


# Nonadaptive One-Way to Hiding Implies Adaptive Quantum Reprogramming

Joseph Jaeger 

School of Cybersecurity and Privacy  
Georgia Institute of Technology  
Atlanta, Georgia, US  
josephjaeger@gatech.edu

**Abstract.** An important proof technique in the random oracle model involves reprogramming it on hard to predict inputs and arguing that an attacker cannot detect that this occurred. In the quantum setting, a particularly challenging version of this considers adaptive reprogramming wherein the points to be reprogrammed (or output values they should be programmed to) are dependent on choices made by the adversary. Frameworks for analyzing adaptive reprogramming were given by, e.g., by Unruh (CRYPTO 2014), Grilo-Hövelmanns-Hülsing-Majenz (ASIACRYPT 2021), and Pan-Zeng (PKC 2024). We show, counterintuitively, that these adaptive results follow directly from the *non-adaptive* one-way to hiding theorem of Ambainis-Hamburg-Unruh (CRYPTO 2019). These implications contradict beliefs (whether stated explicitly or implicitly) that some properties of the adaptive frameworks cannot be provided by the Ambainis-Hamburg-Unruh result.

## 1 Introduction

Hash functions are a pillar of modern practical cryptography. Many of the most efficient algorithms for a given task (public key encryption, digital signatures, authenticated key exchange, ...) crucially rely on hash functions for their security. Often the security cannot be reduced to standard model assumptions about the hash function and is instead justified by modeling it as a random oracle [4]. A variety of methods of expressing random oracle model proofs are known which can make it easy to express analyses based on basic probabilistic analysis [8,5,18,21,22]. An important aspect of this is bounding the probability that an attacker notices if we adaptively modify the behavior of the oracle on inputs which are statistically/computationally hard for the attacker to guess.

As we prepare for a post-quantum future, there is a natural desire to port these benefits over to the quantum random oracle model [7] which captures that an attacker locally computing a hash function may use a quantum computer to do so in superposition. With this change in model, existing classical proofs no longer apply and, more importantly, the standard proof techniques no longer work. Motivated by this challenge, a variety of techniques have been introduced for quantum random oracle model analysis [3,6,11,12,13,15,17,20,24,25,26,30,31,32].

Rather than providing new analysis tools, we provide a new perspective on how to use an existing tool by Ambainis, Hamburg, and Unruh [3] (AHU). This “one-way to hiding” (O2H) theorem (building on earlier versions [11,15,24,25,26]) bounds an attacker’s advantage in distinguishing between randomly chosen functions based on the probability a related algorithm can extract an input on which they differ. The common impression [3,12,20] seems to be that this result is highly non-adaptive because these two functions must be fixed at the beginning of the experiment, and thus it cannot be used for adaptive analysis where the definitions of the functions can update throughout the experiment (except in a few special corner cases where an adaptive problem can cleverly be expressed non-adaptively).

We dispel this notion, showing that through a change of viewpoint we can easily analyze many highly adaptive problems. As concrete applications of this we prove that an “adaptive reprogramming framework” of Pan and Zeng [20], a “tight adaptive reprogramming theorem” of Grilo, Hövelmanns, Hülsing, Majenz [12], and “adaptive O2H” lemmas of Unruh [24,25] are all implied by the AHU O2H result. We use straightforward proofs that rely on almost entirely classical reasoning. The concrete bounds we establish are essentially equivalent to or better than the existing bounds.

The main idea underlying this new viewpoint is to switch away from viewing the O2H functions as strictly applied to the attacker’s input. We instead use a priori fixed permutations that take both the attacker’s input and the current state of the “security game”, using the latter to respond to the former. Updating the state of the game thereby adaptively changes the inputs on which the oracles differ. In essence, we view the O2H distinguisher as internally running both the attacker and the security game, only exporting very specific pieces of the computation (which it could have done itself) to an oracle. We call this new perspective the Fixed Permutation O2H, but emphasize that we are using the AHU result directly. Our approach is inspired by a proof of Jaeger, Song, and Tessaro [14] which used AHU’s O2H with fixed permutations to analyze the quantum security of a key-length extension technique they call FFX.

### 1.1 Technique Overview

Consider a setting where an attacker makes  $q$  queries  $x_1, \dots, x_q$  to random oracle  $H$ . It’s allowed to adaptively select points  $x_i^*$ , asking for  $H(x_i^*)$  to be redefined to some  $y_i^*$  up to  $n$  times. Let  $p_1$  be the probability it outputs 1 at the end of its execution and  $p_0$  be the probability it outputs 1 if instead  $H$  is never redefined. Our goal is to bound  $|p_1 - p_0|$ .

This setting is adaptive in two senses. First, the differences between the oracles in the experiment change over time, rather than being chosen at the beginning of the experiment. Second, the particular ways in which the oracles are changed may depend on earlier queries of the adversary.

**Classical Analysis.** To analyze this classically, we might use a Bellare-Rogaway style “equivalent-until-bad” approach [5] (or analogous approaches by Mau-

$$\begin{array}{ll}
O_b(x_j) & P_b(X, Y : H, X^*, Y^*, I) \\
\text{If } \exists i, x_j = x_i^*: & \text{If } \exists i \leq I, X = X_i^* \text{ // } \mathbf{bad} \\
\quad \mathbf{bad} \leftarrow \mathbf{true} & \quad \text{If } b = 1: Y \leftarrow Y \oplus Y_i^* \\
\quad \text{If } b = 1: \text{Return } y_i^* & \quad \text{If } b = 0: Y \leftarrow Y \oplus H(X_i^*) \\
\text{Return } H(x_j) & \text{Else } Y \leftarrow Y \oplus H(X) \\
& \text{Return } (X, Y : H, X^*, Y^*, I)
\end{array}$$

**Fig. 1. Left:** Expression of oracle as pseudocode for classical equivalent-until-bad analysis. **Right:** Expression of oracle as a classical permutation queried in superposition for quantum Fixed Permutation O2H analysis.

rer [18] or Shoup [22]). Therein we express this setting as a pair of pseudocode games, parameterized by a bit  $b$ , which are syntactically identical except after a flag  $\mathbf{bad}$  is set. This could, for example, be captured by using the pseudocode oracle  $O_b$  on the left of Fig. 1. Now the fundamental lemma of game playing tells us that  $|p_0 - p_1| \leq \Pr[\mathbf{bad}]$ .

At this point, one bounds  $\Pr[\mathbf{bad}]$  based on some assumption about  $\mathcal{A}$  (e.g., that the  $x_i^*$  are statistically or computationally unpredictable). Applying a union bound across all of the queries of  $\mathcal{A}$  gives

$$\Pr[\mathbf{bad}] \leq \sum_j \Pr[x_j \in \{x_i^*\}] = q \mathbb{E}_j[\Pr[x_j \in \{x_i^*\}]].$$

For example, if the  $x_i^*$  are from adaptively chosen distributions that always have min-entropy at least  $\mu$  and the  $x_i^*$  are used nowhere else we get  $|p_0 - p_1| \leq nq2^{-\mu}$ . Notably, (treating the fundamental lemma of game playing as given) the analysis consists entirely of syntactic rewriting of the setting as pseudocode combined with basic probability calculation.

**Non-adaptive O2H.** Now consider a setting where  $x_i^*, y_i^*$  are still chosen classically, but the attacker has quantum access to  $H$ . The standard formalization of this allows computing the classical permutational  $H[\oplus] : (x, y) \mapsto (x, y \oplus x)$  in superposition. We can no longer apply the approach above, as the oracle can be queried in a superposition over all  $x$  at once so the bad event that it was queried on some  $x_i^*$  is not even well defined. One approach to this are “one-way to hiding” (O2H) results [3,11,15,24,25,26] which can be thought of as a quantum analog to equivalent-until-bad analysis. Consider using an O2H lemma of AHU [3], which considers a distribution over functions  $H_0, H_1$  and tells us that

$$|p_{H_0} - p_{H_1}| \leq 2q \sqrt{\mathbb{E}_j[\Pr[\text{Measure}(X_j) \in S]]}.$$

Here  $p_{H_b}$  is the probability an adversary outputs 1 when interacting with  $H_b[\oplus]$  and the last probability considers running the adversary with access to either oracle  $H_b$ , measuring its  $j$ -th query to the oracle, and checking whether the resulting  $x_j$  is in the set  $S = \{x : H_0(x) \neq H_1(x)\}$ .

Unfortunately, this result is non-adaptive. The two functions  $H_0$  and  $H_1$  (and thus the points where they differ) are fixed at the beginning of the game. Consequently, it seems that the result can only be applied in the limited case that all  $x_i^*, y_i^*$  are chosen at the beginning of the game and thus the programming of  $H$  occurs immediately. (For this, consider the distribution that samples the  $x_i^*, y_i^*$ , defines  $H_0$  to be a random oracle, and defines  $H_1$  to be that oracle reprogrammed so  $H_1(x_i^*) = y_i^*$  for all  $i$ .) For example, if the  $x_i^*$  are from distributions that have min-entropy at least  $\mu$  and the  $x_i^*$  are used nowhere else we get  $|p_0 - p_1| \leq \sqrt{nq^2 2^{-\mu}}$ .

**Fixed Permutation O2H.** This impression is incorrect. We can analyze many adaptive reprogramming settings using AHU’s O2H. Start by simplifying it so that rather than considering distributions over permutations of the form  $H_b[\oplus]$  we consider two fixed permutations  $P_0$  and  $P_1$ . It follows from AHU [3] that

$$|p_{P_0} - p_{P_1}| \leq 2q \sqrt{\mathbb{E}_j [\Pr[\text{Measure}(P_0(X_j) \neq P_1(X_j))]]}.$$

We call this special case of AHU’s O2H the Fixed Permutation O2H. To apply this result, we switch our viewpoint. Rather than thinking of  $P_b$  being the functions the attacker might have access to (and so the O2H distinguisher is essentially identical to the attacker) we will think of the distinguisher as jointly running the attacker and the “security game”. Then the permutations  $P_b$  will be permutations that process oracle queries as a function of both the attacker’s state and the game’s.

In our running example, to simulate the game the distinguisher will store the random function in a quantum register  $H$  and the reprogramming points  $x_i^*, y_i^*$  in registers  $X_i^*$  and  $Y_i^*$  (together with a register  $I$  counting how many points have been chosen so far). Then when the original attack wants to query  $H_b[\oplus]$  with registers  $X, Y$  the distinguisher forwards this with the game registers as a query to its own oracle  $P_b$  defined on the right side of Fig. 1. Notationally, we use a colon as syntactic sugar to distinguish the input registers controlled by the attacker or the game.

Note that the distinguisher perfectly simulates the view of the attacker and that the two permutations only differ on inputs for which  $X$  is one of the reprogrammed points. Thus the above bound on  $|p_{P_0} - p_{P_1}|$  gives a meaningful bound on  $|p_0 - p_1|$ . For example, if the  $x_i^*$  are from adaptively chosen distributions that always have min-entropy at least  $\mu$  and the  $x_i^*$  are used nowhere else we get  $|p_0 - p_1| \leq \sqrt{nq^2 2^{-\mu}}$ . Notably, (treating the Fixed Permutation O2H as given) the analysis consisted entirely of syntactic rewriting of the setting as permutations combined with basic probability calculation.

**Backwards Bounds from Sparse Functions.** Thinking classically, if each  $y_i^*$  is uniformly random, then swapping it with  $H(x_i^*)$  will only actually be detectable if the attacker queries its oracle at  $x_i^*$  both before and after the reprogramming. This can be important because in some settings  $x_i^*$  may be hard

$\frac{\text{CRO}(x)}{\text{If } T[x] = \perp:$ $\quad \text{Sample } T[x]$ $\text{Return } T[x]$ $\frac{\text{CREP}_b(x_i^*)}{\text{If } T[x_i^*] \neq \perp:$ $\quad \text{bad} \leftarrow \text{true}$ $\quad \text{If } b = 1: \text{ Sample } T[x]$	$\frac{\text{FRO}(X, Y : H)}{H[X] \leftarrow H[X] \oplus Y}$ $\text{Return } (X, Y : H)$ $\frac{\text{FREP}_b(X^* : H, I, Z)}{\text{If } H[X^*] \neq Z[I]: \text{ // bad}}$ $\quad \text{If } b = 1: \text{ Swap } H[X^*] \text{ and } Z[I]$ $\quad I \leftarrow I + 1 \bmod n$ $\text{Return } (X^* : H, I, Z)$
--	--

**Fig. 2. Left:** Pseudocode for classical proof using lazily sampled random function. **Right:** Permutations for Fixed Permutation O2H proof using sparse representation of random function. Tables  $H$  and  $Z$  are initially all zero.

---

to query to  $H$  before the reprogramming occurred but easy to query afterwards. Our approach so far only considering the probability of  $x_i^*$  being queried after reprogramming and thus could not be applied.

Fortunately, the solution to this in the classical setting can be applied to the Fixed Permutation O2H approach as well. The core idea is to consider the “bad event” as occurring when  $x_i^*$  is chosen. Then we will look backwards in time to see if  $x_i^*$  was previously queried to the random oracle. To do this, we lazily sample the random oracle and then check whether a new  $x_i^*$  matches any of the values currently in the table. This is captured by the pseudocode oracles CRO and CREP $_b$  on the left of Fig. 2. Applying the fundamental lemma of game playing and union bounds gives.

$$|p_0 - p_1| \leq \sum_i \Pr[x_i^* \in T] = n \mathbb{E}[\Pr[x_i^* \in T]].$$

If the  $x_i^*$  are from adaptively chosen distributions that always have min-entropy at least  $\mu$  we get  $|p_0 - p_1| \leq nq2^{-\mu}$ . Notably, (treating the fundamental lemma of game playing as given) the analysis consists entirely of straightforward syntactic rewriting of the setting as pseudocode combined with basic probability calculation.

