Non-uniformity and Quantum Advice in the Quantum Random Oracle Model

Qipeng Liu[1] [0000−0002−3994−7061]

Simons Institute for the Theory of Computing, Berkeley, USA qipengliu0@gmail.com

Abstract. QROM (quantum random oracle model), introduced by Boneh et al. (Asiacrypt 2011), captures all generic algorithms. However, it fails to describe non-uniform quantum algorithms with preprocessing power, which receives a piece of bounded classical or quantum advice.

As non-uniform algorithms are largely believed to be the right model for attackers, starting from the work by Nayebi, Aaronson, Belovs, and Trevisan (QIC 2015), a line of works investigates non-uniform security in the random oracle model. Chung, Guo, Liu, and Qian (FOCS 2020) provide a framework and establish non-uniform security for many cryptographic applications. Although they achieve nearly optimal bounds for many applications with classical advice, their bounds for quantum advice are far from tight.

In this work, we continue the study on quantum advice in the QROM. We provide a new idea that generalizes the previous multi-instance framework, which we believe is more quantum-friendly and should be the quantum analog of multi-instance games. To this end, we *match* the bounds with *quantum advice* to those with *classical advice* by Chung et al., showing quantum advice is almost as good/bad as classical advice for many natural security games in the QROM.

Finally, we show that for some contrived games in the QROM, quantum advice can be exponentially better than classical advice for some parameter regimes. To our best knowledge, it provides an evidence of a general separation between quantum and classical advice relative to an unstructured oracle.

1 Introduction

Many practical cryptographic constructions are analyzed in idealized models, for example, the random oracle model which treats an underlying hash function as a uniformly random oracle (ROM) [BR93]. On a high level, the random oracle model captures all algorithms that use the underlying hash function in a generic (black-box) way; often, the best attacks are generic. Whereas the random oracle methodology guides the actual security of practical constructions, it fails to describe non-uniform security: that is, an algorithm consists of two parts, the offline and the online part; the offline part can take forever, and at the end of the day, it produces a piece of bounded advice for its online part; the online part given the advice, tries to attack cryptographic constructions efficiently.

Non-uniform algorithms are largely believed to be the right model for attackers and usually show advantages over uniform algorithms [Unr07, CDGS18, CDG18]. The famous non-uniform example is Hellman's algorithm [Hel80] for inverting permutations or functions. When a permutation of range and domain size N is given, Hellman's algorithm can invert any image (with certainty) with roughly advice size $\sqrt{N}$ and running time $\sqrt{N}$. In contrast, uniform algorithms require running time N to achieve constant success probability. Another more straightforward example is collision resistance. When non-uniform algorithms are presented, no single fixed hash function is collision-resistant as an algorithm can hardcode a pair of collisions in its advice.

Non-uniform security in idealized models has been studied extensively in the literature. Let us take the two most simple yet fundamental security games as examples: one search game and one decision game. The first one is one-way function inversion (or OWFs) as mentioned above. The goal is to invert a random image of the random oracle. The study was initialized by Yao [Yao90] and later improved by a line of works [DTT10, Unr07, DGK17, CDGS18]. They show that any T-query algorithm with arbitrary S-bit advice, can win this game with probability at most $\tilde{O}(ST/N)$, assuming the random oracle has equal domain and range size. The other example is pseudorandom generators (or PRG). The task is to distinguish between a random image $H(x)$ (x is uniformly at random and H is the hash function) or a random element y in its range. Since it is a decision game, some techniques for OWFs may not apply to PRGs, which we will see later. Its non-uniform security is $O(1/2 + T/N + \sqrt{ST/N})$ by Coretti et al. [CDGS18], and later improved by Garvin et al. [GGKL21].

The quantum setting is very similar to the classical one, except an algorithm can query the random oracle in superposition. Boneh et al. [BDF+11] justify the ability to make superposition queries since a quantum computer can always learn the description of a hash function and compute it coherently. Besides, advice can be either a sequence of **bits** or **qubits**. We should carefully distinguish between the two different models. Indeed, we believe non-uniform quantum algorithms with quantum advice are important to understand and should be considered the "right" attacker model when full-scale quantum computers are widely viable and quantum memory is affordable.

Nayebi, Aaronson, Belovs, and Trevisan [NABT14] initiated the study of quantum non-uniform security with classical advice of OWFs and PRGs. Hhan, Xagawa and Yamakawa [HXY19], Chung, Liao and Qian [CLQ19] extended the study to quantum advice. Most recently, Chung, Guo, Liu and Qian [CGLQ20] improved the bounds for both examples. For OWFs, their bounds are almost optimal in terms of query complexity for both classical and quantum advice. They show that to invert a random image with at least constant probability, advice size S and the number of queries T should satisfy $ST + T^2 \geq \tilde{\Omega}(N)$. However, a gap between classical and quantum advice appears when we choose security parameters for practical hash functions against non-uniform attacks. In practice, we ensure that an adversary with bounded resources (for example, $S = T = 2^{128}$) only has probability smaller than 2^{-128}. The bounds in

[CGLQ20] suggest that for OWF, the security parameter needs to be $n = 384$ (and $N = 2^{384}$) for classical advice and $n = 640$ for quantum advice, leaving a big gap between two types of advice. Even worse, when it comes to PRGs, the security parameters are $n = 640$ for classical advice v.s. $n = 3200$ for quantum advice; not to mention a large gap between their query complexity, unlike OWFs.

As understanding quantum advice is beneficial to both practical cryptography efficiency and may inspire general computation theory (such as, QMA v.s. QCMA [AK07, Aar21] and BQP/poly v.s. BQP/qpoly [Aar05]), we raise the following natural question:

Can quantum advice outperform classical advice in the QROM?

In this work, we provide a new technique for analyzing quantum advice in the QROM and show that for many games, the non-uniform security with quantum advice matches the best-known security with classical advice, including OWFs and PRGs. It gives strong evidence that for many cryptographic games in the QROM, quantum advice provides no or little advantage over classical one.

So far, we have seen no advantage of quantum advice in the QROM for common cryptographic games. We then ask the second question:

Is there any (contrived) game in the QROM, in which quantum advice is "exponentially better" than classical advice?

We give an affirmative answer to this question, for some parameters of S, T. We show that when algorithms can not make online queries (i.e., $T = 0$), there is an exponential separation between quantum and classical advice for certain games. This result is inspired by the recent work by Yamakawa and Zhandry [YZ22] on verifiable quantum advantages in the QROM. We elaborate on both results now.

1.1 Our Results

Our first result is to give a quantum analog of "multi-instance games" via "alternating measurement games" (introduced in Section 5) and develop a new technique for analyzing non-uniform bounds with quantum advice. Our techniques do not need to rewind a non-uniform quantum algorithm and completely avoid the rewinding issues/difficulties in the prior work [CGLQ20].

To show the power of our technique, we incorporate it into three important applications: OWFs, PRGs, and salted cryptography. Note that our result below is a non-exhaustive list of applications. With little effort, we can show improved non-uniform security with quantum advice of Merkle-Damgård [GLLZ21], Yao's box [CGLQ20] and other games.

One-Way Functions. In this application, a random oracle is interpreted as a one-way function. A (non-uniform) algorithm needs to win the OWF security game with the random oracle as a OWF. Formally, let $H : [N] \to [M]$ be a random oracle.

1. A challenger samples a uniformly random input $x \in [N]$ and sends $y = H(x)$ to the algorithm.
2. The algorithm returns x' and it wins if and only if $H(x') = y$.

When both advice and queries are classical, the best lower bound is $\tilde{O}(ST/\alpha)$ by [CDGS18], where $\alpha = \min\{N, M\}$ and N, M are the domain and range size of the random oracle. In other words, no algorithm with S bits of advice and T classical queries can win with probability more than $\tilde{O}(ST/\alpha)$. There is a gap between this lower bound and the upper bound $\approx T/\alpha + (S^2T/\alpha^2)^{1/3}$ provided by Hellman's algorithm[1]. Later, Corrigan-Gibbs and Kogan [CGK19] study the possible improvement on the lower bound and conclude that any improvement will lead to improved results in circuit lower bounds. Thus, $\tilde{O}(ST/\alpha)$ is the best one can hope for in light of the barrier.

Chung et al. [CGLQ20] show that if S bits of classical advice and T quantum queries are given, the maximum winning probability is bounded by $\tilde{O}\left(\frac{ST+T^2}{\alpha}\right)$. They further argue that this bound is almost optimal. Intuitively, one can think of this as T^2/α comes from a brute-force Grover's algorithm [Gro96], without using any advice, and ST/α comes from classical advice and hits the classical barrier by [CGK19].

For quantum advice and quantum queries, they show the maximum success probability is $\tilde{O}\left(\frac{ST+T^2}{\alpha}\right)^{1/3}$. As mentioned early, although the bound is optimal regarding query complexity, the exponent seems non-tight. Thus, they ask the following question:

> *... Can this loss (of the exponent) be avoided, or is there any speed up in terms of S and T for sub-constant success probability?.*

Our first result gives a positive answer to the above question and proves that the loss on exponent can be avoided.

Theorem 1. *Let H be a random oracle $[N] \to [M]$ and $\alpha = \min\{N, M\}$. One-way function games in the QROM have security $O\left(\frac{ST+T^2}{\alpha}\right)$ against non-uniform quantum algorithms with S-qubits of advice and T quantum queries.*

The theorem guides security parameter choices of hash functions to be secure against non-uniform attacks. The security parameter n should be 384 to have security 2^{-128} against non-uniform quantum attacks with $S = T = 2^{128}$. Another direct implication of our theorem is that, when quantum advice $S = O(\sqrt{\alpha})$, quantum advice is useless for speeding up function inversion. To put it

[1] Hellman's algorithm on functions does not behave as well as on permutations. Upper and lower bounds meet at ST/α only when we consider permutations.

in another way, Grover's algorithm can not be sped up and only has probability T^2/α to succeed even with quantum advice of size $O(\sqrt{\alpha})$, relative to a random oracle. We list a comparison of best-known bounds and our result below.

