Non-Observable Quantum Random Oracle Model

Navid Alamati[*] Varun Maram [†] Daniel Masny[‡]

Abstract

The random oracle model (ROM), introduced by Bellare and Rogaway (CCS 1993), enables a formal security proof for many (efficient) cryptographic primitives and protocols, and has been quite impactful in practice. However, the security model also relies on some very strong and non-standard assumptions on how an adversary interacts with a cryptographic hash function, which might be unrealistic in a real world setting and thus could lead one to question the validity of the security analysis. For example, the ROM allows adaptively programming the hash function or observing the hash evaluations that an adversary makes.

We introduce a substantially weaker variant of the random oracle model in the post-quantum setting, which we call *non-observable quantum random oracle model* (NO QROM). Our model uses weaker heuristics than the quantum random oracle model by Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry (ASIACRYPT 2011), or the non-observable random oracle model proposed by Ananth and Bhaskar (ProvSec 2013). At the same time, we show that our model is a viable option for establishing the post-quantum security of many cryptographic schemes by proving the security of important primitives such as extractable non-malleable commitments, digital signatures, and chosen-ciphertext secure public-key encryption in the NO QROM.

1 Introduction

The random oracle model (ROM), introduced by Bellare and Rogaway [BR93], is an influential tool to argue the *heuristic* security of advanced cryptographic primitives such as existentially-unforgeable (EUF-CMA secure) digital signature schemes and chosen-ciphertext secure (CCA-secure) public-key encryption (PKE). In the ROM, a hash function is modeled as a random function, i.e. with a random truth table. This paradigm has turned out to be very useful in constructing very efficient and practically relevant cryptographic schemes [FS87, PS00, FO99]. Constructions that establish similar results without using ROs are typically very inefficient and thus seem to have less practical relevance [CCH+19, PS19].

Nevertheless, the model has a negative side in that there are signature and PKE schemes that are secure in the ROM but become insecure when the random oracle is replaced with any concrete hash function [CGH98]. Therefore, we need to treat security arguments in the ROM with caution. Despite this weakness of the ROM, many results also require strong properties of the ROM: for example, the model allows security arguments to *program* the random oracle or to *observe* the queries made to the oracle by an adversary. These seem to be rather strong assumptions, or in other words, seem to significantly limit the class of adversaries against which security holds. Therefore, there have been proposals to weaken the ROM to *non-programmability* [FLR+10] or *non-observability* [AB13]. In this paper, we will be focusing on the latter aspect.

The non-observable ROM (NO ROM) [AB13] has received less attention (compared to its non-programmable counterpart [FLR+10]) and there are almost no non-trivial positive results known in the model. For example, Ananth and Bhaskar [AB13] have proposed a secure *extractable* commitment scheme in the NO ROM but it is much less efficient compared to standard commitment schemes in the plain ROM. Hence, this raises the following question:

Does security of cryptographic primitives, such as extractable commitment schemes, in the NO ROM necessarily come with a significant loss in efficiency?

[*]VISA Research.
[†]ETH Zürich.
[‡]Meta Research.

A different line of research arose with the rising threat of quantum computers, which extended the ROM to the quantum ROM (QROM) [BDF+11]. In the QROM, an adversary is allowed to make superposition queries to a quantum random oracle (QRO). This models the ability of a quantum algorithm to evaluate a hash function over an input in superposition. It was also shown that the QROM is a strictly weaker model than the ROM [YZ21], in the sense that we make strictly weaker assumptions with respect to an adversary in the former. At the same time, many security proofs in the ROM have been adapted to hold in the QROM with respect to important cryptographic primitives such as digital signatures [LZ19, DFMS19, DFMS22b] and CCA-secure PKE schemes [TU16, JZC+18, Zha19, HHM22]. However, similar to our discussion of the ROM above, most of these security proofs in the QROM crucially rely on a strong property of the model: namely, that one can observe – or more precisely, *measure* – the quantum queries made by an adversary to the random oracle. This raises another natural question:

Can we prove security of cryptographic primitives, such as digital signatures and CCA-secure PKE schemes, in the QROM without *relying on measuring/observing queries?*

1.1 Our Contributions

In this paper, we make significant progress towards answering the questions above by obtaining the following results.