For porting this idea over to the quantum regime, the important aspect of lazy sampling was that the random oracle was represented by a sparse table (one which had been written to in at most  $q$  locations after  $q$  queries). Zhandry [32] showed that we can similarly represent quantum random oracles with (superpositions over) sparse tables. Thereby, we can move from the traditional quantum random oracle which does  $y \leftarrow y \oplus H(x)$  for an  $H$  initialized at random to the Fourier random oracle which does  $H(x) \leftarrow y \oplus H(x)$  for an  $H$  initialized to be all zero. In this domain, reprogramming  $H(x_i^*)$  to a random output can be performed by swapping its register with a register initialized to be zero. This is captured by the permutations FRO and FREP $_b$  on the right of Fig. 2. Here registers  $H$ ,  $I$ , and  $Z$  are initialized as 0.

We can now apply the Fixed Permutation O2H. The distinguisher runs the attacker, internally simulating FRO for it. Whenever the original attacker wants to reprogram on the value in register  $X$ , the distinguisher adds the game registers and then forwards this as a query to its own oracle  $\text{FREP}_b$ . Note that the  $\text{FREP}_b$  permutations differ only if  $H[X^*]$  and  $Z[I]$  differ (and  $Z[I]$  is necessarily zero), so we get

$$|p_0 - p_1| \leq 2n \sqrt{\mathbb{E}_i[\text{Pr}[\text{Measure}(H[X_i^*] \neq 0)]]}.$$

This result can give better bounds in the natural setting that  $q \gg n$  because it (implicitly) switches a factor of  $q\sqrt{n}$  with  $n\sqrt{q}$ . For example, if the  $x_i^*$  are from adaptively chosen distributions that always have min-entropy at least  $\mu$  we get  $|p_0 - p_1| \leq \sqrt{n^2 q 2^{-\mu}}$ . Notably, (treating the Fixed Permutation O2H as given) the analysis consisted entirely of straightforward syntactic rewriting of the setting as permutations combined with basic probability calculation.<sup>1</sup>

## 1.2 Applications of Our Technique

To show the broad applicability of our new perspective, we use it to imply an “adaptive reprogramming framework” of Pan and Zeng [20], a “tight adaptive reprogramming theorem” of Grilo, Hövelmanns, Hülsing, Majenz [12] (GHHM), and “adaptive O2H” lemmas of Unruh [24,25]. We summarize these below.

For some of these results, the concrete bounds we establish have to be parameterized slightly differently than the original results, but we show that they are essentially equivalent (or better) in actual use. Moreover, AHU’s O2H shows that their upper bound also applies to the difference of square roots  $|\sqrt{p_0} - \sqrt{p_1}|$ . This gives better bounds when used to prove  $p_0$  is small based on a  $p_1$  which is known to be small. We thus get square root versions of all the results we consider for free. These were not previously known.

**Pan-Zeng Adaptive Reprogramming Framework.** Pan and Zeng [20] introduced an adaptive reprogramming framework which they use to analyze the selective-opening security of Fujisaki-Okamoto-style public key encryption algorithms. They express a belief that AHU’s O2H result lacked the properties needed for these proofs, saying that,

Our core technical contribution is a computational adaptive reprogramming framework in the QROM that enables a security reduction to adaptively and simultaneously reprogram polynomially many RO-queries which are computationally hidden from a quantum adversary. This is a property that *cannot be provided* by previous techniques in the QROM, such as ... the semi-classical O2H lemma [3]...<sup>2</sup>

<sup>1</sup> Prior to Zhandry’s work, rewriting quantum random functions sparsely was not known to be straightforward. In light of the work, it is quite simple to do so for our purposes.

<sup>2</sup> This quote is from p.4 (aka p.95) of the proceedings version or p.3 of the current ePrint version. Emphasis ours. We’ve changed the citation to match our numbers.

We prove that their computational adaptive reprogramming result is implied by the Fixed Permutation O2H with a short proof, thereby establishing that the O2H lemma *can* provide this property.<sup>3</sup> Their framework considers arbitrary reprogramming of the oracle and upper bounds distinguishing advantage by the probability that measuring the input of a random query gives a value at which the function differ. In essence, their result follows directly from the first use of Fixed Permutation O2H that we described above.

**GHHM Adaptive Reprogramming Framework.** GHHM [12] gave a tight adaptive reprogramming theorem for information theoretic settings where the reprogrammed points are from adaptively chosen distributions with high min-entropy, but are immediately given to the attacker. Consequently, the distinguishing advantage must be bound by the probability that one of the reprogrammed points is queried before being selected and does not seem to imply or be implied by the Pan-Zeng result. Our proof of GHHM’s theorem follows from our second use of Fixed Permutation O2H by using Zhandry’s technique for sparsely representing functions to provide “backwards bounds”. GHHM used their tool for tighter proofs of hash and sign techniques (e.g., used by XMSS), tighter proofs for Fiat Shamir signatures, and fault resistance for the hedged Fiat-Shamir transform. Their theorem was later used by [1,10,9,16,19,28,29].

**Unruh’s Adaptive O2H.** Unruh [24,25] gave adaptive variants of early O2H results for reprogramming on a single statistically hidden input. These results obtain improved concrete bounds by separately considering the probability that reprogrammed point is queried before or after it is sampled. Consequently, they do not seem to imply or be implied by either the Pan-Zeng or the GHHM result.

Notably, AHU proved a theorem that had previously been shown using the first adaptive O2H result [24]. While doing so, they note that “at least in the proof from [23]” they could replace the adaptive O2H result with their nonadaptive version by programming the random oracle on many points. Our proof of the [24] result applies the Fixed Permutation O2H two times, one of which similarly programs the random oracle on many points. Thereby we show that the approach of AHU actually extends to any application of the adaptive O2H, not just that particular proof.

We reprove the [25] result through two applications of the Fixed Permutation O2H using “backwards bounds”. The setting of this result is more general than in [24], but the concrete bounds based on collision-entropy of the input distribution are incomparable. Our proof gives a bound in terms of min-entropy which implies both the collision-entropy bound [25] and an improved version of the bound in [24] (replacing a  $q_0$  factor with  $\sqrt{q_0}$ ).

---

<sup>3</sup> Technically, the mentioned semi-classical O2H lemma is a different O2H result, but it is known [3] to directly imply the O2H lemma we prove equivalent to the Fixed Permutation O2H in Section 2.

**A Non-Application.** The Fixed Permutation O2H is not a panacea. We conclude the paper by discussing two results that seem out of reach of the Fixed Permutation O2H with current techniques. The first result, by Alagic, Bai, Katz, and Majenz [1], gives a variant of the GHHM result for random permutations reprogrammed on uniformly random points. The result proves an  $O(\sqrt{q/2^n})$  bound while we are only able to prove  $O(\sqrt{q^2/2^n})$ . The second result, by Alagic, Bai, Katz, Majenz, and Struck [2], generalizes the result when a reprogrammed point comes from an adaptively chosen, high entropy distribution. For both, we identify that the gap between our success in proving the GHHM result and inability to prove these results stems from lacking techniques for expressing quantum random permutations sparsely.

### 1.3 Implications of the Results

Formally, the claim that Fixed Permutation O2H implies any of these other theorems is essentially tautological. The results were already unconditionally proven to be true, so it is vacuously the case that any statement implies them. The essence of the result is not that the implications hold, but rather that the proofs thereof are straightforward and require almost exclusively classical reasoning. (The quantum complexity is instead hidden inside of the O2H result we take as assumed.)

There are two ways we imagine this being used in future work. If one likes to have a “toolbox” of adaptive reprogramming results each targeted narrowly at a particular type of problem that they are well suited to expressing, then our results show that the Fixed Permutation O2H is useful to build such tools. Alternatively, because of the simplicity of our proofs, one could choose to jettison the use of individual adaptive reprogramming results and instead use Fixed Permutation O2H directly in security proofs as a single powerful “multi-tool”.<sup>4</sup>

### 1.4 Overview

In Section 2 describe our notation conventions, summarize necessary background on quantum computation, and provides the Fixed Permutation O2H lemma we use throughout the paper. In Section 3 we prove that the lemma implies the adaptive programming result of Pan and Zeng [20]. In Section 4 we prove that the lemma implies the tight adaptive programming result of GHHM [12]. In Section 5 we prove that the lemma implies two adaptive one-way-to-hiding results of Unruh [24,25]. We conclude in Section 6 by discussing the challenges in proving the random permutation resampling results of Alagic, Bai, Katz, and Majenz [1] or Alagic, Bai, Katz, Majenz, and Struck [2]. A change log follows the references.

---

<sup>4</sup> As an example, we note that several works [10,12,16,28] use both GHHM’s result and O2H theorems from AHU.



## 2 Preliminaries

**Notation.** We write  $y \leftarrow^s \mathcal{A}[O](x)$  for randomized execution of  $\mathcal{A}$  with input  $x$  and oracle access to  $O$  which produces output  $y$ . We consider quantum  $\mathcal{A}$  that can access  $O$  in superposition. We let  $\Pr[\mathbf{G}]$  denote the probability that game  $\mathbf{G}$  returns **true**. Registers are implicitly initialized to store the all zero string.

If  $\mathcal{S}$  is a set, then  $y \leftarrow^s \mathcal{S}$  denotes sampling  $y$  uniformly from  $\mathcal{S}$ . We let  $\text{Fcs}(n, m)$  denote the set of all functions mapping  $\{0, 1\}^n$  to  $\{0, 1\}^m$ . Sampling  $H \leftarrow^s \text{Fcs}(n, m)$  gives a uniform random function.

### 2.1 Quantum Computation Background

We assume familiarity with basic quantum computation, as performing unitary operations on registers which each contain a fixed number of qubits that can be measured in the computational basis. Our main results are primarily based on a “one-way to hiding” theorem (defined soon) which when treated as a blackbox allow us to primarily think “classically”. We summarize the most important ideas used in our proofs.

**Computing Permutations.** If  $P$  is a permutation, then there is a quantumly computable unitary  $U_P$  which maps according to  $U_P |x\rangle = |P(x)\rangle$  for  $x \in \{0, 1\}^n$ . The runtime of this unitary grows with the maximum time required to compute  $P$  and  $P^{-1}$  classically. We write  $P$  in place of  $U_P$ . If  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  is a function, we define the permutation  $f[\oplus](x, y) = (x, f(x) \oplus y)$ .

We define permutations that will be provided as (possibly quantum accessible) oracles using the following notation.

```
Oracle O( $X_1, \dots : Z_1, \dots$ )  
//Code updating  $X_1, \dots$  and  $Z_1, \dots$   
Return ( $X_1, \dots : Z_1, \dots$ )
```

Formally, the colon separating the two sets of inputs is syntactic sugar with the same meaning as a comma. Informally, we use it to separate the variables/registers that we think of as being attacker controlled ( $X_1, \dots$ ) from those we think of as being controlled by the game they interact with ( $Z_1, \dots$ ).

**Principle of Deferred Measurement.** In proofs, we find it convenient to defer any classical measurements until the end of execution by writing the result of the measurement (in superposition) into an auxiliary register that will otherwise be unused. This is a standard technique, which we express informally as follows.

**Lemma 1 (Principle of Joint Deferred Measurement, Informal).** *Let  $R_1, R_2, \dots$  be a collection of registers that would be measured at time  $T$ . If between  $T$  and  $T' > T$  these registers are only ever swapped with each other or used to control operations on other registers, then it would be equivalent to defer measuring them until time  $T'$ .*

Game $G_O^{\text{hide}}(\mathcal{D})$	Game $G_{P,P'}^{\text{ow}}(\mathcal{D})$
$b \leftarrow_s \mathcal{D}[O]$	$i \leftarrow_s \{1, \dots, q\}$
Return $b = 1$	Run $\mathcal{D}[P]$ until its $i$ -th query
	Measure the input $x$ to this query
	Return $(P(x) \neq P'(x))$

**Fig. 3.** Games used for O2H Theorem 1

In the case that  $T'$  is the end of an experiment and we only care about the measured value of some other register, then the measurement can be deferred indefinitely.

**Sparse Representation of a Uniformly Random Function.** In two proofs we make use of Zhandry’s [32] technique for representing random functions with sparse tables.

**Lemma 2 (Sparse QROM Representation, Informal).** *Using the principle of deferred measurement, we can represent a uniformly random function with a table in the uniform superposition that is xored into attacker chosen values when oracle queries are made. Switching to the Fourier domain (via the Hadamard transform), we can represent it with a table initially of all zeros for which the attacker chosen values are xored into the table on oracle queries. Thus, after  $q$  oracle queries, we have a (superposition over) tables with at most  $q$  non-zero entries.*

The full compressed oracle technique of Zhandry combines the above with the ability to represent such a sparse table compactly (with  $q$  registers). When we first make use of this approach we will, in an appendix, provide a rigorous, non-informal breakdown of the technique into individual steps for readers unfamiliar with the technique.

Unruh [27] gives a generalization of Zhandry’s technique, exhibiting that the particular choices of using the Fourier domain or the Hadamard transform are inessential for the result. We nonetheless stick with the original framing of it for concreteness.

