{F}$. Let $\{\rho_H\}_{H \in \mathcal{F}}$ be the family of advice states, each of which depends on H and is stored in advice register A . Without loss of generality, we can

Salted Game	Known Bound	Ours
PRG	$O\left(\sqrt[3]{\frac{ST}{K}} + \sqrt{\frac{T^2}{N}}\right)$	$O\left(\sqrt{\frac{ST}{KN}} + \frac{T^2}{N}\right)$
Yao's box	$\tilde{O}\left(\sqrt[19]{\frac{S^5 T}{KN}}\right)$	$O\left(\sqrt{\frac{ST}{KN}}\right)$
OWF	$O\left(\frac{ST}{K} + \frac{T^2}{\min\{N, M\}}\right)$	$O\left(\frac{ST}{K \min\{N, M\}} + \frac{T^2}{\min\{N, M\}}\right)$
PermInv	$\tilde{O}\left(\left(\frac{ST^2}{KN} + \frac{T^2}{N}\right)^{1/3}\right)$	$O\left(\frac{ST}{KN} + \frac{T^2}{N}\right)$

Table 2: We assume $T \geq 1$ in this table. PRG and OWF bounds are from [Liu23, Theorem 1.3]. Yao's box bound follows from [CGLQ20, Theorem 1.4] after substituting $N \mapsto KN$. PermInv bound is from [HXY19, Theorem 6].

purify the algorithm and assume that $\mathcal{A}$ applies a unitary V^H on the joint registers AW . Let Π be the final projection to the acceptance space. Define the Hermitian operator

$$E^H := (I_A \otimes \langle 0|_W)(V^H)^\dagger \Pi V^H (I_A \otimes |0\rangle_W).$$

Then, for the search game $\mathcal{G}$, the winning probability is $\mathbb{E}_H[\text{Tr}(\rho_H E^H)]$.

For a decision game, we define two projections Π_T to the accepted space and $\Pi_F = I - \Pi_T$ to the rejected space. As in the search game case, for each projection, we define the Hermitian operator

$$\begin{aligned} E_T^H &:= (I_A \otimes \langle 0|_W)(V^H)^\dagger \Pi_T V^H (I_A \otimes |0\rangle_W) \\ E_F^H &:= (I_A \otimes \langle 0|_W)(V^H)^\dagger \Pi_F V^H (I_A \otimes |0\rangle_W). \end{aligned}$$

Finally, we define $E^H := (E_T^H - E_F^H)/2$. Then, its decision advantage is $|\mathbb{E}_H[\text{Tr}(\rho_H E^H)]|$.

Instead of bounding $|\mathbb{E}_H[\text{Tr}(\rho_H E^H)]|$ directly, we bound it through the high-order moment of its operator norm as follows: for any integer $k \geq 1$,

$$\begin{aligned} |\mathbb{E}_H[\text{Tr}(\rho_H E^H)]| &\leq \mathbb{E}_H[\|E^H\|_{\text{op}}] \\ &\leq (\mathbb{E}_H[\|E^H\|_{\text{op}}^{2k}])^{1/(2k)} \leq (\mathbb{E}_H[\text{Tr}|E^H|^{2k}])^{1/(2k)}. \end{aligned}$$

The second inequality follows from the monotonicity of L^p norms, and the last from $\|E^H\|_{\text{op}}^{2k} \leq \text{Tr}|E^H|^{2k}$.

The next step is to bound this spectral moment by expressing it as the norm of a vector. We start our argument from the purified oracle state $|\Omega_{\mathcal{F}}\rangle \sim \sum_{H \in \mathcal{F}} |H\rangle$ in oracle register O . We purify the family of operators $\{E^H\}_{H \in \mathcal{F}}$ into $M_{\mathcal{E}}$:

$$M_{\mathcal{E}} := \sum_{H \in \mathcal{F}} |H\rangle\langle H| \otimes E^H.$$

Now, assume the algorithm starts with a maximally mixed advice state, but purified as a maximally entangled state using an additional reference register R ,

$$|\Phi\rangle := \frac{1}{\sqrt{d}} \sum_{a \in [d]} |a\rangle_A |a\rangle_R.$$

Since E^H only applies to the advice register, we have $d = \dim \mathcal{H}_A \leq 2^S$. Let $|v_0\rangle := |\Omega_{\mathcal{F}}\rangle |\Phi\rangle$ be the initial state, with the purified oracle and the maximally entangled state.

We can define $|v_j\rangle := M_{\mathcal{E}}|v_{j-1}\rangle = M_{\mathcal{E}}^j|v_0\rangle$ for $j \geq 1$. Therefore, we have for all integers $k \geq 1$,

$$\|v_k\|_2^2 = \mathbb{E}_H \left[\frac{1}{d} \sum_{a=1}^d \langle a | (E^H)^{2k} | a \rangle \right] = \mathbb{E}_H \left[\frac{1}{d} \text{Tr} |E^H|^{2k} \right]. \quad (1)$$

Thus, from the inequality above, the advantage is at most $d^{1/(2k)} \|v_k\|_2^{1/k}$.

Remark 1.3 (Comparison to the existing high-moment method.). The high-moment viewpoint already appears in [CGLQ20, Liu23]. In the alternating-measurement framework of [Liu23], they use two types of rounds: odd rounds test success, while even rounds project the randomness register back onto its initial uniform superposition. This argument relates the success probability of a non-uniform algorithm to the success probability in the so-called alternating-measurement game. Our method works directly on the operator that represents the advantage, rather than the success probability, while the alternating measurement framework does not extend to the case when the operator E^H is no longer positive semi-definite (in the decision games).

Bit-fixing security as a database-size-restricted operator norm. Next, we will analyze the state $|v_k\rangle$. Since it corresponds to a repeated application of $M_{\mathcal{E}}$ on the initial state $|v_0\rangle$, we will use the compressed-oracle technique [Zha19] for analyzing the joint state over the algorithm and oracle. It has already been applied to analyze non-uniform security in the QROM [CGLQ20], as well as in the QRPM using its permutation counterpart [ABC⁺26]. We will mostly focus on the function case in the overview.

Intuitively, the compressed oracle uses the database size to capture the amount of information an algorithm has learned about the random function so far; the database size can only be increased by one per query. Thus, we can formally define the space of joint states having database size at most P by

$$\mathcal{L}_P := \text{span}\{|x, y\rangle_{A,R} |\phi_D\rangle_O : |D| \leq P\}.$$

Let $\Pi_{\leq P}$ be the orthogonal projection onto $\mathcal{L}_P$.

We observe that $M_{\mathcal{E}}$ increases the database size by at most $r = 2(T + T_{\text{Sample}} + T_{\text{Verify}})$ where the 2 factor comes from both the applications of $(V^H)^\dagger$ and V^H . Since $|v_j\rangle \in \mathcal{L}_{jr} \subseteq \mathcal{L}_{(j+1)r}$ and $|v_{j+1}\rangle \in \mathcal{L}_{(j+1)r}$, for $0 \leq j < k$,

$$|v_{j+1}\rangle = \Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq jr} |v_j\rangle = \Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r} |v_j\rangle.$$

Hence,

$$\|v_{j+1}\|_2 \leq \|\Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r}\|_{op} \|v_j\|_2.$$

Here, we call terms like $\|\Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r}\|_{op}$ the database-size-restricted operator norm.

Iterating gives, for any $k \geq 1$,

$$\|v_k\|_2 \leq \prod_{j=0}^{k-1} \|\Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r}\|_{op} \leq \|\Pi_{\leq kr} M_{\mathcal{E}} \Pi_{\leq kr}\|_{op}^k. \quad (2)$$

Combining Eq. (1) and Eq. (2) with $k = S$ gives

$$|\mathbb{E}_H[\text{Tr}(\rho_H E^H)]| \leq \sqrt{2} \|\Pi_{\leq Sr} M_{\mathcal{E}} \Pi_{\leq Sr}\|_{op}.$$

The value $\|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{op}$ is in fact related to the (P, T) -bit-fixing model, as implicitly proposed by [CGLQ20] and defined in [GLLZ21]. The bit-fixing model has two phases: the offline phase and the online phase. In the offline phase, the adversary can make P quantum queries to the oracle $H \in \mathcal{F}$ and do any post-selection to produce a state $|\psi\rangle$. In the online phase, a challenge is received, and the adversary makes at most T quantum queries to solve the challenge starting from $|\psi\rangle$. Let A be the shared register between the offline phase and the online phase. Then $|\langle \psi | M_{\mathcal{E}} | \psi \rangle|$ is nothing but the online phase's advantage on the game $\mathcal{G}$ starting from $|\psi\rangle$.

Surprisingly, we show that the offline phase can produce any unit vector $|\psi\rangle \in \mathcal{L}_P$, and therefore the (P, T) -bit-fixing model has exactly the same security as the database-size-restricted operator norm³! Take an arbitrary unit vector $|\psi\rangle \in \mathcal{L}_P$. Then by definition, it has an expression $|\psi\rangle \sim \sum_{|D| \leq P} |\phi_D\rangle_O |z_D\rangle_A$. We prepare the state

$$|\Psi_P\rangle \sim \sum_{|D| \leq P} |\phi_D\rangle_O |0\rangle_A |D\rangle_R,$$

which can be done by applying P quantum queries on each support of D , on the state $|\Psi_0\rangle \sim |\Omega_{\mathcal{F}}\rangle_O \otimes |0\rangle_A \otimes \sum_{|D| \leq P} |D\rangle_R$ where R is a helper register. Setting the operator acting on register RA ,

$$F := \sum_{|D| \leq P} |0\rangle\langle D|_R \otimes |z_D\rangle\langle 0|_A,$$

we have $(I_O \otimes F)|\Psi_P\rangle \sim |\psi\rangle_{OA} |0\rangle_R$. Taking a constant $c \in \mathbb{R}_{>0}$ sufficiently small, we obtain $K := cF$ with $\|K\|_{op} \leq 1$. From the singular value decomposition of K , we observe that K can be implemented by postselection.

Taking a supremum over $|\psi\rangle \in \mathcal{L}_P$ and online algorithms, we get

$$\text{Adv}_{\mathcal{G}}^{\text{BF}}(P, T) = \sup_{\mathcal{A}} \|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{op}.$$

Therefore,

$$|\mathbb{E}_H[\text{Tr}(\rho_H E^H)]| \leq \sqrt{2} \text{Adv}_{\mathcal{G}}^{\text{BF}}(Sr, T).$$

Salting and the database contribution. From the discussion above, it suffices to bound $\|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{op}$. For many decision games like PRGs and Yao's box, it is already studied in [CGLQ20]; thus we can immediately get an improved bound for these decision games using the new operator-norm-based reduction. We also improve a term in the PRG security using the polynomial method [BBC⁺98]. We omit this detail in this overview. Next, we will mostly focus on salting.

As $M_{\mathcal{E}}$ is Hermitian, it suffices to bound $|\langle \psi | M_{\mathcal{E}} | \psi \rangle|$ for any $|\psi\rangle \in \mathcal{L}_P$. Let $\Pi_{=j}$ be the orthogonal projection to the space of joint states having database size exactly j . We define the database-size observable $\Lambda := \sum_j j \Pi_{=j}$ to measure the expected size of the database with which $|\psi\rangle$ is entangled. Its value is $\langle \psi | \Lambda | \psi \rangle$ and it is less than or equal to P for $|\psi\rangle \in \mathcal{L}_P$. We bound $|\langle \psi | M_{\mathcal{E}} | \psi \rangle|$ with $f(\langle \psi | \Lambda | \psi \rangle)$ for some real-valued function f .

We define the salted database hierarchy. Let $[K]$ be the salt space. Every salted oracle is of the form $(H_1, \dots, H_K)$. Let O_s be the oracle register for the salt $s \in [K]$. Then the joint oracle register O is $O_1 \otimes \dots \otimes O_K$. Each salt s has its own database D_s . The salted database is $D = (D_1, \dots, D_K)$ and its size is $\sum_{s \in [K]} |D_s|$. Let Λ_s be the database-size observable on O_s , acting as the identity on all other registers. Define $\mathcal{L}_P^{(K)}$ as the subspace spanned by eigenvectors of $\sum_{s \in [K]} \Lambda_s$ with eigenvalues at most P . Thus every unit vector $|\psi\rangle \in \mathcal{L}_P^{(K)}$ satisfies

$$\sum_{s \in [K]} \langle \psi | \Lambda_s | \psi \rangle \leq P.$$

We define the operator $M_{\mathcal{E}_s}$ in a similar way for a fixed salt s , acting on register $O_s AZ$ where Z includes the oracle registers O_t for $t \neq s$. For a uniformly random salt, the salted game operator is

$$M_{\mathcal{E}^{(K)}} := \frac{1}{K} \sum_{s \in [K]} M_{\mathcal{E}_s}.$$

Since each $M_{\mathcal{E}_s}$ raises the database size by at most r , the same is true for $M_{\mathcal{E}^{(K)}}$.

³The other half—any state produced in the (P, T) -bit-fixing model is in $\mathcal{L}_P$ —holds immediately by definition, and was proved in [CGLQ20].

We prove that the adversary's advantage in the salted game is bounded by the uniform security of the base game plus Sr/K for a search game and $\sqrt{Sr/K}$ for a decision game. For a fixed salt s , we may treat all other oracle registers other than O_s as auxiliary workspace and absorb their queries into H_s -independent local unitaries. It follows that if a joint state has $|D_s| = 0$, it can be considered a valid base-game uniform security experiment on the oracle H_s . Let $\Pi_{s,=0}$ be the projection to the space of joint states with $|D_s| = 0$.

For any $|\psi\rangle \in \mathcal{L}_P^{(K)}$, we split it into $|\psi_0\rangle := \Pi_{s,=0}|\psi\rangle$ and $|\psi_1\rangle := (I - \Pi_{s,=0})|\psi\rangle$. Then $|\langle\psi_0|M_{\mathcal{E}_s}|\psi_0\rangle|$ can be bounded by its uniform security, and $|\langle\psi_1|M_{\mathcal{E}_s}|\psi_1\rangle|$ can be bounded by $\langle\psi|\Lambda_s|\psi\rangle$ as $I - \Pi_{s,=0} \preceq \Lambda_s$. For a search game, we exploit the fact that $M_{\mathcal{E}_s}^{1/2}$ exists and use the triangle inequality. Then, we get

$$\langle\psi|M_{\mathcal{E}_s}|\psi\rangle \leq \left(\sqrt{\langle\psi_0|M_{\mathcal{E}_s}|\psi_0\rangle} + \sqrt{\langle\psi_1|M_{\mathcal{E}_s}|\psi_1\rangle}\right)^2 \leq \left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{\langle\psi|\Lambda_s|\psi\rangle}\right)^2.$$

Averaging it over $s \in [K]$ gives $\langle\psi|M_{\mathcal{E}^{(K)}}|\psi\rangle \leq \left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{P/K}\right)^2$.

For a decision game, as $-I/2 \preceq M_{\mathcal{E}_s} \preceq I/2$, it need not admit a positive semi-definite square root, and thus a triangle inequality does not apply. We expand $\langle\psi|M_{\mathcal{E}_s}|\psi\rangle$ in terms of $\langle\psi_i|M_{\mathcal{E}_s}|\psi_j\rangle$ where $i, j \in \{0, 1\}$ and bound each term. This results in the weaker exponent $1/2$.

These generic bounds can be loose for specific games, as already observed in the classical setting [CDGS18]. For example, when a database of expected size L contributes only $O(L/N)$, averaging over salts gives an $O(P/(KN))$ contribution, yielding an $O(Sr/(KN))$ term after our reduction. The following diffuseness condition captures such additional structure. We say a game is a (γ, Δ) -diffuse game if there exist $\tau_T \geq 0$ and $\kappa \geq 0$ such that, for any $|\psi\rangle$,

$$|\langle\psi|M_{\mathcal{E}}|\psi\rangle| \leq \tau_T + \kappa \left(\frac{\langle\psi|\Lambda|\psi\rangle}{\Delta}\right)^\gamma.$$

Then, in the salting case, the same thing applies: for any $|\psi\rangle$,

$$|\langle\psi|M_{\mathcal{E}_s}|\psi\rangle| \leq \tau_T + \kappa \left(\frac{\langle\psi|\Lambda_s|\psi\rangle}{\Delta}\right)^\gamma.$$

Averaging the above inequality over $s \in [K]$ proves that if a base game is a (γ, Δ) -diffuse game, then its salt term is $\kappa(Sr/K\Delta)^\gamma$. We prove that many games satisfy this property, including OWF, PRG, and Yao's box; this naturally gives tighter or even tight non-uniform bounds with quantum advice, as in [Tables 1 and 2](#).

2 Preliminaries

We assume that the readers are familiar with the basics of quantum computation and information, and refer to [NC10] for standard background. A positive operator-valued measure (POVM) on a register A is a family $\{E_z\}_z$ of positive semidefinite operators satisfying $\sum_z E_z = I_A$. For a state ρ on A , outcome z occurs with probability $\text{Tr}(\rho E_z)$. We call E_z the POVM element corresponding to outcome z ; in particular, $0 \preceq E_z \preceq I_A$.

2.1 Compressed Oracle and Function Database Hierarchy

In this section, we briefly review several key concepts from [Zha19]. We refer the reader to the original paper for further details.

In the quantum random oracle model (QROM), a query to a fixed oracle $H \in \mathcal{F} := \{H : [N] \rightarrow [M]\}$ is coherently processed by the following unitary

$$|x\rangle|u\rangle \mapsto |x\rangle|u + H(x)\rangle.$$

We work with the *purified* oracles by default. In this setting, the oracle register O is initialized to

$$|\Omega_{\mathcal{F}}\rangle_O := \frac{1}{\sqrt{|\mathcal{F}|}} \sum_{H \in \mathcal{F}} |H\rangle_O$$

and the queries to the oracle are implemented by the unitary

$$|H\rangle|x\rangle|u\rangle \mapsto |H\rangle|x\rangle|u + H(x)\rangle.$$

Another equivalent and useful formulation is the phase oracle:

$$|H\rangle|x\rangle|u\rangle \mapsto \omega_M^{uH(x)}|H\rangle|x\rangle|u\rangle$$

where $\omega_M := e^{2\pi i/M}$ is the primitive M -th root of unity. It is well known that the output distribution of any algorithm having access to the phase oracles is identical to the output distribution with the quantum random oracles by changing the response register to the Fourier basis. Therefore, results for one oracle imply the same results for the other. From now on, $\mathcal{O}$ denotes the phase-oracle query to the underlying oracle H .