New Model: "NO QROM". We first introduce a new post-quantum security model which we call *non-observable quantum random oracle model* (NO QROM). Essentially, the model is a weakened version of the NO ROM of [AB13], in terms of the heuristics used, which also accounts for quantum adversaries. In the original NO ROM, the random oracle is modeled with a Turing machine that can have a state which could be, for example, a list of random elements and the first query would be answered with the first element in the list. However, such a state is inherently incompatible with queries over superpositions. We therefore adapt the NO ROM to the quantum setting via NO QROM which allows superposition queries as in the QROM, while at the same time, forbids observing/measuring adversarial queries in the security proofs as in the NO ROM. The NO QROM therefore relies on weaker assumptions than the NO ROM and the QROM. In other words, security proofs in the NO QROM also hold in both the NO ROM and the QROM.

Efficient Extractable Commitments. Regarding the first question above on whether security of basic cryptographic primitives such as extractable commitments in the NO ROM is inherently tied with a loss in efficiency, we answer it in the negative. In fact, we go one step further and answer the same question in the weaker NO QROM; as mentioned previously, our results hold in the classical NO ROM as well. Specifically, prior work on extractable commitment schemes in the NO ROM [AB13] has some significant drawbacks. Namely, to commit to a message of size $|\mathsf{m}|$ it requires a commitment of size $2\omega(\log\kappa)\cdot|\mathsf{m}|$ using $|\mathsf{m}|$ hash evaluations for security parameter κ. Furthermore, their security proof does not seem to translate to the quantum setting. That is, in their corresponding reduction, the outcome of a random oracle query solely depends on how many queries have been made before. But it is unclear how this strategy could translate to queries in quantum superposition, where multiple queries could be made in parallel.

In our work, by leveraging well-known techniques from the QROM setting [Ben81, Zha12b, Zha12a], we show that the standard "textbook" commitment scheme $H(r,\mathsf{m})$ is in fact extractable in the NO QROM and significantly more efficient. It is computationally binding for a length $|\mathsf{m}|+2\omega(\log\kappa)$ with perfect extraction. We achieve a length of $|\mathsf{m}|+\omega(\log\kappa)$ for a *computationally* binding, extractable commitment scheme[1] with the following drawback that the extractor has either at most an inverse polynomial (in κ) success probability or runs in superpolynomial time.

Additionally, as mentioned in [BGR+15], $H(r,\mathsf{m})$ is also a *non-malleable* commitment [DDN91] in the ROM. We show that $H(r,\mathsf{m})$ is also non-malleable in the NO QROM whenever $H(r,\mathsf{m})$ is statistically binding as required by the notion of non-malleability with respect to commitments [DDN91, PR05]. However, intuitively $H(r,\mathsf{m})$ also seems non-malleable in the computationally binding setting. Hence, we make this intuition concrete by first weakening the definition of [DDN91, PR05] by a slight adaptation and then showing that $H(r,\mathsf{m})$ is non-malleable with respect to our slightly weaker definition whenever the commitment is computationally binding. Furthermore, we give bounds on the commitment length for the commitment being statistically binding and show how this could be significantly improved using a NO QRO that is a permutation.

[1] $|\mathsf{m}|+\omega(\log\kappa)$ is optimal for a statistically binding commitment since for every message, there needs to be at least $2^{\omega(\log\kappa)}$ many commitments to not violate hiding and each of these commitments is a commitment to a unique message.