**(Fixed Permutation) One-way to Hiding.** Ambainis, Hamburg, and Unruh [3] proved a “one-way to hiding” (O2H) theorem which bounds the ability of an attacker to distinguish between two oracles by the probability that the attacker can be used to find an input on which the two oracles differ. Their theorem and typical uses thereof consider distributions over the oracles. We focus on using a variant where the oracles are permutations that are fixed ahead of time, inspired by Jaeger, Song, and Tessaro [14]. We will define both and show that they are essentially equivalent.

Consider the game  $G^{\text{hide}}$  defined in Fig. 3 wherein the distinguisher  $\mathcal{D}$  is given access to an oracle  $O$  and then outputs a bit  $b$ . For  $e \in \{1, 1/2\}$ , we measure the ability of  $\mathcal{D}$  to distinguish between permutations  $P$  and  $P'$  by

$$\text{Adv}_{P,P',e}^{\text{hide}}(\mathcal{D}) = \left( \Pr \left[ G_P^{\text{hide}}(\mathcal{D}) \right] \right)^e - \left( \Pr \left[ G_{P'}^{\text{hide}}(\mathcal{D}) \right] \right)^e.$$

The O2H theorem bounds this in terms of the game  $G^{\text{ow}}$  shown in the same figure. There the distinguisher is run with access to oracle  $P$ . One of its oracle queries (chosen at random) is measured and the game returns **true** if the permutations  $P$  and  $P'$  would give different outputs on this input. We define

$$\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}) = \Pr \left[ G_{P,P'}^{\text{ow}}(\mathcal{D}) \right].$$

**Theorem 1 (Fixed Permutation O2H).** *Let  $P, P'$  be permutations,  $\mathcal{D}$  be an distinguisher making at most  $q$  oracle queries, and  $e \in \{1, 1/2\}$ . Then*

$$\left| \text{Adv}_{P,P',e}^{\text{hide}}(\mathcal{D}) \right| \leq 2q \sqrt{\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})}.$$

Note that the two permutations are a priori fixed. Assuming  $P \neq P'$ , there trivially exist distinguishers which can distinguish between the two permutations by simply querying them on an input where they differ. Thus, when making productive use of this theorem we will always be considering some restricted class of distinguishers. Generally, the distinguisher will internally be running an adversary interacting with a security game and the permutations will be used to process when the adversary makes an oracle query to its game.

The original result of Ambainis, Hamburg, and Unruh considered distributions over oracles of the form  $f[\oplus]$ , rather than arbitrary permutations.<sup>5</sup> Let  $\mathbf{D}$  be a distribution over  $(f, f', \mathcal{D})$  where  $f, f'$  are functions and  $\mathcal{D}$  is a distinguisher (for comparison to AHU's original statements, think of it as a fixed distinguisher on input a random string  $z$ ). Then we define

$$\begin{aligned} \text{Adv}_e^{\text{hide}}(\mathbf{D}) &= \left( \mathbb{E} \left[ \Pr \left[ G_{f[\oplus]}^{\text{hide}}(\mathcal{D}) \right] \right] \right)^e - \left( \mathbb{E} \left[ \Pr \left[ G_{f'[\oplus]}^{\text{hide}}(\mathcal{D}) \right] \right] \right)^e \text{ and} \\ \text{Adv}^{\text{ow}}(\mathbf{D}) &= \mathbb{E} \left[ \Pr \left[ G_{f[\oplus], f'[\oplus]}^{\text{ow}}(\mathcal{D}) \right] \right] \end{aligned}$$

where the expectations are over  $(f, f', \mathcal{D}) \leftarrow \mathbf{D}$ .

We can capture the relevant parts of their theorem as follows.

**Theorem 2 ([3], Thm. 3).** *Let  $\mathbf{D}$  be a distribution as above where  $\mathcal{D}$  makes at most  $q$  oracle queries. Let  $e \in \{1, 1/2\}$ . Then*

$$\left| \text{Adv}_e^{\text{hide}}(\mathbf{D}) \right| \leq 2q \sqrt{\text{Adv}^{\text{ow}}(\mathbf{D})}.$$

The following result notes that these are equivalent.

<sup>5</sup> It additionally gave a slightly better bound for distinguishers that can make multiple queries in parallel, but we omit this for simplicity.

**Proposition 1.** *Theorem 1 and Theorem 2 directly imply each other (up to constant factors).*

*Proof.* Let  $\mathbf{D}$  be given. Then define the permutations

$$\begin{aligned} P(X, Y : f, f') &= (X, f(X) \oplus Y : f, f') \\ P'(X, Y : f, f') &= (X, f'(X) \oplus Y : f, f'). \end{aligned}$$

Then let  $\mathcal{D}^*$  sample  $(f, f', \mathcal{D}) \leftarrow \mathbf{D}$  and start running  $\mathcal{D}$  internally. Whenever  $\mathcal{D}$  makes an oracle query with registers  $(X, Y)$ , the distinguisher  $\mathcal{D}^*$  will query its oracle with  $(X, Y : f, f')$ . When  $\mathcal{D}$  halts and outputs  $b$ ,  $\mathcal{D}^*$  halts and outputs  $b$  as well. It is clear that

$$\begin{aligned} \Pr[G_P^{\text{hide}}(\mathcal{D}^*)] &= \mathbb{E} \left[ \Pr[G_{f[\oplus]}^{\text{hide}}(\mathcal{D})] \right], \Pr[G_{P'}^{\text{hide}}(\mathcal{D}^*)] = \mathbb{E} \left[ \Pr[G_{f'[\oplus]}^{\text{hide}}(\mathcal{D})] \right], \text{ and} \\ \Pr[G_{P, P'}^{\text{ow}}(\mathcal{D}^*)] &= \mathbb{E} \left[ \Pr[G_{f[\oplus], f'[\oplus]}^{\text{ow}}(\mathcal{D})] \right] \end{aligned} \quad (1)$$

and  $\mathcal{D}^*$  makes  $q$  queries. Hence Theorem 1 implies Theorem 2.

Now let  $P, P'$  and  $\mathcal{D}^*$  be given where  $\mathcal{D}^*$  makes  $q$  oracle queries. Define  $\mathbf{D}$  to be the distribution which always outputs  $(P_{\pm}, P'_{\pm}, \mathcal{D})$  where  $P_{\pm}(d, X) = P(X)$  if  $d = 1$  and  $P^{-1}(X)$  if  $d = 0$ . Permutation  $P'_{\pm}$  is defined likewise. Now define  $\mathcal{D}$  to be a distinguisher which runs  $\mathcal{D}^*$  internally. Whenever  $\mathcal{D}^*$  makes an oracle query to its oracle with register  $X$ ,  $\mathcal{D}$  prepares a register  $Y = 0^{|X|}$ , queries  $O[\oplus](1, X, Y)$  and  $O[\oplus](0, Y, X)$  then swaps  $X$  and  $Y$  before returning  $X$  to  $\mathcal{D}^*$ . When  $\mathcal{D}^*$  halts and outputs  $b$ ,  $\mathcal{D}$  halts and outputs  $b$  as well.

It is clear that the equalities in Eq. 1 hold again, but now  $\mathcal{D}$  makes  $2q$  oracle queries. Hence Theorem 2 implies Theorem 1 up to an additional multiplicative factor of 2 being added to the latter theorem's bound.  $\square$

A direct emulation of the original proof for Theorem 2 in [3] gives the constant claimed in Theorem 1.

### 3 Pan-Zeng Adaptive Reprogramming Framework

In this section we prove that (a version of) the Pan-Zeng framework for computational adaptive reprogramming [20] is directly implied by the Fixed Permutation O2H (Theorem 1). We start by recalling their framework in Section 3.1. In Section 3.2, we state and prove our variant of the framework. The bounds provided by the results are complex and hard to compare. In Section 3.3 we apply the same simplifications that Pan and Zeng use when applying their result in theorems and show that our theorem provides better concrete bounds in this case.

#### 3.1 Pan-Zeng Framework and Security Theorem

In the Pan-Zeng framework for computational adaptive reprogramming we consider multi-stage adversary  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  trying to distinguish a non-adaptive

<p>Game <math>G_{\mathcal{E},b}^{\text{pz-hide}}(\mathcal{A})</math></p> <p><math>(\text{Init}, \text{Orac}, \text{Repro}) \leftarrow \mathcal{E}</math></p> <p><math>(s, x, H_0, H_1) \leftarrow \text{Init}</math></p> <p><math>y \leftarrow \mathcal{A}_0[H_b[\oplus]](x)</math></p> <p>For <math>i = 1, \dots, n</math> do</p> <p style="padding-left: 2em;"><math>(x, a) \leftarrow \text{Orac}(s, y)</math></p> <p style="padding-left: 2em;"><math>H_1 \leftarrow \text{Repro}(s, a, H_1)</math></p> <p style="padding-left: 2em;"><math>y \leftarrow \mathcal{A}_i[H_b[\oplus]](x)</math></p> <p>Return <math>y = 1</math></p>	<p>Game <math>G_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})</math></p> <p><math>t \leftarrow \{1, \dots, q_i\}</math></p> <p>Run <math>G_{\mathcal{E},1}^{\text{pz-hide}}</math> until <math>\mathcal{A}_i</math> is initiated</p> <p>Run <math>\mathcal{A}_i[H_1[\oplus]](x)</math> until its <math>t</math>-th query</p> <p>Measure the input <math>X</math> to this query</p> <p>Return <math>(H_0(X) \neq H_1(X))</math></p>
--	--

**Fig. 4.** Games used for the Pan-Zeng computational adaptive reprogramming framework. Different stages of  $\mathcal{A}$  implicitly share state.

world from an adaptive world. This world is parameterized by an environment  $\mathcal{E}$  which specifies  $\text{Init}$ ,  $\text{Orac}$ , and  $\text{Repro}$ . The interactions are defined by the game  $G^{\text{pz-hide}}$  defined in Fig. 4.

First  $\text{Init}$  samples parameter string  $s$  (later given to  $\text{Orac}$  and  $\text{Repro}$ ), an initial input  $x$  for  $\mathcal{A}$ , and two functions  $H_0$  and  $H_1$ . In the nonadaptive world ( $b = 0$ ) each stage of  $\mathcal{A}$  is given oracle access to  $H_0[\oplus]$ , produces outputs  $y$ , and is given inputs  $x$  from  $\text{Orac}$ . In the adaptive world ( $b = 1$ ) it is instead given access to  $H_1[\oplus]$  and this function  $H_1$  is adaptively updated by  $\text{Repro}$  in between each stage of  $\mathcal{A}$  based on an auxiliary string passed to it by  $\text{Orac}$ . Note that the only quantum behavior of this game is internal computation by  $\mathcal{A}$  and its superposition queries to its  $H_b[\oplus]$  oracle. For  $e \in \{1, 1/2\}$ , we define  $\text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A}) = \left(\Pr[G_{\mathcal{E},1}^{\text{pz-hide}}(\mathcal{A})]\right)^e - \left(\Pr[G_{\mathcal{E},0}^{\text{pz-hide}}(\mathcal{A})]\right)^e$ .

The Pan-Zeng framework (similar to O2H results) bounds the distinguishing advantage of  $\mathcal{A}$  in relation to an experiment where one of  $\mathcal{A}$ 's queries are measured at random and we see if that query differentiates the two oracles. Let  $i \in \{0, \dots, n\}$  and define  $q_i$  to be the number of oracle queries that  $\mathcal{A}_i$  makes. This is captured by the game  $G^{\text{pz-ow}}$  which is parameterized by  $\mathcal{E}$  and the choice of  $i$ . In it, we run  $\mathcal{A}$  in the adaptive world until stage  $i$ . A random one of its queries in that stage are measured to see if  $H_0$  and  $H_1$  differ on that input. We define  $\text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A}) = \Pr[G_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})]$ .

Pan and Zeng proved the following (Lemma 2 in the proceedings version or Lemma 3.1 in the current ePrint version).

**Theorem 3 (Pan-Zeng Adaptive Reprogramming, [20]).** *Let  $\mathcal{E}$  be an environment and  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries. Then*

$$\left| \text{Adv}_{\mathcal{E},1}^{\text{pz-hide}}(\mathcal{A}) \right| \leq \sum_{k=0}^n \sum_{i=0}^k 2q_i \sqrt{\text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})}.$$

### 3.2 The Pan-Zeng Theorem is Implied by O2H

Now we state and prove a variant of Theorem 3 which follows from the Fixed Permutation O2H (Theorem 1).

**Theorem 4.** *Let  $\mathcal{E}$  be an environment and  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i \geq 1$  oracle queries. Let  $q = q_0 + \dots + q_n$ . Then*

$$\left| \text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A}) \right| \leq 2q \sqrt{\sum_{i=0}^n \frac{q_i}{q} \text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})}$$

for  $e \in \{1, 1/2\}$ .

*Proof.* To apply the Fixed Permutation O2H (Theorem 1) we will define appropriate  $P$ ,  $P'$ , and  $\mathcal{D}$  from  $\mathcal{E}$  and  $\mathcal{A}$ . We define the permutations as follows.

$$\begin{aligned} P(X, Y : H_0, H_1) &= (X, Y \oplus H_1(X) : H_0, H_1) \\ P'(X, Y : H_0, H_1) &= (X, Y \oplus H_0(X) : H_0, H_1) \end{aligned}$$

Note that  $P(X, Y : H_0, H_1) \neq P'(X, Y : H_0, H_1)$  if and only if  $H_1(X) \neq H_0(X)$ .