Classical Advice in [CGLQ20]	Quantum Advice in [CGLQ20]	Quantum Advice in This Work
$\tilde{O}\left(\frac{ST+T^2}{\alpha}\right)$	$\tilde{O}\left(\frac{ST+T^2}{\alpha}\right)^{1/3}$	$O\left(\frac{ST+T^2}{\alpha}\right)$

Table 1: Non-uniform security for OWFs with T queries and S bits (qubits) of advice, where $\alpha = \min\{N, M\}$ and N, M are the domain and range size of the random oracle. Our bound is a "big-O" instead of "big-$\tilde{O}$" as we also remove the dependence on $\log N$ and $\log M$.

Pseudorandom Generators. Another important application we will focus on is pseudorandom generators. One fundamental difference from one-way functions is its being a decision game. We will later see that publicly verifiable games such as one-way functions are easy to deal with in the previous work [CGLQ20]. For games that can not be publicly verified, such as decision games, [CGLQ20] often gives worse bounds.

In this game, an algorithm tries to distinguish between an image of a random input, and a uniformly random element in the range. Let $H : [N] \to [M]$ be a random oracle.

– A challenger samples a uniformly random bit b. If $b = 0$, it samples a uniformly random $x \in [N]$ and outputs $y = H(x)$; otherwise, it samples a uniform $y \in [M]$ and outputs y.
– The algorithm is given y and returns b'. It wins if and only if $b' = b$.

Our new technique demonstrates the following theorem about PRGs.

Theorem 2. *Let H be a random oracle $[N] \to [M]$. PRG games in the QROM have security $1/2 + O\left(\frac{T^2}{N}\right)^{1/2} + O\left(\frac{ST}{N}\right)^{1/3}$ against non-uniform quantum algorithms with S-qubits of advice and T quantum queries.*

"Salting Defeats Preprocessing". Finally, instead of proving more concrete non-uniform bounds like Merkle-Damgård [GLLZ21], we demonstrate that the generic mechanism "salting" helps prevent quantum preprocessing attacks even with quantum advice. Maybe the most illustrating example is collision-resistant hash functions. As mentioned before, no single fixed hash function can be collision resistant against non-uniform attacks. A typical solution is to add "salt" to the hash function. A salt is a piece of random data that will be fed into a hash function as an additional input. To attack a salted collision resistant hash function, an adversary gets a salt s and is required to come out with two input $m \neq m'$

Classical Advice in [CGLQ20]	Quantum Advice in [CGLQ20]	Quantum Advice in This Work
$\frac{1}{2} + \tilde{O}\left(\frac{ST+T^2}{N}\right)^{1/3}$	$\frac{1}{2} + \tilde{O}\left(\frac{S^5T+S^4T^2}{N}\right)^{1/19}$	$\frac{1}{2} + O\left(\frac{T^2}{N}\right)^{1/2} + O\left(\frac{ST}{N}\right)^{1/3}$

Table 2: Non-uniform security of PRGs with T queries and S bits (qubits) of advice. Our bound also improves the previous result on classical advice by reducing the exponent on T^2/N from $1/3$ to $1/2$; we note that the improvement on the exponent only follows from a simple observation and can also be applied to the previous work as well.

such that the hash evaluation on (s, m) equals that of (s, m'). Intuitively, since salt s is chosen uniformly at random from a large space, advice is not long enough to include collisions for every possible salt. Thus, salting is a mechanism that compiles a game into another game, by adding a random extra input s and restricting the execution of the game always under oracle access to $H(s, \cdot)$.

Chung et al. [CLMP13], and Coretti et al. [CDGS18] formally proved the non-uniform security of salted collision-resistant hash in the classical ROM. Chung et al. [CGLQ20] extended the statement in the quantum setting. For quantum advice, their result roughly says that if an underlying game G is publicly verifiable or a decision game, then the salted version of G is secure against non-uniform attacks.

Our third results improve the prior ones in two different aspects. First, our theorem works not only for publicly verifiable or decision games, but for any types of games (see our definition of games Definition 2). Second, our theorem is tighter and provides a more pictorial statement for "salting defeats preprocessing", elaborated below. Our bounds match those with classical advice in [CGLQ20].

Theorem 3 (Informal, Theorem 10). *For any game G in the QROM, let $\nu(T)$ be its uniform security in the QROM. Let G_S be the salted game with salt space $[K]$. Then G_S has security $\delta(S, T)$ against non-uniform quantum adversaries with T queries and S-qubits of advice,*

1. $\delta(S, T) \leq 4\nu(T) + O(ST/K)$;
2. *If G_S is a decision game, then* $\delta(S, T) \leq \nu(T) + O(ST/K)^{1/3}$.

That is to say, the non-uniform security of G_S and uniform security of G only differs by a term of $O(ST/K)$ or $O(ST/K)^{1/3}$ depending on the type of the game. When the game G is a search game, G_S has non-uniform security $4\nu(T) + O(ST/K)$. We can choose S to ensure $ST/K \leq \nu(T)$ so that the non-uniform security of G_S is in the same order of G's security $\nu(T)$. For decision games, we choose S such that $(ST/K)^{1/3}$ is extremely small.

In [CGLQ20], they show that for publicly verifiable games, $\delta := \delta(S, T)$ satisfies $\delta \leq \tilde{O}\left(\nu(T/\delta) + \frac{ST}{K\delta}\right)$ whereas ours works for any games and $\delta(S, T) \leq 4\nu(T) + O(ST/K)$. For decision games, ours also significantly improves prior results (see Table 3 and Theorem 7.6 in [CGLQ20] for a comparison). The dependence in their theorems on uniform security ν is much more complicated and yields loose bounds. Most notably, for decision games, when the salt size $K \to \infty$, the bound in [CGLQ20] does not rule out the speed up from having S-qubits of advice (corresponding to the term $\nu'(S^2T/\epsilon^8)$); whereas our bound gives $\nu(T)$ — exactly the security in the uniform case, completely ruling out the influence of quantum advice.

	Quantum Advice in [CGLQ20]	Quantum Advice in This Work
Any Games	$\delta \leq \tilde{O}\left(\nu(T/\delta) + ST/(K\delta)\right)$	$\delta \leq 4\nu(T) + O(ST/K)$
Decision Games	$\delta \leq 1/2 + \epsilon$ where $\epsilon \leq \tilde{O}\left(\nu'(S^2T/\epsilon^8) + \sqrt{S^5T/(K\epsilon^{17})}\right)$ and $\nu'(T) := \nu(T) - 1/2$	$\delta \leq \nu(T) + O(ST/K)^{1/3}$

Table 3: Salting "defeats" preprocessing.

Separation of Quantum and Classical Advice in the QROM. So far, we have seen many examples that quantum advice is as good/bad as classical advice. Below, we show that it is not always the case in the QROM: there exists a game in the QROM such that quantum advice is exponentially better than classical advice.

Theorem 4 (Separation of Quantum and Classical Advice in the QROM). *Let H be a random oracle $[2^{\mathsf{poly}(n)}] \to \{0,1\}$. There exists a game G in the QROM such that,*

- *G has security $2^{-\Omega(n)}$ against non-uniform adversaries with S-bits of* **classical** *advice and making no queries, for $S = 2^{n^c}/n$ and some constant $0 < c < 1$;*
- *There is a non-uniform adversary with S-qubits of* **quantum** *advice and making no queries, that achieves winning probability $1 - \mathsf{negl}(n)$, for $S = \tilde{O}(n)$.*

Although the bound only works in the parameter regime $T = 0$, to our best knowledge, it is the first example of an exponential separation between quantum and classical advice in the QROM (or for inputs without structures).

Remark 1. For the parameter regime $T = 0$, the above separation can be alternatively viewed as an exponential separation of quantum/classical one-way communication complexity for some relation $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{Y} \times Z$. In the context of one-way communication complexity, there are two players, Alice and Bob. Alice gets an input $x \in \mathcal{X}$ and Bob gets an input $y \in \mathcal{Y}$; Alice sends one (classical or quantum) message to Bob and Bob tries to output $z \in \mathcal{Z}$ such that $(x, y, z) \in \mathcal{R}$. Our result in Theorem 4 is a separation of quantum/classical one-way communication complexity when $\mathcal{X} = \{0,1\}^{2^{\mathsf{poly}(n)}}$, $\mathcal{Y} = \{0,1\}^n$, $\mathcal{Z} = \{0,1\}^{n \times \mathsf{poly}(n)}$; when the message is allow to be quantum, $\tilde{O}(n)$ qubits are sufficient; on the other hand, the classical communication complexity is $\Omega(2^{n^c}/n)$.

Exponential separation of quantum/classical one-way communication complexity is already known, starting from the work by [BYJK04] (later by [Gav08]) based on the so-called hidden matching problem. We believe the hidden matching problem can be also turned into a separation of quantum/classical advice in the parameter regime $T = 0$, in the QROM. However, [BYJK04] only proved *average-case* hardness against *deterministic* classical Bob. Therefore, we pick the recent result by Zhandry and Yamakawa for simplicity of presentation.

1.2 Organization

The rest of the paper is organized as follows. In **??**, we give an overview of our main technical contribution and achieve non-uniform bounds for OWFs. Section 2 and Section 3 recall the notations and backgrounds on quantum computing, random oracles models, non-uniform security and bit-fixing models. Section 4 introduces decomposition of advice with respect to a game, which helps the proof of our main theorem. Section 5 proves the main theorem whereas Section 6 applies the main theorem to various applications. Finally in Section 7, we give the separation of quantum and classical advice.

Acknowledgements

We would like to thank Kai-Min Chung for his discussion on an early write-up and providing an intuitive explanation of the decomposition of quantum advice in our work; Jiahui Liu and Luowen Qian for their comments on an early draft of this paper; Luowen Qian and Makrand Sinha for mentioning the connections between our impossibility result and quantum one-way communication complexity.

Qipeng Liu is supported in part by the Simons Institute for the Theory of Computing, through a Quantum Postdoctoral Fellowship, by DARPA under Agreement No. HR00112020023 and by the NSF QLCI program through grant number OMA-2016245. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA.

2 Preliminaries

We assume readers are familiar with the basics of quantum information and computation. All backgrounds on quantum information can be found in [NC10].