EUF-CMA secure Signatures. We now consider our second question on the NO QROM security of commonly used cryptographic primitives such as digital signatures and CCA-secure PKE schemes. Focusing on the former cryptographic primitive, in the classical setting, a well-known class of ROM digital signatures called *full-domain hash* (FDH) signature schemes [BR93] is known to be secure in the NO ROM [AB13]. However, in the quantum setting, their security proof breaks down if the adversary is also allowed to query the random oracle in a quantum superposition. One of the reasons is the inherent incompatibility of maintaining a state with respect to a random oracle in a quantum setting. Another reason is that, at a high level, the prior proof strategy [AB13] crucially relies on working with a polynomial number of inputs/outputs of the random oracle. But in the quantum setting, an adversary's random oracle query can be a superposition over *exponentially* many inputs.

Fortunately, Zhandry [Zha12b] overcame the above barrier using a novel technique related to indistinguishability of quantum random oracles, and subsequently proved the security of FDH signatures in the QROM. In this work, we adapt Zhandry's proof in the context of "non-observability" to show that the FDH signatures are also secure in the weaker NO QROM. In other words, our result shows that we don't need the full "machinery" of QROM, namely observability, to prove the post-quantum security of FDH signatures, and that relying on *weaker* heuristics is sufficient.

Boneh *et al.* [BDF$^+$11] identified a relatively broad class of ROM signature schemes whose security can be shown in the QROM setting. To be specific, such a class of signatures have their classical ROM security proofs following a general structure known as *history-free reductions* [BDF$^+$11]; roughly speaking, such reductions answer adversarial random oracle queries independently of the history of previous queries. It was shown in [BDF$^+$11] that history-free reductions lift ROM security of the corresponding signatures to QROM security. More importantly, the above class of "history-free signatures" include schemes with concrete post-quantum instantiations (in contrast to FDH signatures), e.g., lattice-based GPV-style signatures [GPV08]. We extend the lifting theorem of [BDF$^+$11] to show that such history-free signatures are secure in the NO QROM, i.e., we *explicitly* establish that weaker heuristics are sufficient to prove post-quantum security of the above broad class of signatures with history-free reductions.

Hinting Pseudorandom Generators and CCA-secure Encryption. We show that any CPA-secure PKE can be transformed into a CCA-secure PKE in the NO QROM. More specifically, we provide a simple construction of a special cryptographic primitive in the NO QROM called *hinting* pseudorandom generator (hinting PRG), which was introduced by Koppula and Waters [KW19] to boost CPA-to-CCA security for PKE and related primitives. Therefore, we obtain CCA-secure encryption PKE in the NO QROM.

By proving the security of commonly used primitives in NO QROM, we establish the NO QROM paradigm as a viable option for analyzing the post-quantum security of cryptographic schemes with the advantage that it uses a weaker heuristic than the ROM, QROM, and NO ROM. Nevertheless, we emphasize that the NO QROM does not resolve the uninstantiability of the ROM [CGH98] since in their result, they do not rely on observing oracle queries.

1.2 Related Works

Regarding post-quantum security of extractable commitment schemes, Don *et al.* [DFMS22a] made significant progress with respect to online-extractability in the QROM ; however, their techniques rely on measuring the adversarial random oracle queries. In another recent work, Bitansky, Lin, and Shmueli [BLS22] proposed a $\log^*(\kappa)$-round non-malleable commitment based on post-quantum one-way functions. Their construction is the first non-malleable commitment scheme (with security against quantum attacks) in the standard model.

Lombardi *et al.* [LMS22] observed that in many natural applications of extractable commitments in the context of post-quantum secure zero-knowledge protocols, we require an additional property of the extractable commitments wherein the extractor E (Definition 4.4) must also simulate the adversary $\mathcal{A}$'s view, in addition to extracting the message m from $\mathcal{A}$'s commitment c; the authors use the term *"state-preserving" extractable commitments* for such enhanced commitments, and proceed to give constructions in the standard model. We note that our analysis of the standard hash-based commitment $H(r, \mathsf{m})$ in the NO QROM (Theorems 4.5 and 4.7) also imply the "state-preserving" extractability notion since there is no rewinding of the adversary $\mathcal{A}$ in the online setting that we consider in this work.