Lemma 2.1 ([Zha19, Lemma 3]). *Let $\mathcal{A}$ be an (unbounded) quantum algorithm making queries to a standard oracle. Let $\mathcal{B}$ be the algorithm that is identical to $\mathcal{A}$, except it performs QFT and QFT[†] before and after each query. Then the output distributions of $\mathcal{A}$ (given access to a standard oracle) and $\mathcal{B}$ (given access to a phase oracle) are identical. Therefore, a quantum random oracle can be perfectly simulated as a phase oracle.*

The compressed oracle analysis shows that, after P queries, the oracle state lies in the span of Fourier basis states supported on at most P inputs. We formalize database hierarchies below, building on these approaches. We follow the notation of [CGLQ20, Section 2.3]. We identify the set $\mathcal{F} := \{H : [N] \rightarrow [M]\}$ with $\mathbb{Z}_M^N$ by the map $D \mapsto (D(1), \dots, D(N))$. For $D \in \mathbb{Z}_M^N$, define

$$\langle D, H \rangle := \sum_{x \in [N]} D(x)H(x) \pmod{M}, \quad |\phi_D\rangle := \frac{1}{M^{N/2}} \sum_{H \in \mathcal{F}} \omega_M^{\langle D, H \rangle} |H\rangle$$

where the state $|\phi_D\rangle$ is called the Fourier (basis) state. The set of Fourier states $|\phi_D\rangle$ forms an orthonormal basis for all $D \in \mathbb{Z}_M^N$.

Let $|D|$ denote the number of nonzero coordinates of D , which is often referred to as “database size” in the original [Zha19]. For an oracle register O and an integer $P \geq 0$, define the space spanned by database states of size at most P by

$$\mathcal{L}_P := \text{span}\{|\phi_D\rangle_O : |D| \leq P\}$$

Let $\Pi_{\leq j}$ be the orthogonal projection onto $\mathcal{L}_j$. The function database hierarchy refers to the nested family

$$\mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \dots \subseteq \mathcal{L}_N$$

where $\mathcal{L}_N$ is the full ambient space of the database. A state has database size at most P if it lies in $\mathcal{L}_P$.

The following fact shows that the database size of the states is consistent with the number of queries made by the algorithm. We include the proof in [Appendix B](#) for completeness.

Fact 2.2 (Database Size Increase for Random Functions [Zha19]). *Let R contain the query registers and any auxiliary registers. For every integer $P \geq 0$, a phase-oracle query $\mathcal{O}$ on the register OR satisfies*

$$\mathcal{O}(\mathcal{L}_P \otimes \mathcal{H}_R) \subseteq \mathcal{L}_{P+1} \otimes \mathcal{H}_R.$$

Thus one query increases the database size by at most one, even allowing arbitrary entanglement between the oracle and the registers in R .

We will use the subspaces of exact database size, which are defined by $\mathcal{D}_0 := \mathcal{L}_0$ and, for $j \geq 1$, $\mathcal{D}_j := \mathcal{L}_j \cap \mathcal{L}_{j-1}^\perp$. Orthogonality of the Fourier states gives

$$\mathcal{D}_j = \text{span}\{|\phi_D\rangle_O : |D| = j\}. \tag{3}$$

We define the orthogonal projection $\Pi_{=j}$ onto $\mathcal{D}_j$ for $j \geq 0$. For $j \geq 1$, $\Pi_{=j} = \Pi_{\leq j} - \Pi_{\leq j-1}$ and for $j = 0$, $\Pi_{=0} = \Pi_{\leq 0}$. We define the associated database-size observable by

$$\Lambda = \sum_{j=1}^N j \Pi_{=j}.$$

By the orthogonality of the Fourier states $|\phi_D\rangle$, Λ can be rewritten as

$$\Lambda = \sum_{D \in \mathbb{Z}_M^N} |D| |\phi_D\rangle \langle \phi_D|. \quad (4)$$

It shows that for any unit vector $|\psi\rangle \in \mathcal{L}_P$, $\langle \psi | \Lambda | \psi \rangle \leq P$.

2.2 Permutation Analogue and Permutation Database Hierarchy

In the quantum random permutation model (QRPM), the oracle is a uniformly random permutation $H \in \mathcal{F}^{\text{perm}} := S_N$, where S_N is the set of permutations of $[N]$. We only consider the forward evaluation access: for a fixed H , a query acts as

$$|x\rangle|u\rangle \mapsto |x\rangle|u + H(x)\rangle$$

where the addition in the response register is modulo N . Thus, the query interface is the same as for random functions, with the oracle distribution restricted to permutations.

We again use the purified oracle representation. Initialize the oracle register O to the uniform superposition of permutations

$$|\Omega_{\mathcal{F}^{\text{perm}}}\rangle_O := \frac{1}{\sqrt{N!}} \sum_{H \in S_N} |H\rangle_O,$$

and implement each query by the controlled unitary

$$|H\rangle|x\rangle|u\rangle \mapsto |H\rangle|x\rangle|u + H(x)\rangle.$$

As in [Section 2.1](#), we use the equivalent phase-oracle representation, obtained by changing the response register to the Fourier basis:

$$\mathcal{O} : |H\rangle|x\rangle|u\rangle \mapsto \omega_N^{uH(x)} |H\rangle|x\rangle|u\rangle.$$

To track the oracle states generated by these queries, we use the database subspaces of [\[ABC⁺26, Section 2.3\]](#) which stem from [\[Ros22\]](#). While their formalization requires the representation theory of symmetric groups, we only need a hierarchy structure of the permutation database. We introduce the relevant definitions and results in this section.

A permutation database in the QRPM is represented by a *partial permutation assignment*, which is an injective function $\alpha : D \rightarrow [N]$ for a subset $D \subseteq [N]$. The size of a partial permutation assignment (henceforth, a database) is $|\alpha| := |D|$. For $H \in \mathcal{F}^{\text{perm}}$, write $\alpha \subseteq H$ if $H(x) = \alpha(x)$ for every $x \in D$. Let $\text{im}(\alpha)$ denote the image of α . For any $x \notin D$ and $y \notin \text{im}(\alpha)$, let $\alpha \cup \{x \mapsto y\}$ denote a larger database with domain $D \cup \{x\}$ that agrees with α on D and maps x to y .

Define the partial assignment state

$$|v_\alpha\rangle := \frac{1}{\sqrt{(N-|\alpha|)!}} \sum_{\alpha \subseteq H \in \mathcal{F}^{\text{perm}}} |H\rangle.$$

This is the uniform superposition over all permutations consistent with the database α . There are $(N-|\alpha|)!$ such permutations, which explains the normalization. In particular, the empty database gives $|v_\emptyset\rangle = |\Omega_{\mathcal{F}^{\text{perm}}}\rangle$.

For an oracle register O and an integer $P \geq 0$, we define the space spanned by (permutation) database states of size at most P by

$$\mathcal{L}_P^{\text{perm}} := \text{span}\{|v_\alpha\rangle_O : |\alpha| \leq P\}.$$

Let $\Pi_{\leq j}^{\text{perm}}$ be the orthogonal projection onto $\mathcal{L}_j^{\text{perm}}$. This gives the permutation database hierarchy

$$\mathcal{L}_0^{\text{perm}} \subseteq \mathcal{L}_1^{\text{perm}} \subseteq \mathcal{L}_2^{\text{perm}} \subseteq \dots \subseteq \mathcal{L}_{N-1}^{\text{perm}}$$

where the last term is $\mathcal{L}_{N-1}^{\text{perm}}$ because it is already the full ambient space. Analogously, we say a state has database size at most P if it lies in $\mathcal{L}_P^{\text{perm}}$.

Remark 2.3. In [ABC⁺26], they define the space spanned by (permutation) database states by $\mathcal{L}_P^{\text{perm}} = \text{span}\{|v_\alpha\rangle_O : |\alpha| = P\}$, i.e., the span of the database states of size exactly P . The two definitions are identical for $0 \leq P \leq N$ because of the identity

$$|v_\alpha\rangle = \frac{1}{\sqrt{N-j}} \sum_{y \notin \text{im}(\alpha)} |v_{\alpha \cup \{x \rightarrow y\}}\rangle,$$

for any $|\alpha| = j < N$ and $x \notin \text{dom}(\alpha)$. If $P > N$, $\mathcal{L}_P^{\text{perm}}$ is the full ambient space.

Similarly to [Fact 2.2](#), the database size of the states is consistent with the number of queries made by the algorithm. See [Appendix B](#) for the proof.

Fact 2.4 (Database Size Increase for Random Permutations [ABC⁺26]). *Let R contain the query registers and any auxiliary registers. For every integer $P \geq 0$, a phase-oracle query $\mathcal{O}$ on OR satisfies*

$$\mathcal{O}(\mathcal{L}_P^{\text{perm}} \otimes \mathcal{H}_R) \subseteq \mathcal{L}_{P+1}^{\text{perm}} \otimes \mathcal{H}_R.$$

Thus one query increases the database size by at most one, allowing arbitrary entanglement between the oracle and the registers in R .

The subspaces of exact database size for permutations are defined analogously to the function case. Define $\mathcal{D}_0^{\text{perm}} := \mathcal{L}_0^{\text{perm}}$ and, for $j \geq 1$, define $\mathcal{D}_j^{\text{perm}} := \mathcal{L}_j^{\text{perm}} \cap (\mathcal{L}_{j-1}^{\text{perm}})^\perp$. We define the orthogonal projection $\Pi_{=j}^{\text{perm}}$ onto $\mathcal{D}_j^{\text{perm}}$ for $j \geq 0$. For $j \geq 1$, $\Pi_{=j}^{\text{perm}} := \Pi_{\leq j}^{\text{perm}} - \Pi_{\leq j-1}^{\text{perm}}$ and for $j = 0$, $\Pi_{=0}^{\text{perm}} := \Pi_{\leq 0}^{\text{perm}}$. Note that

$$\sum_{j=0}^{N-1} \Pi_{=j}^{\text{perm}} = \Pi_{\leq N-1}^{\text{perm}} = I, \quad \Pi_{=i}^{\text{perm}} \Pi_{=j}^{\text{perm}} = \delta_{i,j} \Pi_{=i}^{\text{perm}} \quad (5)$$

where $\delta_{i,j} = 1$ if and only if $i = j$. This gives an orthogonal decomposition of the space of permutations.

The associated database-size observable is defined by

$$\Lambda^{\text{perm}} := \sum_{j=1}^{N-1} j \Pi_{=j}^{\text{perm}}.$$

We remark that the vectors $|v_\alpha\rangle$ are not mutually orthogonal in the permutation case. Consequently, the subspaces of exact database size and the database-size observable do not admit the simple basis description as in the function case (see [Eqs. \(3\)](#) and [\(4\)](#)).

For permutations, database size is measured by the orthogonal hierarchy sectors using [Eq. \(5\)](#) instead; $|v_\alpha\rangle$ may have components at several sizes, all at most $|\alpha|$. For any unit vector $|\psi\rangle \in \mathcal{L}_P^{\text{perm}}$ with $P \leq N-1$, decompose $|\psi\rangle$ orthogonally as $|\psi\rangle = \sum_{j=0}^P |\psi_j\rangle$, where $|\psi_j\rangle := \Pi_{=j}^{\text{perm}} |\psi\rangle \in \mathcal{D}_j^{\text{perm}}$. Then

$$\langle \psi | \Lambda^{\text{perm}} | \psi \rangle = \sum_{j=1}^P j \cdot \|\psi_j\|_2^2 \leq P.$$

2.3 Uniform One-Point Reprogramming

We introduce one-point reprogramming. Let $H \in \mathcal{F}$ and $h \in [M]$. For each $x \in [N]$, define the one-point reprogrammed function

$$H_{x \rightarrow h}(w) := \begin{cases} h, & w = x, \\ H(w), & w \neq x. \end{cases}$$

The following lemma bounds the change in acceptance probability when the reprogrammed point is uniformly random and independent of the circuit. We present a direct proof of the stated version using the polynomial method [BBC⁺98] in [Section A.1](#).

Lemma 2.5 (Uniform one-point reprogramming). *Fix an arbitrary oracle $H : [N] \rightarrow \mathbb{Z}_M$, $h \in \mathbb{Z}_M$, and a quantum circuit making at most T oracle queries. Suppose that its initial state, inter-query operations, and final measurement are independent of $x \xleftarrow{\$} [N]$. Write $a(x)$ for the circuit's acceptance probability with oracle $H_{x \rightarrow h}$ and $a(\emptyset)$ for its acceptance probability with oracle H . Then*

$$\left| \mathbb{E}_{x \xleftarrow{\$} [N]}[a(x)] - a(\emptyset) \right| \leq \frac{4T^2}{N}.$$

3 Connecting Non-uniform Security with Bit-Fixing Security

This section gives a new reduction from the non-uniform security to the bit-fixing security. Our reduction gives a better bound for the decision games, improving upon [CGLQ20, Liu23]. To this end, we provide an operational view of the security games.

3.1 Game, QROM and QRPM

A game $\mathcal{G} = (\mathcal{C})$, where $\mathcal{C} = (\text{Sample}, \text{Query}, \text{Verify})$, is an interactive protocol between a challenger and an adversary $\mathcal{A}$. Before beginning the game, we sample a uniformly random function $H : [N] \rightarrow [M]$ in the QROM or a uniformly random permutation $H \in S_N$ in the QRPM. Throughout this section, $\mathcal{F}$ denotes the corresponding oracle space, and $\{\mathcal{L}_P\}_{P \geq 0}$ denotes its database hierarchy from [Section 2](#).

The game $\mathcal{G}$ proceeds as follows. The challenger runs Sample^H and gives the resulting challenge y to $\mathcal{A}$. The adversary accesses H through Query^H , which is H itself in most games except for Yao's box problem. Each query increases the database size by at most one. The challenger then runs Verify^H and stores the resulting bit in the verification register V .

For any joint register R of the algorithm and the challenger (which is disjoint from the oracle register O), we extend the definition of the bounded-size database spaces, associated projections, and the database-size observable by

$$\mathcal{L}_P(R) := \mathcal{L}_P \otimes \mathcal{H}_R, \quad \Pi_{\leq P}(R) := \Pi_{\leq P} \otimes I_R, \quad \Lambda(R) := \Lambda \otimes I_R.$$

We use the same convention for exact size spaces and their projectors and implicitly extend operators by appending the identity on untouched registers. We omit R when it is clear from the context.

3.2 Bit-Fixing, Quantum Auxiliary-Input, and Advantage

Bit-Fixing Model. We use the quantum bit-fixing framework of [GLLZ21].

Definition 3.1 (Bit-Fixing Model). *A (P, T) -bit-fixing adversary $\mathcal{A}$ for a game $\mathcal{G} = (\mathcal{C})$, where $\mathcal{C} = (\text{Sample}, \text{Query}, \text{Verify})$, consists of the following two stages.*

– **Offline phase.**

1. A uniformly random oracle $H \in \mathcal{F}$ is sampled;
2. The offline algorithm makes at most P quantum queries to H , and outputs a bit b such that $\Pr[b = 0] > 0$;

3. If $b \neq 0$, the process restarts from Step 1.

– **Online phase.**

1. The challenger runs Sample^H , gives the resulting challenge y to the online algorithm, and retains the state required for the verification;
2. On input y , the online algorithm makes at most T additional quantum queries through Query^H and outputs ans ;
3. The challenger runs Verify^H .

The purified oracle version of the bit-fixing model is naturally defined by starting with the initial state

$$|\phi_0\rangle := |\Omega_{\mathcal{F}}\rangle_O |0\rangle_{AZB},$$

where O denotes the oracle register, A, Z denote the adversary's workspace and auxiliary register, and B denotes the flag qubit register, respectively. The final step of the offline algorithm can be understood as a postselection. The offline algorithm outputs the postselected state $|\psi_0\rangle_{OAZB}$, and it becomes the input of the online algorithm. The online algorithm can access register A but not registers ZB . Let W denote the joint register of all other online workspace registers. We refer the reader to [ABC⁺26, Section 2.2] for a more detailed discussion.

Quantum Auxiliary-Input Model.

Definition 3.2 (Quantum Auxiliary-Input Model). *An (S, T) -quantum-auxiliary-input adversary $\mathcal{A}$ for a game $\mathcal{G} = (\mathcal{C})$, where $\mathcal{C} = (\text{Sample}, \text{Query}, \text{Verify})$, consists of the following single stage.*

1. A uniformly random oracle $H \in \mathcal{F}$ is sampled;
2. $\mathcal{A}$ receives an S -qubit auxiliary-input state ρ_H in register A , which may depend on H ;
3. The challenger runs Sample^H , gives the resulting challenge y to $\mathcal{A}$, and retains the state required for the verification;
4. $\mathcal{A}$ makes at most T quantum queries to Query^H , and outputs an answer ans ;
5. The challenger runs Verify^H .

With respect to the purified oracles, we can view the input to the online algorithm as the mixed state, up to normalization,

$$\sum_{H \in \mathcal{F}} |H\rangle\langle H| \otimes \rho_H.$$

Adversary's Advantage. We define the adversary's advantage according to whether the game is a search or decision game and whether the adversary is in the bit-fixing or quantum auxiliary-input model. For a search game $\mathcal{G}$, the adversary's advantage is defined to be the supremum of the winning probability

$$\delta_{\mathcal{G}}^{\text{QAI}}(S, T) := \sup_{\mathcal{A}} \Pr[\mathcal{A} \text{ wins}], \quad \delta_{\mathcal{G}}^{\text{BF}}(P, T) := \sup_{\mathcal{A}} \Pr[\mathcal{A} \text{ wins}]$$

where the first supremum is over the (S, T) -auxiliary-input adversaries, and the second is over the (P, T) -bit-fixing adversaries.