2.1 Quantum Random Oracle Model

In the quantum random oracle model, a hash function is modeled as a random classical function H. The function H is sampled at the beginning of any security game and then gets fixed. Oracle access to H is defined by a unitary

$U_H : |x, y\rangle \to |x, y + H(x)\rangle$. A quantum oracle algorithm with oracle access to H is then denoted by a sequence of unitary $U_1, U_H, U_2, U_H, \cdots, U_T, U_H, U_{T+1}$ followed by a computational basis measurement, where U_i is a local unitary operating on the algorithm's internal register. The number of queries, in this case, is T — the number of U_H calls.

2.2 Other Useful Lemmas

We use the lemmas in this section to prove bounds in the alternating measurement games (Section 5). Readers can safely skip and return to this section for (Section 5.

We omit the proof for the following lemmas and refer readers to the appendix for more the proofs.

Lemma 1. *Let N be a positive integer and $p_1, \cdots, p_N \in \mathbb{R}^{\geq 0}$. Let $c_1, \cdots, c_N$ be a distribution over $[N]$. Assume $\sum_{i\in[N]} c_i p_i > 0$. Define S_k for every integer $k \geq 1$:*

$$S_k = \frac{\sum_{i\in[N]} c_i p_i^k}{\sum_{i\in[N]} c_i p_i^{k-1}}.$$

Then $\{S_k\}_{k\geq 1}$ is monotonically non-decreasing.

Lemma 2 (Jensen's inequality). *Let N, g be two positive integers and $p_1, \cdots, p_N \in \mathbb{R}^{\geq 0}$. Let $c_1, \cdots, c_N$ be a distribution over $[N]$. Assume $\sum_{i\in[N]} c_i p_i > 0$. If the following holds $\sum_{i\in[N]} c_i p_i^g \leq \delta^g$, then $\sum_{i\in[N]} c_i p_i \leq \delta$.*

3 (S, T) Quantum Algorithms and Games in the QROM

In this work, we consider non-uniform algorithms against games in the QROM. We start by defining (S, T) non-uniform quantum algorithms with either S classical bits of advice or S qubits of advice. The definitions below more or less follow definitions in [CGLQ20] but are adapted for our setting.

Definition 1 ((S, T) Non-Uniform Quantum Algorithms in the QROM). *A (S, T) non-uniform quantum algorithm with* **classical** *advice in the QROM is modeled by a collection $\{s_H\}_{H:[N]\to[M]}$ and $\{U_{\mathsf{inp}}\}_{\mathsf{inp}}$: for every function H, s_H is a piece of S-bit advice and U_{inp}^H is a unitary that calls the oracle H at most T times.*

A (S, T) non-uniform quantum algorithm with **quantum** *advice in the QROM is modeled by a collection $\{|\sigma_H\rangle\}_H$ and $\{U_{\mathsf{inp}}\}_{\mathsf{inp}}$: for every function H, $|\sigma_H\rangle$ is a piece of S-qubit advice and U_{inp}^H is a unitary that calls the oracle H at most T times.*

Similarly, we denote a **uniform** *quantum algorithm by a collection of unitaries $\{U_{\mathsf{inp}}\}_{\mathsf{inp}}$: it is a non-uniform quantum algorithm satisfying $|\sigma_H\rangle = |0^S\rangle$ for all H.*

When the algorithm is working with oracle access to H, its initial state is $|s_H\rangle |0^L\rangle$ or $|\sigma_H\rangle |0^L\rangle$, respectively. On input inp, it applies U_{inp}^H on the initial state and measures its internal register in the computational basis.

Since we are working in the idealized model, we require neither L nor the size of the unitary U_{inp} to be polynomially bounded. In the rest of the work, we will focus on non-uniform algorithms with quantum advice as our new reduction works for both cases. Therefore, 'non-uniform algorithms' denotes 'non-uniform algorithms with quantum advice'.

Remark 2. We can assume quantum advice is a **pure** state. Due to convexity, the optimal non-uniform algorithm can always have advice as a pure state. If the advice is a mixed state and achieves a winning probability p, there always exists a pure state that achieves a winning probability at least p.

Next, we define games in the QROM.

Definition 2 (Games in the QROM). *A game G in the QROM is specified by two classical algorithms Samp^H and Verify^H:*

- $\mathsf{Samp}^H(r)$*: it is a deterministic algorithm that takes uniformly random coins $r \in \mathcal{R}$ as input, and outputs a challenge* ch.
- $\mathsf{Verify}^H(r, \mathsf{ans})$*: it is a deterministic algorithm that takes the same random coins for generating a challenge and an alleged answer* ans*, and outputs b indicating whether the game is won ($b = 0$ for winning).*

Let T_{Samp} be the number of queries made by Samp *and T_{Verify} be the number of queries made by* Verify.

For a fixed H and a quantum algorithm $\mathcal{A}$, the game $G_{\mathcal{A}}^H$ is executed as follows:

- *A challenger $\mathcal{C}$ samples* $\mathsf{ch} \leftarrow \mathsf{Samp}^H(r)$ *using uniformly random coins r.*
- *A (uniform or non-uniform) quantum algorithm $\mathcal{A}$ has oracle access to H, takes* ch *as input and outputs* ans*. We call $\mathcal{A}$ an online adversary/algorithm.*
- $b \leftarrow \mathsf{Verify}^H(r, \mathsf{ans})$ *is the game's outcome.*

Remark 3. In the above definition, a quantum algorithm makes at most T oracle queries to H. However, in some particular games, the algorithm can not get access to H. One famous example is Yao's box, in which an adversary is given a challenge input x and the goal is to output $H(x)$. The adversary can query H on any input except x (otherwise, the game is trivial). The definition Definition 2 does not capture this case. Nonetheless, we will stick with the current definition. For the special case when an algorithm has access to a different oracle H', the technique in this work extends as well. This extension requires a similar definition of games (Definition 3.3) in [CGLQ20].

Let us warm up by having a close look at the following examples.

Example 1. The first example is function inversion (or OWFs) G_{OWF}. $r = x \in [N]$ is a uniformly random pre-image and $\mathsf{ch} := H(x)$. The goal is to find a pre-image of ch. The verification procedure takes $r = x$ and $\mathsf{ans} = x'$, it outputs 0 (winning) if and only if x' is a pre-image of $H(x)$.

The other example G_{PRG} is to distinguish images of PRG from a uniformly random element. In this example, r consists of (b, x, y) where b is a single bit, x is a uniformly random pre-image in $[N]$ and y is a uniformly random element in $[M]$. The challenge ch is $H(x)$ if $b = 0$, otherwise $\mathsf{ch} = y$. The goal is to distinguish whether an image of a random input or a random element in the range is given. The verification procedure takes $r = (b, x, y)$ and $\mathsf{ans} = b'$, it outputs 0 if and only if $b = b'$.

Definition 3. *We say a game G has $\delta(S, T) := \delta$ maximum winning probability (or has security δ, for cryptographic games) against all (S, T) non-uniform quantum adversaries with classical or quantum advice if*

$$\max_{\mathcal{A}} \Pr_{H} \left[G_{\mathcal{A}}^{H} = 1 \right] \leq \delta,$$

where max *is taken over all (S, T) non-uniform quantum adversaries $\mathcal{A}$ with classical or quantum advice, respectively.*

3.1 Quantum Bit-Fixing Model

Here we recall a different model called the quantum bit-fixing model. In the following sections, we will relate winning probability of a game G against (S, T) non-uniform quantum algorithms with that in the quantum bit-fixing model (BF-QROM). Since the previous quantum non-uniform bounds require analyzing the quantum bit-fixing model, winning probabilities in the bit-fixing model are already known for many games, and our improved bounds only need a new reduction. The following definitions are adapted from [GLLZ21].

Definition 4 (Games in the P-BF-QROM). *It is similar to games in the standard QROM, except now H has a different distribution.*

- *Before a game starts, a quantum algorithm f (having no input) with at most P queries to an oracle is picked and fixed by an adversary.*
- **Rejection Sampling Stage:** *A random oracle H is picked uniformly at random, then conditioned on f^H outputs 0. In other words, the distribution of H is defined by a rejection sampling:*
  1. *$H \leftarrow \{f : [N] \to [M]\}$.*
  2. *Run f^H and obtain a binary outcome b together with a quantum state τ*[2]*.*
  3. *Restart from step 1 if $b \neq 0$.*
- **Online Stage:** *The game is then executed with oracle access to H, and an algorithm $\mathcal{B}$ gets τ.*

A (P, T) algorithm in the P-BF-QROM consists of f for sampling the distribution and $\mathcal{B}$ for playing the game, with f making at most P queries and $\mathcal{B}$ making at most T queries. We also call $\mathcal{B}$ an **online** algorithm/adversary.

We will also consider the following classical analog P-BF-ROM only when showing a separation between classical and quantum advice in Section 7.

[2] In [GLLZ21], they do not need quantum or classical memory τ shared between f and $\mathcal{A}$. However, this is essential in our proof. Nonetheless, all security proofs in the P-BR-QROM work in the stronger setting (with τ shared between stages).

Definition 5 (Games in the P-BF-ROM). *It is similar to the above Definition 4, except both f and $\mathcal{B}$ can only make classical queries.*

Definition 6. *We say a game G has $\nu(P,T) := \nu$ maximum winning probability (or is ν-secure, for cryptographic games) in the P-BF-QROM if*

$$\max_{f,\mathcal{B}} \Pr_{H}\left[f^H = 0 \wedge G^H_{\mathcal{B}} = 1\right] \leq \nu,$$

where max *is taken over all (P,T) quantum adversaries $(f,\mathcal{B})$ with f making at most P queries and $\mathcal{B}$ making at most T queries.*

We know the following two lemmas from [CGLQ20, GLLZ21].

Lemma 3 (Function Inversion in the P-BF-QROM). *The OWF game has $\nu(P,T) = (P+T^2)/\min\{N,M\}$ in the P-BF-QROM.*

See the proof for Lemma 5.2 in [CGLQ20] and Lemma 10 in [GLLZ21].