In this paper, we consider both statistical and computational binding properties for commitments. Regarding the latter, Unruh [Unr16] argues that the "classical" definition of computational binding of commitments (Definition 2.8) in the post-quantum setting is inadequate in the context of constructing post-quantum zero-knowledge protocols. He then provides a more satisfactory definition for computationally binding commitments in the quantum setting called *collapse-binding*, and shows simple constructions in the plain QROM. Specifically, he shows a black-box construction of collapse-binding commitments from collapsing hash-functions, and later shows that quantum random oracles are indeed collapsing. Unruh essentially bases his latter result on a related result of Zhandry [Zha15] which shows that quantum random oracles are collision-resistant. Given that Zhandry's analysis [Zha15] does not use the *observability* nor the *adaptive-programmability* features of the QROM, we expect one can extend Unruh's results to construct collapse-binding commitments in the weaker NO QROM heuristic, especially given their importance in post-quantum zero-knowledge applications.

Recently, Zhandry [Zha22] argued that there is little theoretical justification for preferring the NO ROM of Ananth and Bhaskar [AB13] over the standard ROM, because certain "ROM failures" also apply to the NO ROM. Specifically, for any concrete hash function H, there exists a cryptographic scheme with a (NO) ROM security proof such that instantiating the random oracle with H will make the scheme insecure (called "Type 2 failures" [Zha22]). It's not hard to see that the example scheme used by Zhandry to exhibit the above failure – namely, the *Encrypt-with-Hash* transform of [BBO07] – can also be used to exhibit a similar failure in our NO QROM.

However, when it comes to the specific cryptographic schemes that we consider in this paper: namely, *hash-based extractable commitments*, *full domain hash signatures*, *hinting pseudorandom generators* and *CCA-secure encryption schemes*, it is not so clear if these schemes fall under the above failure with respect to the NO QROM. Yet our security analysis of these schemes is still going to be heuristic at the end of the day. Nevertheless, the main goal of this paper, as already outlined previously, is to *weaken* such heuristics – while not completely eliminating them. Unfortunately at the current state of art, we still need heuristics to have efficient constructions and a formal (even though heuristic) security analysis of widely adopted cryptographic primitives.

2 Preliminaries

We denote the security parameter by κ. For a positive integer k, we write $[k] = \{1, \ldots, k\}$. For $n \in \mathbb{N}$, we use 0^n to denote the zero string of length n. For finite set X, we write $x \leftarrow \mathsf{X}$ to denote that x is uniformly at random sampled from X; also $|\mathsf{X}|$ denotes the cardinality of X. For a set element $x \in \mathsf{X}$ and an operation $+$ that might not be defined over X, we define $x + 0^*$ as x. For an algorithm $\mathcal{A}$ and oracle $\mathcal{O}$, we use $\mathcal{A}^{\mathcal{O}}$ to denote $\mathcal{A}$ with oracle access to $\mathcal{O}$. PPT stands for probabilistic polynomial time. We refer the reader to [NC00] for the basics of quantum computation and information.

2.1 Quantum Random Oracle Model (QROM)

In the QROM, we model hash functions as ideal functionalities called random oracles, which can be quantumly accessible. Namely, an adversary is allowed to query a random oracle $H : \{0,1\}^n \to \{0,1\}^\ell$ on an arbitrary quantum superposition of inputs, where we use the mapping $|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus H(x)\rangle$ with input register $x \in \{0,1\}^n$ and output register $y \in \{0,1\}^\ell$. We refer to [BDF+11] for a more detailed description of the model. The following lemma describes the collision-resistance of such quantum random oracles.

Lemma 2.1 ([Zha15, Theorem 3.1]). *There is a universal constant C such that the following holds. Let $H : \{0,1\}^n \to \{0,1\}^\ell$ be a random oracle. If an unbounded algorithm $\mathcal{A}$ makes a query to H at most q times, then*

$$\Pr[H(x) = H(x')] \leq C(q+1)^3/2^\ell,$$

where $(x, x') \leftarrow \mathcal{A}^H$ and $x, x' \in \{0,1\}^n$ with $x \neq x'$. Here the oracle access of $\mathcal{A}$ to H can be quantum.