For a decision game $\mathcal{G}$, the adversary's advantage is the supremum of the absolute bias of its winning probability from $1/2$:

$$\varepsilon_{\mathcal{G}}^{\text{QAI}}(S, T) := \sup_{\mathcal{A}} \left| \Pr[\mathcal{A} \text{ wins}] - \frac{1}{2} \right|, \quad \varepsilon_{\mathcal{G}}^{\text{BF}}(P, T) := \sup_{\mathcal{A}} \left| \Pr[\mathcal{A} \text{ wins}] - \frac{1}{2} \right|$$

where the ranges of the supremum are the same as above.

When a statement applies to either type of game, we simply write

$$\text{Adv}_{\mathcal{G}}^{\text{QAI}}(S, T), \quad \text{Adv}_{\mathcal{G}}^{\text{BF}}(P, T)$$

3.3 Game Operators and Their Purified Representation

Recall that A denotes the workspace of the algorithm. In the bit-fixing model, this register may contain some state after the postselection. In the quantum auxiliary input model, this register includes an S -qubit advice state depending on the oracle.

Theorem 3.3. *Fix a game $\mathcal{G} = (\mathcal{C})$ and the algorithm $\mathcal{A}$ used after the challenge is generated. There exists a game-operator family $\mathcal{E} := \{E^H\}_{H \in \mathcal{F}}$ on register A , induced by $(\mathcal{G}, \mathcal{A})$, such that every E^H is Hermitian and $\|E^H\|_{\text{op}} \leq 1$; moreover, $0 \preceq E^H \preceq I$ if $\mathcal{G}$ is a search game. Define the corresponding purified game operator on OA by*

$$M_{\mathcal{E}} := \sum_{H \in \mathcal{F}} |H\rangle\langle H|_O \otimes E^H.$$

For a quantum auxiliary-input adversary using $\mathcal{A}$ with advice family $\{\rho_H\}_{H \in \mathcal{F}}$, the advantage of this adversary is

$$|\mathbb{E}_H[\text{Tr}(\rho_H E^H)]|.$$

For a bit-fixing adversary whose online algorithm is $\mathcal{A}$, let $|\psi_0\rangle_{OAZB}$ be the joint state produced by its offline phase, including the algorithm's register as well as oracle registers. The advantage of this adversary is

$$|\langle \psi_0 | (M_{\mathcal{E}} \otimes I_{ZB}) | \psi_0 \rangle|.$$

Proof. Let W collect all registers used in the game $\mathcal{G}$ by the sampler, the adversary $\mathcal{A}$, and the verifier other than A ; these registers are initialized to $|0\rangle_W$. By purifying the computation and deferring measurements, we may assume that, for each fixed $H \in \mathcal{F}$, the sampler, $\mathcal{A}$, and the verifier are jointly implemented by a unitary V^H .

Search Game. Let $\Pi := |1\rangle\langle 1|_V \otimes I$ be the projection onto the accepting subspace acting on the verify register V . Conditioned on H , the winning probability of $\mathcal{A}$ is

$$\Pr[\text{win} \mid H] = \text{Tr}(\Pi V^H (\rho_H \otimes |0\rangle\langle 0|_W) (V^H)^\dagger).$$

Let E^H be the operator defined by

$$E^H := (I_A \otimes \langle 0|_W) (V^H)^\dagger \Pi V^H (I_A \otimes |0\rangle_W).$$

This is the POVM element on the initial advice register A corresponding to the winning outcome, so that $\Pr[\text{win} \mid H] = \text{Tr}(\rho_H E^H)$.

Decision Game. Let $\Pi_T := |1\rangle\langle 1|_V \otimes I$ and $\Pi_F := |0\rangle\langle 0|_V \otimes I$ be the final projectors corresponding to a true and a false decision, respectively. Define the POVM elements on A corresponding to these two outcomes:

$$E_T^H := (I_A \otimes \langle 0|_W) (V^H)^\dagger \Pi_T V^H (I_A \otimes |0\rangle_W),$$

$$E_F^H := (I_A \otimes \langle 0|_W) (V^H)^\dagger \Pi_F V^H (I_A \otimes |0\rangle_W),$$

and define the decision-game operator as half their difference

$$E^H := \frac{1}{2}(E_T^H - E_F^H).$$

We use the same notation E^H in both cases, although the construction differs. In the search case, $0 \preceq E^H \preceq I$; in either case, E^H is Hermitian and $\|E^H\|_{\text{op}} \leq 1$. The fixed-oracle identities above hold for any input state on A . In the quantum auxiliary-input model, this state is ρ_H , and averaging over uniformly random H gives the claimed formula. In the bit-fixing model, the online phase starts from the normalized postselected state $|\psi_0\rangle_{OAZB}$ produced by the offline phase. The online algorithm receives register A from the offline phase, while ZB remain untouched. The same operators E^H apply, since their construction depends only on the online experiment, not on how its input state was prepared. Since the joint experiment is controlled by O and acts trivially on ZB , its pulled-back operator on $OAZB$ is $M_{\mathcal{E}} \otimes I_{ZB}$, which gives the bit-fixing formula. $\square$

3.4 QAI Security from Database-Size-Restricted Operator Bounds

The following theorem bounds quantum auxiliary-input advantage by bit-fixing advantage. We first characterize bit-fixing security by database-size-restricted norms of the purified game operators, and then prove the reduction using a moment argument.

Theorem 3.4. *Let $\mathcal{G} = (\mathcal{C})$ be a game with $\mathcal{C} = (\text{Sample}, \text{Query}, \text{Verify})$. Let $T_{\text{Sample}}, T, T_{\text{Verify}}$ be the numbers of queries that the sampler, adversary, and verifier make, respectively. Then,*

$$\text{Adv}_{\mathcal{G}}^{\text{QAI}}(S, T) \leq \sqrt{2} \text{Adv}_{\mathcal{G}}^{\text{BF}}(2S(T_{\text{Sample}} + T + T_{\text{Verify}}), T).$$

Theorem 3.4 strengthens the results of [Liu23] for decision games; it establishes a previously unknown bound, which eventually enables improvement for many decision games, including PRG and Yao’s box. We defer the proof to the end of the section, after establishing the following theorem.

Theorem 3.5 (Size-Restricted Operator Norm and Bit-Fixing Model). *Fix a game $\mathcal{G} = (\mathcal{C})$ and integers $P, T \geq 0$. For each online algorithm $\mathcal{A}$ making at most T queries through Query^H , let $\mathcal{E}_{\mathcal{A}}$ be its induced game-operator family on its input register A . Then*

$$\text{Adv}_{\mathcal{G}}^{\text{BF}}(P, T) = \sup_{\mathcal{A}} \|\Pi_{\leq P} M_{\mathcal{E}_{\mathcal{A}}} \Pi_{\leq P}\|_{\text{op}}, \quad (6)$$

where the supremum ranges over all such online algorithms and their input-register choices. For each fixed online algorithm, its database-size-restricted operator norm equals the optimal bit-fixing advantage over offline phases making at most P queries.

The key idea is that every joint state of the oracle and algorithm registers produced by a (P, T) -bit-fixing offline phase is supported on $\text{im}(\Pi_{\leq P} \otimes I)$, and conversely every state with this support can be prepared using at most P queries and postselection.

Proof of Theorem 3.5. Fix an online algorithm $\mathcal{A}$, and write $\mathcal{E} := \mathcal{E}_{\mathcal{A}}$. Any offline phase making at most P queries produces, after postselection, a normalized state $|\psi_0\rangle_{OAZB} \in \mathcal{L}_P(AZB)$: the initial oracle state has size zero; each query increases the size by at most one by **Facts 2.2** and **2.4**, and postselection on the algorithm’s registers preserves membership in this subspace. Its reduced state $\sigma_{OA} := \text{Tr}_{ZB} |\psi_0\rangle\langle\psi_0|$ therefore satisfies $\sigma_{OA} = \Pi_{\leq P} \sigma_{OA} \Pi_{\leq P}$. The bit-fixing advantage is consequently bounded by

$$|\text{Tr}(\sigma_{OA} M_{\mathcal{E}})| = |\text{Tr}(\sigma_{OA} \Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P})| \leq \|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{\text{op}}.$$

Conversely, we show that every unit vector $|\psi\rangle_{OA} \in \mathcal{L}_P(A)$ can be prepared using at most P queries and postselection with positive probability. We give the construction for both database hierarchies.

Case 1: Function. Let $C_F := \sum_{j=0}^P \binom{N}{j} (M-1)^j$ be the number of all possible databases of size at most P . Adjoining the register R to the purified oracle state $|\Omega_{\mathcal{F}}\rangle = |\phi_0\rangle$, prepare

$$|\Psi_0^F\rangle_{OR} := \frac{1}{\sqrt{C_F}} \sum_{\substack{D \in \mathbb{Z}_M^N \\ |D| \leq P}} |\phi_0\rangle_O |D\rangle_R.$$

For each D , write $\text{supp}(D) = \{x_1 < \dots < x_k\}$, where $k = |D|$. For $1 \leq i \leq k$, coherently compute $(x_i, D(x_i))$ from D , apply the phase oracle, and uncompute the query registers. If $k < P$, each of the remaining queries is made at a fixed point with phase label 0. Since

$$\mathcal{O}(|\phi_{D'}\rangle_O |x, u\rangle) = |\phi_{D' + ue_x}\rangle_O |x, u\rangle,$$

the resulting state is

$$|\Psi_P^F\rangle_{OR} = \frac{1}{\sqrt{C_F}} \sum_{\substack{D \in \mathbb{Z}_M^N \\ |D| \leq P}} |\phi_D\rangle_O |D\rangle_R.$$

Case 2: Permutation. First suppose that $P \leq N - 1$. Prepare

$$|\Psi_0^{\text{perm}}\rangle_{OR} := \frac{1}{\sqrt{\binom{N}{P} N!}} \sum_{X \in \binom{[N]}{P}} \sum_{H \in \mathcal{F}^{\text{perm}}} |H\rangle_O |X, 0^P\rangle_R.$$

For $X = \{x_1 < \dots < x_P\}$, query $x_1, \dots, x_P$ in the standard oracle form, implemented using one phase-oracle query per point by [Lemma 2.1](#), and store their images in R . This gives

$$|\Psi_P^{\text{perm}}\rangle_{OR} = \frac{1}{\sqrt{\binom{N}{P} N!}} \sum_{X \in \binom{[N]}{P}} \sum_{H \in \mathcal{F}^{\text{perm}}} |H\rangle_O |H|_X\rangle_R.$$

Since $\sum_{H \supseteq \alpha} |H\rangle_O = \sqrt{(N-P)!} |v_\alpha\rangle_O$, we have

$$|\Psi_P^{\text{perm}}\rangle_{OR} = \sqrt{\frac{(N-P)!}{\binom{N}{P} N!}} \sum_{\substack{\alpha \text{ database} \\ |\alpha| = P}} |v_\alpha\rangle_O |\alpha\rangle_R.$$

By [Section 2.2](#), the vectors $|v_\alpha\rangle$ with $|\alpha| = P$ span $\mathcal{L}_P^{\text{perm}}$. For $P > N - 1$, use the construction with $P = N - 1$, since $\mathcal{L}_P^{\text{perm}} = \mathcal{L}_{N-1}^{\text{perm}}$.

Constructing the unitary. In either case, the resulting state has the form

$$|\Psi_P\rangle_{OR} = \gamma \sum_a |w_a\rangle_O |a\rangle_R,$$

where $\gamma > 0$ is the corresponding coefficient above, and $(a, |w_a\rangle)$ denotes $(D, |\phi_D\rangle)$ in the function case and $(\alpha, |v_\alpha\rangle)$ in the permutation case. Since the vectors $|w_a\rangle$ span $\mathcal{L}_P$, choose vectors $|z_a\rangle_A$ such that

$$|\psi\rangle_{OA} = \sum_a |w_a\rangle_O |z_a\rangle_A.$$

Define an operator F on RA by

$$F := \sum_a |0\rangle\langle a|_R \otimes |z_a\rangle\langle 0|_A.$$

Then

$$(I_O \otimes F)(|\Psi_P\rangle_{OR} |0\rangle_A) = \gamma |\psi\rangle_{OA} |0\rangle_R.$$

Take $c := 1/(1 + \|F\|_{op}) > 0$ and set $K := cF$. Then $\|K\|_{op} \leq 1$. Let $K = U\Sigma V^\dagger$ be its singular value decomposition, and choose an orthonormal basis $\{|j\rangle\}$ of RA such that $\Sigma|j\rangle = s_j|j\rangle$, where $0 \leq s_j \leq 1$. We implement K by postselection.

Let B be a flag qubit. For an arbitrary state $|r\rangle_{RA}$, start with $|r\rangle_{RA} |0\rangle_B$. Apply $V^\dagger$:

$$|r\rangle_{RA} |0\rangle_B \mapsto \sum_j r_j |j\rangle |0\rangle_B, \quad r_j := \langle j|V^\dagger|r\rangle.$$

Apply the rotation:

$$|j\rangle |0\rangle_B \mapsto |j\rangle (s_j |0\rangle_B + \sqrt{1 - s_j^2} |1\rangle_B).$$

After applying U , the resulting state is

$$\begin{aligned} & \sum_j r_j U|j\rangle (s_j |0\rangle_B + \sqrt{1 - s_j^2} |1\rangle_B) \\ &= U\Sigma V^\dagger |r\rangle |0\rangle_B + U\sqrt{I - \Sigma^2} V^\dagger |r\rangle |1\rangle_B \\ &= K|r\rangle |0\rangle_B + L|r\rangle |1\rangle_B \end{aligned}$$

where $L := U\sqrt{I - \Sigma^2}V^\dagger$. Let this unitary be $\mathcal{U}$. It follows that

$$\begin{aligned} & (I_O \otimes \mathcal{U})(|\Psi_P\rangle_{OR}|0\rangle_A|0\rangle_B) \\ &= c\gamma|\psi\rangle_{OA}|0\rangle_R|0\rangle_B + (I_O \otimes L)(|\Psi_P\rangle_{OR}|0\rangle_A)|1\rangle_B. \end{aligned}$$

Thus, postselecting on $B = 0$, which occurs with probability $c^2\gamma^2 > 0$, leaves R in the fixed state $|0\rangle_R$ and the remaining registers in the state $|\psi\rangle_{OA}$.

For each unit vector $|\psi\rangle \in \mathcal{L}_P(A)$, the construction gives a valid bit-fixing adversary with online algorithm $\mathcal{A}$ and advantage $|\langle\psi|M_{\mathcal{E}}|\psi\rangle|$. The maximum of this expression is the database-size-restricted operator norm, attained by an eigenvector whose eigenvalue has the largest absolute value. Together with the upper bound, this proves the characterization for each fixed online algorithm. Taking the supremum over online algorithms proves Eq. (6). $\square$

Proof of Theorem 3.4. For $S = 0$, the conclusion is obvious as there is no advice and no offline part in both games.

We assume $S \geq 1$. Fix an arbitrary (S, T) -quantum auxiliary-input adversary with online algorithm $\mathcal{A}$ and advice family $\{\rho_H\}_{H \in \mathcal{F}}$. Let $\mathcal{E}$ be its induced game-operator family, put $d := \dim \mathcal{H}_A \leq 2^S$, and set $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$. For the fixed online query budget T , set

$$\beta(P) := \text{Adv}_{\mathcal{G}}^{\text{BF}}(P, T) \quad \text{for every integer } P \geq 0.$$

This function is nondecreasing because increasing the offline query budget enlarges the set of allowed adversaries. By Theorem 3.5, the purified game operator of the fixed online algorithm $\mathcal{A}$ satisfies

$$\|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{\text{op}} \leq \beta(P) \quad \text{for every integer } P \geq 0. \quad (7)$$

We consider the iterative application of $M_{\mathcal{E}}$ on the state $|v_0\rangle := |\Omega_{\mathcal{F}}\rangle_O |\Phi_d\rangle_{AR}$, where $|\Phi_d\rangle$ is the maximally entangled state obtained by adjoining a d -dimensional reference register R :

$$|\Phi_d\rangle := \frac{1}{\sqrt{d}} \sum_{a=1}^d |a\rangle_A |a\rangle_R.$$

For $j \geq 1$, set $|v_j\rangle := M_{\mathcal{E}}^j |v_0\rangle$. Since $|v_0\rangle \in \mathcal{L}_0$ and $\| |v_0\rangle \|_2 = 1$, $|v_j\rangle \in \mathcal{L}_{jr}$ for every $j \geq 0$. Moreover, we can write

$$|v_k\rangle = \frac{1}{\sqrt{|\mathcal{F}|d}} \sum_{H \in \mathcal{F}} \sum_{a=1}^d |H\rangle (E^H)^k |a\rangle_A |a\rangle_R.$$

Since every E^H is Hermitian, orthogonality of the oracle and reference-register bases gives

$$\| |v_k\rangle \|_2^2 = \mathbb{E}_H \left[\frac{1}{d} \sum_{a=1}^d \langle a | (E^H)^{2k} | a \rangle \right] = \mathbb{E}_H \left[\frac{1}{d} \text{Tr} |E^H|^{2k} \right]. \quad (8)$$

The right-hand side is the $2k$ -th moment of a random eigenvalue, obtained by sampling H uniformly and then sampling one of the d eigenvalues of E^H uniformly, counting multiplicities.