Lemma 4 (PRGs in the P-BF-QROM). *The game PRG has $\nu(P,T) = 1/2 + \sqrt{(P+T^2)/N}$ in the P-BF-QROM.*

See the proof for Lemma 5.13 in [CGLQ20].

4 Games, POVMs and Decomposition of Advice

In this section, we will formalize an quantum algorithm's winning probability against a game in terms of POVMs and its corresponding eigenvectors.

For any game G and algorithm $\mathcal{A}$, let V_r^H be a projection that operates on the register of $\mathcal{A}$. V_r^H project a quantum state into a subspace spanned by basis states $|\mathsf{ans}\rangle\,|z\rangle$ where $\mathsf{Verify}^H(r,\mathsf{ans}) = 1$ and z be any aux input (depending on the size of $\mathcal{A}$'s working register). As an example, for function inversion problem and $r = x$, V_r^H is defined as $\sum_{x':H(x')=H(x),z} |x',z\rangle\langle x',z|$.

Then for any non-uniform quantum algorithm $\mathcal{A} = (\{|\sigma_H\rangle\}_H, \{U_{\mathsf{inp}}\}_{\mathsf{inp}})$, by definition, its probability $\epsilon_{\mathcal{A}}$ for winning the game G with oracle access to H can be then written as:

$$\epsilon_{\mathcal{A},H} = \frac{1}{|\mathcal{R}|}\sum_{r\in\mathcal{R}} \left\| V_r^H U^H_{\mathsf{Samp}^H(r)} |\sigma_H\rangle\,|0^L\rangle \right\|^2.$$

We define the following projections $P_r^H := \left(U^H_{\mathsf{Samp}^H(r)}\right)^\dagger V_r^H U^H_{\mathsf{Samp}^H(r)}$. Let P_H be a POVM: $P_H := \frac{1}{|\mathcal{R}|}\sum_{r\in\mathcal{R}} P_r^H$. We can equivalently write $\epsilon_{\mathcal{A},H}$ in terms of this POVM: $\epsilon_{\mathcal{A},H} = \langle \sigma_H, 0^L | P^H | \sigma_H, 0^L\rangle$. This is due to:

$$\begin{aligned}
\epsilon_{\mathcal{A},H} =& \frac{1}{|\mathcal{R}|}\sum_{r\in\mathcal{R}} \left\| V_r^H U^H_{\mathsf{Samp}^H(r)} |\sigma_H\rangle\,|0^L\rangle \right\|^2 \\
=& \frac{1}{|\mathcal{R}|}\sum_{r\in\mathcal{R}} \langle\sigma_H|\,\langle 0^L|\, P_r^H\, |\sigma_H\rangle\,|0^L\rangle \\
=& \langle\sigma_H, 0^L|P^H|\sigma_H, 0^L\rangle.
\end{aligned}$$

Since P_H is a Hermitian matrix and $0 \preceq P_H \preceq \mathbf{I}$, let $\{|\phi_{H,j}\rangle\}_j$ be the set of eigenbasis for P_H with eigenvalues $\{p_{H,j}\}_j$ between 0 and 1. We can decompose $|\sigma_H\rangle |0^L\rangle$ under the eigenbasis:

$$|\sigma_H\rangle |0^L\rangle = \sum_i \alpha_{H,i} |\phi_{H,i}\rangle .$$

Therefore, $\epsilon_{\mathcal{A},H}$ can be written in terms of $\alpha_{H,i}$ and $p_{H,i}$: $\epsilon_{\mathcal{A},H} = \sum_i |\alpha_{H,i}|^2 \cdot p_{H,i}$. This is because:

$$\epsilon_{\mathcal{A},H} = \langle \sigma_H, 0^L | P^H | \sigma_H, 0^L \rangle = \sum_i |\alpha_{H,i}|^2 \cdot p_{H,i}.$$

With all the above discussions, we conclude our lemma below.

Lemma 5. *Let G be a game and $\mathcal{A} = (\{|\sigma_H\rangle\}_H, \{U_{\mathsf{inp}}\}_{\mathsf{inp}})$ be any non-uniform quantum algorithm. Let P_H be the corresponding POVMs for function H. Let $\{|\phi_{H,j}\rangle\}_j$ be the set of eigenbasis for P_H with eigenvalues $\{p_{H,j}\}_j$.*

For each H, write $|\sigma_H\rangle |0^L\rangle$ as $\sum_i \alpha_{H,i} |\phi_{H,i}\rangle$. Let $\epsilon_{\mathcal{A}}$ be the winning probability of $\mathcal{A}$, when H is drawn uniformly at random. Then

$$\epsilon_{\mathcal{A}} = \mathbb{E}_H \left[\sum_i |\alpha_{H,i}|^2 \cdot p_{H,i} \right] = \frac{1}{N^M} \sum_H \sum_i |\alpha_{H,i}|^2 \cdot p_{H,i}.$$

5 Non-Uniform Lower Bounds via Alternating Measurements

In this section, we prove the following theorem:

Theorem 5. *Let G be any game with $T_{\mathsf{Samp}}, T_{\mathsf{Verify}}$ being the number of queries made by* Samp *and* Verify. *For any S, T, let $P = S(T + T_{\mathsf{Verify}} + T_{\mathsf{Samp}})$.*

If G has security $\nu(P,T)$ in the P-BF-QROM, then it has security (maximum winning probability) $\delta(S,T) \leq 2 \cdot \nu(P,T)$ against (S,T) non-uniform quantum algorithms with quantum advice.

It also has security

$$\delta(S,T) \leq \min_{\gamma > 0} \{\nu(P/\gamma, T) + \gamma\}$$

against (S,T) non-uniform quantum algorithms with quantum advice.

As a special case of the second result, when G is a decision game and is $\nu(P,T) = \frac{1}{2} + \nu'(P,T)$ secure in the P-BF-QROM, then it has security

$$1/2 + \min_{\gamma > 0} \{\nu'(P/\gamma, T) + \gamma\}$$

against (S,T) non-uniform quantum algorithms with quantum advice.

The section is organized as follows: in the first subsection, we introduce a new multi-instance game, via the so-called alternating measurement games, the idea of alternating measurement was used in witness preserving amplification of QMA ([MW05]); in the next subsection, we elaborate on behaviors of any non-uniform quantum algorithm in the alternating measurement game; then we show that upper bounds (of success probabilities) in the bit-fixing model give rise to the probability of **uniform** quantum algorithms in the alternating measurement game; finally in the last subsection, we give the proof for our main theorem.

5.1 Multi-Instance via Alternating Measurements

For a game G and a quantum non-uniform algorithm $\mathcal{A} = (\{|\sigma_H\rangle\}_H, \{U_{\mathsf{inp}}\}_{\mathsf{inp}})$, we start by recalling the following notations as in Section 4: $P_r^H, P_H, \{|\phi_{H,j}\rangle\}_j$ and $\{p_{H,i}\}_j$. Let $\mathbf{A}$ be the register that $\mathcal{A}$ operates on. The following controlled projection (as defined in [Zha20]) will be used heavily in this section.

Definition 7 (Controlled Projection). *The controlled projection for a game G and a quantum algorithm $\mathcal{A}$ is the following: for every H, the controlled projection is the measurement $\mathsf{CP}^H = (\mathsf{CP}_0^H, \mathsf{CP}_1^H)$:*

$$\mathsf{CP}_0^H = \sum_{r \in \mathcal{R}} |r\rangle\langle r|_{\mathbf{R}} \otimes P_r^H \quad \textit{and} \quad \mathsf{CP}_1^H = \sum_{r \in \mathcal{R}} |r\rangle \langle r|_{\mathbf{R}} \otimes (\mathbf{I_A} - P_r^H).$$

Here CP^H operates on registers $\mathcal{RA}$ where $\mathcal{R}$ are registers storing random coins and $\mathcal{A}$ are $\mathcal{A}$'s working registers.

Similarly, we define the following projection $\mathsf{IsUniform} = (|\mathbb{1}_\mathcal{R}\rangle \langle \mathbb{1}_\mathcal{R}| \otimes \mathbf{I_A}, (\mathbf{I_R} - |\mathbb{1}_\mathcal{R}\rangle \langle \mathbb{1}_\mathcal{R}|) \otimes \mathbf{I_A})$ over the same register as CP^H where $|\mathbb{1}_\mathcal{R}\rangle$ is a uniform superposition over $\mathcal{R}$: i.e., $|\mathbb{1}_\mathcal{R}\rangle = \frac{1}{|\mathcal{R}|}\sum_r |r\rangle$. We denote $|\mathbb{1}_\mathcal{R}\rangle \langle \mathbb{1}_\mathcal{R}| \otimes \mathbf{I_A}$ by $\mathsf{IsUniform}^0$ and $(\mathbf{I} - |\mathbb{1}_\mathcal{R}\rangle \langle \mathbb{1}_\mathcal{R}| \otimes \mathbf{I_A})$ by $\mathsf{IsUniform}^1$.

Now, We are ready to describe the new game via alternating measurements:

Definition 8 (Multi-Instances via Alternating Measurments). *Fix a game G and an integer $k \geq 1$. A uniformly random H is sampled at the beginning. For a (potentially non-uniform) quantum algorithm $\mathcal{A}$, the multi-instance game $G^{\otimes k}$ is defined and executed as follows:*

- *A challenger $\mathcal{C}$ initializes a new register $|\mathbb{1}_\mathcal{R}\rangle_\mathbf{R}$ and controls $\mathcal{A}$'s register $\mathbf{A}$.*
- *It repeats the following procedures k times, for $i = 1, \cdots, k$:*
  - *If the current stage i is odd, $\mathcal{C}$ applies CP^H on $\mathbf{RA}$ and obtains a measurement outcome b_i.*
  - *If the current stage i is even, $\mathcal{C}$ applies $\mathsf{IsUniform}$ on $\mathbf{RA}$ and obtains a measurement outcome b_i.*
- *The game is won if and only if $b_1 = b_2 = \cdots = b_k = 0$.*

With this alternating measurement game, we describe the following theorem that relates the winning probability of a (non-uniform) $\mathcal{A}$ in the game G and that of $\mathcal{A}$ in the corresponding alternating measurement game $G^{\otimes k}$.