The next three lemmas describe techniques to simulate quantum random oracles, which come in handy in security proofs. The first lemma uses $2q$*-wise independent functions*, the second uses *small-range distributions* as defined in [Zha12a], and the third uses *semi-constant distributions* [Zha12b].

Lemma 2.2 ([Zha12b, Theorem 6.1]). *Interpreting the set $\{0,1\}^\ell$ as the finite field $\mathbb{F}_{2^\ell}$, let $f : \{0,1\}^\ell \to \{0,1\}^\ell$ be an oracle drawn uniformly at random from the set of $(2q-1)$-degree polynomials over $\mathbb{F}_{2^\ell}$. Then the advantage* *any quantum algorithm making at most q quantum queries to f has in distinguishing f from a truly random oracle $H : \{0,1\}^\ell \to \{0,1\}^\ell$ is zero.*

In general, if $\hat{f} : \{0,1\}^n \to \{0,1\}^\ell$ is an oracle implementing a $2q$-wise independent function, then it is perfectly *indistinguishable from a uniformly random oracle $H : \{0,1\}^n \to \{0,1\}^\ell$ with respect to a quantum algorithm making at most q quantum oracle queries.*

Definition 2.3 (Small-Range Distributions)**.** *An oracle with an η-range distribution ($\eta \ll 2^\ell$) $\mathsf{SR}_\eta : \{0,1\}^n \to \{0,1\}^\ell$ is defined with the following output distribution on image $\{0,1\}^\ell$:*

- *For each $i \in [\eta]$, choose a uniformly random value $y_i \in \{0,1\}^\ell$.*
- *For each $x \in \{0,1\}^n$, pick a uniformly random $i \in [\eta]$ and set $\mathsf{SR}_\eta(x) := y_i$.*

We also define the range $\mathbb{I}_\eta$ associated to SR_η as follows: $\mathbb{I}_\eta = \{y_i \mid i \in [\eta]\}$.

Lemma 2.4 ([Zha12a, Corollary 7.5])**.** *The statistical distance of output distributions of a quantum algorithm making q quantum queries either to $\mathsf{SR}_\eta : \{0,1\}^n \to \{0,1\}^\ell$ or a random oracle $H : \{0,1\}^n \to \{0,1\}^\ell$ is bounded by $f(q)/\eta$, where $f(q) = \pi^2(2q)^3/6 < 14q^3$.*

Definition 2.5 (Semi-Constant Distributions)**.** *An oracle with a λ-constant distribution $\mathsf{SC}_\lambda : \{0,1\}^n \to \{0,1\}^\ell$ is defined with the following output distribution:*

- *First, fix a uniformly random value $y \in \{0,1\}^\ell$.*
- *For each $x \in \{0,1\}^n$, do:*

  Set $\mathsf{SC}_\lambda(x) := y$ with probability λ.

  Otherwise (with probability $1-\lambda$), set $\mathsf{SC}_\lambda(x)$ to be a uniformly random element in $\{0,1\}^\ell$.

Note that $\mathsf{SC}_0 : \{0,1\}^n \to \{0,1\}^\ell$ is just a uniformly random oracle.

Lemma 2.6 ([Zha12b, Corollary 4.3])**.** *The statistical distance of output distributions of a quantum algorithm making q quantum queries either to $\mathsf{SC}_\lambda : \{0,1\}^n \to \{0,1\}^\ell$ or a random oracle $(\mathsf{SC}_0 =)H : \{0,1\}^n \to \{0,1\}^\ell$ is bounded by $\frac{8}{3}q^4\lambda^2$.*

The following lemma provides a generic reduction from a hiding property (indistinguishability) to a one-wayness property (unpredictability) in the (NO) QROM.