Now our distinguisher for  $P$  and  $P'$  will simply run  $\mathcal{G}_{\mathcal{E},b}^{\text{pz-hide}}(\mathcal{A})$  (that is, internally running both  $\mathcal{A}$  and the algorithms of  $\mathcal{E}$ ) except whenever  $\mathcal{A}$  would query  $(X, Y)$  to  $H_b[\oplus]$  it will query  $(X, Y : H_0, H_1)$  to its own oracle then return the resulting  $(X, Y)$  to  $\mathcal{A}$ . When  $\mathcal{A}$  produces its final output  $y$ ,  $\mathcal{D}$  halts and outputs that as well.

By Theorem 1 we get  $\left| \text{Adv}_{P,P',e}^{\text{hide}}(\mathcal{D}) \right| \leq 2q \sqrt{\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})}$ . Note that  $\mathcal{D}$  perfectly simulated the view of  $\mathcal{A}$  and so  $\text{Adv}_{P,P',e}^{\text{hide}}(\mathcal{D}) = \text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A})$ .

It remains to compute  $\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})$ . Let  $I$  denote a random variable taking the value of  $i$  sampled inside of  $\mathcal{G}_{P,P'}^{\text{ow}}(\mathcal{D})$ . Define  $Q_0 = 1$ , recursively define  $Q_{j+1} = Q_j + q_j + 1$ , and define the intervals  $R_j = \{Q_j, \dots, Q_{j+1} - 1\}$ . Note that if  $I \in R_j$ , then  $\mathcal{D}$  was halted when  $\mathcal{A}_j$  made its  $I - Q_j + 1$ -th query. Then,

$$\begin{aligned} \text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}) &= \Pr[\mathcal{G}_{P,P'}^{\text{ow}}(\mathcal{D})] \\ &= \sum_{j=0}^n \Pr[I \in R_j] \Pr[\mathcal{G}_{P,P'}^{\text{ow}}(\mathcal{D}) | I \in R_j] \\ &= \sum_{j=0}^n (q_j/q) \cdot \text{Adv}_{\mathcal{E},j}^{\text{pz-ow}}(\mathcal{A}). \end{aligned}$$

This completes the proof.  $\square$

### 3.3 Comparing the Pan-Zeng and O2H-based theorems

By depending on  $q_j$  and  $\text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})$ , the bounds in Theorem 3 and Theorem 4 can be hard to parse. Consequently, when applying Theorem 3 in proofs, Pan

and Zeng simplified as follows. Let  $\varepsilon = \max_i \text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})$  and note  $q_i \leq q$ . Then,

$$\sum_{k=0}^n \sum_{i=0}^k 2q_i \sqrt{\text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})} \leq \sum_{k=0}^n \sum_{i=0}^k 2q\sqrt{\varepsilon} \leq 2(n+1)^2 q\sqrt{\varepsilon}.$$

We can do a little better by noting  $q = \sum_{i=0}^n q_i$  and calculating,

$$\sum_{k=0}^n \sum_{i=0}^k 2q_i \sqrt{\text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})} \leq \sum_{k=0}^n \sum_{i=0}^n 2q_i \sqrt{\varepsilon} = 2(n+1)q\sqrt{\varepsilon}.$$

Performing similar simplifications to the bound from Theorem 4 we get the improved result that

$$2q \sqrt{\sum_{i=0}^n \frac{q_i}{q} \text{Adv}_{\mathcal{E},i}^{\text{pz-ow}}(\mathcal{A})} \leq 2q \sqrt{\sum_{i=0}^n \frac{q_i}{q} \varepsilon} \leq 2q\sqrt{\varepsilon}.$$

This analysis implicitly shows that  $\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}) \leq \varepsilon$  for the  $\mathcal{D}$  defined in our proof. We might as well then have stuck with the bound  $|\text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A})| \leq 2q\sqrt{\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})}$  in the theorem where the latter term could have been expressed in terms of measuring one of  $\mathcal{A}$ 's  $q$  queries chosen uniformly at random.

## 4 GHHM Adaptive Reprogramming Framework

In this section we prove that (a version of) the Grilo, Hövelmanns, Hülsing, Majenz (GHHM) framework for tight adaptive reprogramming [12] is implied by Fixed Permutation O2H (Theorem 1). We start by recalling their setting in Section 4.1. We discuss why their security result seems not to imply or be implied by that of Pan and Zeng [20]. In Section 4.2, we state and prove our variant of the framework. The bounds provided by the results are complex and hard to compare directly. In Section 4.3 we apply the same simplifications that GHHM use when applying their result in theorems and show that our theorem provides essentially the same concrete bounds in this case.

### 4.1 GHHM Framework and Security Theorem

The GHHM framework for tight adaptive program can syntactically be captured by the  $G^{\text{pz-hide}}$  game from Fig. 4. Let  $(\text{Init}, \text{Orac}, \text{Repro}) = \mathcal{E}$  be an environment as follows.

- **Init** outputs  $(s, x, H_0, H_1)$  where  $H_0$  and  $H_1$  are the same truly random functions from  $\mathcal{X}$  to  $\mathcal{Y}$ . We will assume without loss of generality that  $\mathcal{X} = \{0, 1\}^l$  and  $\mathcal{Y} = \{0, 1\}^m$ .  $s$  and  $x$  are empty strings.
- **Orac** interprets its input  $y$  as specifying a probability distribution  $p$  over  $\mathcal{X}$  and samples  $x \leftarrow^s p$  and  $y \leftarrow^s \mathcal{Y}$ , then outputs  $(x, a) = (x, (x, y))$ .<sup>6</sup>

<sup>6</sup> The most general version of GHHM's framework has  $p$  output a second "side-information" string  $x'$ . They showed (Appendix A in the current ePrint version) that the weaker version we use implies this stronger version.

- **Repro** given  $a = (x, y)$  outputs a function defined identically to  $H_1$  except it maps  $x$  to  $y$ .

Call such an environment a “GHHM environment”. Then GHHM proved the following information theoretic result (their Theorem 1).

**Theorem 5 (GHHM Adaptive Reprogramming, [12]).** *Let  $\mathcal{E}$  be a GHHM environment and  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries. Then*

$$\left| \text{Adv}_{\mathcal{E},1}^{\text{pz-hide}}(\mathcal{D}) \right| \leq \sum_{i=0}^n \left( \sqrt{\hat{q}_i p_{i,\max}} + 0.5 \hat{q}_i p_{i,\max} \right).$$

Here  $\hat{q}_i = q_0 + \dots + q_{i-1}$  and  $p_{i,\max} = \mathbb{E}[\max_{x \in \mathcal{X}} p_i(x)]$  where the expectation is over the behavior of the game up until the  $i$ -th oracle query and  $p_i$  is a random variable denoting the probability distribution chosen by  $\mathcal{A}_i$ .

Even though we expressed this result using the same game from the Pan and Zeng framework, it’s not clear that Theorem 3 or Theorem 5 implies the other. The GHHM result seems weaker because it requires reprogrammed points to be information-theoretically (rather than computationally) hidden and requires the initial functions and reprogrammed output to be uniform. On the other hand, the Pan and Zeng gives a bound in terms of the probability that  $\mathcal{A}$  finds a point where  $H_1$  differs from  $H_0$ . To get a meaningful bound we need this probability to be small, so the reprogrammed point must be hard to predict even after the reprogramming occurred. GHHM (by **Orac** giving  $x$  to  $\mathcal{A}$ ) is explicitly not such a setting. It instead works for cases where the reprogrammed point is hard to predict ahead of time.<sup>7</sup>

Notably Pan and Zeng are able to apply their result to analyze the selective-opening security of an encryption scheme, a result that a priori would seem like guessing the reprogrammed point should be easy afterwards. They achieve this by choosing an order of programming that differs from what one’s first instinct would use. In essence, the “trick” they are able to use is that in the settings they consider, they can predict ahead of time a small set  $S$  such that only points in  $S$  will ever be programmed. Then the arrange ahead of time for the initial functions  $H_0$  and  $H_1$  to be different on all of these points and so that the later reprogramming will switch them back to being consistent on the reprogrammed point. It does not seem possible in general to capture the GHHM setting in this manner.

## 4.2 The GHHM Theorem is Implied by O2H

Now we state and prove a variant of Theorem 3 which follows from the O2H result Theorem 1.

<sup>7</sup> Technically, the Pan-Zeng result is general enough that one can likely embed a version of the Fixed Permutation O2H by ignoring **Orac** and **Repro**. Then a version of the GHHM result would follow by the techniques in our coming proof.



**Theorem 6.** *Let  $\mathcal{E}$  be a GHHM environment and  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries. Let  $q = q_0 + \dots + q_n$ . Define  $\hat{q}_i$  and  $p_{i,\max}$  as in Theorem 5. Let  $e \in \{1, 1/2\}$ . Then*

$$\left| \text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{D}) \right| \leq 2n \sqrt{\sum_{i=0}^n \hat{q}_i p_{i,\max} / n}.$$

There are two challenges that make it surprising this theorem can be proven from the Fixed-Permutation O2H theorem. The first is that all of the dependence on  $q$  is inside the square root, whereas O2H gives us a bound with  $q$  outside of the square root. Secondly, (and similarly to our comparison with Pan and Zeng’s theorem) after a reprogramming the adversary is told the point  $x$  at which the oracle was redefined. Consequently, we can only hope to rely on the hardness of querying the oracle on input  $x$  before it was reprogrammed. But because the distribution for choosing  $x$  is not fixed ahead of time, if we tried to naively apply O2H it’s not clear how to make the permutations differ on this unknown  $x$  ahead of time.

The same insights tackle both of these challenges. Rather than thinking of the “bad event” happening during queries to  $H$ , we are going to think of the reprogramming process as being performed inside an oracle and the “bad event” is querying that oracle on inputs that make it reprogram  $H$  on places where it has “already been queried”. Note that “already been queried” is not a well defined notion because the adversary could have queried all of  $H$  in superposition. To formalize this idea, we use the techniques of Zhandry [32] to represent the quantum accessible random oracle  $H$  as a “sparse” table which is only non-zero on a few entries that “have been queried” by the attacker. (More precisely, it will be a superposition over such tables.) Then reprogramming at point  $x$  can be viewed as a fixed permutation which swaps  $H(x)$  with an auxiliary all-zero register. We can apply the Fixed Permutation O2H to compare that reprogramming permutation and a permutation which leaves  $H$  untouched. Because the other register is all-zero, the permutations will only differ on inputs where the random  $x$  happens to equal one of the few non-zero entries of  $H$ .

In Section 6, we recall more recent variants of this result for reprogramming of random permutations [1,2]. Because no permutation analog for Zhandry’s result is known, we are unable to show they follow from Fixed-Permutation O2H.

*Proof.* Our first step will be moving to a setting where queries to the hash and requests for reprogramming are both quantum queries to oracles. Consider the game  $\mathbb{G}_0^b$  for  $b \in \{0, 1\}$  defined in Fig. 5 which we will use to emulate the execution of  $\mathbb{G}_{\mathcal{E},b}^{\text{pz-hide}}(\mathcal{A})$  for the given  $\mathcal{A}$  and  $\mathcal{E}$ . The behavior of  $\mathcal{E}$  is embedded into the oracles. The game stores ahead of time the list of random outputs  $Z$  that will be programmed into new locations of the hash function and random strings  $R$  that will seed sampling the programmed point from the distributions chosen by the attacker.

It uses the following quantum registers.

Games $\mathbf{G}_0^b(\mathcal{B})$	$\text{Ro}(X, Y : H)$
$\mathbf{H} \leftarrow \text{Fcs}(l, m)$	$Y \leftarrow Y \oplus H[X]$
$\mathbf{Z} \leftarrow \text{Fcs}(\lceil \lg q \rceil, m)$	Return $(X, Y : H)$
$\mathbf{R} \leftarrow \text{Fcs}(\lceil \lg q \rceil, \infty)$	$\text{FRo}(X, Y : H)$
$ H, Z, R\rangle \leftarrow  \mathbf{H}, \mathbf{Z}, \mathbf{R}\rangle$	$H[X] \leftarrow H[X] \oplus Y$
Run $\mathcal{B}[\text{RO}, \text{REP}_b]$	Return $(X, Y : H)$
Measure $W[1]$	
Return $W[1] = 1$	$\text{REP}_b(X, Y : H, I, Z, R, V)$
Games $\mathbf{G}_1^b(\mathcal{B})$	$V[I] \leftarrow V[I] \oplus (X, Y)$
$\mathbf{R} \leftarrow \text{Fcs}(\lceil \lg q \rceil, \infty)$	Interpret $X$ as prob. dist. $p$
$ R\rangle \leftarrow  \mathbf{R}\rangle$	$x \leftarrow p(R[I])$
Run $\mathcal{B}[\mathcal{H}^Y \circ \text{FRo} \circ \mathcal{H}^Y, \text{REP}_b]$	If $b = 1$ then
Measure $W[1]$	$(H[x], Z[I]) \leftarrow (Z[I], H[x])$
Return $W[1] = 1$	$Y \leftarrow Y \oplus x$
	$I \leftarrow I + 1 \bmod 2^{\lceil \lg q \rceil}$
	Return $(X, Y : H, I, Z, R, V)$

**Fig. 5.** Games used in the analysis of Theorem 6. Registers not explicitly initialized are initialized to all 0.

- $W$ : The local work space of  $\mathcal{A}$ . Its final output guess is obtained by measuring  $W[1]$ .
- $X, Y$ : The registers intended for  $\mathcal{A}$  to provide input and receive output, respectively, from its oracles.
- $H$ : The register storing the table specifying the random oracle.
- $V$ : The registers used to store the reprogramming queries that  $\mathcal{A}$  makes.
- $R$ : The registers storing randomness used to seed the choice of  $x$ 's according to distributions  $p$ .
- $Z$ : The registers storing random strings to be programmed into  $H$ .
- $I$ : The register storing a counter tracking how many reprogramming queries have occurred. It determines which entries of  $V$ ,  $R$ , and  $Z$  are used.