On the other hand, since $|v_j\rangle \in \mathcal{L}_{jr} \subseteq \mathcal{L}_{(j+1)r}$ and $|v_{j+1}\rangle \in \mathcal{L}_{(j+1)r}$, for $0 \leq j < k$,

$$|v_{j+1}\rangle = \Pi_{\leq (j+1)r} |v_{j+1}\rangle = \Pi_{\leq (j+1)r} M_{\mathcal{E}} |v_j\rangle = \Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r} |v_j\rangle.$$

Hence, by Eq. (7),

$$\| |v_{j+1}\rangle \|_2 \leq \|\Pi_{\leq (j+1)r} M_{\mathcal{E}} \Pi_{\leq (j+1)r}\|_{\text{op}} \| |v_j\rangle \|_2 \leq \beta((j+1)r) \| |v_j\rangle \|_2.$$

Iterating gives, because β is nondecreasing,

$$\|v_k\|_2 \leq \prod_{j=0}^{k-1} \beta((j+1)r) \leq \beta(kr)^k. \quad (9)$$

Combining Eq. (8) and Eq. (9) proves the moment bound

$$\mathbb{E}_H \left[\frac{1}{d} \text{Tr} |E^H|^{2k} \right]^{1/(2k)} \leq \beta(kr) \quad (10)$$

for any $k \geq 1$. The bound $|\text{Tr}(\rho_H E^H)| \leq \|E^H\|_{\text{op}}$, monotonicity of L_p norms, and Eq. (10) give, for any $k \geq 1$,

$$\begin{aligned} |\mathbb{E}_H [\text{Tr}(\rho_H E^H)]| &\leq \mathbb{E}_H [\|E^H\|_{\text{op}}] \\ &\leq (\mathbb{E}_H [\|E^H\|_{\text{op}}^{2k}])^{1/(2k)} \\ &\leq d^{1/(2k)} \left(\mathbb{E}_H \left[\frac{1}{d} \text{Tr} |E^H|^{2k} \right] \right)^{1/(2k)} \\ &\leq d^{1/(2k)} \beta(kr). \end{aligned}$$

Taking $k = S$ gives $d^{1/(2S)} \leq (2^S)^{1/(2S)} = \sqrt{2}$ and hence

$$|\mathbb{E}_H [\text{Tr}(\rho_H E^H)]| \leq \sqrt{2} \beta(Sr).$$

Substituting $Sr = 2S(T_{\text{Sample}} + T + T_{\text{Verify}})$ in the bound above and taking the supremum over all (S, T) -adversaries proves the claimed inequality. $\square$

Combining Theorems 3.4 and 3.5 gives the following corollary, which converts database-size-restricted operator bounds into QAI security bounds.

Corollary 3.6 (QAI Security from Database-Size-Restricted Operator Bounds). *Let $\mathcal{G}$ be a game in the QROM or QRPM. For integers $S, T \geq 0$, let $P := 2S(T_{\text{Sample}} + T + T_{\text{Verify}})$. Then*

$$\text{Adv}_{\mathcal{G}}^{\text{QAI}}(S, T) \leq \sqrt{2} \sup_{\mathcal{A}} \|\Pi_{\leq P} M_{\mathcal{E}_{\mathcal{A}}} \Pi_{\leq P}\|_{\text{op}},$$

where the supremum ranges over all online algorithms making at most T queries through Query^H and their input-register choices, and $\Pi_{\leq P}$ is the projector onto the corresponding database hierarchy from Section 2.

Proof. Apply Theorem 3.4 and substitute the bit-fixing bound from Theorem 3.5. $\square$

4 Improving Non-uniform Security for Salting

This section proves a theorem for non-uniform salting security whose decision-game bound improves on [Liu23, Theorem 7.5]. We use the salted game formalization of [CGLQ20, Definition 7.1]. Throughout this section, $\mathcal{F}$ is either a random-function family or a random-permutation family, and each call to Query^H makes at most one query to the underlying oracle H .

Definition 4.1 (Salted Security Game). *Let $\mathcal{G} = (\mathcal{C})$ be a security game whose base-game oracle is sampled as $H \xleftarrow{\$} \mathcal{F}$, where $\mathcal{C} = (\text{Sample}, \text{Query}, \text{Verify})$. Let*

$$\mathbf{H} = (H_1, \dots, H_K) \xleftarrow{\$} \mathcal{F}^K$$

be K independent salt-indexed oracles. The salted game $\mathcal{G}_S = (\mathcal{C}_S)$ is specified by

1. $\text{Sample}_S^{\mathbf{H}}$ samples $s \xleftarrow{\$} [K]$, runs Sample^{H_s} with fresh randomness, outputs (s, y) , and retains (s, t) , where y and t are the base sampler's challenge and retained state, respectively;
2. $\text{Query}_S^{\mathbf{H}}((s, t), (s', x)) = \begin{cases} \text{Query}^{H_s}(t, x), & s' = s, \\ H_{s'}(x), & s' \neq s; \end{cases}$
3. $\text{Verify}_S^{\mathbf{H}}((s, t), a) = \text{Verify}^{H_s}(t, a)$.

Fix an adversary for a salted game. We can similarly define the corresponding game operator and purified operator. For each challenge salt $s \in [K]$, let $E_s^{\mathbf{H}}$ be its fixed-salt game operator on the adversary's input register A . Let $\mathcal{E}_s := \{E_s^{\mathbf{H}}\}_{\mathbf{H} \in \mathcal{F}^K}$ and $\mathcal{E}^{(K)} := \{E_{(K)}^{\mathbf{H}}\}_{\mathbf{H} \in \mathcal{F}^K}$. We define the averaged game operator

$$E_{(K)}^{\mathbf{H}} := \frac{1}{K} \sum_{s \in [K]} E_s^{\mathbf{H}}.$$

By linearity,

$$M_{\mathcal{E}^{(K)}} = \frac{1}{K} \sum_{s \in [K]} M_{\mathcal{E}_s}.$$

4.1 Salted Database Hierarchy

Purify $\mathbf{H} = (H_1, \dots, H_K) \leftarrow \mathcal{F}^K$ in $\mathcal{O} := \mathcal{O}_1 \otimes \dots \otimes \mathcal{O}_K$, where $\mathcal{O}_s$ holds H_s . For the base game without salting, recall that $\mathcal{D}_j$ is the space of exact database size on the purified oracle register, and $\Pi_{=j}$ is the orthogonal projection onto $\mathcal{D}_j$. The database hierarchy and the database-size observable are

$$\mathcal{L}_P = \bigoplus_{j=0}^P \mathcal{D}_j, \quad \Lambda = \sum_{j \geq 0} j \Pi_{=j}.$$

We define the salted database hierarchy and its orthogonal projections by

$$\mathcal{L}_P^{(K)} := \bigoplus_{j_1 + \dots + j_K \leq P} \mathcal{D}_{j_1} \otimes \dots \otimes \mathcal{D}_{j_K}, \quad \Pi_{\leq P}^{(K)} := \text{Proj}_{\mathcal{L}_P^{(K)}}.$$

In other words, it keeps track of the database sizes for each individual salt-indexed oracle, and the sum of them is the total database size.

Corollary 3.6 also applies to the salted database hierarchy. The initial oracle state satisfies $|\Omega_{\mathcal{F}}\rangle^{\otimes K} \in \mathcal{L}_0^{(K)}$, and each query increases the total database size by at most one as shown in **Appendix B**. Thus the moment argument in the proof of **Theorem 3.4**, using the database-size-restricted operator norms directly, gives the corollary with projectors $\Pi_{\leq P}^{(K)}$.

Analogously to the base-game database-size observable, for each salt $s \in [K]$ we define the local database-size observable

$$\Lambda_s := I_{O_1} \otimes \dots \otimes I_{O_{s-1}} \otimes \Lambda \otimes I_{O_{s+1}} \otimes \dots \otimes I_{O_K}$$

where Λ is the database-size observable in O_s . Note that for any unit vector $|\psi\rangle \in \mathcal{L}_P^{(K)}$,

$$\langle \psi | \sum_{s \in [K]} \Lambda_s | \psi \rangle \leq P. \tag{11}$$

This is because on each summand $\mathcal{D}_{j_1} \otimes \dots \otimes \mathcal{D}_{j_K}$ of $\mathcal{L}_P^{(K)}$, the operator $\sum_{s \in [K]} \Lambda_s$ has eigenvalue $j_1 + \dots + j_K \leq P$.

For $s \in [K]$ and $j \geq 0$, let $\Pi_{s=j}$ act as $\Pi_{=j}$ on $\mathcal{O}_s$ and as the identity on every other oracle register:

$$\Pi_{s=j} := I_{O_1} \otimes \dots \otimes I_{O_{s-1}} \otimes \Pi_{=j} \otimes I_{O_{s+1}} \otimes \dots \otimes I_{O_K}.$$

The following inequality will be useful.

$$I - \Pi_{s,=0} = \sum_{j \geq 1} \Pi_{s,=j} \preceq \sum_{j \geq 1} j \Pi_{s,=j} = \Lambda_s. \quad (12)$$

4.2 Salting Defeats Quantum Advice

In this section, we improve the bound of [Liu23, Theorem 7.5] for decision games with quantum advice.

Theorem 4.2 (Generic salting). *Put $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$. For $S \geq 0$, the following statements hold.*

(i) *If the base search game has uniform success probability at most $\nu_{\mathcal{G}}(T)$, then*

$$\delta_{\mathcal{G}_s}^{\text{QAI}}(S, T) = O\left(\nu_{\mathcal{G}}(T) + \frac{Sr}{K}\right).$$

(ii) *If the base decision game has uniform advantage at most $\varepsilon_{\mathcal{G}}(T)$, then*

$$\varepsilon_{\mathcal{G}_s}^{\text{QAI}}(S, T) = O\left(\varepsilon_{\mathcal{G}}(T) + \sqrt{\frac{Sr}{K}}\right).$$

We use the following lemma to relate the experiment with a fixed challenge salt to the base game, which appears in the proof of [CGLQ20, Lemma 7.2]; we restate it here. At a high level, any bound by a function of the expected database size that holds for all base-game states also holds in the experiment with fixed challenge salt s , with the database size measured only in O_s .

Lemma 4.3. *Fix a challenge salt $s \in [K]$.*

(i) *If $|\psi\rangle \in \text{im } \Pi_{s,=0}$, then the fixed-salt experiment is a valid base-game experiment for the uniform oracle H_s , with all remaining registers included in the internal register and with at most T queries to Query^{H_s} .*

(ii) *Suppose there exists a real-valued function f such that, for every T -query base-game adversary with induced game-operator family $\mathcal{E}$ and every unit vector $|\phi\rangle$ on the purified-oracle and auxiliary registers,*

$$|\langle \phi | M_{\mathcal{E}} | \phi \rangle| \leq f(\langle \phi | \Lambda | \phi \rangle). \quad (13)$$

Then every unit vector $|\psi\rangle$ on the salt-indexed oracle and auxiliary registers satisfies

$$|\langle \psi | M_{\mathcal{E}_s} | \psi \rangle| \leq f(\langle \psi | \Lambda_s | \psi \rangle).$$

To see this, treat all other oracle registers as auxiliary workspace and absorb their queries into H_s -independent local unitaries; each query to the salted interface then uses at most one controlled query to Query^{H_s} . At database size zero, O_s is in the uniform oracle state and is independent of the auxiliary workspace, which gives part (i). For arbitrary states, the same circuit reduction identifies the base-game database-size observable Λ with Λ_s , giving part (ii).

Proof of Theorem 4.2. Fix a challenge salt s and a unit vector $|\psi\rangle \in \mathcal{L}_P^{(K)}$. Define $|\psi_0\rangle := \Pi_{s,=0}|\psi\rangle$ and $|\psi_1\rangle := (I - \Pi_{s,=0})|\psi\rangle$. Let $M_{\mathcal{E}_s}$ be the fixed-salt purified game operator of the salted game.

For a search game, $0 \preceq M_{\mathcal{E}_s} \preceq I$, and hence $M_{\mathcal{E}_s}^{1/2}$ is well defined. By Lemma 4.3(i) and the uniform-security assumption,

$$\|M_{\mathcal{E}_s}^{1/2}|\psi_0\rangle\|_2^2 = \langle \psi_0 | M_{\mathcal{E}_s} | \psi_0 \rangle \leq \|\psi_0\|_2^2 \nu_{\mathcal{G}}(T) \leq \nu_{\mathcal{G}}(T) \quad (14)$$

From $M_{\mathcal{E}_s} \preceq I$ and Eq. (12), we have

$$\begin{aligned}\|M_{\mathcal{E}_s}^{1/2}|\psi_1\rangle\|_2^2 &= \langle\psi_1|M_{\mathcal{E}_s}|\psi_1\rangle \\ &\leq \langle\psi_1|I|\psi_1\rangle = \langle\psi|(I - \Pi_{s,=0})|\psi\rangle \\ &\leq \langle\psi|\Lambda_s|\psi\rangle.\end{aligned}\tag{15}$$

Combining Eq. (14) and Eq. (15), we get

$$\begin{aligned}\langle\psi|M_{\mathcal{E}_s}|\psi\rangle &= \|M_{\mathcal{E}_s}^{1/2}|\psi\rangle\|_2^2 \\ &\leq (\|M_{\mathcal{E}_s}^{1/2}|\psi_0\rangle\|_2 + \|M_{\mathcal{E}_s}^{1/2}|\psi_1\rangle\|_2)^2 \\ &\leq \left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{\langle\psi|\Lambda_s|\psi\rangle}\right)^2\end{aligned}\tag{16}$$

Averaging Eq. (16) over $s \in [K]$ and using Eq. (11) and Jensen's inequality gives

$$\langle\psi|M_{\mathcal{E}^{(K)}}|\psi\rangle \leq \left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{P/K}\right)^2.$$

Taking the supremum over unit vectors $|\psi\rangle \in \mathcal{L}_P^{(K)}$ gives, for any $P \geq 0$,

$$\|\Pi_{\leq P}^{(K)} M_{\mathcal{E}^{(K)}} \Pi_{\leq P}^{(K)}\|_{\text{op}} \leq \left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{P/K}\right)^2.$$

This bound holds for every salted online algorithm, so applying Corollary 3.6 with $P = Sr$ gives

$$\delta_{\mathcal{G}_s}^{QAI}(S, T) = O\left(\left(\sqrt{\nu_{\mathcal{G}}(T)} + \sqrt{\frac{Sr}{K}}\right)^2\right) = O\left(\nu_{\mathcal{G}}(T) + \frac{Sr}{K}\right).$$

This proves (i).

For a decision game, $M_{\mathcal{E}_s}$ need not be positive, so the preceding positive-square-root argument does not apply. Lemma 4.3(i), the hypothesis of (ii), and Eq. (12) give

$$|\langle\psi_0|M_{\mathcal{E}_s}|\psi_0\rangle| \leq \varepsilon_{\mathcal{G}}(T), \quad \|\psi_1\|_2^2 \leq \langle\psi|\Lambda_s|\psi\rangle.\tag{17}$$

By the Cauchy-Schwarz inequality and $\|M_{\mathcal{E}_s}\|_{\text{op}} \leq 1$,

$$|\langle\psi_0|M_{\mathcal{E}_s}|\psi_1\rangle| \leq \|M_{\mathcal{E}_s}\|_{\text{op}} \|\psi_0\|_2 \|\psi_1\|_2 \leq \|\psi_1\|_2.\tag{18}$$

Combining Eq. (18) and Eq. (17) yields

$$|\langle\psi|M_{\mathcal{E}_s}|\psi\rangle| \leq \varepsilon_{\mathcal{G}}(T) + 2\sqrt{\langle\psi|\Lambda_s|\psi\rangle} + \langle\psi|\Lambda_s|\psi\rangle.\tag{19}$$

Averaging Eq. (19) over $s \in [K]$ and using the triangle inequality, Eq. (11), and Jensen's inequality gives

$$|\langle\psi|M_{\mathcal{E}^{(K)}}|\psi\rangle| \leq \varepsilon_{\mathcal{G}}(T) + 2\sqrt{P/K} + P/K.$$

As $|\psi\rangle$ and $P \geq 0$ are arbitrary, for any $P \geq 0$,

$$\|\Pi_{\leq P}^{(K)} M_{\mathcal{E}^{(K)}} \Pi_{\leq P}^{(K)}\|_{\text{op}} \leq \varepsilon_{\mathcal{G}}(T) + 2\sqrt{P/K} + P/K.$$

This bound holds for every salted online algorithm, so applying Corollary 3.6 with $P = Sr$ gives

$$\varepsilon_{\mathcal{G}_s}^{QAI}(S, T) = O\left(\varepsilon_{\mathcal{G}}(T) + \sqrt{\frac{Sr}{K}} + \frac{Sr}{K}\right).$$

If $Sr/K \leq 1$, then $Sr/K \leq \sqrt{Sr/K}$. If $Sr/K > 1$, the claimed bound follows from the trivial bound on the decision advantage. Therefore,

$$\varepsilon_{\mathcal{G}_s}^{QAI}(S, T) = O\left(\varepsilon_{\mathcal{G}}(T) + \sqrt{\frac{Sr}{K}}\right).$$

This proves (ii). □

4.3 (γ, Δ) -Diffuse Games

The generic bound in [Theorem 4.2](#) can be loose for games with an additional random challenge: for salted permutation inversion on $[N]$, it gives $O(T^2/N + ST/K)$ for $T \geq 1$. In the classical setting, Dong, Liu, and Wu [\[DLW24, Corollary 4.20\]](#) obtain the bound $O(T/N + ST/(KN))$ by exploiting the randomness of both the salt and the inversion challenge. We introduce the following notion of a (γ, Δ) -diffuse game to capture such improvements through an additive bound on the contributions of the existing database and subsequent queries. This yields $O(T^2/N + ST/(KN))$ for salted permutation inversion with quantum advice and quantum queries ([Theorem 5.16](#)), and also gives improved salting bounds for PRGs, Yao's box, and function inversion.