Theorem 6. *Let G be a game and $\mathcal{A} = (\{|\sigma_H\rangle\}_H, \{U_{\mathsf{inp}}\}_{\mathsf{inp}})$ be any non-uniform quantum algorithm for G. Let P_H be the corresponding POVMs for function H. Let $\{|\phi_{H,j}\rangle\}_j$ be the set of eigenbasis for P_H with eigenvalues $\{p_{H,j}\}_j$.*

For each H, write $|\sigma_H\rangle |0^L\rangle$ as $\sum_i \alpha_{H,i} |\phi_{H,i}\rangle$. Let $\epsilon_{\mathcal{A}}^{\otimes k}$ be the winning probability of $\mathcal{A}$ in the alternating measurement game $G^{\otimes k}$, when H is drawn uniformly at random. Then

$$\epsilon_{\mathcal{A}}^{\otimes k} = \frac{1}{N^M} \sum_H \sum_i |\alpha_{H,i}|^2 \cdot p_{H,i}^k.$$

We leave the explanation of the theorem to the appendix (the proof of Lemma 11) since it is similar to the analysis of QMA amplification [MW05] and quantum traitor tracing [Zha20]. We do not considered the proof as our main contribution. Nonetheless, we believe that the proof inspires our analysis for $\epsilon_{\mathcal{A}}^{\otimes k}$, which together with the new multi-instance reduction is considered the main contribution of this work.

By Lemma 2, we can easily conclude that any upper bound on $\mathcal{A}$'s success probability in $G^{\otimes k}$ yields an upper bound on its winning probability in G. The proof of the following lemma easily follows from Lemma 2.

Lemma 6. *Fix a game G and an integer $k \geq 1$. Let $\epsilon_{\mathcal{A}}$ be the success probability of (uniform or non-uniform) $\mathcal{A}$ in G and $\epsilon_{\mathcal{A}}^{\otimes k}$ be that of $\mathcal{A}$ in the alternating measurement game $G^{\otimes k}$. Then $\epsilon_{\mathcal{A}} \leq \left(\epsilon_{\mathcal{A}}^{\otimes k}\right)^{1/k}$.*

Thereby, to bound $\epsilon_{\mathcal{A}}$, it is enough to bound $\epsilon_{\mathcal{A}}^{\otimes k}$ for some appropriate positive integer k.

5.2 Advantages of Uniform Algorithms in Alternating Measurement Games

In this section, we relate success probabilities of **uniform** quantum algorithms in alternating measurements with probabilities in the corresponding bit-fixing model. We will show the following theorem:

Theorem 7. *Let G be a game in the QROM and $\mathcal{A}$ be any* **uniform** *quantum algorithm for G making T oracle queries. Let $\nu(P, T)$ be the security of G in the P-BF-QROM. For every $k > 0$, every $P \geq k\,(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$,*

$$\epsilon_{\mathcal{A}}^{\otimes k} \leq \nu(P, T)^k.$$

Recall that $T_{\mathsf{Samp}}, T_{\mathsf{Verify}}$ are the numbers of queries made by Samp *and* Verify*, respectively.*

To bound $\epsilon_{\mathcal{A}}^{\otimes k}$ for any uniform quantum algorithm, it is sufficient to bound the following conditional probability: $\epsilon_{\mathcal{A}}^{(t)}$ for $t = 1, \cdots, k$.

Definition 9 (Conditional Probability for the t-th Outcome). *$\epsilon_{\mathcal{A}}^{(t)}$ is the conditional probability $\Pr[b_t = 0 \,|\, \mathbf{b}_{<t} = \mathbf{0}]$, where $\mathbf{b}_{<t}$ and b_t are the first t outcomes produced by the game $G^{\otimes k}$ with $\mathcal{A}$, when H is picked uniformly at random.*

Next, we characterize the conditional probability in terms of eigenvalues $\{p_{H,j}\}_j$ and amplitudes under the corresponding eigenbasis $\{|\phi_{H,j}\rangle\}_j$.

Lemma 7. *Let G be a game and $\mathcal{A} = (\{U_{\mathsf{inp}}\}_{\mathsf{inp}})$ be any* **uniform** *quantum algorithm for G. Let P_H be the corresponding POVMs for function H. Let $\{|\phi_{H,j}\rangle\}_j$ be the set of eigenbasis for P_H with eigenvalues $\{p_{H,j}\}_j$.*

For each H, write the starting state $|0^S\rangle\,|0^L\rangle$ as $\sum_i \alpha_{H,i}\,|\phi_{H,i}\rangle$. Let $\epsilon_{\mathcal{A}}^{(t)}$ for $1 \leq t \leq k$ be the conditional probability defined in Definition 9. Then

$$\epsilon_{\mathcal{A}}^{(t)} = \frac{\sum_{H,i} |\alpha_{H,i}|^2 \cdot p_{H,i}^t}{\sum_{H,i} |\alpha_{H,i}|^2 \cdot p_{H,i}^{t-1}}.$$

Proof. By definition, $\epsilon_{\mathcal{A}}^{(t)} = \Pr[b_t = 0 \,|\, \mathbf{b}_{<t} = \mathbf{0}] = \Pr[\mathbf{b}_t = \mathbf{0}] / \Pr[\mathbf{b}_{t-1} = \mathbf{0}]$. Since $\Pr[\mathbf{b}_k = \mathbf{0}] = \sum_{H,i} |\alpha_{H,i}|^2 \cdot p_{H,i}^k$, we conclude the lemma. □

In order to bound $\epsilon_{\mathcal{A}}^{\otimes k}$, it is enough to bound $\epsilon_{\mathcal{A}}^{(t)}$ for every $1 \leq t \leq k$ and $\epsilon_{\mathcal{A}}^{\otimes k} = \prod_{1 \leq t \leq k} \epsilon_{\mathcal{A}}^{(t)}$. Indeed, with Lemma 1, we have the following straightforward corollary.

Corollary 1. *For every game G and* **uniform** *quantum algorithm $\mathcal{A}$, $\{\epsilon^{(t)}\}_{t \geq 1}$ is monotonically non-decreasing. Therefore, $\epsilon_{\mathcal{A}}^{\otimes k} \leq \left(\epsilon_{\mathcal{A}}^{(k^*)}\right)^k$ for any $k^* \geq k$. In particular, $\epsilon_{\mathcal{A}}^{\otimes k} \leq \left(\epsilon_{\mathcal{A}}^k\right)^k$.*

Proof. The proof is direct by setting $\{c_i\}$, $\{p_i\}$ in the statement of Lemma 1 as $\left\{|\alpha_{H,i}|^2 \cdot p_{H,i}^t / N^M\right\}$ and $\{p_{H,i}\}$. □

Finally, we show a connection between $\epsilon_{\mathcal{A}}^{(k)}$ and $\nu(P,T)$ of the game G in the P-BF-QROM for $P \geq k\,(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$.

Lemma 8. *For every game G and* **uniform** *quantum T-query algorithm $\mathcal{A}$, every* **odd** *$k > 0$, every $P \geq (k-1)\,(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$,*

$$\epsilon_{\mathcal{A}}^k \leq \nu(P,T).$$

As a direct corollary by the monotonicity of $\epsilon_{\mathcal{A}}^{(t)}$, for **even** *$k > 0$, every $P \geq k(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$,*

$$\epsilon_{\mathcal{A}}^k \leq \epsilon_{\mathcal{A}}^{(k+1)} \leq \nu(P,T).$$

Together with Corollary 1, we conclude the main theorem (Theorem 7) in this subsection.

Proof for Lemma 8. We only need to prove the lemma for odd k (or even $(k-1)$).

Recall in Definition 4, we need to specify a P-query quantum algorithm f and a T-query algorithm $\mathcal{B}$ to describe an algorithm in the P-BF-QROM. The game is executed if and only if f^H outputs 0. We define $f, \mathcal{B}$ as follows (Figure 1).

P-query quantum algorithm f:
- Initialize $|\mathbb{1}_{\mathcal{R}}\rangle_{\mathbf{R}} |0^S, 0^L\rangle_{\mathbf{A}}$.
- Run the alternating measurement game for $(k-1)$-rounds (Definition 8). Let τ be the leftover state.
- Let a boolean variable $b = 0$ if and only if all outcomes in $(k-1)$-rounds are 0s.
- Output b and $\tau_{\mathbf{RA}}$.

T-query online algorithm $\mathcal{B}$:
- Take $\tau_{\mathbf{RA}}$ as input.
- On an online challenge $\mathsf{ch} \leftarrow \mathsf{Samp}^H(r)$, it runs $\mathcal{A}$ on internal state $\tau[\mathbf{A}]$ and outputs the answer produced by $\mathcal{A}$.

Fig. 1: Turn $\mathcal{A}$ into an algorithm in the P-BF-QROM.

First, we show that $(f, \mathcal{B})$ is a (P, T) algorithm in the P-BR-QROM. It is easy to see that $\mathcal{B}$ makes at most T queries as $\mathcal{A}$ makes at most that many queries. The number of queries made by f is equal to that made in the alternating measurement game:

- In odd rounds, one needs to apply CP^H, which takes $2(T + T_{\mathsf{Samp}}) + T_{\mathsf{Verify}}$ queries; here $2(T + T_{\mathsf{Samp}})$ is for both $U^H_{\mathsf{Samp}^H(r)}$ and its inverse $\left(U^H_{\mathsf{Samp}^H(r)}\right)^\dagger$ and T_{Verify} is for applying the projection V_r^H (recall the definitions in Section 4).
- In even rounds, no queries are needed.

Thus, when $(k-1)$ is even, the total number of queries is at most $(k-1)(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$.

Next we prove that $(f, \mathcal{B})$ succeeds with probability $\epsilon_{\mathcal{A}}^{(k)}$. Thus by the definition of $\nu(P, T)$, $\epsilon_{\mathcal{A}}^{(k)}$ is at most $\nu(P, T)$, concluding the lemma.