We think of  $\mathcal{B}$  having direct access to the registers  $W, X, Y$ . All other registers are controlled exclusively by the game and may not directly be modified by  $\mathcal{B}$ . Note that both oracles of the game are defined by classical permutations.

Given  $\mathcal{A} = (\mathcal{A}_0, \dots, \mathcal{A}_n)$  we can map it to an algorithm  $\mathcal{B}$  playing  $\mathbf{G}_0^b$  as follows. It initially runs on  $\mathcal{A}_0$  on input  $\varepsilon$ . Whenever it queries  $X, Y$  to its hash oracle,  $\mathcal{B}$  forwards this to its RO oracle. When  $\mathcal{A}_i$  would end a stage, outputting probability distributions  $p$ ,  $\mathcal{B}$  puts the representation of this into  $X$  and prepares  $Y$  on in the all-zero state. It makes a  $\text{REP}_b$  query and returns the result to the next phase of  $\mathcal{A}$ . When  $\mathcal{A}_n$  halts with output  $y$ ,  $\mathcal{B}$  stores that in  $W[1]$  and halts.

When  $b = 1$ , each reprogram oracle query programs a fresh random output (from  $Z$ ) into the location of  $H$  chosen according to  $p$ . When  $b = 0$ , nothing is ever programmed into  $H$ . These match the behaviors of  $H_1$  and  $H_0$  in  $\mathbf{G}^{\text{pz-hide}}$

so  $\mathcal{B}$  perfectly simulates the view of  $\mathcal{A}$ , giving  $\text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A}) = (\Pr[\mathcal{G}_0^1(\mathcal{B})])^e - (\Pr[\mathcal{G}_0^0(\mathcal{B})])^e$ .

Note that  $\mathcal{B}$  makes purely classical queries to  $\text{REP}_b$ . By storing these queries in fresh entires of  $V$  which are otherwise unused the oracle itself ensures that it is accessed classically (by the principle of deferred measurement) so we will not have to explicitly account for the fact that  $\mathcal{B}$  accesses this classically, the analysis goes through even if  $\mathcal{B}$  makes superposition queries to  $\text{REP}_b$ .

Next we will transition to the games  $\mathcal{G}_1^b$ . In these games, rather than being sampled at random, the registers  $H$  and  $Z$  are initialized to zeros. The oracle  $\text{RO}$  which writes  $H[X]$  into  $Y$  has instead been replaced with  $\mathcal{H}^Y \circ \text{FRO} \circ \mathcal{H}^Y$  here  $\mathcal{H}^Y$  is the Hadamard transform applied to register  $Y$  and  $\text{FRO}$  is the Fourier version of  $\text{RO}$  where instead  $Y$  is written into  $H[X]$ .

By the sparse QROM representation technique of Zhandry, these games are completely identical so  $\text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A}) = (\Pr[\mathcal{G}_1^1(\mathcal{B})])^e - (\Pr[\mathcal{G}_1^0(\mathcal{B})])^e$  and the view of  $\mathcal{A}$  inside of  $\mathcal{B}$  is unchanged. In Appendix A we break this claim into smaller atomic steps.

Now we can compare the behavior of the permutations  $\text{REP}_1$  and  $\text{REP}_0$ . They only differ in whether  $H[x]$  and  $Z[I]$  are swapped ( $b = 1$ ) or not ( $b = 0$ ). Thus  $\text{REP}_1$  and  $\text{REP}_0$  will only differ on inputs for which  $H[x] \neq Z[I]$ .

We bound the difference between the  $b = 1$  and  $b = 0$  worlds of the game using the Fixed Permutation O2H (Theorem 1). Let  $P = \text{REP}_0$ ,  $P' = \text{REP}_1$ , and  $\mathcal{D}$  be the distinguisher that runs the all of  $\mathcal{G}_1^b$  internally, except it calls its oracle on  $(X, Y : H, I, Z, R, V)$  whenever  $\mathcal{B}$  calls its reprogramming oracle on  $X, Y$ . Note that it makes  $n$  oracle queries. We have that  $\text{Adv}_{\mathcal{E},e}^{\text{pz-hide}}(\mathcal{A}) = \text{Adv}_{P,P',e}^{\text{hide}}(\mathcal{D})$ .

We complete the proof by analyzing  $\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})$ .<sup>8</sup> Consider a fixed choice of  $i \in \{1, \dots, n\}$  in  $\mathcal{G}_{P,P'}^{\text{ow}}(\mathcal{D})$ . As discussed above, the permutations differ on the measured input iff  $H[x] \neq Z[i-1]$ . By construction of the game  $Z[i-1]$  is necessarily all zeros so this is equivalent to asking whether  $H[x]$  is zero. Note that  $H$  is independent of  $R[i-1]$  so  $x = p(R[i-1])$  looks like a fresh sample from  $p$ . At this point,  $\mathcal{B}$  inside of  $\mathcal{D}$  has made at most  $\hat{q}_i$  queries to  $\text{FRO}$  so  $H$  is a superposition of tables each of which has at most  $\hat{q}_i$  non-zero entries. The probability of a non-zero entry being hit can be bound by  $\hat{q}_i \cdot p_{i,\max}$ .

Thus, averaging over the possible choice of  $i$  we have

$$\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}) = \sum_{i=0}^n \Pr[i] \Pr[\mathcal{G}_{P,P'}^{\text{ow}}(\mathcal{D})|i] \leq \sum_{i=0}^n (1/n) \hat{q}_i \cdot p_{i,\max}.$$

Applying Theorem 1 gives the claimed bound □

### 4.3 Comparing the GHM and O2H-based theorems

By depending on  $\hat{q}_j$  and  $p_{i,\max}$ , the bounds in Theorem 5 and Theorem 6 can be hard to parse. Consequently, when applying Theorem 5 in proofs, GHMM

<sup>8</sup> Leaving the bound in terms of  $\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D})$  would make it applicable to settings where the reprogrammed points are only computationally hard to predict.

simplified as follows (e.g., from their proposition 2). Let  $p_{\max} = \max_i p_{i,\max}$ . Note that  $\hat{q}_i \leq q$ , and  $qp_{\max} \leq \sqrt{qp_{\max}}$ . Then,

$$\sum_{i=0}^n \left( \sqrt{\hat{q}_i p_{i,\max}} + 0.5 \hat{q}_i p_{i,\max} \right) \leq \sum_{i=0}^n 1.5 \sqrt{qp_{\max}} = 1.5n \sqrt{qp_{\max}}.$$

Performing analogous simplifications from the bound in Theorem 6 with gives

$$2n \sqrt{\sum_{i=0}^n \hat{q}_i p_{i,\max} / n} \leq 2n \sqrt{\sum_{i=0}^n qp_{\max} / n} = 2n \sqrt{qp_{\max}}.$$

## 5 Unruh's Adaptive O2H

In this section, we show that Unruh's Adaptive O2H's results [24,25] (which generalize an earlier result Unruh [26]) are implied by the Fixed Permutation O2H (Theorem 1). To proving the stronger version [25] we emulate the ideas from our proof in Section 4.

### 5.1 First Adaptive O2H

The first adaptive O2H result we analyze bounds how well an adversary can distinguish between  $H(x, m)$  and a random string where the attacker chooses  $m$  and  $x$  is uniformly random. This is defined by the games shown in Fig. 6 for which we define

$$\text{Adv}_e^{\text{un-hide}}(\mathcal{A}) = \left( \Pr \left[ \mathbf{G}_1^{\text{un-hide}}(\mathcal{A}) \right] \right)^e - \left( \Pr \left[ \mathbf{G}_0^{\text{un-hide}}(\mathcal{A}) \right] \right)^e.$$

The bound will consist of two terms. Intuitively, the first information theoretically bounds the how much  $\mathcal{A}_0$  can contribute the advantage because  $x$  is independent of its view. The second terms bounds in terms of how likely  $\mathcal{A}_1$  is to query  $(x, m)$  to its oracle, captured formally by  $\text{Adv}^{\text{un-ow}}(\mathcal{A}) = \Pr[\mathbf{G}^{\text{un-ow}}(\mathcal{A})]$ .

Of these advantages, Unruh proves the following relationship (Lemma 14 in the current ePrint version).

**Theorem 7 (Unruh Adaptive O2H, [24]).** *Let  $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries. Then*

$$\left| \text{Adv}_1^{\text{un-hide}}(\mathcal{A}) \right| \leq q_0 2^{-l/2+2} + 2q_1 \sqrt{\text{Adv}^{\text{un-ow}}(\mathcal{A})}.$$

We prove this result for  $\text{Adv}_e^{\text{un-hide}}(\mathcal{A})$  with  $e \in \{1, 1/2\}$  from the Fixed Permutation O2H (Theorem 1). Starting from the real world, the proof will first use O2H to program  $\mathcal{A}_0$ 's oracle to be different on *all* inputs starting with  $x$ . Then  $H(x, m)$  will only ever be used to as input to  $\mathcal{A}_1$  and in response to its oracle queries. We switch both uses to use  $B_1$  instead, which is equivalent. Then we apply O2H again to switch  $\mathcal{A}_1$ 's oracle back to using  $H(x, m)$ .

Game $G_b^{\text{un-hide}}(\mathcal{A})$	Game $G^{\text{un-ow}}(\mathcal{A})$
$H \leftarrow \text{Fcs}(l+k, n)$	$i \leftarrow \{1, \dots, q_1\}$
$m \leftarrow \mathcal{A}_0[H]$	$H \leftarrow \text{Fcs}(l+k, n)$
$x \leftarrow \{0, 1\}^l$	$m \leftarrow \mathcal{A}_0[H]$
$B_0 \leftarrow H(x, m)$	$x \leftarrow \{0, 1\}^l$
$B_1 \leftarrow \{0, 1\}^n$	$B_1 \leftarrow \{0, 1\}^n$
$b' \leftarrow \mathcal{A}_1[H](x, B_b)$	Run $\mathcal{A}_1[H](x, B_1)$ until its $i$ -th query
Return $b' = 1$	Measure the input $(x', m')$ to this query
	Return $(x, m) = (x', m')$

**Fig. 6.** Games used for Unruh’s adaptive O2H [24]. Different stages of  $\mathcal{A}$  implicitly share state.

In Section 5.2 our proof of Unruh’s second result will actually imply this theorem with a better concrete bound, replacing  $q_0 2^{-l/2+2} \rightarrow \sqrt{q_0} 2^{-l/2+1}$ . We find it pedagogically useful to start with this proof first. Our proof of Unruh’s second result will apply the ideas we used for proving GHHM’s result in Section 4 — in particular, using a sparse representation of the random oracle so that we can check for whether  $\mathcal{A}_0$  “queried”  $x$  only after it has stopped executing.

AHU [3] used their O2H theorem to prove post-quantum security of a Fujisaki-Okamoto variant — a result previously proven by using Unruh’s adaptive O2H result [23].<sup>9</sup> While discussing the differences AHU say,

While our O2H Theorem is not adaptive (in the sense that the input where the oracle is reprogrammed has to be fixed at the beginning of the game), it turns out that in the present case our new O2H Theorem can replace the adaptive one. This is because our new O2H Theorem allows us to reprogram the oracle at a large number of inputs (not just a single one). It turns out we do not need to adaptively choose the one input to reprogram, we just reprogram all potential inputs. At least in the proof from [23], this works without problems.

Our proof uses this idea of reprogramming the oracle at a large number of points, showing that the O2H theorem can replace Theorem 7 in *any* proof, not just the one from [3]. Our stronger proof in Section 5.2 will only require reprogramming at a single point.

*Proof.* Our proof will use the hybrid games  $H_{(a,b,c)}$  shown in Fig. 7 which are parameterized by  $(a, b, c) \in \{0, 1\}^3$ . Informally, we will show the following.

$$G_0^{\text{hide}} \equiv H_{(0,0,0)} \underset{2q_0\sqrt{2^{-l}}}{\approx} H_{(1,0,0)} \equiv H_{(1,1,1)} \underset{2q_0\sqrt{2^{-l}}}{\approx} H_{(0,1,1)} \underset{2q_1\sqrt{\epsilon^{\text{ow}}}}{\approx} H_{(0,1,0)} \equiv G_1^{\text{hide}}.$$

<sup>9</sup> In fact, both the proofs had flaws (see the ePrint version of [3]). This is orthogonal to our discussion here.