Definition 4.4 ((γ, Δ) -diffuse game). *Fix a query budget $T \geq 0$, an exponent $0 < \gamma \leq 1$, and a scale $\Delta > 0$. A game $\mathcal{G}$ is (γ, Δ) -diffuse at query budget T , with parameters $\tau_T \geq 0$ and $\kappa > 0$, if every T -query adversary with induced game-operator family $\mathcal{E}$ and every unit vector $|\psi\rangle$ on the purified-oracle and auxiliary registers satisfy*

$$|\langle \psi | M_{\mathcal{E}} | \psi \rangle| \leq \tau_T + \kappa \left(\frac{\langle \psi | \Lambda | \psi \rangle}{\Delta} \right)^\gamma.$$

Write $L := \langle \psi | \Lambda | \psi \rangle$ for the expected size of the existing database. The bound says that the advantages can come from a query-dependent baseline τ_T and a database contribution $\kappa(L/\Delta)^\gamma$, in an additive form. The name “diffuse” reflects the weak contribution of a database with $L \ll \Delta$: for fixed γ and κ , obtaining a constant advantage above τ_T requires an expected database size of at least a constant multiple of Δ . This is an additive upper bound; it does not require the database and subsequent queries to act on orthogonal subspaces.

The exponent γ controls how the database contribution grows. Our applications use $\gamma = 1/2$ for PRG and Yao's box, and $\gamma = 1$ for OWF and permutation inversion. For a salted database of total database size at most P , averaging over the challenge salt gives expected database size at most P/K . The salting argument therefore replaces the database contribution by $\kappa(P/(K\Delta))^\gamma$, while leaving the baseline τ_T unchanged.

Theorem 4.5 (Salting for (γ, Δ) -diffuse games). *Fix $T \geq 0$ and suppose that the base game $\mathcal{G}$ is (γ, Δ) -diffuse at query budget T , with parameters τ_T and κ . Put $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$. Then, for every integer $S \geq 0$ and salt-space size $K \geq 1$,*

$$\text{Adv}_{\mathcal{G}_S}^{\text{QAI}}(S, T) \leq \sqrt{2} \left[\tau_T + \kappa \left(\frac{Sr}{K\Delta} \right)^\gamma \right].$$

This bound holds for both search and decision games.

Proof. Fix a T -query salted online algorithm and a unit vector $|\psi\rangle \in \mathcal{L}_P^{(K)}$. By [Lemma 4.3\(ii\)](#),

$$\begin{aligned} |\langle \psi | M_{\mathcal{E}^{(K)}} | \psi \rangle| &\leq \frac{1}{K} \sum_{s \in [K]} |\langle \psi | M_{\mathcal{E}_s} | \psi \rangle| \\ &\leq \tau_T + \frac{\kappa}{K} \sum_{s \in [K]} \left(\frac{\langle \psi | \Lambda_s | \psi \rangle}{\Delta} \right)^\gamma \\ &\leq \tau_T + \kappa \left(\frac{P}{K\Delta} \right)^\gamma. \end{aligned}$$

The last inequality follows from [Eq. \(11\)](#) and Jensen's inequality, since $x \mapsto x^\gamma$ is concave and nondecreasing for $0 < \gamma \leq 1$.

Since $M_{\mathcal{E}^{(K)}}$ is Hermitian, this gives

$$\left\| \Pi_{\leq P}^{(K)} M_{\mathcal{E}^{(K)}} \Pi_{\leq P}^{(K)} \right\|_{\text{op}} \leq \tau_T + \kappa \left(\frac{P}{K\Delta} \right)^\gamma.$$

This bound holds for every T -query salted online algorithm, so applying [Corollary 3.6](#) with $P = Sr$ proves the claim. $\square$

By [Theorem 3.5](#), bit-fixing bounds control the size-restricted operator norm at each database size. For salting, total database size at most P bounds the sum of expected local database sizes by P , but each salt's local support can still reach database size P . The following lemma converts a linear size cutoff bound into a bound in terms of the expected database size. We use it for OWF and permutation inversion; the decision-game analogue appears in [Section A.2](#). See [Section A.3](#) for a full proof.

Lemma 4.6. *Fix an integer $T \geq 0$. For a search game $\mathcal{G} = (\mathcal{C})$ with $C = (\text{Sample}, \text{Query}, \text{Verify})$, put $r := \max\{1, 2(T_{\text{Sample}} + T + T_{\text{Verify}})\}$. Suppose there exist $\tau_T \geq 0$, a universal constant $\kappa > 0$, and a constant $\Delta > 0$ determined by $\mathcal{G}$ such that, for every T -query online algorithm and every integer $P \geq 0$,*

$$\|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{op} \leq \tau_T + \kappa \frac{P}{\Delta}. \quad (20)$$

Then $\mathcal{G}$ is $(1, \Delta)$ -diffuse at query budget T with parameters

$$\tau'_T := 2 \left(\tau_T + \frac{\kappa(r-1)}{\Delta} \right), \quad \kappa' := 2\kappa.$$

5 Details of Applications

We apply the reductions established in [Section 3](#) and [Section 4](#) to the PRG, Yao's box, OWF, and permutation-inversion games, and to their salted variants. For PRG and Yao's box, we prove the required diffuse bounds directly; for OWF and permutation inversion, we derive them from known bit-fixing bounds using [Lemma 4.6](#). We use the formulations of the first three games from [\[CGLQ20\]](#) and that of permutation inversion from [\[ABC⁺26\]](#). The supporting lemmas are proved in [Appendix A](#).

5.1 PRG Game

Definition 5.1 (PRG Game). *Let $H \xleftarrow{\$} \mathcal{F} := \{H : [N] \rightarrow [M]\}$. The decision game $\mathcal{G}_{\text{PRG}} = (\mathcal{C}_{\text{PRG}})$ is specified by*

1. $\text{Sample}^H(b, x, y)$ outputs $H(x)$ if $b = 0$ and outputs y if $b = 1$, where $b \xleftarrow{\$} \{0, 1\}$, $x \xleftarrow{\$} [N]$, and $y \xleftarrow{\$} [M]$;
2. $\text{Query}^H((b, x, y), x') = H(x')$;
3. $\text{Verify}^H((b, x, y), b') = 1$ if and only if $b = b'$.

Throughout this subsection, the adversary outputs 0 when it decides that the challenge is a random image. Fix a T -query adversary $\mathcal{A}$. For every oracle H and challenge $y \in [M]$, let E_y^H be the POVM element on the advice register A corresponding to output 0. Define

$$B_{H, \text{unif}}^{\text{PRG}} := \frac{1}{M} \sum_{y \in [M]} E_y^H, \quad B_{H, \text{img}}^{\text{PRG}} := \frac{1}{N} \sum_{x \in [N]} E_{H(x)}^H.$$

Let p_{unif} and p_{img} denote the probabilities that the adversary outputs 0 in the uniform and random-image branches, respectively. Then

$$\Pr[\text{win}] = \frac{1}{2}(1 - p_{\text{unif}}) + \frac{1}{2}p_{\text{img}} = \frac{1}{2} + \frac{1}{2}(p_{\text{img}} - p_{\text{unif}}).$$

Define the PRG game operator by

$$E_{\text{PRG}}^H := \frac{1}{2}(B_{H, \text{img}}^{\text{PRG}} - B_{H, \text{unif}}^{\text{PRG}}).$$

We have $0 \preceq B_{H,\text{img}}^{\text{PRG}} \preceq I$ and $0 \preceq B_{H,\text{unif}}^{\text{PRG}} \preceq I$. Hence, E_{PRG}^H is Hermitian and $\|E_{\text{PRG}}^H\|_{\text{op}} \leq 1$.
 For an advice family $\{\rho_H\}_H$,

$$\frac{1}{2}(p_{\text{img}} - p_{\text{unif}}) = \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{PRG}}^H)].$$

Consequently,

$$\varepsilon_{\text{PRG}}^{\text{QAI}}(S, T) = \sup_{\mathcal{A}} |\mathbb{E}_H[\text{Tr}(\rho_H E_{\text{PRG}}^H)]|.$$

Let $\mathcal{E}_{\text{PRG}} := \{E_{\text{PRG}}^H\}_{H \in \mathcal{F}}$ and let $M_{\mathcal{E}_{\text{PRG}}}$ be its purified game operator. $M_{\mathcal{E}_{\text{PRG}}}$ and $M_{\mathcal{E}_{\text{PRG}}^{(K)}}$ increase the database size by at most $r_{\text{PRG}} = 2(T+1)$.

Lemma 5.2. *For every unit vector $|\psi\rangle$ on the purified-oracle register and any auxiliary registers,*

$$|\langle \psi | M_{\mathcal{E}_{\text{PRG}}} | \psi \rangle| \leq \min \left\{ 1, \sqrt{\frac{\langle \psi | \Lambda | \psi \rangle}{N}} + \frac{2T^2}{N} \right\}. \quad (21)$$

Consequently, for every integer $P \geq 0$,

$$\|\Pi_{\leq P} M_{\mathcal{E}_{\text{PRG}}} \Pi_{\leq P}\|_{\text{op}} \leq \min \left\{ 1, \sqrt{\frac{P}{N}} + \frac{2T^2}{N} \right\}. \quad (22)$$

Proof. See [Section A.4](#). □

Theorem 5.3 (QAI bound for the PRG game). *For all integers $S, T \geq 0$,*

$$\varepsilon_{\text{PRG}}^{\text{QAI}}(S, T) = O \left(\sqrt{\frac{S(T+1)}{N}} + \frac{T^2}{N} \right).$$

Proof. The size-restricted bound in [Lemma 5.2](#) holds uniformly over all T -query online algorithms. Applying [Corollary 3.6](#) with $P = Sr_{\text{PRG}} = 2S(T+1)$ gives

$$\varepsilon_{\text{PRG}}^{\text{QAI}}(S, T) \leq 2\sqrt{\frac{S(T+1)}{N}} + 2\sqrt{2}\frac{T^2}{N}.$$

□

Theorem 5.4 (QAI bound for salted PRG game). *Let PRG_5 be the salted PRG game with salt space $[K]$. For all $K, N, M \geq 1$ and $S, T \geq 0$,*

$$\varepsilon_{\text{PRG}_5}^{\text{QAI}}(S, T) = O \left(\sqrt{\frac{S(T+1)}{KN}} + \frac{T^2}{N} \right).$$

Proof. [Lemma 5.2](#) shows that the PRG game is $(1/2, N)$ -diffuse at query budget T with

$$\tau_T = \frac{2T^2}{N}, \quad \kappa = 1.$$

[Theorem 4.5](#) proves the theorem. □

5.2 Yao's Box

Definition 5.5 (Yao's Box). Let $H \xleftarrow{\$} \mathcal{F} := \{H : [N] \rightarrow \{0, 1\}\}$. The decision game $\mathcal{G}_{\text{YB}} = (\mathcal{C}_{\text{YB}})$ is specified by

1. $\text{Sample}^H(x) = x$ for $x \xleftarrow{\$} [N]$;
2. $\text{Query}^H(x, x') = H(x')$ when $x' \neq x$, and $\text{Query}^H(x, x) = 1$;
3. $\text{Verify}^H(x, b) = 1$ if and only if $b = H(x)$.

The query interface is independent of the hidden bit $H(x)$. Fix a T -query adversary $\mathcal{A}$. For every oracle H and challenge $x \in [N]$, let $E_{x,b}^H$ be the POVM element on the advice register A corresponding to output $b \in \{0, 1\}$. Then, $E_{x,0}^H + E_{x,1}^H = I$. Defining

$$A_x^H := E_{x,0}^H - E_{x,1}^H,$$

we have

$$E_{x,H(x)}^H = \frac{1}{2}(I + (-1)^{H(x)} A_x^H).$$

Letting $\chi_x(H) := (-1)^{H(x)}$, define

$$E_{\text{YB}}^H := \frac{1}{2N} \sum_{x \in [N]} \chi_x(H) A_x^H.$$

For an advice family $\{\rho_H\}_H$, the winning probability is

$$\Pr[\text{win}] = \mathbb{E}_{H,x}[\text{Tr}(\rho_H E_{x,H(x)}^H)] = \frac{1}{2} + \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{YB}}^H)]. \quad (23)$$

Therefore,

$$\varepsilon_{\text{YB}}^{\text{QAI}}(S, T) = \sup_{\mathcal{A}} |\mathbb{E}_H[\text{Tr}(\rho_H E_{\text{YB}}^H)]|.$$

Let $\mathcal{E}_{\text{YB}} := \{E_{\text{YB}}^H\}_{H \in \mathcal{F}}$ and let $M_{\mathcal{E}_{\text{YB}}}$ be its purified game operator. $M_{\mathcal{E}_{\text{YB}}}$ and $M_{\mathcal{E}_{\text{YB}}^{(\kappa)}}$ increase the database size by at most $r_{\text{YB}} = 2(T+1)$.

Lemma 5.6. For every unit vector $|\psi\rangle$ on the purified-oracle register and any auxiliary registers,

$$|\langle \psi | M_{\mathcal{E}_{\text{YB}}} | \psi \rangle| \leq \min \left\{ \frac{1}{2}, (1 + \sqrt{2}) \sqrt{\frac{|\langle \psi | \Lambda | \psi \rangle|}{N}} \right\}.$$

Consequently, for every integer $P \geq 0$,

$$\|\Pi_{\leq P} M_{\mathcal{E}_{\text{YB}}} \Pi_{\leq P}\|_{\text{op}} \leq \min \left\{ \frac{1}{2}, (1 + \sqrt{2}) \sqrt{\frac{P}{N}} \right\}.$$

Proof. See [Section A.5](#). □

Theorem 5.7 (QAI bound for Yao's box). For all integers $S, T \geq 0$,

$$\varepsilon_{\text{YB}}^{\text{QAI}}(S, T) = O \left(\sqrt{\frac{S(T+1)}{N}} \right).$$

Proof. The size-restricted bound in [Lemma 5.6](#) holds uniformly over all T -query online algorithms. Applying [Corollary 3.6](#) with $P = Sr_{\text{YB}} = 2S(T+1)$ gives

$$\varepsilon_{\text{YB}}^{\text{QAI}}(S, T) \leq (2\sqrt{2} + 2) \sqrt{\frac{S(T+1)}{N}}.$$

□

Theorem 5.8 (QAI bound for salted Yao's box). *Let YB_S be the salted Yao's box with salt space $[K]$. For all $K, N \geq 1$ and $S, T \geq 0$,*

$$\varepsilon_{\text{YB}_S}^{\text{QAI}}(S, T) = O\left(\sqrt{\frac{S(T+1)}{KN}}\right).$$

Proof. [Lemma 5.6](#) shows that the Yao's-box game is $(1/2, N)$ -diffuse at query budget T with

$$\tau_T = 0, \quad \kappa = 1 + \sqrt{2}.$$

[Theorem 4.5](#) proves the theorem. □

5.3 OWF Game

Definition 5.9 (OWF Game). *Let $H \xleftarrow{\$} \mathcal{F} := \{H : [N] \rightarrow [M]\}$. The security game $\mathcal{G}_{\text{OWF}} = (C_{\text{OWF}})$ is specified by*

1. **Sample** ^{H} (x) takes $x \xleftarrow{\$} [N]$, outputs $y = H(x)$, and retains (x, y) ;
2. **Query** ^{H} $((x, y), x') = H(x')$;
3. **Verify** ^{H} $((x, y), x') = 1$ if and only if $x' \in [N]$ and $y = H(x')$.

Fix a T -query adversary $\mathcal{A}$. For every oracle H and challenge $y \in [M]$, let $E_{y,z}^H$ be the POVM element on the advice register A corresponding to output $z \in [N] \cup \{\perp\}$. Define

$$W_y^H := \sum_{z: H(z)=y} E_{y,z}^H, \quad E_{\text{OWF}}^H := \frac{1}{N} \sum_{x \in [N]} W_{H(x)}^H.$$

Then, E_{OWF}^H is the game operator corresponding to the winning outcome and satisfies $0 \preceq E_{\text{OWF}}^H \preceq I$. For an advice family $\{\rho_H\}_H$,

$$\Pr[\text{win}] = \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{OWF}}^H)].$$

Consequently,

$$\delta_{\text{OWF}}^{\text{QAI}}(S, T) = \sup_{\mathcal{A}} \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{OWF}}^H)].$$

Let $\mathcal{E}_{\text{OWF}} := \{E_{\text{OWF}}^H\}_{H \in \mathcal{F}}$ and let $M_{\mathcal{E}_{\text{OWF}}}$ be its purified game operator. $M_{\mathcal{E}_{\text{OWF}}}$ and $M_{\mathcal{E}_{\text{OWF}}}^{(K)}$ increase the database size by at most $r_{\text{OWF}} = 2(T+2)$.