For a fixed hash function H and even $(k-1)$ (or equivalently, odd k), conditioned on f^H outputting 0, the leftover state $\tau_{\mathbf{RA}}$ is (by Lemma 11):

$$\tau_{\mathbf{RA}} \propto \sum_i \alpha_i p_i^{(k-1)/2} |v_i^0\rangle_{\mathbf{RA}} = |\mathbb{1}_{\mathcal{R}}\rangle_{\mathbf{R}} \otimes \sum_i \alpha_i p_i^{(k-1)/2} |\phi_i\rangle_{\mathbf{A}} .$$

Here we ignore H for subscripts or superscripts.

Therefore, $\tau[\mathbf{A}] = c \sum_i \alpha_i p_i^{(k-1)/2} |\phi_i\rangle_{\mathbf{A}}$ where c is a normalization factor such that $1/c^2 = \sum_i |\alpha_i|^2 p_i^{k-1}$. The winning probability of $\mathcal{B}$ for this fixed H is

$$\begin{aligned} \mathbb{E}_r \left[\left| V_r^H U^H_{\mathsf{Samp}^H(r)} \tau[\mathbf{A}] \right|^2 \right] &= c^2 \sum_i |\alpha_i|^2 p_i^{(k-1)} \langle \phi_i | P_H | \phi_i \rangle \\ &= c^2 \sum_i |\alpha_i|^2 p_i^k, \end{aligned}$$

By taking the weighted sum of the winning probability for each H, the winning probability of $\mathcal{B}$ is

$$\frac{\sum_{H,i} |\alpha_{H,i}|^2 p_{H,i}^k}{\sum_{H,i} |\alpha_{H,i}|^2 p_{H,i}^{k-1}} = \epsilon_{\mathcal{A}}^{(k)}.$$

Finally, since G is $\nu(P,T)$ secure in the P-BF-QROM, $\epsilon_{\mathcal{A}}^{(k)} \leq \nu(P,T)$ for every T query quantum algorithm $\mathcal{A}$ and $P \geq (k-1)(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$. □

Lastly, we prove Theorem 7.

Proof for Theorem 7. It follows easily by combining Corollary 1 and Lemma 8. □

5.3 Proof of Main Theorem

In this section, we prove our main theorem, Theorem 5.

We start by proving the first part of the theorem.

Proof for the first part. Let G be any game. For any S, T, let $k = S$ and $P = k(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}}) = S(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$. G is $\nu(P,T)$ secure in the P-BF-QROM.

By Theorem 7, for any uniform T-query quantum algorithm and $k = S$, its winning probability in the alternating measurement game $G^{\otimes k}$ is at most $\nu(P,T)^k$.

Therefore, for any (S,T) non-uniform quantum algorithm $\mathcal{A}$, its success probability $\epsilon_{\mathcal{A}}^{\otimes k}$ is at most $2^S \nu(P,T)^k = (2\nu(P,T))^S$. This is because for any non-uniform algorithm of winning probability p with advice being an S-bit advice $|\sigma_H\rangle$, we can turn it into a uniform quantum algorithm with winning probability at least $2^{-S}p$ as follows ([Aar05]):

> As the uniform algorithm does not know $|\sigma_H\rangle$, it samples an S-qubit maximally mixed state and runs the non-uniform algorithm on the maximally mixed state.

Since an S-qubit maximally mixed state can be written as $1/2^S |\sigma_H\rangle\langle\sigma_H| + (1 - 1/2^S)\sigma'$, the uniform algorithm has success probability at least $p/2^S$.

Finally, due to Lemma 6, any non-uniform algorithm $\mathcal{A}$ is at most $2\nu(P,T)$ secure in G for $P = S(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$. □

The proof for the second part is similar but more laborious. Since we are dealing with decision games, we need to carefully deal with the factor 2^{-S} in the previous proof.

Proof for the second part. The theorem trivially holds when $\gamma \geq 1$. We prove it for $\gamma \in (0,1]$.

Let G be a decision game. For any P, T, G is $\nu(P,T)$ secure in the P-BF-QROM.

Similarly by Theorem 7, for any uniform T-query quantum algorithm and k, its security in the alternating measurement game $G^{\otimes k}$ is at most $\nu(P,T)^k$ where $P = k(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})$. Thus, for any (S,T) non-uniform quantum algorithm $\mathcal{A}$, $\epsilon_{\mathcal{A}}^{\otimes k}$ is at most $2^S \nu(P,T)^k$.

Since for any $\gamma \in (0,1]$, $2 \leq (1+\gamma)^{1/\gamma}$. By setting $k = S/\gamma$, we have:

$$\epsilon_{\mathcal{A}}^{\otimes k} \leq 2^S \nu(P,T)^k \leq ((1+\gamma)\nu(P,T))^k \leq \left(\frac{1}{2} + \nu'(P,T) + \gamma\right)^k.$$

The last inequality follows the union bound and $\nu(P,T) = 1/2 + \nu'(P,T)$.

Since the above inequality holds for all $\gamma \in (0,1]$, we conclude the second part of our theorem, following Lemma 6.

□

6 Applications

We show several applications of our main theorem (Theorem 5) in this section. We first apply our theorem to OWF and PRG games and achieve improved lower bounds for both games. The former ones are publicly verifiable, and the latter games are decision games and thus not publicly verifiable. The applications for both types of games show our main theorem is general and achieve pretty good bounds for almost all kinds of security games in the QROM against quantum/classical advice, as long as we can analyze their security in the P-BF-QROM.

Finally, we show that "salting defeats preprocessing" in the QROM, which extends the classical theorem by Coretti et al. [CDGS18] and improved the result by Guo et al. [CGLQ20].

OWF. Recall the definition of G_{OWF} in Example 1. It is shown that G_{OWF} has the following security in the in the P-BF-QROM, $\nu(P,T) = O\left((P+T^2)/\min\{N,M\}\right)$, where N and M are the sizes of the domain and range of the random oracle, by Lemma 1.5 in [CGLQ20].

By our main theorem Theorem 5, we have the following theorem.

Theorem 8. *G_{OWF} has security $\delta(S,T) = O\left(\frac{ST+T^2}{\min\{N,M\}}\right)$ against (S,T) non-uniform quantum adversaries, even with quantum advice.*

The above theorem improves the bound for quantum advice, which was shown to be $\tilde{O}\left(\frac{ST+T^2}{\min\{N,M\}}\right)^{1/3}$ in [CGLQ20].

PRG. Recall G_{PRG} is defined in Example 1. G_{PRG} has security $\nu(P,T) = 1/2 + O\left(\frac{P+T^2}{N}\right)^{1/2}$ where N is the size of the domain, by Lemma 1.6 in [CGLQ20]. Again by our main theorem Theorem 5, we have the following theorem.

Theorem 9. *G_{PRG} has security $\delta(S,T) = 1/2 + O\left(\frac{T^2}{N}\right)^{1/2} + O\left(\frac{ST}{N}\right)^{1/3}$ against (S,T) non-uniform quantum adversaries, even with quantum advice.*

This improves the previous result on G_{PRG} with quantum advice [CGLQ20], which was $1/2 + \tilde{O}\left(\frac{S^5T+S^4T^2}{N}\right)^{1/19}$.

6.1 Salting Defeats Quantum Advice

We start by defining the cryptographic mechanism called "salting".

Definition 10 (Salted Games in the QROM). *Let G be a game in the QROM as defined in Definition 2, with respect to a random oracle $H : [N] \to [M]$. It consists of two deterministic algorithms Samp^H and Verify^H and both algorithms make T_{Samp} (or T_{Verify}) queries, respectively.*

A salted game G_S with salt space $[K]$ is defined as the following: G_S consists of two deterministic algorithms Samp_S and Verify_S:

- *Samp_S^H: on input s, r, it returns $(s, \mathsf{Samp}^{H_s}(r))$. Here H_s denotes oracle access to the oracle $H(s,\cdot)$.*
- *Verify_S^H: on input s, r, ans, it returns $\mathsf{Verify}^{H_s}(r, \mathsf{ans})$.*

In other words, for a fixed $H : [K] \times [N] \to [M]$ and a quantum algorithm $\mathcal{A}$, the game $G_{S,\mathcal{A}}^H$ is executed as follows:

- *A challenger $\mathcal{C}$ samples a uniformly random salt $s \leftarrow [K]$ and $\mathsf{ch} \leftarrow \mathsf{Samp}^{H_s}(r)$ using uniformly random coins r.*
- *A (uniform or non-uniform) quantum algorithm $\mathcal{A}$ has oracle access to H, takes (s, ch) as input and outputs ans.*
- *$b \leftarrow \mathsf{Verify}^{H_s}(r, \mathsf{ans})$ is the outcome of the game.*

Lemma 9 (Salted Games in the P-BF-QROM, Lemma 7.2 in [CGLQ20]).

Let G be a game in the QROM, with security $\nu(T)$ against T-query quantum adversaries. Then for any P,

- *G has security $\nu(P,T) \leq 2\nu(T) + O(P/K)$ in the P-BF-QROM;*
- *G has security $\nu(P,T) \leq \nu(T) + O(\sqrt{P/K})$ in the P-BF-QROM.*

The second bullet point is better than the first one, when G is a decision game.

Proof. The proof is subsumed by the proof for Lemma 7.2 [CGLQ20]. Although Lemma 7.2 shows the multi-instance security of G_S, its P-BF-QROM security is an intermediate step. □

Combining with Theorem 5, we have the following results about salting in the QROM.

Theorem 10. *For any game G (as defined in Definition 2) in the QROM, let $\nu(T)$ be its security in the QROM. Let G_S be the salted game with salt space $[K]$. Then G_S has security $\delta(S,T)$ against (S,T) non-uniform quantum adversaries with quantum advice,*

- $\delta(S,T) \leq 4\nu(T) + O(S(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})/K)$;
- *If G_S is a decision game, then* $\delta(S,T) \leq \nu(T) + O(S(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}})/K)^{1/3}$.

Proof. We only show the second bullet point. The first one is similar and more straightforward.