Hybrids $H_{(a,b,c)}$	$RO_a^0(X, M, Y : H, h, x)$
$H \leftarrow \text{Fcs}(l+k, n)$	If $X = x$ then
$h \leftarrow \text{Fcs}(k, n)$	$Y \leftarrow Y \oplus H[X, M] \quad // a = 0$
$x \leftarrow \{0, 1\}^i$	$Y \leftarrow Y \oplus h[M] \quad // a = 1$
$m \leftarrow \mathcal{A}_0[RO_a^0]$	Else $Y \leftarrow Y \oplus H[X, M]$
$B \leftarrow H(x, m) \quad // b = 0$	Return $(X, M, Y : H, h, x)$
$B_1 \leftarrow \{0, 1\}^n$	$RO_c^1(X, M, Y : H, B_1, x, m)$
$B \leftarrow B_1 \quad // b = 1$	If $(X, M) = (x, m)$ then
$b' \leftarrow \mathcal{A}_1[RO_c^1](x, B)$	$Y \leftarrow Y \oplus H[X, M] \quad // c = 0$
Return $b' = 1$	$Y \leftarrow Y \oplus B_1 \quad // c = 1$
	Else $Y \leftarrow Y \oplus H[X, M]$
	Return $(X, M, Y : H, B_1, x, m)$

**Fig. 7.** Hybrid games used for proof of Theorem 7

We proceed from left to right. Compared to  $G_0^{\text{un-hide}}$ , hybrid  $H_{(0,0,0)}$  samples an additional (unused) random function  $h$  and samples  $x$  at the beginning of the game. All three parameters being zero means both random oracles respond correctly using  $H$  and that  $\mathcal{A}_1$  is given  $H(x, m)$  as input. So game  $G_0^{\text{un-hide}}$  is equivalent to game  $H_{(0,0,0)}$ .

Now compare  $H_{(0,0,0)}$  to  $H_{(1,0,0)}$ . The change to  $a$  means that  $\mathcal{A}_0$ 's oracle will return  $h(M)$  on any input of the form  $(x, M)$ . Consider a distinguisher  $\mathcal{D}$  for the Fixed Permutation O2H (Theorem 1) which runs all of  $H_{(? , 0, 0)}$  except it forwards  $\mathcal{A}_0$ 's oracle queries to its own oracle which is either  $P = RO_0^0$  or  $P' = RO_1^0$ . The adversary provides  $X, M, Y$  while  $\mathcal{D}$  provides the rest of the inputs. It outputs the same bit  $\mathcal{A}_1$  does. Clearly  $\mathcal{D}$  correctly simulates the view of  $\mathcal{A}$ .

Note that the permutations only differ on inputs for which  $X = x$  and that  $\mathcal{A}_0$ 's view is independent of  $x$  when interacting with  $RO_0^0$ . Consequently,  $\text{Adv}_{P, P'}^{\text{ow}}(\mathcal{D}) \leq 1/2^l$  and so  $|\text{Pr}[H_{(0,0,0)}] - \text{Pr}[H_{(1,0,0)}]| \leq 2q_0\sqrt{2^{-l}}$ .

In  $H_{(1,0,0)}$ ,  $\mathcal{A}_1$  is given the random string  $H(x, m)$  as input and then its oracle returns  $H(x, m)$  on input  $(x, m)$ . In  $H_{(1,1,1)}$ ,  $\mathcal{A}_1$  is given the random string  $B_1$  as input and then its oracle returns  $B_1$  on input  $(x, m)$ . Note that these variables are otherwise unused because  $\mathcal{A}_0$  cannot access  $H(x, m)$ . Consequently the games are perfectly equivalent. Then we can move back to  $H_{(0,1,1)}$  with analysis analogous to the transition from  $H_{(0,0,0)}$  to  $H_{(1,0,0)}$ . Putting these steps together gives  $|\text{Pr}[H_{(1,0,0)}] - \text{Pr}[H_{(0,1,1)}]| \leq 2q_0\sqrt{2^{-l}}$ .

Now comparing  $H_{(0,1,1)}$  and  $H_{(0,1,0)}$  we see that they differ only in the behavior of  $\mathcal{A}_1$ 's oracle. The former will return  $B_1$  on input  $(x, m)$  while the latter will return  $H(x, m)$ . Consider a distinguisher  $\mathcal{D}'$  for the Fixed Permutation O2H (Theorem 1) which runs all of  $H_{(0,1,?)}$  except it forwards  $\mathcal{A}_1$ 's oracle queries to its own oracle which is either  $P = RO_1^1$  or  $P' = RO_0^1$ . The adversary provides  $X, M, Y$  while  $\mathcal{D}'$  provides the rest of the inputs. It outputs the same bit  $\mathcal{A}_1$  does. Clearly  $\mathcal{D}'$  correctly simulates the view of  $\mathcal{A}$ .

Game $G_b^{\text{un-hide}^2}(\mathcal{A})$	Game $G^{\text{un-ow}^2}(\mathcal{A})$
$H \leftarrow \$ \text{Fcs}(l, n)$	$i \leftarrow \$ \{1, \dots, q_1\}$
$m \leftarrow \$ \mathcal{A}_0[H]$	$H \leftarrow \$ \text{Fcs}(l, n)$
$x \leftarrow \$ \mathcal{A}_C(m)$	$m \leftarrow \$ \mathcal{A}_0[H]$
$B_0 \leftarrow H(x)$	$x \leftarrow \$ \mathcal{A}_C(m)$
$B_1 \leftarrow \$ \{0, 1\}^n$	$B_1 \leftarrow \$ \{0, 1\}^n$
$b' \leftarrow \$ \mathcal{A}_1[H](x, B_b)$	Run $\mathcal{A}_1[H](x, B_1)$ until its $i$ -th query
Return $b' = 1$	Measure the input $x'$ to this query
	Return $x = x'$

**Fig. 8.** Games used for Unruh’s second adaptive O2H [25]. Algorithm  $\mathcal{A}_C$  is classical. Algorithm  $\mathcal{A}_1$  can access the final state of  $\mathcal{A}_0$  and  $\mathcal{A}_C$ .

We have  $|\left(\Pr[H_{(0,1,1)}]\right)^e - \left(\Pr[H_{(0,1,0)}]\right)^e| \leq 2q_1 \sqrt{\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}')}.$  Note that the permutations only differ on inputs for which  $(X, M) = (x, m)$  and that the view of  $\mathcal{A}$  run by  $\mathcal{D}'$  in  $G_{P,P'}^{\text{ow}}$  matches the view it would get in  $G^{\text{un-ow}}$ . Consequently,  $\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}') \leq \text{Adv}^{\text{un-ow}}(\mathcal{A}).$

Finally, we can compare  $H_{(0,1,0)}$  and  $G_0^{\text{un-hide}}$  to see that they are equivalent. Putting together our claims and using the triangle inequality gives the bound

$$\left| \text{Adv}_e^{\text{un-hide}}(\mathcal{A}) \right| \leq 4q_0 \sqrt{2^{-l}} + 2q_1 \sqrt{\text{Adv}_{P,P'}^{\text{ow}}(\mathcal{D}')}.$$

□

## 5.2 Second Adaptive O2H

In [25], Unruh improved on his adaptive O2H result with a version that allowed the hidden point to be chosen according to a arbitrary adaptively chosen distribution, as long as this distribution has sufficient entropy. We can capture the result using games  $G^{\text{un-hide}^2}$  and  $G^{\text{un-ow}^2}$  defined in Fig. 8. In both, sampling  $x$  is now done with the classical algorithm  $\mathcal{A}_C$ . It cannot access  $\mathcal{A}_0$ ’s state beyond the input  $m$  passed to it. Algorithm  $\mathcal{A}_1$  is allowed allow access the state of both  $\mathcal{A}_0$  and  $\mathcal{A}_1$ . Defining  $\text{Adv}_e^{\text{un-hide}^2}(\mathcal{A}) = \left(\Pr[G_1^{\text{un-hide}^2}(\mathcal{A})]\right)^e - \left(\Pr[G_0^{\text{un-hide}^2}(\mathcal{A})]\right)^e$  and  $\text{Adv}^{\text{un-ow}^2}(\mathcal{A}) = \Pr[G^{\text{un-ow}^2}(\mathcal{A})].$

We define the collision entropy  $k$  and min-entropy  $\mu$  of  $\mathcal{A}_C$  by

$$k = \min_m -\log_2 \Pr[x = y : x \leftarrow \$ \mathcal{A}_C(m), y \leftarrow \$ \mathcal{A}_C(m)]$$

$$\mu = \min_{m,x} -\log_2 \Pr[x = y : y \leftarrow \$ \mathcal{A}_C(m)].$$

Note that  $2\mu \geq k \geq \mu.$

Then we can state Unruh’s result (Lemma 9 in the current ePrint version).

**Theorem 8 (Unruh Adaptive O2H, [25]).** *Let  $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries and  $\mathcal{A}_C$  be a classical algorithm with collision entropy  $k$ . Then*

$$\left| \text{Adv}_1^{\text{un-hide2}}(\mathcal{A}) \right| \leq 2q_1 \sqrt{\text{Adv}^{\text{un-ow2}}(\mathcal{A})} + (4 + \sqrt{2})\sqrt{q_0}2^{-k/4}.$$

We prove the following slightly generalized result.

**Theorem 9.** *Let  $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$  be an adversary for which  $\mathcal{A}_i$  makes at most  $q_i$  oracle queries and  $\mathcal{A}_C$  be a classical algorithm with min-entropy  $\mu$  and collision entropy  $k$ . Then for  $e \in \{1, 1/2\}$ .*

$$\begin{aligned} \left| \text{Adv}_e^{\text{un-hide2}}(\mathcal{A}) \right| &\leq 2q_1 \sqrt{\text{Adv}^{\text{un-ow2}}(\mathcal{A})} + 2\sqrt{q_0}2^{-\mu/2} \\ &\leq 2q_1 \sqrt{\text{Adv}^{\text{un-ow2}}(\mathcal{A})} + 2\sqrt{q_0}2^{-k/4}. \end{aligned}$$

Unruh conjectured that the  $2^{-k/4}$  factor is an artifact of their proof technique. If so, our proof technique has the same artifact but removes it when min-entropy is an acceptable replacement. This, for example, allows us to directly imply a version of Theorem 7 with the bound improved to replace  $q_0$  with  $\sqrt{q_0}$ .

Our proof combines the ideas from our proof of Unruh’s first adaptive O2H (Theorem 7) and our proof of the GHHM adaptive reprogramming result (Theorem 5). We first move to a hybrid where we reprogram  $H(x)$  to equal  $B_1$  before  $\mathcal{A}_1$  is executed (more precisely, we swap the values of  $H(x)$  and  $B_1$ ). To obtain a tighter bound for this step than in Theorem 7, we switch to a sparse representation of  $H$  and bound the “bad event” at the time of the swap, as in our Theorem 5 proof. Then we show the difference between this hybrid and the final game by reprogramming  $\mathcal{A}_1$ ’s access to  $H$  on input  $x$ .

*Proof.* For this proof we use the games shown in Fig. 9. We start with  $G_b$  which is simply a rewritten version of  $G_b^{\text{un-hide2}}$ . It writes the use of  $\mathcal{A}_C$  as a single query to an oracle SAMP and make everything quantum. Algorithm  $\mathcal{A}_0$  acts on registers  $W, X, Y$ , while  $\mathcal{A}_1$  may additionally act on  $R$ . (Here  $R$  stores the randomness that will be used by  $\mathcal{A}_C$ . Giving it to  $\mathcal{A}_1$  is equivalent for our purposes to letting  $\mathcal{A}_1$  access the final state of  $\mathcal{A}_C$  and additionally allows  $\mathcal{A}_1$  to recompute the  $x$  which is stored in  $X^*$ .) Registers  $H$  and  $B$  are controlled by the game. To enforce that the SAMP query is classical, it writes the query  $X$  (which stores  $m$  at this time) into the otherwise unused register  $V$ . So we have  $\Pr[G_b^{\text{un-hide2}}(\mathcal{A})] = \Pr[G_b(\mathcal{A})]$ .<sup>10</sup>

Our proof will use the hybrid games  $H_{(a,b,c)}$  shown in Fig. 9 which are parameterized by  $(a, b, c) \in \{0, 1\}^3$ . Informally, we will show the following.

$$G_0 \equiv H_{(0,0,0)} \underset{2\sqrt{q_0}2^{-\mu}}{\approx} H_{(1,0,0)} \equiv H_{(0,1,1)} \underset{2q_1\sqrt{\varepsilon^{\text{ow}}}}{\approx} H_{(0,1,0)} \equiv G_1.$$

<sup>10</sup> Formally, the syntax of  $\mathcal{A}$  changed, so on the right-hand side it should have been replaced with an appropriately defined  $\mathcal{A}'$ .