Lemma 5.10. *There exists a universal constant $C_{\text{OWF}} > 0$ such that for every unit vector $|\psi\rangle$ on the purified-oracle register and any auxiliary registers,*

$$\langle \psi | M_{\mathcal{E}_{\text{OWF}}} | \psi \rangle \leq \min \left\{ 1, C_{\text{OWF}} \frac{\langle \psi | \Lambda | \psi \rangle + (T+1)^2}{\min\{N, M\}} \right\}.$$

Consequently, for every integer $P \geq 0$,

$$\|\Pi_{\leq P} M_{\mathcal{E}_{\text{OWF}}} \Pi_{\leq P}\|_{\text{op}} \leq \min \left\{ 1, C_{\text{OWF}} \frac{P + (T+1)^2}{\min\{N, M\}} \right\}.$$

Proof. See [Section A.6](#). □

Theorem 5.11 (QAI bound for the OWF game). *For all integers $S, T \geq 0$,*

$$\delta_{\text{OWF}}^{\text{QAI}}(S, T) = O\left(\frac{S(T+1) + (T+1)^2}{\min\{N, M\}}\right).$$

Proof. The size-restricted bound in [Lemma 5.10](#) holds uniformly over all T -query online algorithms. Applying [Corollary 3.6](#) with $P = S r_{\text{OWF}} = 2S(T+2)$ gives

$$\delta_{\text{OWF}}^{\text{QAI}}(S, T) \leq C_{\text{OWF}} \sqrt{2} \frac{2S(T+2) + (T+1)^2}{\min\{N, M\}}.$$

□

Theorem 5.12 (QAI bound for salted OWF game). *Let OWF_S be the salted OWF game with salt space $[K]$. For all $K, N, M \geq 1$ and $S, T \geq 0$,*

$$\delta_{\text{OWF}_S}^{\text{QAI}}(S, T) = O\left(\frac{S(T+1)}{K \min\{N, M\}} + \frac{(T+1)^2}{\min\{N, M\}}\right).$$

Proof. [Lemma 5.10](#) shows that the OWF game is $(1, \min\{N, M\})$ -diffuse at query budget T with

$$\tau_T = C_{\text{OWF}} \frac{(T+1)^2}{\min\{N, M\}}, \quad \kappa = C_{\text{OWF}}.$$

[Theorem 4.5](#) proves the theorem. □

5.4 Permutation inversion game

Definition 5.13 (Permutation Inversion Game). *Let $H \xleftarrow{\$} \mathcal{F}^{\text{perm}} := S_N$. The security game $\mathcal{G}_{\text{Permlnv}} = (\mathcal{C}_{\text{Permlnv}})$ is specified by*

1. *Sample* ^{H} $(y) = y$ for $y \xleftarrow{\$} [N]$;
2. *Query* ^{H} $(y, x) = H(x)$;
3. *Verify* ^{H} $(y, x) = 1$ if and only if $y = H(x)$.

Fix a T -query adversary $\mathcal{A}$. For every oracle H and challenge $y \in [N]$, let $E_{y,z}^H$ be the POVM element on the advice register A corresponding to output $z \in [N]$. Define

$$E_{\text{Permlnv}}^H := \frac{1}{N} \sum_{y \in [N]} E_{y, H^{-1}(y)}^H.$$

Then, E_{Permlnv}^H is the game operator corresponding to the winning outcome and satisfies $0 \preceq E_{\text{Permlnv}}^H \preceq I$. For an advice family $\{\rho_H\}_H$,

$$\Pr[\text{win}] = \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{Permlnv}}^H)].$$

Consequently,

$$\delta_{\text{Permlnv}}^{\text{QAI}}(S, T) = \sup_{\mathcal{A}} \mathbb{E}_H[\text{Tr}(\rho_H E_{\text{Permlnv}}^H)].$$

Let $\mathcal{E}_{\text{Permlnv}} := \{E_{\text{Permlnv}}^H\}_{H \in \mathcal{F}^{\text{perm}}}$ and let $M_{\mathcal{E}_{\text{Permlnv}}}$ be its purified game operator. $M_{\mathcal{E}_{\text{Permlnv}}}$ and $M_{\mathcal{E}_{\text{Permlnv}}^{(K)}}$ increase the database size by at most $r_{\text{Permlnv}} = 2(T+1)$.

Lemma 5.14. *There exists a universal constant $C_{\text{perm}} > 0$ such that for every unit vector $|\psi\rangle$ on the purified-oracle and auxiliary registers,*

$$\langle \psi | M_{\mathcal{E}_{\text{Permlnv}}} | \psi \rangle \leq \min \left\{ 1, C_{\text{perm}} \frac{\langle \psi | \Lambda^{\text{perm}} | \psi \rangle + (T+1)^2}{N} \right\}.$$

Consequently, for every integer $P \geq 0$,

$$\| \Pi_{\leq P}^{\text{perm}} M_{\mathcal{E}_{\text{Permlnv}}} \Pi_{\leq P}^{\text{perm}} \|_{op} \leq \min \left\{ 1, C_{\text{perm}} \frac{P + (T+1)^2}{N} \right\}.$$

Proof. See [Section A.7](#). □

Theorem 5.15 (QAI bound for Permutation Inversion Game). *For all integers $S, T \geq 0$,*

$$\delta_{\text{Permlnv}}^{\text{QAI}}(S, T) = O \left(\frac{S(T+1) + (T+1)^2}{N} \right).$$

Proof. The size-restricted bound in [Lemma 5.14](#) holds uniformly over all T -query online algorithms. Applying [Corollary 3.6](#) with $P = Sr_{\text{Permlnv}} = 2S(T+1)$ gives

$$\delta_{\text{Permlnv}}^{\text{QAI}}(S, T) \leq C_{\text{perm}} \sqrt{2} \frac{2S(T+1) + (T+1)^2}{N}.$$

□

Theorem 5.16 (QAI bound for salted Permutation Inversion game). *Let Permlnv_S be the salted permutation inversion game with salt space $[K]$. For all integers $S, T \geq 0$ and $K, N \geq 1$,*

$$\delta_{\text{Permlnv}_S}^{\text{QAI}}(S, T) = O \left(\frac{S(T+1)}{KN} + \frac{(T+1)^2}{N} \right).$$

Proof. [Lemma 5.14](#) shows that the permutation-inversion game is $(1, N)$ -diffuse at query budget T with

$$\tau_T = C_{\text{perm}} \frac{(T+1)^2}{N}, \quad \kappa = C_{\text{perm}}.$$

[Theorem 4.5](#) proves the theorem. □

References

- [ABC⁺26] Akshima, Tyler Besselman, Kai-Min Chung, Siyao Guo, and Tzu-Yi Yang. Tight quantum time-space tradeoffs for permutation inversion. In *Advances in Cryptology–EUROCRYPT 2026*, volume 16541 of *Lecture Notes in Computer Science*, pages 431–456. Springer, 2026. [3](#), [5](#), [7](#), [11](#), [12](#), [14](#), [24](#), [40](#)
- [BBC⁺98] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *39th FOCS*, pages 352–361. IEEE Computer Society Press, November 1998. [4](#), [8](#), [13](#)
- [BDF⁺11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Berlin, Heidelberg, December 2011. [3](#)

- [BHNZ26] John Bostanci, Jonas Haferkamp, Chinmay Nirkhe, and Mark Zhandry. Separating QMA from QCMA with a classical oracle. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC 2026)*. ACM, 2026. [3](#)
- [BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993. [3](#)
- [CDG18] Sandro Coretti, Yevgeniy Dodis, and Siyao Guo. Non-uniform bounds in the random-permutation, ideal-cipher, and generic-group models. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 693–721. Springer, Cham, August 2018. [3](#)
- [CDGS18] Sandro Coretti, Yevgeniy Dodis, Siyao Guo, and John P. Steinberger. Random oracles and non-uniformity. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 227–258. Springer, Cham, April / May 2018. [3](#), [4](#), [5](#), [9](#)
- [CGLQ20] Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. Tight quantum time-space tradeoffs for function inversion. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 673–684. IEEE, 2020. [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [10](#), [13](#), [19](#), [21](#), [24](#), [37](#), [39](#)
- [CLQ20] Kai-Min Chung, Tai-Ning Liao, and Luowen Qian. Lower bounds for function inversion with quantum advice. In Yael Tauman Kalai, Adam D. Smith, and Daniel Wichs, editors, *ITC 2020*, volume 163 of *LIPIcs*, pages 8:1–8:15. Schloss Dagstuhl, June 2020. [3](#)
- [DGK17] Yevgeniy Dodis, Siyao Guo, and Jonathan Katz. Fixing cracks in the concrete: Random oracles with auxiliary input, revisited. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 473–495. Springer, Cham, April / May 2017. [3](#), [4](#)
- [DLW24] Fangqi Dong, Qipeng Liu, and Kewen Wu. Tight characterizations for preprocessing against cryptographic salting. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part IV*, volume 14923 of *LNCS*, pages 377–411. Springer, Cham, August 2024. [3](#), [4](#), [23](#)
- [DTT10] Anindya De, Luca Trevisan, and Madhur Tulsiani. Time space tradeoffs for attacks against one-way functions and PRGs. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 649–665. Springer, Berlin, Heidelberg, August 2010. [3](#), [4](#)
- [GGKL21] Nick Gravin, Siyao Guo, Tsz Chiu Kwok, and Pinyan Lu. Concentration bounds for almost k -wise independence with applications to non-uniform security. In Dániel Marx, editor, *32nd SODA*, pages 2404–2423. ACM-SIAM, January 2021. [3](#), [5](#)
- [GLLZ21] Siyao Guo, Qian Li, Qipeng Liu, and Jiapeng Zhang. Unifying presampling via concentration bounds. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part I*, volume 13042 of *LNCS*, pages 177–208. Springer, Cham, November 2021. [3](#), [4](#), [7](#), [13](#)
- [Hel80] Martin E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4):401–406, July 1980. [4](#), [5](#)
- [HXY19] Minki Hhan, Keita Xagawa, and Takashi Yamakawa. Quantum random oracle model with auxiliary input. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 584–614. Springer, Cham, December 2019. [3](#), [4](#), [5](#), [6](#)
- [Liu23] Qipeng Liu. Non-uniformity and quantum advice in the quantum random oracle model. In *Advances in Cryptology–EUROCRYPT 2023*, volume 14004 of *Lecture Notes in Computer Science*, pages 117–143. Springer, 2023. [3](#), [4](#), [5](#), [6](#), [7](#), [13](#), [16](#), [19](#), [21](#), [40](#)

- [LLPY24] Xingjian Li, Qipeng Liu, Angelos Pelecanos, and Takashi Yamakawa. Classical vs quantum advice and proofs under classically-accessible oracle. In Venkatesan Guruswami, editor, *ITCS 2024*, volume 287, pages 72:1–72:19. LIPIcs, January / February 2024. [3](#)
- [LMY25] Jiahui Liu, Saachi Mutreja, and Henry Yuen. QMA vs QCMA and pseudorandomness. In Michal Koucký and Nikhil Bansal, editors, *57th ACM STOC*, pages 1520–1531. ACM Press, June 2025. [3](#)
- [Mar90] A. A. Markov. On a question by D. I. Mendelev. *Zapiski Imperatorskoi Akademii Nauk*, 62:1–24, 1890. In Russian. [31](#)
- [NABT14] Aran Nayebi, Scott Aaronson, Aleksandrs Belovs, and Luca Trevisan. Quantum lower bound for inverting a permutation with advice. *arXiv preprint arXiv:1408.3193*, 2014. [3](#)
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition, 2010. [9](#)
- [Ros22] Ansis Rosmanis. Tight bounds for inverting permutations via compressed oracle arguments. *arXiv preprint arXiv:2103.08975*, 2022. [11](#)
- [Unr07] Dominique Unruh. Random oracles and auxiliary input. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 205–223. Springer, Berlin, Heidelberg, August 2007. [3](#)
- [Yao90] Andrew Chi-Chih Yao. Coherent functions and program checkers (extended abstract). In *22nd ACM STOC*, pages 84–94. ACM Press, May 1990. [3](#)
- [Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indistinguishability. In *Advances in Cryptology – CRYPTO 2019*, pages 239–268. Springer, 2019. [7](#), [9](#), [10](#)

A Missing Proofs

In this section, we present proofs omitted from earlier sections. Throughout this section, we fix an orthonormal basis $\{|z\rangle\}_Z$ of $\mathcal{H}_Z$ for the internal register Z .

A.1 Proof for the Uniform one-point reprogramming lemma

We use the following classical polynomial inequality.

Lemma A.1 (Markov’s polynomial inequality [[Mar90](#)]). *Every real polynomial p of degree at most d satisfies*

$$\max_{s \in [-1, 1]} |p'(s)| \leq d^2 \max_{s \in [-1, 1]} |p(s)|.$$

Proof of [Lemma 2.5](#). Purify the circuit’s initial state and defer all intermediate measurements, so that the computation is unitary until a final projective measurement. These transformations can be chosen independently of x .

For $v \in \mathbb{Z}_M$, let S_v be the shift operator defined by $S_v|u\rangle = |u + v\rangle$, where addition is modulo M . For each $z \in \{0, 1\}^N$, define the oracle query

$$U_z := \sum_{w \in [N]} |w\rangle\langle w| \otimes ((1 - z_w)S_{H(w)} + z_w S_h).$$

Thus, U_0 is the query to H , while U_{e_x} is the query to $H_{x \rightarrow h}$, where e_x denotes the Boolean vector whose only nonzero coordinate is x . We run the same circuit with U_z in place of each oracle query, keeping the initial state, inter-query operations, and final measurement fixed for every z .

Every matrix entry of U_z is affine in z . Consequently, if we write the final state as

$$|\Psi(z)\rangle = \sum_j q_j(z) |j\rangle$$

in a fixed orthonormal basis, each amplitude $q_j(z)$ is a polynomial of degree at most T . Let Π be the final accepting projector and define

$$A(z) := \langle \Psi(z) | \Pi | \Psi(z) \rangle.$$

The acceptance probability $A(z)$ is therefore a polynomial of degree at most $2T$. Multilinearizing using $z_w^2 = z_w$ on $\{0, 1\}^N$, we obtain

$$A(z) = \sum_{\substack{S \subseteq [N] \\ |S| \leq 2T}} c_S \prod_{w \in S} z_w, \quad (24)$$

where the coefficients c_S are real. Moreover, $0 \leq A(z) \leq 1$ for every $z \in \{0, 1\}^N$, and

$$A(0) = a(\emptyset), \quad A(e_x) = a(x).$$

For each $t \in [0, N]$, let $Z_1(t), \dots, Z_N(t)$ be independent Bernoulli(t/N) random variables, and write $Z(t) := (Z_1(t), \dots, Z_N(t))$. Taking expectations in [Eq. \(24\)](#) gives

$$q(t) := \mathbb{E}[A(Z(t))] = \sum_{\substack{S \subseteq [N] \\ |S| \leq 2T}} c_S \left(\frac{t}{N} \right)^{|S|}. \quad (25)$$

Hence q is a real polynomial of degree at most $2T$. Since $q(t)$ is an average of acceptance probabilities,

$$0 \leq q(t) \leq 1 \quad \text{for every } t \in [0, N].$$

Differentiating [Eq. \(25\)](#) at zero leaves only the singleton terms:

$$q'(0) = \frac{1}{N} \sum_{x \in [N]} c_{\{x\}}.$$

On the other hand, [Eq. \(24\)](#) gives $A(0) = c_\emptyset$ and $A(e_x) = c_\emptyset + c_{\{x\}}$. Therefore,

$$q'(0) = \frac{1}{N} \sum_{x \in [N]} (A(e_x) - A(0)) = \mathbb{E}_{x \leftarrow [N]} [a(x)] - a(\emptyset).$$

Finally, define

$$r(s) := 2q\left(\frac{N(s+1)}{2}\right) - 1.$$

Then $\deg r \leq 2T$ and $|r(s)| \leq 1$ on $[-1, 1]$. By [Lemma A.1](#),

$$|r'(-1)| \leq (2T)^2.$$

Since $r'(-1) = Nq'(0)$, it follows that

$$\left| \mathbb{E}_{x \leftarrow [N]} [a(x)] - a(\emptyset) \right| = |q'(0)| \leq \frac{4T^2}{N},$$

as claimed. □

A.2 Diffuse Bounds for Decision Games

For completeness, we give the decision-game analogue of [Lemma 4.6](#).

Lemma A.2. *Fix an integer $T \geq 0$. For a decision game $\mathcal{G} = (\mathcal{C})$ with $C = (\text{Sample}, \text{Query}, \text{Verify})$, put $r := \max\{1, 2(T_{\text{Sample}} + T + T_{\text{Verify}})\}$. Suppose there exist $\tau_T \geq 0$, a universal constant $\kappa > 0$, and a constant $\Delta > 0$ determined by $\mathcal{G}$ such that, for every T -query online algorithm and every integer $P \geq 0$,*

$$\|\Pi_{\leq P} M_{\mathcal{E}} \Pi_{\leq P}\|_{op} \leq \tau_T + \kappa \sqrt{\frac{P}{\Delta}}. \quad (26)$$

Then $\mathcal{G}$ is $(1/2, \Delta/(1 + \lceil \log_2 r \rceil))$ -diffuse at query budget T with parameters

$$\tau'_T := 4\tau_T, \quad \kappa' := 12\kappa.$$

Proof. We simply write $r := \max\{1, 2(T_{\text{Sample}} + T + T_{\text{Verify}})\}$. Define the block projector, block vector, and block expectation for $m \geq 0$,

$$\Pi_m^{\mathbf{B}} := \sum_{j=mr}^{(m+1)r-1} \Pi_{=j}, \quad |\psi_m\rangle := \Pi_m^{\mathbf{B}} |\psi\rangle, \quad d_m := \langle \psi_m | M_{\mathcal{E}} | \psi_m \rangle.$$

We adopt the convention $\Pi_{=j} = 0$ for $j > N$. As $M_{\mathcal{E}}$ increases the database size by at most r ,

$$\Pi_m^{\mathbf{B}} M_{\mathcal{E}} \Pi_n^{\mathbf{B}} = 0$$

for $|m - n| \geq 2$. Thus we have

$$\langle \psi | M_{\mathcal{E}} | \psi \rangle = \sum_{m \geq 0} \langle \psi_m | M_{\mathcal{E}} | \psi_m \rangle + 2 \sum_{m \geq 0} \text{Re}(\langle \psi_m | M_{\mathcal{E}} | \psi_{m+1} \rangle).$$

Here, we used $M_{\mathcal{E}} = M_{\mathcal{E}}^\dagger$. As $|\psi_m\rangle \in \mathcal{L}_{(m+1)r-1}$ and $|\psi_{m+1}\rangle \in \mathcal{L}_{(m+2)r-1}$,

$$\begin{aligned} |\langle \psi_m | M_{\mathcal{E}} | \psi_m \rangle| &\leq \left(\tau_T + \kappa \sqrt{\frac{(m+1)r-1}{\Delta}} \right) \|\psi_m\|_2^2 \\ |\langle \psi_m | M_{\mathcal{E}} | \psi_{m+1} \rangle| &\leq \left(\tau_T + \kappa \sqrt{\frac{(m+2)r-1}{\Delta}} \right) \|\psi_m\|_2 \|\psi_{m+1}\|_2. \end{aligned}$$