By Theorem 5, $\delta(S,T) \leq \min_{\gamma>0} \{\gamma + \nu(P/\gamma, T)\}$ where $P = S(T + T_{\mathsf{Verify}} + T_{\mathsf{Samp}})$. Since $\nu(P/\gamma, T) \leq \nu(T) + O(\sqrt{P/(K\gamma)})$ by Lemma 9, $\delta(S,T)$ takes its minimum when $\gamma = O(P/K)^{1/3}$. Our second result follows. □

7 Advantages of Quantum Advice in the QROM

This section demonstrates a game in which non-uniform quantum algorithms with quantum advice have an exponential advantage over those with classical advice for some parameter regime S,T. Although the advantage only applies to some S,T ranges [3], we believe it is the first step toward understanding a game in which quantum advice has an exponential advantage over classical advice for a wider range of S,T.

The game is based on the recent work by Yamakawa and Zhandry [YZ22]. We start by explaining and recalling the basic ideas in their work.

Definition 11 ([YZ22], YZ Functions). *Let n be a positive integer, Σ be an exponentially (in n) sized alphabet and $C \subseteq \Sigma^n$ be an error correcting code over Σ. Let $H : [n] \times \Sigma \to \{0,1\}$ be a random oracle. The following function is called a YZ function with respect to C and Σ:*

$$f_C^H : C \to \{0,1\}^n$$
$$f_C^H(c_1, c_2, \cdots, c_n) = H(1, c_1) || H(2, c_2) || \cdots || H(n, c_n)$$

We will consider the following game, which we call G_{YZ}. The game is to invert a uniformly random image with respect to the YZ function. More formally,

Definition 12 (Inverting YZ Functions). *The game G_{YZ} is specified by two classical algorithms:*

- $\mathsf{Samp}^H(r)$: *it samples a uniformly random image $y = r \in \{0,1\}^n$;*
- $\mathsf{Verify}^H(r, \mathsf{ans})$: *it checks whether ans is a code in C and $f_C^H(\mathsf{ans}) = r$.*

The queries made by each algorithm satisfy $T_{\mathsf{Samp}} = 0$ and $T_{\mathsf{Verify}} = n$.

[3] Specifically, we require $T = 0$, i.e., no online query.

Their idea is that, if we want to find a pre-image in Σ^n of any $y \in \{0,1\}^n$, it is easy: simply inverting each $H(i, y_i)$. Nevertheless, to find a pre-image in C, this entry-by-entry brute-force no longer works. In their work, Yamakawa and Zhandry show that for some appropriate C, the above function is classically one-way and quantumly easy to invert.

Theorem 11 (Theorem 6.1, Lemma 6.3 and 6.9 in [YZ22]). *There exists some appropriate C, such that*

- *The game G_{YZ} has security $2^{-\Omega(n)}$ against 2^{n^c}-query classical adversaries for some constant $0 < c < 1$;*
- *There is a $\tilde{O}(n)$-query quantum algorithm that wins the game G_{YZ} with probability $1 - \mathsf{negl}(n)$. Here $\tilde{O}$ hides a polylog factor.*

Moreover, we observe that the quantum algorithm makes non-adaptive queries and the queries are independent of the challenge. Upon a challenge y is received, the quantum algorithm does post-processing on the quantum queries without making further queries [4].

We show our separation result below.

Theorem 12 (Separation of classical and quantum advice in the QROM). *There exists some appropriate C (the same in [YZ22]) such that,*

- *G_{YZ} has security $2^{-\Omega(n)}$ against $(S, T = 0)$ non-uniform adversaries with* **classical** *advice, for $S = 2^{n^c}/n$ and some constant $0 < c < 1$;*
- *There is an $(S, T = 0)$ non-uniform adversary with* **quantum** *advice that achieves success probability $1 - \mathsf{negl}(n)$, for $S = \tilde{O}(n)$.*

We refer readers to a detailed proof in the appendix.

References

Aar05. Scott Aaronson. Limitations of quantum advice and one-way communication. *Theory Comput.*, 1(1):1–28, 2005.

Aar21. Scott Aaronson. Open problems related to quantum query complexity, 2021.

AK07. Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 115–128. IEEE, 2007.

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, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[4] For more details, please refer to Fig 1. in [YZ22]

BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

BYJK04. Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137, 2004.

CDG18. Sandro Coretti, Yevgeniy Dodis, and Siyao Guo. Non-uniform bounds in the random-permutation, ideal-cipher, and generic-group models. In *Annual International Cryptology Conference*, pages 693–721. Springer, 2018.

CDGS18. Sandro Coretti, Yevgeniy Dodis, Siyao Guo, and John Steinberger. Random oracles and non-uniformity. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 227–258. Springer, 2018.

CGK19. Henry Corrigan-Gibbs and Dmitry Kogan. The function-inversion problem: Barriers and opportunities. In *Theory of Cryptography Conference*, pages 393–421. Springer, 2019.

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.

CLMP13. Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, and Rafael Pass. On the power of nonuniformity in proofs of security. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 389–400, 2013.

CLQ19. Kai-Min Chung, Tai-Ning Liao, and Luowen Qian. Lower bounds for function inversion with quantum advice. *arXiv preprint arXiv:1911.09176*, 2019.

DGK17. Yevgeniy Dodis, Siyao Guo, and Jonathan Katz. Fixing cracks in the concrete: Random oracles with auxiliary input, revisited. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 473–495. Springer, 2017.

DTT10. Anindya De, Luca Trevisan, and Madhur Tulsiani. Time space tradeoffs for attacks against one-way functions and prgs. In *Annual Cryptology Conference*, pages 649–665. Springer, 2010.

Gav08. Dmitry Gavinsky. Classical interaction cannot replace a quantum message. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 95–102, 2008.

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 *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2404–2423. SIAM, 2021.

GLLZ21. Siyao Guo, Qian Li, Qipeng Liu, and Jiapeng Zhang. Unifying presampling via concentration bounds. In *Theory of Cryptography Conference*, pages 177–208. Springer, 2021.

Gro96. Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

Hel80. Martin Hellman. A cryptanalytic time-memory trade-off. *IEEE transactions on Information Theory*, 26(4):401–406, 1980.

HXY19. Minki Hhan, Keita Xagawa, and Takashi Yamakawa. Quantum random oracle model with auxiliary input. In *AsiaCrypt*. Springer, 2019.

MW05. Chris Marriott and John Watrous. Quantum arthur–merlin games. *computational complexity*, 14(2):122–152, 2005.

NABT14. Aran Nayebi, Scott Aaronson, Aleksandrs Belovs, and Luca Trevisan. Quantum lower bound for inverting a permutation with advice. *CoRR*, abs/1408.3193, 2014.

NC10. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

Unr07. Dominique Unruh. Random oracles and auxiliary input. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 205–223. Springer, 2007.

Yao90. AC-C Yao. Coherent functions and program checkers. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 84–94, 1990.

YZ22. Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *arXiv preprint arXiv:2204.02063*, 2022.

Zha20. Mark Zhandry. Schrödinger's pirate: How to trace a quantum decoder. In *Theory of Cryptography Conference*, pages 61–91. Springer, 2020.

A Proofs for the Useful Lemmas

Lemma 10. *Let N be a positive integer and $p_1, \cdots, p_N \in \mathbb{R}^{\geq 0}$. Let $\alpha_1, \cdots, \alpha_N$ be a distribution over $[N]$: i.e., $\alpha_i \in [0,1]$ and $\sum_{i\in[N]} \alpha_i = 1$.*

Assume $\mu := \sum_{i\in[N]} \alpha_i p_i > 0$. Let $\beta_1, \cdots, \beta_N$ be another distribution over $[N]$: $\beta_i := \alpha_i p_i/\mu$. The following holds:

$$\sum_{i\in[N]} \beta_i p_i \geq \sum_{i\in[N]} \alpha_i p_i.$$

Proof. Let $\mathbf{X}$ be a random variable that takes value p_i w.p. α_i. It is easy to see that $\mathbb{E}[\mathbf{X}] = \sum_i \alpha_i p_i$ and $\mathbb{E}[\mathbf{X}^2] = \sum_i \alpha_i p_i^2$.

Since we assume $\mu = \mathbb{E}[\mathbf{X}] > 0$, we rewrite the inequality as follows:

$$\sum_i \alpha_i p_i^2 \geq \left(\sum_i \alpha_i p_i\right)^2.$$

The lemma holds by observing that L.H.S. is $\mathbb{E}[\mathbf{X}^2]$, R.H.S. is $\mathbb{E}[\mathbf{X}]^2$ and the fact that $\mathbf{Var}[\mathbf{X}] := \mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2 \geq 0$. □

Proof for Lemma 1. We fix any integer $k \geq 1$. Let $\alpha_i = c_i p_i^{k-1}/(\sum_i c_i p_i^{k-1})$. It it easy to see that $S_k = \sum_i \alpha_i p_i$.

Let $\beta_i = \alpha_i p_i/\mu$ where $\mu = \sum_i \alpha_i p_i$. We have

$$\begin{aligned}\beta_i &= \alpha_i p_i/\mu \\ &= \frac{c_i p_i^k}{\sum_i c_i p_i^{k-1} \cdot \mu} \\ &= \frac{c_i p_i^k}{\sum_i c_i p_i^{k-1} \cdot (\sum_i c_i p_i^k/(\sum_i c_i p_i^{k-1}))} \\ &= \frac{c_i p_i^k}{\sum_i c_i p_i^k}.\end{aligned}$$

Therefore, $S_{k+1} = \sum_i \beta_i p_i$. By Lemma 10, $S_{k+1} = \sum_i \beta_i p_i \geq \sum_i \alpha_i p_i = S_k$. $\square$

B Characterization of Alternating Measurements and Proof of Theorem 6

Fixing a function H, the intial internal register $\mathbf{A}$ of $\mathcal{A}$ is $|\sigma_H\rangle |0^L\rangle = \sum_i \alpha_{H,i} |\phi_{H,i}\rangle$. Let us define the following states $|v^0_{H,i}\rangle, |v^1_{H,i}\rangle, |w^0_{H,i}\rangle, |w^1_{H,i}\rangle$ (for convenience, we ignore H in the subscripts in the analysis below). We will also ignore H for other notations like $P_r^H, |\phi_{H,i}\rangle, p_{H,i}$ as our analysis does not depend on H and the final conclusion follows by taking expectation over uniformly random functions H. Instead, we are using $P_r := P_r^H, |\phi_i\rangle := |\phi_{H,i}\rangle, p_i := p_{H,i}$ in the analysis.