Games $G_b$	$\text{SAMP}_b(X, Y : H, B, V, R, X^*)$
$\mathbf{H} \leftarrow_s \text{Fcs}(l, n)$	$V \leftarrow V \oplus X$
$\mathbf{B} \leftarrow_s \{0, 1\}^n$	$X^* \leftarrow X^* \oplus \mathcal{A}_C(X; R[I])$
$\mathbf{R} \leftarrow_s \{0, 1\}^\infty$	$Y \leftarrow Y \oplus H[X^*] \quad // \text{ If } b = 0$
$ H, B, R\rangle \leftarrow  \mathbf{H}, \mathbf{B}, \mathbf{R}\rangle$	$Y \leftarrow Y \oplus B \quad // \text{ If } b = 1$
Run $\mathcal{A}_0[\text{RO}]$	Return $(X, Y : H, B, V, R, X^*)$
Run $\text{SAMP}_b$	$\text{Ro}(X, Y : H)$
Run $\mathcal{A}_1[\text{RO}]$	$\bar{Y} \leftarrow Y \oplus H[X]$
Measure $W[1]$	Return $(X, Y : H)$
Return $W[1] = 1$	
Hybrids $H_{(a,b,c)}$	$\text{FSAMP}_{a,b}(X, Y : H, B, V, R, X^*)$
$\mathbf{R} \leftarrow_s \text{Fcs}(\lceil \lg q \rceil, m)$	$V \leftarrow V \oplus X$
$ R\rangle \leftarrow  \mathbf{R}\rangle$	$X^* \leftarrow X^* \oplus \mathcal{A}_C(X; R[I])$
Run $\mathcal{A}_0[\mathcal{H}^Y \circ \text{FRO}^0 \circ \mathcal{H}^Y]$	$(B, H[X^*]) \leftarrow (H[X^*], B) \quad // \text{ If } a = 1$
Run $\mathcal{H}^Y \circ \text{FSAMP}_{a,b} \circ \mathcal{H}^Y$	$H[X^*] \leftarrow Y \oplus H[X^*] \quad // \text{ If } b = 0$
Run $\mathcal{A}_1[\mathcal{H}^Y \circ \text{FRO}_c^1 \circ \mathcal{H}^Y]$	$B \leftarrow Y \oplus B \quad // \text{ If } b = 1$
Measure $W[1]$	Return $(X, Y : H, B, V, R, X^*)$
Return $W[1] = 1$	$\text{FRO}_c^1(X, Y : H, B)$
$\text{FRO}^0(X, Y : H)$	If $X = X^*$ then
$H[X] \leftarrow Y \oplus H[X]$	$H[X^*] \leftarrow Y \oplus H[X^*] \quad // \text{ If } c = 0$
Return $(X, Y : H)$	$B \leftarrow Y \oplus B \quad // \text{ If } c = 1$
	Else $H[X] \leftarrow Y \oplus H[X]$
	Return $(X, Y : H, B)$

**Fig. 9.** Hybrid games for proof of Theorem 9, implying the adaptive O2H result of Unruh [25]. Algorithm  $\mathcal{A}_1$ , but not  $\mathcal{A}_0$ , may access register  $R$ .

We proceed from left to right. Consider  $H_{(0,0,0)}$ . In this game, rather than being sampled at random, the registers  $H$  and  $B$  are initialized to zeros. The oracle  $\text{RO}$  which writes  $H[X]$  into  $Y$  has instead been replaced with two (for now equivalent) oracles  $\mathcal{H}^Y \circ \text{FRO}^i \circ \mathcal{H}^Y$  where  $\mathcal{H}^Y$  is the Hadamard transform applied to register  $Y$  and  $\text{FRO}$  is the Fourier version of  $\text{RO}$  where instead  $Y$  is written into  $H[X]$ . Similarly,  $\text{FSAMP}$  which writes  $H[X^*]$  or  $B$  into  $Y$  has been replaced with  $\mathcal{H}^Y \circ \text{SAMP}_{a,b} \circ \mathcal{H}^Y$  which writes  $Y$  into  $H[X^*]$  or  $B$ . By the sparse QROM representation technique of Zhandry, these games are completely equivalent, giving  $\Pr[G_b(\mathcal{A})] = \Pr[H_{(0,b,0)}(\mathcal{A})]$ . See our proof of Theorem 6 and in particular Appendix A for an example of how to break this equivalence claims into smaller atomic steps.

Now in  $H_{(0,1,0)}$  we perform an additional swap of  $B$  and  $H[X^*]$ . Note that  $\text{FSAMP}_{a,0}$  and  $\text{FSAMP}_{a,1}$  differ as permutations only if  $B \neq H[X^*]$ .

We apply the Fixed Permutation O2H (Theorem 1) with  $\mathcal{D}$  that runs all of  $H_{(0,?,0)}$  internally, except it calls its oracle to emulate  $\text{FSAMP}$ . Note that  $\mathcal{D}$  makes one oracle query and at that time  $H$  has at most  $q_0$  non-zero entries (which thus

<p style="margin: 0;">Game <math>G_b^{\text{perm}}(\mathcal{A})</math></p> <p style="margin: 0;"><math>\Pi_0 \leftarrow_s \text{Perm}(n)</math></p> <p style="margin: 0;"><math>\mathcal{A}_0[\Pi_0[\oplus], \Pi_0^{-1}[\oplus]]</math></p> <p style="margin: 0;"><math>s, s' \leftarrow_s \{0, 1\}^n</math></p> <p style="margin: 0;"><math>\Pi_1 \leftarrow \Pi_0 \circ S_{s, s'}</math></p> <p style="margin: 0;"><math>b' \leftarrow_s \mathcal{A}_1[\Pi_b[\oplus], \Pi_b^{-1}[\oplus]](s, s')</math></p> <p style="margin: 0;">Return <math>b' = 1</math></p>
--

**Fig. 10.** Game for ABKH resampling for permutations result

differ from  $B$  which is zero). Thus  $\text{Adv}_{\text{FSAMP}_{0,0}, \text{FSAMP}_{1,0}}^{\text{ow}}(\mathcal{D}) \leq q_0/2^{-\mu}$  from the min-entropy of  $\mathcal{A}_C$  and  $|\text{Pr}[\text{H}_{(0,0,0)}(\mathcal{A})]^e - \text{Pr}[\text{H}_{(0,1,0)}(\mathcal{A})]^e| \leq 2\sqrt{q_0/2^\mu}$ .

Hybrid  $\text{H}_{(0,1,0)}$  swaps the registers  $B$  and  $H[X^*]$  before  $\mathcal{A}_1$  is run. Note  $\mathcal{A}_1$  does not have direct access to these registers, so it would be equivalent to leave  $B$  and  $H[X^*]$  unswapped, but instead switch which of the two is used in all future accesses to the registers. This is what's done in the equivalent game  $\text{H}_{0,1,1}$ .

Now  $\text{H}_{(0,1,1)}$  differs from  $\text{H}_{(0,1,0)}$  only when  $X^*$  is queried to  $\text{FRO}^1$ . Apply the Fixed Permutation O2H (Theorem 1) with  $\mathcal{D}'$  that runs all of  $\text{H}_{(0,1,?)}$  internally except it uses its own oracle to respond to  $\text{FRO}^1$ . We get  $|\text{Pr}[\text{H}_{(0,1,0)}(\mathcal{A})]^e - \text{Pr}[\text{H}_{(0,1,1)}(\mathcal{A})]^e| \leq 2q_1\sqrt{\text{Adv}_{\text{FRO}_1^1, \text{FRO}_0^1}^{\text{ow}}(\mathcal{D}')}.$

The previously discussed equivalence between  $\text{H}_{(0,1,0)}$ ,  $G_1$ , and  $G_1^{\text{un-hide}^2}(\mathcal{A})$  allows us to conclude that  $\text{Adv}_{\text{FRO}_1^1, \text{FRO}_0^1}^{\text{ow}}(\mathcal{D}') = \text{Adv}^{\text{un-ow}^2}(\mathcal{A})$  and complete the proof using the triangle inequality.  $\square$

## 6 Limitations of Fixed Permutation O2H

Alagic, Bai, Katz, and Majenz [1] gave a result for the resampling of random permutations which they call an extension of the GHHM adaptive reprogramming lemma (Theorem 5) to the case of two-way accessible random permutations which we cannot reproduce from Fixed-Permutation O2H because it is not known if quantumly accessible random permutations can be sparsely represented.

Define the swap permutation  $S_{s, s'}$  by  $S(s) = s'$ ,  $S(s') = s$ , and  $S(x) = x$  otherwise. Let  $\text{Perm}(n)$  denote the set of all permutations on  $\{0, 1\}^n$ . Then the relevant security game is shown in Fig. 10 for which we define  $\text{Adv}_e^{\text{perm}}(\mathcal{A}) = (\text{Pr}[G_1^{\text{perm}}(\mathcal{A})]^e) - (\text{Pr}[G_0^{\text{perm}}(\mathcal{A})]^e).$

Of this game, they prove the following bound (their Lemma 5).

**Theorem 10 (ABKH Permutation Resampling, [1]).** *Let  $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$  be an adversary for which  $\mathcal{A}_0$  makes at most  $q_0$  oracle queries. Then*

$$|\text{Adv}^{\text{perm}}(\mathcal{A})| \leq 4\sqrt{q_0/2^n}.$$

While this result is intuitively related to the GHHM adaptive reprogramming result, we cannot port over our proof from Section 4, because it relied on

Zhandry’s technique for sparse representation of a random oracle. No sufficiently analogous technique is currently known for random permutations. (Indeed it is a notoriously difficult problem [27].)

Recall that there were two reasons we relied on Zhandry’s technique in that section. First because the reprogramming points were sampled from an adaptively chosen distribution and then immediately given to the attacker we could only rely on the “bad event” of querying these points before the reprogramming occurred. But at that time we don’t know what points are bad! That is not an issue for this theorem, as  $s$  and  $s'$  could have been sampled at the beginning of the game.

The second reason is an issue. We wanted bounds of the form  $n\sqrt{q\varepsilon}$  (note Theorem 10 has this form, as  $n = 1$ ). This was obtained by thinking of reprogramming being its own oracle and the “bad event” being that the chosen reprogramming point happened to coincide with a previous oracle query, formally a non-zero entry in the sparse representation of the random oracle. Without a sparse representation for random permutations, it is unclear how to emulate this.

Below for comparison, we prove a bound of the form  $q\sqrt{n\varepsilon}$  for Theorem 10 using Fixed-Permutation O2H by exploiting the fact that  $s, s'$  are non-adaptively chosen.

In essence, the issues here correspond to the differences between the two proofs in Section 5. The proof we provide here is in this sense analogous to our proof of Theorem 7, and we are unable to prove an analog of Theorem 8 because we lack techniques for sparsely representing permutations.

*Proof (Weakened Theorem 10).* First note that  $s, s' \leftarrow_{\$} \{0, 1\}^n$  could have been sampled at the beginning of the game. Then it would have been completely equivalent to give  $\mathcal{A}_0$  access to  $\Pi_b$  and  $\mathcal{A}_1$  access to  $\Pi_0$ . We can define the fixed permutations  $\text{PERM}_b(X, Y, d : \Pi, s, s')$  to implement  $\Pi_b$  if  $d = 1$  and  $\Pi_b^{-1}$  if  $d = 0$ . They differ only on inputs for which  $(X, d) \in \{(s, 1), (s', 1), (\Pi_0(s), 0), (\Pi_0(s'), 0)\}$ . So applying Theorem 1 with these two permutations and  $\mathcal{D}$  that picks  $s, s'$ , runs  $\mathcal{A}_0$  with access to the permutation, then internally simulates the rest of the game and outputs whatever  $\mathcal{A}$  does we get

$$\text{Adv}_e^{\text{perm}}(\mathcal{A}) = \text{Adv}_{\text{PERM}_1, \text{PERM}_0, e}^{\text{hide}}(\mathcal{D}) \leq 2q_0 \sqrt{\text{Adv}_{P, P'}^{\text{ow}}(\mathcal{D})} = 2q_0 \sqrt{2/2^n}.$$

The last equality comes from noting the view of  $\mathcal{A}_0$  is independent of  $s, s'$  and that for a given choice of  $d$  there are at most two uniformly random  $X$ ’s on which the permutations differ.  $\square$

Alagic, Bai, Katz, Majenz, and Struck [2] introduced a stronger version of this theorem which allows  $s$  to be sampled according to an adaptively chosen distribution with high min-entropy ( $s'$  is still uniform). For this version, the proof technique above would not work because we cannot sample  $s$  at the beginning of the game. At best, we could prove a variant in which  $\mathcal{A}_1$  is never told  $s, s'$  and so we can bound its success based its ability to query the permutations on the bad points after they are chosen.

## References

1. Alagic, G., Bai, C., Katz, J., Majenz, C.: Post-quantum security of the Even-Mansour cipher. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 458–487. Springer, Heidelberg (May / Jun 2022). [https://doi.org/10.1007/978-3-031-07082-2\\_17](https://doi.org/10.1007/978-3-031-07082-2_17)
2. Alagic, G., Bai, C., Katz, J., Majenz, C., Struck, P.: Post-quantum security of tweakable even-mansour, and applications. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 310–338. Springer Nature Switzerland, Cham (2024). [https://doi.org/10.1007/978-3-031-58716-0\\_11](https://doi.org/10.1007/978-3-031-58716-0_11)
3. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 269–295. Springer, Heidelberg (Aug 2019). [https://doi.org/10.1007/978-3-030-26951-7\\_10](https://doi.org/10.1007/978-3-030-26951-7_10)
4. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 93. pp. 62–73. ACM Press (Nov 1993). <https://doi.org/10.1145/168588.168596>
5. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (May / Jun 2006). [https://doi.org/10.1007/11761679\\_25](https://doi.org/10.1007/11761679_25)
6. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part II. LNCS, vol. 11892, pp. 61–90. Springer, Heidelberg (Dec 2019). [https://doi.org/10.1007/978-3-030-36033-7\\_3](https://doi.org/10.1007/978-3-030-36033-7_3)
7. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (Dec 2011). [https://doi.org/10.1007/978-3-642-25385-0\\_3](https://doi.org/10.1007/978-3-642-25385-0_3)
8. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (May 2014). [https://doi.org/10.1007/978-3-642-55220-5\\_19](https://doi.org/10.1007/978-3-642-55220-5_19)
9. Devevey, J., Fallahpour, P., Passelègue, A., Stehlé, D.: A detailed analysis of Fiat-Shamir with aborts. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023, Part V. LNCS, vol. 14085, pp. 327–357. Springer, Heidelberg (Aug 2023). [https://doi.org/10.1007/978-3-031-38554-4\\_11](https://doi.org/10.1007/978-3-031-38554-4_11)
10. Don, J., Fehr, S., Huang, Y.H., Struck, P.: On the (in)security of the buff transform. Cryptology ePrint Archive (2023), <http://eprint.iacr.org/2023/1634>
11. Eaton, E.: Leighton-Micali hash-based signatures in the quantum random-oracle model. In: Adams, C., Camenisch, J. (eds.) SAC 2017. LNCS, vol. 10719, pp. 263–280. Springer, Heidelberg (Aug 2017). [https://doi.org/10.1007/978-3-319-72565-9\\_13](https://doi.org/10.1007/978-3-319-72565-9_13)
12. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the QROM. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 637–667. Springer, Heidelberg (Dec 2021). [https://doi.org/10.1007/978-3-030-92062-3\\_22](https://doi.org/10.1007/978-3-030-92062-3_22)
13. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.)