We bound $\langle \psi | M_{\mathcal{E}} | \psi \rangle - \langle \psi_0 | M_{\mathcal{E}} | \psi_0 \rangle$. We have

$$\begin{aligned} \sum_{m \geq 1} ((m+1)r-1) \|\psi_m\|_2^2 &= \sum_{m \geq 1} \sum_{j=mr}^{(m+1)r-1} ((m+1)r-1) \|\Pi_{=j} \psi\|_2^2 \\ &\leq \sum_{m \geq 1} \sum_{j=mr}^{(m+1)r-1} 2j \|\Pi_{=j} \psi\|_2^2 \\ &\leq 2 \langle \psi | \Lambda | \psi \rangle. \end{aligned} \quad (27)$$

By Cauchy–Schwarz and [Eq. \(27\)](#),

$$\sum_{m \geq 1} \sqrt{(m+1)r-1} \|\psi_m\|_2^2 \leq \sqrt{\sum_{m \geq 1} ((m+1)r-1) \|\psi_m\|_2^2} \sqrt{\sum_{m \geq 1} \|\psi_m\|_2^2}$$

$$\leq \sqrt{2\langle\psi|\Lambda|\psi\rangle}. \quad (28)$$

Similarly,

$$\begin{aligned} \sum_{m \geq 0} \sqrt{(m+2)r-1} \|\psi_m\|_2 \|\psi_{m+1}\|_2 &\leq \sqrt{\sum_{m \geq 0} \|\psi_m\|_2^2} \sqrt{\sum_{m \geq 0} ((m+2)r-1) \|\psi_{m+1}\|_2^2} \\ &\leq \sqrt{\sum_{m \geq 1} ((m+1)r-1) \|\psi_m\|_2^2} \\ &\leq \sqrt{2\langle\psi|\Lambda|\psi\rangle}. \end{aligned} \quad (29)$$

By Cauchy–Schwarz,

$$\sum_{m \geq 0} \|\psi_m\|_2 \|\psi_{m+1}\|_2 \leq \sqrt{\sum_{m \geq 0} \|\psi_m\|_2^2} \sqrt{\sum_{m \geq 0} \|\psi_{m+1}\|_2^2} \leq 1. \quad (30)$$

Combining Eqs. (28) to (30), we have

$$|\langle\psi|M_{\mathcal{E}}|\psi\rangle - \langle\psi_0|M_{\mathcal{E}}|\psi_0\rangle| \leq (3 - \|\psi_0\|_2^2)\tau_T + 3\kappa\sqrt{\frac{2\langle\psi|\Lambda|\psi\rangle}{\Delta}}.$$

It remains to bound $|d_0|$. Set

$$q := \max \left\{ 1, \left\lceil \frac{\Delta\tau_T^2}{\kappa^2} \right\rceil \right\}, \quad J := \max \{0, \lceil \log_2(r/q) \rceil\}.$$

Define

$$|\phi_0\rangle := \Pi_{\leq q-1}|\psi_0\rangle.$$

For $1 \leq j \leq J$, define

$$q_j := \min\{2^j q - 1, r - 1\}, \quad |\phi_j\rangle := \sum_{k=2^{j-1}q}^{q_j} \Pi_{=k}|\psi_0\rangle.$$

These vectors are mutually orthogonal and satisfy

$$|\psi_0\rangle = \sum_{j=0}^J |\phi_j\rangle.$$

If $q \geq r$, then $J = 0$ and $|\phi_0\rangle = |\psi_0\rangle$. Since $q \geq 1$, we have $J \leq \lceil \log_2 r \rceil$.

The choice of q gives

$$\kappa\sqrt{\frac{q-1}{\Delta}} \leq \tau_T.$$

As $|\phi_0\rangle \in \mathcal{L}_{q-1}$, it follows that

$$\begin{aligned} |\langle\phi_0|M_{\mathcal{E}}|\phi_0\rangle| &\leq \left(\tau_T + \kappa\sqrt{\frac{q-1}{\Delta}} \right) \|\phi_0\|_2^2 \\ &\leq 2\tau_T \|\phi_0\|_2^2. \end{aligned}$$

For $1 \leq j \leq J$, we have $q_j \geq q \geq \Delta\tau_T^2/\kappa^2$, and hence

$$\tau_T + \kappa\sqrt{\frac{q_j}{\Delta}} \leq 2\kappa\sqrt{\frac{q_j}{\Delta}}.$$

Both $|\phi_j\rangle$ and $\sum_{i=0}^{j-1} |\phi_i\rangle$ belong to $\mathcal{L}_{q_j}$. Moreover, orthogonality gives

$$\|\phi_j\|_2 \leq \|\psi_0\|_2, \quad \left\| \sum_{i=0}^{j-1} \phi_i \right\|_2 \leq \|\psi_0\|_2.$$

Expanding d_0 in this decomposition gives

$$d_0 = \sum_{j=0}^J \langle \phi_j | M_{\mathcal{E}} | \phi_j \rangle + 2 \sum_{j=1}^J \operatorname{Re} \left(\sum_{i=0}^{j-1} \langle \phi_i | M_{\mathcal{E}} | \phi_j \rangle \right).$$

For $1 \leq j \leq J$, both $\sum_{i=0}^{j-1} |\phi_i\rangle$ and $|\phi_j\rangle$ belong to $\mathcal{L}_{q_j}$. Hence,

$$\begin{aligned} \left| \sum_{i=0}^{j-1} \langle \phi_i | M_{\mathcal{E}} | \phi_j \rangle \right| &= \left| \left\langle \sum_{i=0}^{j-1} \phi_i \left| \Pi_{\leq q_j} M_{\mathcal{E}} \Pi_{\leq q_j} \right| \phi_j \right\rangle \right| \\ &\leq \|\Pi_{\leq q_j} M_{\mathcal{E}} \Pi_{\leq q_j}\|_{\text{op}} \left\| \sum_{i=0}^{j-1} \phi_i \right\|_2 \|\phi_j\|_2 \\ &\leq 2\kappa \sqrt{\frac{q_j}{\Delta}} \left\| \sum_{i=0}^{j-1} \phi_i \right\|_2 \|\phi_j\|_2. \end{aligned}$$

Similarly,

$$|\langle \phi_j | M_{\mathcal{E}} | \phi_j \rangle| \leq 2\kappa \sqrt{\frac{q_j}{\Delta}} \|\phi_j\|_2^2.$$

Applying the preceding bounds, we obtain

$$\begin{aligned} |d_0| &\leq 2\tau_T \|\phi_0\|_2^2 + 2\kappa \sum_{j=1}^J \sqrt{\frac{q_j}{\Delta}} \left(\|\phi_j\|_2^2 + 2 \left\| \sum_{i=0}^{j-1} \phi_i \right\|_2 \|\phi_j\|_2 \right) \\ &\leq 2\tau_T \|\psi_0\|_2^2 + \frac{6\kappa \|\psi_0\|_2}{\sqrt{\Delta}} \sum_{j=1}^J \sqrt{q_j} \|\phi_j\|_2. \end{aligned}$$

For every k in the j th interval, $q_j < 2(2^{j-1}q) \leq 2k$. Therefore,

$$\begin{aligned} \sum_{j=1}^J q_j \|\phi_j\|_2^2 &= \sum_{j=1}^J \sum_{k=2^{j-1}q}^{q_j} q_j \|\Pi_{=k} \psi_0\|_2^2 \\ &\leq 2 \sum_{j=1}^J \sum_{k=2^{j-1}q}^{q_j} k \|\Pi_{=k} \psi_0\|_2^2 \\ &\leq 2 \langle \psi_0 | \Lambda | \psi_0 \rangle. \end{aligned}$$

By Cauchy–Schwarz,

$$\begin{aligned} \sum_{j=1}^J \sqrt{q_j} \|\phi_j\|_2 &\leq \sqrt{J} \sqrt{\sum_{j=1}^J q_j \|\phi_j\|_2^2} \\ &\leq \sqrt{2J \langle \psi_0 | \Lambda | \psi_0 \rangle}. \end{aligned}$$

Thus,

$$|d_0| \leq 2\tau_T \|\psi_0\|_2^2 + 6\kappa \|\psi_0\|_2 \sqrt{\frac{2J \langle \psi_0 | \Lambda | \psi_0 \rangle}{\Delta}}.$$

Combining this with the preceding bound on the terms outside the first block gives

$$\begin{aligned}
|\langle \psi | M_{\mathcal{E}} | \psi \rangle| &\leq (3 + \|\psi_0\|_2^2) \tau_T + 3\kappa \sqrt{\frac{2\langle \psi | \Lambda | \psi \rangle}{\Delta}} + 6\kappa \|\psi_0\|_2 \sqrt{\frac{2J\langle \psi_0 | \Lambda | \psi_0 \rangle}{\Delta}} \\
&\leq 4\tau_T + \sqrt{2}(3 + 6\sqrt{J})\kappa \sqrt{\frac{\langle \psi | \Lambda | \psi \rangle}{\Delta}} \\
&\leq 4\tau_T + 12\kappa \sqrt{\frac{(1 + \lceil \log_2 r \rceil) \langle \psi | \Lambda | \psi \rangle}{\Delta}}.
\end{aligned}$$

The second inequality uses $\|\psi_0\|_2 \leq 1$ and $\langle \psi_0 | \Lambda | \psi_0 \rangle \leq \langle \psi | \Lambda | \psi \rangle$. The last inequality follows from $J \leq \lceil \log_2 r \rceil$ and

$$\sqrt{2}(3 + 6\sqrt{J}) \leq 3\sqrt{10}\sqrt{1 + J} \leq 12\sqrt{1 + J}. \quad \square$$

A.3 Proof of Lemma 4.6

Proof. We simply write $r := \max\{1, 2(T_{\text{Sample}} + T + T_{\text{Verify}})\}$. Define the block projector for $m \geq 0$,

$$\Pi_m^{\text{B}} := \sum_{j=mr}^{(m+1)r-1} \Pi_{=j}.$$

We adopt the convention $\Pi_{=j} = 0$ for $j > N$. As $M_{\mathcal{E}}$ increases the database size by at most r ,

$$\Pi_m^{\text{B}} M_{\mathcal{E}} \Pi_n^{\text{B}} = 0 \quad (31)$$

for $|m - n| \geq 2$. Define the odd and even parts

$$|\psi_e\rangle := \sum_{2|m} \Pi_m^{\text{B}} |\psi\rangle, \quad |\psi_o\rangle := \sum_{2 \nmid m} \Pi_m^{\text{B}} |\psi\rangle.$$

Define

$$d_e := \langle \psi_e | M_{\mathcal{E}} | \psi_e \rangle, \quad d_o := \langle \psi_o | M_{\mathcal{E}} | \psi_o \rangle, \quad d_m := \langle \psi | \Pi_m^{\text{B}} M_{\mathcal{E}} \Pi_m^{\text{B}} | \psi \rangle.$$

Then we have

$$\langle \psi | M_{\mathcal{E}} | \psi \rangle \leq d_e + d_o + |\langle \psi_e | M_{\mathcal{E}} | \psi_o \rangle| + |\langle \psi_o | M_{\mathcal{E}} | \psi_e \rangle|. \quad (32)$$

By Eq. (31), d_e and d_o can be written as

$$d_e = \sum_{2|m} d_m, \quad d_o = \sum_{2 \nmid m} d_m.$$

Since $0 \preceq M_{\mathcal{E}}$, the Cauchy–Schwarz inequality gives, for any vectors $|u\rangle$ and $|v\rangle$,

$$|\langle u | M_{\mathcal{E}} | v \rangle| \leq \sqrt{\langle u | M_{\mathcal{E}} | u \rangle \langle v | M_{\mathcal{E}} | v \rangle}.$$

This gives

$$|\langle \psi_e | M_{\mathcal{E}} | \psi_o \rangle| \leq \sqrt{d_e d_o}.$$

Hence, Eq. (32) and $2\sqrt{ab} \leq a + b$ for nonnegative a, b yield

$$\langle \psi | M_{\mathcal{E}} | \psi \rangle \leq d_e + d_o + 2\sqrt{d_e d_o} \leq 2(d_e + d_o) \leq 2 \sum_m d_m. \quad (33)$$

Applying Eq. (20) to $\Pi_m^{\text{B}} |\psi\rangle \in \mathcal{L}_{(m+1)r-1}$, we get

$$d_m \leq \tau_T \|\Pi_m^{\text{B}} |\psi\rangle\|_2^2 + \kappa \frac{(m+1)r-1}{\Delta} \|\Pi_m^{\text{B}} |\psi\rangle\|_2^2.$$

The equality

$$\Pi_m^B \Lambda \Pi_m^B + (r-1)\Pi_m^B - ((m+1)r-1)\Pi_m^B = \sum_{j=mr}^{(m+1)r-1} (j-mr)\Pi_{=j} \succeq 0$$

gives

$$((m+1)r-1)\|\Pi_m^B \psi\|_2^2 \leq \langle \psi | \Pi_m^B \Lambda \Pi_m^B | \psi \rangle + (r-1)\|\Pi_m^B \psi\|_2^2.$$

This implies

$$\begin{aligned} \sum_m d_m &\leq \frac{\kappa}{\Delta} \sum_m ((m+1)r-1)\|\Pi_m^B \psi\|_2^2 + \sum_m \tau_T \|\Pi_m^B \psi\|_2^2 \\ &\leq \frac{\kappa}{\Delta} \sum_m \langle \psi | \Pi_m^B \Lambda \Pi_m^B | \psi \rangle + \sum_m \left(\tau_T + \frac{\kappa(r-1)}{\Delta} \right) \|\Pi_m^B \psi\|_2^2 \\ &= \frac{\kappa \langle \psi | \Lambda | \psi \rangle}{\Delta} + \left(\tau_T + \frac{\kappa(r-1)}{\Delta} \right) \end{aligned}$$

Applying it to [Eq. \(33\)](#) gives

$$\langle \psi | M_{\mathcal{E}} | \psi \rangle \leq \frac{2\kappa \langle \psi | \Lambda | \psi \rangle}{\Delta} + 2 \left(\tau_T + \frac{\kappa(r-1)}{\Delta} \right). \quad \square$$

A.4 Proof of [Lemma 5.2](#)

Proof. Consider an arbitrary unit vector $|\psi\rangle$ which can be expressed as

$$|\psi\rangle = \sum_{z,D} \alpha_{z,D} |\phi_D\rangle_O |z\rangle_Z, \quad \sum_{z,D} |\alpha_{z,D}|^2 = 1, \quad \langle \psi | \Lambda | \psi \rangle = \sum_{z,D} |D| |\alpha_{z,D}|^2.$$

In oracle-conditioned components,

$$|\psi\rangle = \frac{1}{M^{N/2}} \sum_H |H\rangle |\psi(H)\rangle, \quad |\psi(H)\rangle = \sum_{z,D} \alpha_{z,D} \omega_M^{\langle D, H \rangle} |z\rangle.$$

Then $\mathbb{E}_H[\|\psi(H)\|_2^2] = 1$.

For $x \in [N]$ and $h \in [M]$, recall the one-point reprogrammed function $H_{x \rightarrow h}$. Introduce an environment register env with orthonormal basis $\{|x, H, h\rangle\}$, a challenge register ch , and a fresh workspace W , and define

$$|\Gamma_{\text{unif}}\rangle := \frac{1}{\sqrt{NM^{N+1}}} \sum_{x,H,h} |x, H, h\rangle_{\text{env}} |h\rangle_{\text{ch}} |\psi(H)\rangle_Z |0\rangle_W, \quad (34)$$

$$|\Gamma_{\text{img}}\rangle := \frac{1}{\sqrt{NM^{N+1}}} \sum_{x,H,h} |x, H, h\rangle_{\text{env}} |h\rangle_{\text{ch}} |\psi(H_{x \rightarrow h})\rangle_Z |0\rangle_W. \quad (35)$$

We compute the two norms and the Euclidean distance between the states. We have $\|\Gamma_{\text{unif}}\|_2^2 = \mathbb{E}_H[\|\psi(H)\|_2^2] = 1$. For fixed x , the map

$$(H, h) \longleftrightarrow (G = H_{x \rightarrow h}, a = H(x)) \quad (36)$$

is a bijection.