1. $|w_i^0\rangle = \frac{1}{\sqrt{p_i|\mathcal{R}|}} \sum_r |r\rangle P_r |\phi_i\rangle$.
   It is easy to verify that it has norm 1:
   $$\langle w_i^0 | w_i^0\rangle = \frac{1}{p_i|\mathcal{R}|}\sum_r \langle \phi_i|P_r|\phi_i\rangle = \frac{1}{p_i|\mathcal{R}|}\langle\phi_i|(\sum_r P_r)|\phi_i\rangle = \frac{p_i|\mathcal{R}|}{p_i|\mathcal{R}|} = 1.$$
   $\mathsf{CP}_0^H |w_i^0\rangle = |w_i^0\rangle$ and $\mathsf{CP}_1^H |w_i^0\rangle = 0$.
   After seeing the definition of $|v_i^0\rangle$ and $|v_i^1\rangle$ below, we also observe that $|w_i^0\rangle = \sqrt{p_i}\,|v_i^0\rangle + \sqrt{1-p_i}\,|v_i^1\rangle$.
2. $|w_i^1\rangle = \frac{1}{\sqrt{(1-p_i)|\mathcal{R}|}} \sum_r |r\rangle (\mathbf{I}_{\mathbf{A}} - P_r) |\phi_i\rangle$.
   Similarly, it has norm 1, $\mathsf{CP}_1^H |w_i^1\rangle = |w_i^1\rangle$ and $\mathsf{CP}_0^H |w_i^1\rangle = 0$.
3. $|v_i^0\rangle = |\mathbb{1}\rangle_{\mathcal{R}} |\phi_i\rangle = \sqrt{p_i}\,|w_i^0\rangle + \sqrt{1-p_i}\,|w_i^1\rangle$.
   By the description of the game $G^{\otimes k}$ (Definition 8), the overall register $\mathbf{RA}$ at the beginning of the game can be written as $\sum_i \alpha_i |v_i^0\rangle$ (which we will prove below).
   The state has norm 1, $\mathsf{IsUniform}^0 |v_i^0\rangle = |v_i^0\rangle$ and $\mathsf{IsUniform}^1 |v_i^0\rangle = 0$.
4. $|v_i^1\rangle = \sqrt{1-p_i}\,|w_i^0\rangle - \sqrt{p_i}\,|w_i^1\rangle$.
   We will not use the property of $|v_i^1\rangle$ in the proof and we thus omit all the details here.

Lemma 11. *For any fixed H, for any non-negative integer k, the leftover state over* **RA** *conditioned on all outcomes in the first k rounds being 0s is in proportion to:*

$$\sum_i \alpha_i p_i^{k/2} \begin{cases} |v_i^0\rangle & \text{if } k \text{ is even,} \\ |w_i^0\rangle & \text{if } k \text{ is odd.} \end{cases}$$

The probability of all outcomes being 0s is $\sum_i |\alpha_i|^2 p_i^k$.

The proof follows the proof of Claim 6.3 in [Zha20]. We reprove this claim for completeness.

Proof. This lemma holds for $k = 0$, when no measurement is applied. This is the state is

$$\sum_i \alpha_i |v_i^0\rangle = \sum_i \alpha_i |\mathbb{1}_{\mathcal{R}}\rangle_{\mathbf{R}} |\phi_i\rangle_{\mathbf{A}} = |\mathbb{1}_{\mathcal{R}}\rangle_{\mathbf{R}} |\sigma_H, 0^L\rangle_{\mathbf{A}}.$$

We now prove by induction. Assume the lemma holds up to some even k. We prove it holds for odd $k+1$.

The leftover state after the first k rounds is $c \sum_i \alpha_i p_i^{k/2} |v_i^0\rangle$ for some normalization c. Note that $|v_i^0\rangle = \sqrt{p_i} |w_i^0\rangle + \sqrt{1-p_i} |w_i^1\rangle$. The state can be rewritten as

$$c \sum_i \alpha_i p_i^{k/2} \left(\sqrt{p_i} |w_i^0\rangle + \sqrt{1-p_i} |w_i^1\rangle \right).$$

In the $(k+1)$-th round, the challenger measures the state under CP^H. Note that $\mathsf{CP}_0^H |w_i^0\rangle = |w_i^0\rangle$ and $\mathsf{CP}_0^H |w_i^1\rangle = 0$. Thus, conditioned on the $(k+1)$-th outcome being 0, the state is in proportion to $\sum_i \alpha_i p_i^{(k+1)/2} |w_i^0\rangle$. We complete the induction for k being even.

For odd k, the analysis is almost identical, by observing $|w_i^0\rangle = \sqrt{p_i} |v_i^0\rangle + \sqrt{1-p_i} |v_i^1\rangle$ and also following from the fact that $\mathsf{IsUniform}^0 |v_i^0\rangle = |v_i^0\rangle$ and $\mathsf{IsUniform}^1 |v_i^0\rangle = 0$.

Finally, the probability can be bounded by looking at the un-normalized states above. □

Theorem 6 follows from summing over all functions H and Lemma 11.

C Classical Version of Our Main Theorem

The following theorem is a classical version of our main theorem (Theorem 5), improved from Theorem 1 in [GLLZ21].

Theorem 13. *Let G be any game with $T_{\mathsf{Samp}}, T_{\mathsf{Verify}}$ being the number of queries made by Samp and Verify. For any S, T, let $P = S(T + T_{\mathsf{Verify}} + T_{\mathsf{Samp}})$.*

If G has security $\nu(P,T)$ in the P-BF-ROM, then it has security $\delta(S,T) \leq 2 \cdot \nu(P,T)$ against (S,T) non-uniform classical algorithms with classical advice.

In Theorem 1 in [GLLZ21], $P = (S + \log \gamma^{-1})(T + T_{\mathsf{Verify}} + T_{\mathsf{Samp}})$ and there is an extra additive term γ for $\delta(S, T)$.

Theorem 14 (Theorem 1 in [GLLZ21]). *Let G be any game with $T_{\mathsf{Samp}}, T_{\mathsf{Verify}}$ being the number of queries made by* Samp *and* Verify*. For any $S, T, \gamma > 0$, let $P = (S + \log \gamma^{-1})(T + T_{\mathsf{Verify}} + T_{\mathsf{Samp}})$.*

If G has security $\nu(P, T)$ in the P-BF-ROM, then it has security $\delta(S, T) \leq 2 \cdot \nu(P, T) + \gamma$ against (S, T) non-uniform classical algorithms with classical advice.

D Proof for the separation result

Proof. We first show the second bullet point. Let the quantum algorithm in Theorem 11 be $\mathcal{B}$. In the non-uniform quantum adversary, quantum advice is the non-adaptive queries made by $\mathcal{B}$ and the online stage is the post-processing by $\mathcal{B}$. It is straightforward that the non-uniform algorithm achieves the same probability as $\mathcal{B}$, which is $1 - \mathsf{negl}(n)$. Since each query has $O(\log n)$ qubits and $\mathcal{B}$ makes $\tilde{O}(n)$ queries, the total size of the quantum advice is still $\tilde{O}(n)$.

Next, we show the first bullet point. In the first bullet point of this theorem, we do not distinguish between non-uniform quantum adversaries with classical advice and non-uniform classical adversaries. The reason is that the online algorithm does not make any query, i.e., $T = 0$. These two types of algorithms are equivalent when $T = 0$.

Thus, we consider success probabilities of non-uniform classical adversaries. By a classical analog of our main theorem Theorem 5 (Theorem 13), we only need to show its success probability in the P-BF-ROM (Definition 5) where $P = S(T + T_{\mathsf{Samp}} + T_{\mathsf{Verify}}) = ST_{\mathsf{Verify}} = 2^{n^c}$.

Assume a random oracle is lazily sampled. In other words, an outcome of the random oracle on x is sampled only if the outcome is queried by an algorithm; otherwise, the outcome is marked as "not sampled". Conditioned on any P-query f outputs 0, the random oracle is only fixed on P positions and the rest of its outputs are still not sampled. The error correcting code C used in [YZ22] satisfies a property called (ζ, ℓ, L) list recoverability:

- For any subset $S_i \subseteq \Sigma$ such that $|S_i| \leq \ell$ for every $i \in [n]$, we have

  $$|\mathsf{Good}| = |\{(x_1, \cdots, x_n) \in C : |\{i \in [n] : x_i \in S_i\}| \geq (1 - \zeta)n\}| \leq L.$$

  In other words, the total number of codewords in C with hamming distance to $S_1 \times S_2 \times \cdots \times S_n$ smaller than ζn is bounded by L. Here hamming distance to $S_1 \times S_2 \times \cdots \times S_n$ is defined as the number of coordinates i whose x_i is not in the corresponding S_i.
  We call this set of codewords Good.
- $P = 2^{n^c} < \ell, \zeta = \Omega(1)$ and $L = 2^{n^{c'}}$ for some $0 < c' < 1$.

In G_{YZ}, when a challenge y is sampled uniformly at random from $\{0, 1\}^n$, there are two cases:

- **Case 1**: there exists a codeword c in Good, such that $y = f_C^H(c)$. This case happens with probability at most $|\mathsf{Good}|/2^n \leq L/2^n$.
- **Case 2**: complement of Case 1. In this case, an adversary wins only if it outputs a codeword that is not in Good.
  For every codeword $c = (x_1, x_2, \cdots, x_n) \notin \mathsf{Good}$, there are at least ζn coordinates whose random oracle outputs (i.e., $H(i, x_i)$) have not been sampled yet in the lazily sampled random oracle. For any $c \notin \mathsf{Good}$, $\Pr[f_C^H(c) = y] \leq 2^{-\zeta n}$. Therefore, regardless of the algorithm's output, the success probability is at most $2^{-\zeta n}$.

The overall winning probability is bounded by $L/2^n + 2^{-\zeta n} = 2^{-\Omega(n)}$. We conclude the first bullet point of the theorem.

□