- PKC 2016, Part I. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (Mar 2016). [https://doi.org/10.1007/978-3-662-49384-7\\_15](https://doi.org/10.1007/978-3-662-49384-7_15)
14. Jaeger, J., Song, F., Tessaro, S.: Quantum key-length extension. In: Nissim, K., Waters, B. (eds.) TCC 2021, Part I. LNCS, vol. 13042, pp. 209–239. Springer, Heidelberg (Nov 2021). [https://doi.org/10.1007/978-3-030-90459-3\\_8](https://doi.org/10.1007/978-3-030-90459-3_8)
  15. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part III. LNCS, vol. 10993, pp. 96–125. Springer, Heidelberg (Aug 2018). [https://doi.org/10.1007/978-3-319-96878-0\\_4](https://doi.org/10.1007/978-3-319-96878-0_4)
  16. Kosuge, H., Xagawa, K.: Probabilistic hash-and-sign with retry in the quantum random oracle model. In: Tang, Q., Teague, V. (eds.) PKC 2024, Part I. LNCS, vol. 14601, pp. 259–288. Springer, Heidelberg (Apr 2024). [https://doi.org/10.1007/978-3-031-57718-5\\_9](https://doi.org/10.1007/978-3-031-57718-5_9)
  17. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.: Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part III. LNCS, vol. 12107, pp. 703–728. Springer, Heidelberg (May 2020). [https://doi.org/10.1007/978-3-030-45727-3\\_24](https://doi.org/10.1007/978-3-030-45727-3_24)
  18. Maurer, U.M.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 110–132. Springer, Heidelberg (Apr / May 2002). [https://doi.org/10.1007/3-540-46035-7\\_8](https://doi.org/10.1007/3-540-46035-7_8)
  19. Morimae, T., Yamakawa, T.: Classically verifiable NIZK for QMA with preprocessing. In: Agrawal, S., Lin, D. (eds.) ASIACRYPT 2022, Part IV. LNCS, vol. 13794, pp. 599–627. Springer, Heidelberg (Dec 2022). [https://doi.org/10.1007/978-3-031-22972-5\\_21](https://doi.org/10.1007/978-3-031-22972-5_21)
  20. Pan, J., Zeng, R.: Selective opening security in the quantum random oracle model, revisited. In: Tang, Q., Teague, V. (eds.) PKC 2024, Part II. LNCS, vol. 14603, pp. 92–122. Springer, Heidelberg (Apr 2024). [https://doi.org/10.1007/978-3-031-57725-3\\_4](https://doi.org/10.1007/978-3-031-57725-3_4)
  21. Patarin, J.: The “coefficients H” technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (Aug 2009). [https://doi.org/10.1007/978-3-642-04159-4\\_21](https://doi.org/10.1007/978-3-642-04159-4_21)
  22. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332 (2004), <https://eprint.iacr.org/2004/332>
  23. Targhi, E.E., Unruh, D.: Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In: Hirt, M., Smith, A.D. (eds.) TCC 2016-B, Part II. LNCS, vol. 9986, pp. 192–216. Springer, Heidelberg (Oct / Nov 2016). [https://doi.org/10.1007/978-3-662-53644-5\\_8](https://doi.org/10.1007/978-3-662-53644-5_8)
  24. Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 1–18. Springer, Heidelberg (Aug 2014). [https://doi.org/10.1007/978-3-662-44381-1\\_1](https://doi.org/10.1007/978-3-662-44381-1_1)
  25. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 755–784. Springer, Heidelberg (Apr 2015). [https://doi.org/10.1007/978-3-662-46803-6\\_25](https://doi.org/10.1007/978-3-662-46803-6_25)
  26. Unruh, D.: Revocable quantum timed-release encryption. J. ACM **62**(6) (Dec 2015). <https://doi.org/10.1145/2817206>

27. Unruh, D.: Towards compressed permutation oracles. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part IV. LNCS, vol. 14441, pp. 369–400. Springer, Heidelberg (Dec 2023). [https://doi.org/10.1007/978-981-99-8730-6\\_12](https://doi.org/10.1007/978-981-99-8730-6_12)
28. Yuan, Q., Sun, C., Takagi, T.: Revisiting the security of fiat-shamir signature schemes under superposition attacks. In: ACISP 24 (2024), <http://eprint.iacr.org/2024/590>
29. Yuan, Q., Tibouchi, M., Abe, M.: Quantum-access security of hash-based signature schemes. In: Simpson, L., Bae, M.A.R. (eds.) ACISP 23. LNCS, vol. 13915, pp. 343–380. Springer, Heidelberg (Jul 2023). [https://doi.org/10.1007/978-3-031-35486-1\\_16](https://doi.org/10.1007/978-3-031-35486-1_16)
30. Zhandry, M.: How to construct quantum random functions. In: 53rd FOCS. pp. 679–687. IEEE Computer Society Press (Oct 2012). <https://doi.org/10.1109/FOCS.2012.37>
31. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (Aug 2012). [https://doi.org/10.1007/978-3-642-32009-5\\_44](https://doi.org/10.1007/978-3-642-32009-5_44)
32. Zhandry, M.: How to record quantum queries, and applications to quantum indistinguishability. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 239–268. Springer, Heidelberg (Aug 2019). [https://doi.org/10.1007/978-3-030-26951-7\\_9](https://doi.org/10.1007/978-3-030-26951-7_9)

## Change Log

- May 25, 2024: Fixed recurring typo pointed out by Hans Heum

## A Details of Sparse QROM Representation in Theorem 4.2

We provide a detailed analysis of why the games  $G_0^b$  and  $G_1^b$  as defined in Fig. 11 (reproduced from Fig. 5 in the proof of Theorem 6) are equivalent.

We will consider a sequence of hybrid games  $H_1^b$  through  $H_3^b$  for which we justify that  $G_0^b$  is equivalent to  $H_1^b$ ,  $G_1^b$  is equivalent to  $H_3^b$ , and  $H_\kappa$  is equivalent to  $H_{\kappa+1}$  for each  $\kappa$ . Formal pseudocode for the games is given in Fig. 11.

**Hybrid 1.** First we define  $H_1^b$  identically to  $G_0^b$  except that  $H$  and  $Z$  are initialized by applying the Hadamard transform to the all zeros strings. Recall that  $\mathcal{H}|x\rangle = 1/\sqrt{2^n} \cdot \sum_{x'} (-1)^{x \cdot x'} |x'\rangle$  if  $x$  is a bitstring  $x \in \{0, 1\}^n$ . When  $x$  is the all zeros string, this gives the uniform superposition  $1/\sqrt{2^n} \cdot \sum_{x'} |x'\rangle$ . Thus, if we measured  $H$  and  $Z$  immediately, we would be assigning them a uniformly random function as in  $G_0^b$ . Values in  $H$  and  $Z$  are only ever swapped with each other or used to control xor’s into other registers. So by the principle of joint deferred measurement, leaving them unmeasured is equivalent.

Games $G_0^b(\mathcal{B})$	$\text{Ro}(X, Y : H)$
$\mathbf{H} \leftarrow \text{Fcs}(l, m)$	$Y \leftarrow Y \oplus H[X]$
$\mathbf{Z} \leftarrow \text{Fcs}(\lceil \lg q \rceil, m)$	Return $(X, Y : H)$
$\mathbf{R} \leftarrow \text{Fcs}(\lceil \lg q \rceil, \infty)$	$\text{FRo}(X, Y : H)$
$ H, Z, R\rangle \leftarrow  \mathbf{H}, \mathbf{Z}, \mathbf{R}\rangle$	$H[X] \leftarrow H[X] \oplus Y$
Run $\mathcal{B}[\text{RO}, \text{REP}_b]$	Return $(X, Y : H)$
Measure $W[1]$	$\text{REP}_b(X, Y : H, I, Z, R, V)$
Return $W[1] = 1$	$V[I] \leftarrow V[I] \oplus (X, Y)$
Games $G_1^b(\mathcal{B})$	Interpret $X$ as prob. dist. $p$
$\mathbf{R} \leftarrow \text{Fcs}(\lceil \lg q \rceil, m)$	$x \leftarrow p(R[I])$
$ R\rangle \leftarrow  \mathbf{R}\rangle$	If $b = 1$ then
Run $\mathcal{B}[\mathcal{H}^Y \circ \text{FRo} \circ \mathcal{H}^Y, \text{REP}_b]$	$(H[x], Z[I]) \leftarrow (Z[I], H[x])$
Measure $W[1]$	$Y \leftarrow Y \oplus x$
Return $W[1] = 1$	$I \leftarrow I + 1 \bmod 2^{\lceil \lg q \rceil}$
	Return $(X, Y : H, I, Z, R, V)$

Hybrid $H_\kappa^b$
$\mathbf{R} \leftarrow \text{Fcs}(\lceil \lg q \rceil, \infty)$
$ R\rangle \leftarrow  \mathbf{R}\rangle$
$ H, Z\rangle \leftarrow \mathcal{H} H, Z\rangle$ // $H_1, H_2$
Run $\mathcal{B}[\text{RO}, \text{REP}_b]$ // $H_1$
Run $\mathcal{B}[\mathcal{H}^{Y,H} \circ \text{FRo} \circ \mathcal{H}^{Y,H}, \mathcal{H}^{Z,H} \circ \text{REP}_b \circ \mathcal{H}^{Z,H}]$ // $H_2$
Run $\mathcal{B}[\mathcal{H}^Y \circ \text{FRo} \circ \mathcal{H}^Y, \text{REP}_b]$ // $H_3$
$ H, Z\rangle \leftarrow \mathcal{H} H, Z\rangle$ // $H_3$
Measure $W[1]$
Return $W[1] = 1$

**Fig. 11. Above:** Reproduction of games from the proof of Theorem 6. **Below:** Hybrid games for using Zhandry's sparse representation technique. Registers not explicitly initialized are initialized to all 0.

**Hybrid 2.** Next we define  $H_2^b$  identically to  $H_1^b$  except the oracles  $\text{RO}$  and  $\text{REP}_b$  have been replaced with  $\mathcal{H}^{Y,H} \circ \text{FRo} \circ \mathcal{H}^{Y,H}$  and  $\mathcal{H}^{Z,H} \circ \text{REP}_b \circ \mathcal{H}^{Z,H}$ . These do not change the behavior of the game because  $\text{RO} = \mathcal{H}^{Y,H} \circ \text{FRo} \circ \mathcal{H}^{Y,H}$  and  $\text{REP}_b = \mathcal{H}^{Z,H} \circ \text{REP}_b \circ \mathcal{H}^{Z,H}$ . These equalities follow from the following lemma (and the fact that  $\mathcal{H}$  is its own inverse).

**Lemma 3.** Define permutations  $P(x, y) = (x \oplus y, y)$ ,  $P'(x, y) = (x, x \oplus y)$ ,  $S(x, y) = (y, x)$ , and  $I(x, y) = (x, y)$ . Then

$$\begin{aligned}
P &= \mathcal{H} \circ P' \circ \mathcal{H} \\
S &= (U \otimes U) \circ S \circ (U^{-1} \otimes U^{-1}) \\
I &= (U \otimes U) \circ I \circ (U^{-1} \otimes U^{-1})
\end{aligned}$$

where  $U$  is an arbitrary unitary with inverse  $U^{-1}$ .

**Hybrid 3.** We define  $H_3^b$  by cancelling out many Hadamard transforms in  $H_2$ , using that it is its own inverse.

First note that  $\mathcal{B}$  does not act on register  $H$  so transform  $\mathcal{H}^H$  will commute with it. Thereby, the initial  $\mathcal{H}^H$  used to setup  $H$  cancels with the  $\mathcal{H}^H$  before the first oracle call. The  $\mathcal{H}^H$ 's between any two oracle queries cancel with each other. This leaves only the  $\mathcal{H}^H$  after the last oracle query, which we've deferred to the end of the game.

Similarly, neither  $\mathcal{B}$  nor RO act on register  $Z$  so transform  $\mathcal{H}^Z$  will commute with them. This similarly allows us to cancel out all  $\mathcal{H}^Z$  except the one after the last query which is deferred until the end of the game.

Finally, comparing  $H_3^b$  with  $G_1^b$  we see they are identical except the former has an additional  $|H, Z\rangle \leftarrow \mathcal{H}|H, Z\rangle$  at the end. At that point of execution all that matters is the measurement of  $W[1]$  which is unaffected by this operation, so it can be removed.