Two states $|\Gamma_{\text{unif}}\rangle, |\Gamma_{\text{img}}\rangle$ correspond to $|\phi_1\rangle, |\phi_2\rangle$ defined in [\[CGLQ20, Section 5.2\]](#), respectively. From the proof of [\[CGLQ20, Lemma 5.10\]](#), we have

$$\|\Gamma_{\text{unif}} - \Gamma_{\text{img}}\|_2^2 \leq \frac{4\langle \psi | \Lambda | \psi \rangle}{N}. \quad (37)$$

For an oracle J and challenge h , let V_h^J denote the corresponding adversary unitary. On the environment register storing (x, H, h) , define

$$\begin{aligned}\widehat{V}_{\text{unif}} &:= \sum_{x, H, h} |x, H, h\rangle\langle x, H, h| \otimes V_h^H, \\ \widehat{V}_\star &:= \sum_{x, H, h} |x, H, h\rangle\langle x, H, h| \otimes V_h^{H \rightarrow h}.\end{aligned}$$

Define

$$|\Phi_{\text{unif}}\rangle := \widehat{V}_{\text{unif}}|\Gamma_{\text{unif}}\rangle, \quad |\Phi_\star\rangle := \widehat{V}_\star|\Gamma_{\text{unif}}\rangle, \quad |\Phi_{\text{img}}\rangle := \widehat{V}_\star|\Gamma_{\text{img}}\rangle.$$

Let Π_0 be the projector corresponding to adversary output 0, and put

$$p_{\text{unif}} := \|\Pi_0\Phi_{\text{unif}}\|_2^2, \quad p_\star := \|\Pi_0\Phi_\star\|_2^2, \quad p_{\text{img}} := \|\Pi_0\Phi_{\text{img}}\|_2^2.$$

The last two experiments apply the same controlled unitary $\widehat{V}_\star$. Equivalently, they use the same POVM element

$$\widetilde{E}_\star := \widehat{V}_\star^\dagger \Pi_0 \widehat{V}_\star, \quad 0 \preceq \widetilde{E}_\star \preceq I.$$

For unit vectors $|u\rangle, |v\rangle$ and an operator $0 \preceq E \preceq I$, applying Cauchy-Schwarz to $E - \frac{1}{2}I$ gives

$$\begin{aligned}|\langle u|E|u\rangle - \langle v|E|v\rangle| &\leq 2\|E - \tfrac{1}{2}I\|_{\text{op}} \|u - v\|_2 \\ &\leq \|u - v\|_2.\end{aligned}$$

Applying this to $\widetilde{E}_\star$ and the normalized states $|\Gamma_{\text{img}}\rangle, |\Gamma_{\text{unif}}\rangle$, and using [Eq. \(37\)](#), gives

$$|p_{\text{img}} - p_\star| \leq \|\Gamma_{\text{img}} - \Gamma_{\text{unif}}\|_2 \leq \sqrt{\frac{4\langle\psi|\Lambda|\psi\rangle}{N}}. \quad (38)$$

Orthogonality of the environment labels gives

$$p_{\text{unif}} = \frac{1}{NM^{N+1}} \sum_{x, H, h} \langle\psi(H)|E_h^H|\psi(H)\rangle, \quad (39)$$

$$p_\star = \frac{1}{NM^{N+1}} \sum_{x, H, h} \langle\psi(H)|E_h^{H \rightarrow h}|\psi(H)\rangle. \quad (40)$$

For each H , put $w_H := \|\psi(H)\|_2^2$ and normalize the nonzero oracle-conditioned component as $|\eta_H\rangle = w_H^{-1/2}|\psi(H)\rangle$. For $w_H > 0$, define

$$a_{H,h}(x) := \langle\eta_H|E_h^{H \rightarrow h}|\eta_H\rangle, \quad a_{H,h}(\emptyset) := \langle\eta_H|E_h^H|\eta_H\rangle.$$

When $w_H = 0$, set both quantities equal to zero. [Eqs. \(39\) and \(40\)](#) give

$$p_\star - p_{\text{unif}} = \frac{1}{M^{N+1}} \sum_{H,h} w_H \left(\frac{1}{N} \sum_x a_{H,h}(x) - a_{H,h}(\emptyset) \right).$$

Condition on H and h . Then the base oracle H , the replacement value h , the normalized initial state $|\eta_H\rangle$, and the entire T -query adversary for challenge h are fixed, while only $x \xleftarrow{\$} [N]$ varies. Hence [Lemma 2.5](#) applies. So, the absolute value of the parenthesis is at most $4T^2/N$. Hence

$$|p_\star - p_{\text{unif}}| \leq \frac{4T^2}{N} \frac{1}{M^{N+1}} \sum_{H,h} w_H = \frac{4T^2}{N} \mathbb{E}_H[w_H] = \frac{4T^2}{N}. \quad (41)$$

The same change of variables gives

$$\frac{1}{2}(p_{\text{img}} - p_{\text{unif}}) = \langle \psi | M_{\mathcal{E}_{\text{PRG}}} | \psi \rangle. \quad (42)$$

Indeed, the uniform experiment simplifies to

$$p_{\text{unif}} = \frac{1}{M^N} \sum_H \left\langle \psi(H) \left| \frac{1}{M} \sum_h E_h^H \right| \psi(H) \right\rangle.$$

For the image experiment, apply the bijection [Eq. \(36\)](#) and sum over the original value a :

$$\begin{aligned} p_{\text{img}} &= \frac{1}{NM^{N+1}} \sum_{x, H, h} \langle \psi(H_{x \rightarrow h}) | E_h^{H_{x \rightarrow h}} | \psi(H_{x \rightarrow h}) \rangle \\ &= \frac{1}{NM^N} \sum_{x, G} \langle \psi(G) | E_{G(x)}^G | \psi(G) \rangle \\ &= \frac{1}{M^N} \sum_G \left\langle \psi(G) \left| \frac{1}{N} \sum_x E_{G(x)}^G \right| \psi(G) \right\rangle \end{aligned}$$

Subtracting these two identities proves [Eq. \(42\)](#). Combining [Eq. \(38\)](#), [Eq. \(42\)](#) and [Eq. \(41\)](#) with the triangle inequality proves [Eq. \(21\)](#). Since $\|E_{\text{PRG}}^H\|_{\text{op}} \leq 1$ for every H , we have $\|M_{\mathcal{E}_{\text{PRG}}}\|_{\text{op}} \leq 1$, which gives the cap. Restricting to $\mathcal{L}_P$ and using $\langle \psi | \Lambda | \psi \rangle \leq P$ on $\mathcal{L}_P$ proves [Eq. \(22\)](#). $\square$

A.5 Proof of [Lemma 5.6](#)

We prove the lemma by using the method introduced in the proof of [\[CGLQ20, Lemma 6.2\]](#).

Proof. Fix an arbitrary unit vector $|\psi\rangle$. Define the projector on the oracle register, for $x \in [N]$,

$$F_x := \sum_{D: D(x)=0} |\phi_D\rangle\langle\phi_D|_O.$$

Then, $I - F_x$ corresponds to the projection P_x defined in [\[CGLQ20, Section 6\]](#). Define

$$p_x := \|(I - F_x)\psi\|_2^2$$

which corresponds to $p_x^{(0)}$ defined in [\[CGLQ20, Section 6\]](#). Calculation yields

$$\sum_{x \in [N]} p_x = \langle \psi | \Lambda | \psi \rangle.$$

In the proof of [\[CGLQ20, Lemma 6.2\]](#), they showed

$$\sqrt{\Pr[\text{win}|x]} \leq \sqrt{p_x} + \sqrt{1/2}.$$

Squaring both sides and averaging over $x \in [N]$ gives

$$\Pr[\text{win}] - \frac{1}{2} \leq \frac{\langle \psi | \Lambda | \psi \rangle}{N} + \sqrt{\frac{2\langle \psi | \Lambda | \psi \rangle}{N}} \leq (1 + \sqrt{2}) \sqrt{\frac{\langle \psi | \Lambda | \psi \rangle}{N}}.$$

Applying the same argument to the adversary with its output bit flipped bounds $1/2 - \Pr[\text{win}]$. Combining the two bounds yields

$$\left| \Pr[\text{win}] - \frac{1}{2} \right| \leq (1 + \sqrt{2}) \sqrt{\frac{\langle \psi | \Lambda | \psi \rangle}{N}}.$$

$|\langle \psi | M_{\mathcal{E}_{\text{VB}}} | \psi \rangle| = |\Pr[\text{win}] - \frac{1}{2}|$ proves the lemma. $\square$

A.6 Proof of Lemma 5.10

We use the following result from [Liu23].

Lemma A.3 ([Liu23, Lemma 4.10]). *There exists a universal constant $C_{\text{BF}} > 0$ such that, for all integers $P, T \geq 0$,*

$$\delta_{\text{OWF}}^{\text{BF}}(P, T) \leq \min \left\{ 1, C_{\text{BF}} \frac{P + (T + 1)^2}{\min\{N, M\}} \right\}.$$

For $T \geq 1$, this follows from the cited result after absorbing its implicit constant into C_{BF} and using $T^2 \leq (T + 1)^2$; the case $T = 0$ follows by monotonicity in T from the case $T = 1$, and the cap by 1 is trivial.

We now prove Lemma 5.10.

Proof. By Theorem 3.5 and Lemma A.3, for any $P \geq 0$,

$$\|\Pi_{\leq P} M_{\mathcal{E}_{\text{OWF}}} \Pi_{\leq P}\|_{\text{op}} \leq C_{\text{BF}} \frac{P + (T + 1)^2}{\min\{N, M\}}.$$

Set

$$\tau_T := C_{\text{BF}} \frac{(T + 1)^2}{\min\{N, M\}}, \quad \kappa := C_{\text{BF}}, \quad \Delta := \min\{N, M\}.$$

Applying Lemma 4.6 to the inequality above yields

$$\begin{aligned} \langle \psi | M_{\mathcal{E}_{\text{OWF}}} | \psi \rangle &\leq \frac{2C_{\text{BF}} \langle \psi | \Lambda | \psi \rangle}{\min\{N, M\}} + \frac{2C_{\text{BF}}(T + 1)^2}{\min\{N, M\}} + \frac{2C_{\text{BF}}(r_{\text{OWF}} - 1)}{\min\{N, M\}} \\ &\leq 8C_{\text{BF}} \frac{\langle \psi | \Lambda | \psi \rangle + (T + 1)^2}{\min\{N, M\}}. \end{aligned}$$

□

A.7 Proof of Lemma 5.14

We recall the following result from [ABC⁺26].

Lemma A.4 ([ABC⁺26, Lemma 2]). *There exists a universal constant $C_{\text{BF}} > 0$ such that, for all integers $P, T \geq 0$,*

$$\delta_{\text{PermInv}}^{\text{BF}}(P, T) \leq \min \left\{ 1, C_{\text{BF}} \frac{P + (T + 1)^2}{N} \right\}.$$

For $T \geq 1$, this follows from the cited result after absorbing its implicit constant into C_{BF} and using $T^2 \leq (T + 1)^2$; the case $T = 0$ follows by monotonicity in T from the case $T = 1$, and the cap by 1 is trivial.

We now prove Lemma 5.14.

Proof. By Theorem 3.5 and Lemma A.4, for any $P \geq 0$,

$$\|\Pi_{\leq P} M_{\mathcal{E}_{\text{PermInv}}} \Pi_{\leq P}\|_{\text{op}} \leq C_{\text{BF}} \frac{P + (T + 1)^2}{N}.$$

Set

$$\tau_T := C_{\text{BF}} \frac{(T + 1)^2}{N}, \quad \kappa := C_{\text{BF}}, \quad \Delta := N.$$

Lemma 4.6 with the inequality above yields

$$\begin{aligned} \langle \psi | M_{\mathcal{E}_{\text{PermInv}}} | \psi \rangle &\leq \frac{2C_{\text{BF}} \langle \psi | \Lambda | \psi \rangle}{N} + \frac{2C_{\text{BF}}(T + 1)^2}{N} + \frac{2C_{\text{BF}}(r_{\text{PermInv}} - 1)}{N} \\ &\leq 8C_{\text{BF}} \frac{\langle \psi | \Lambda | \psi \rangle + (T + 1)^2}{N}. \end{aligned}$$

□

B Database Size Increment per Query

We examine how one family query acts on $\mathcal{L}_P^{(K)}$. In the following calculation, s , x , and u denote the family-query salt index, the query input, and the Fourier-basis response value, respectively; all remaining basis labels of Z are suppressed. For random functions, by linearity, it suffices to consider a basis component of $\mathcal{L}_P^{(K)}$. Fix $D_1, \dots, D_K$ with $\sum_{t=1}^K |D_t| \leq P$ and consider

$$\begin{aligned}
|\psi\rangle &= \sum_s c_s |s, x, u\rangle_Z \otimes |\phi_{D_1}, \dots, \phi_{D_K}\rangle_O \\
&= \frac{1}{M^{NK/2}} \sum_{s, \mathbf{H}} c_s \omega_M^{\sum_{t=1}^K \langle D_t, H_t \rangle} |s, x, u\rangle_Z |H_1, \dots, H_K\rangle_O \\
&\xrightarrow{\mathcal{O}} \frac{1}{M^{NK/2}} \sum_{s, \mathbf{H}} c_s \omega_M^{\sum_{t=1}^K \langle D_t, H_t \rangle + u H_s(x)} |s, x, u\rangle_Z |H_1, \dots, H_K\rangle_O \\
&= \frac{1}{M^{NK/2}} \sum_{s, \mathbf{H}} c_s \omega_M^{\sum_{t \neq s} \langle D_t, H_t \rangle + \langle D_s + u e_x, H_s \rangle} |s, x, u\rangle_Z |H_1, \dots, H_K\rangle_O \\
&= \sum_s c_s |s, x, u\rangle_Z \otimes |\phi_{D_1}, \dots, \phi_{D_s + u e_x}, \dots, \phi_{D_K}\rangle_O.
\end{aligned}$$

As $|D_s + u e_x| \leq |D_s| + 1$, one family query increases total database size by at most one.

For random permutations, by linearity, it suffices to fix $s \in [K]$, $x \in [N]$, $u \in \mathbb{Z}_N$, and a tensor product of database states in $\mathcal{L}_P^{(K)}$. Fix $\alpha_1, \dots, \alpha_K$ satisfying $\sum_{t=1}^K |\alpha_t| \leq P$, and consider

$$\begin{aligned}
|\psi\rangle &= |s, x, u\rangle_Z \otimes |v_{\alpha_1}, \dots, v_{\alpha_K}\rangle_O \\
&= \frac{1}{\sqrt{\prod_{t=1}^K (N - |\alpha_t|)!}} \sum_{H_1 \supseteq \alpha_1, \dots, H_K \supseteq \alpha_K} |s, x, u\rangle_Z |H_1, \dots, H_K\rangle_O \\
&\xrightarrow{\mathcal{O}} \frac{1}{\sqrt{\prod_{t=1}^K (N - |\alpha_t|)!}} \sum_{H_1 \supseteq \alpha_1, \dots, H_K \supseteq \alpha_K} \omega_N^{u H_s(x)} |s, x, u\rangle_Z |H_1, \dots, H_K\rangle_O.
\end{aligned}$$

If $x \in \text{dom}(\alpha_s)$, then

$$\mathcal{O}|\psi\rangle = \omega_N^{u \alpha_s(x)} |s, x, u\rangle_Z \otimes |v_{\alpha_1}, \dots, v_{\alpha_K}\rangle_O.$$

Hence, the total database size is unchanged. Suppose $x \notin \text{dom}(\alpha_s)$. Then,

$$\begin{aligned}
\sum_{H_s \supseteq \alpha_s} \omega_N^{u H_s(x)} |H_s\rangle &= \sum_{H_s \supseteq \alpha_s} \sum_{y \notin \text{im}(\alpha_s)} \omega_N^{uy} \mathbf{1}[H_s(x) = y] |H_s\rangle \\
&= \sum_{y \notin \text{im}(\alpha_s)} \omega_N^{uy} \sum_{H_s \supseteq \alpha_s \cup \{x \mapsto y\}} |H_s\rangle.
\end{aligned}$$

Note that $|\alpha_s \cup \{x \mapsto y\}| = |\alpha_s| + 1$ and

$$|v_{\alpha_s \cup \{x \mapsto y\}}\rangle = \frac{1}{\sqrt{(N - |\alpha_s| - 1)!}} \sum_{H_s \supseteq \alpha_s \cup \{x \mapsto y\}} |H_s\rangle.$$

Hence,

$$\sum_{H_s \supseteq \alpha_s} \omega_N^{u H_s(x)} |H_s\rangle = \sqrt{(N - |\alpha_s| - 1)!} \sum_{y \notin \text{im}(\alpha_s)} \omega_N^{uy} |v_{\alpha_s \cup \{x \mapsto y\}}\rangle.$$

For $t \neq s$,

$$\sum_{H_t \supseteq \alpha_t} |H_t\rangle = \sqrt{(N - |\alpha_t|)!} |v_{\alpha_t}\rangle.$$

The calculation above gives

$$\begin{aligned} \mathcal{O}|\psi\rangle &= \frac{1}{\sqrt{N - |\alpha_s|}} \sum_{y \notin \text{im}(\alpha_s)} \omega_N^{uy} |s, x, u\rangle_Z \\ &\quad \otimes |v_{\alpha_1}, \dots, v_{\alpha_s \cup \{x \mapsto y\}}, \dots, v_{\alpha_K}\rangle_O. \end{aligned}$$

Thus every component in the second case has total database size at most $P + 1$. By linearity, the two cases show that one query to $\mathbf{H}$ raises the total database size by at most one.

Lemma B.1. *The salted purified game operator raises the total database size by at most $r := 2(T_{\text{Sample}} + T + T_{\text{Verify}})$; namely, for every $P \geq 0$,*

$$M_{\mathcal{E}(K)} \mathcal{L}_P^{(K)} \subseteq \mathcal{L}_{P+r}^{(K)}.$$

Proof. Let U be the joint unitary implemented by the sampler, adversary, and verifier in the purified-oracle representation. It contains at most $T_{\text{Sample}} + T + T_{\text{Verify}}$ underlying oracle queries. By the one-query calculations above,

$$U \mathcal{L}_P^{(K)} \subseteq \mathcal{L}_{P+T_{\text{Sample}}+T+T_{\text{Verify}}}^{(K)}.$$

The same inclusion holds for $U^\dagger$, since each adjoint phase query is obtained by negating the response label before and after a phase query; these relabelings act only on the query registers and preserve the database size.

For a search game, the purified game operator has the form

$$(I \otimes \langle 0|) U^\dagger \Pi U (I \otimes |0\rangle)$$

and therefore increases the total database size by at most $2(T_{\text{Sample}} + T + T_{\text{Verify}})$. For a decision game, the purified game operator is a signed linear combination of two operators of this form. Since the target subspace in the database hierarchy is linear, the same inclusion holds. $\square$

When $K = 1$, the salted database hierarchy reduces to that of the base game, $\mathcal{L}_P^{(1)} = \mathcal{L}_P$, and the salted query interface reduces to the base-game query interface. Hence, [Lemma B.1](#) also gives

$$M_{\mathcal{E}} \mathcal{L}_P \subseteq \mathcal{L}_{P+2(T_{\text{Sample}}+T+T_{\text{Verify}})}.$$