Lemma 2.7 ([AHU19, Theorem 1, adapted])**.** *Let $H : \{0,1\}^n \to \{0,1\}^\ell$ be a random oracle, $\hat{x} \leftarrow \{0,1\}^n$ be a uniformly random value and y be a random bitstring which is independent of $\hat{x}$. Then, for any function $G : \{0,1\}^n \to \{0,1\}^\ell$ satisfying $\forall x \in \{0,1\}^n \setminus \{\hat{x}\}$, $G(x) = H(x)$ that might depend on ($\hat{x}$, y), and any algorithm $\mathcal{A}$ making at most q queries,*

$$|\Pr[\mathcal{A}^H(y) = 1] - \Pr[\mathcal{A}^G(y) = 1]| \leq 4\sqrt{\frac{q(q+1)}{2^n}}.$$

2.2 Commitments

We recap the syntax and basic properties of commitments such as hiding, binding, and non-malleability.

Definition 2.8. *A commitment scheme is a tuple of PPT algoritms $(\mathsf{Com}, \mathsf{Open})$ and a message space M with the following syntax.*

Com**:** *Takes as input 1^κ, $\mathsf{m} \in \mathsf{M}$ and outputs a commitment c and an opening o.*

Open**:** *Takes as input a commitment c and an opening o and outputs $\mathsf{m} \in \mathsf{M}$ or $\perp$, such that $\mathsf{Open}(\mathsf{Com}(1^\kappa, \mathsf{m})) = \mathsf{m}$.*

Additionally, it suffices two properties, hiding and binding.

Hiding: *For any PPT adversary $\mathcal{A}$ and any* $\mathsf{m}_0, \mathsf{m}_1 \in \mathsf{M}$*,*

$$|\Pr[\mathcal{A}(1^\kappa, \mathsf{c}_0) = 1] - \Pr[\mathcal{A}(1^\kappa, \mathsf{c}_1) = 1]| \leq \mathsf{negl}.$$

where $(\mathsf{c}_0, \mathsf{o}_0) \leftarrow \mathsf{Com}(1^\kappa, \mathsf{m}_0)$ *and* $(\mathsf{c}_1, \mathsf{o}_1) \leftarrow \mathsf{Com}(1^\kappa, \mathsf{m}_1)$*.*

Binding: *For any PPT adversary $\mathcal{A}$,*

$$\Pr[\mathsf{Open}(\mathsf{c}, \mathsf{o}_0) = \mathsf{m}_0 \wedge \mathsf{Open}(\mathsf{c}, \mathsf{o}_1) = \mathsf{m}_1] \leq \mathsf{negl},$$

where $(\mathsf{c}, \mathsf{o}_0, \mathsf{o}_1) \leftarrow \mathcal{A}(1^\kappa)$ *and* $\mathsf{m}_0, \mathsf{m}_1 \in \mathsf{M}$ *with* $\mathsf{m}_0 \neq \mathsf{m}_1$*.*

We call it statistically hiding (binding) if hiding (binding) holds even for any unbounded algorithm $\mathcal{A}$ and unbounded oracle algorithm $\mathcal{A}^{\mathcal{O}}$ that is allowed to make an unbounded amount of queries to the oracle $\mathcal{O}$.

Concurrent Non-Malleability. We follow the definition of non-malleable commitments of Pass and Rosen [PR05] with the slight change that we include the view of the man-in-the-middle adversary as input for the distinguisher similar to the definition of [LPV08]. Notice that an adversary can include its view in the input through committed messages. For the sake of simplicity, we use the weaker definition in which an adversary only receives a single commitment. As shown by [PR05], this implies the stronger version in which it receives many commitments. We recap the formal definition below.

Definition 2.9 (Concurrent Non-Malleability)**.** *Let the random variables* mim *and* sim *be defined as follows.*

$\mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \mathsf{m})$: *The man-in-the-middle adversary $\mathcal{A}$ receives a commitment c to a message m and auxiliary input z. $\mathcal{A}$ then generates m commitments $\mathsf{c}_1, \ldots, \mathsf{c}_m$. For every $i \in [m]$, m_i is defined as the unique committed message in c_i or $\perp$ if no such message exists. Since we consider statistically binding commitments, there will be only one message except with negligible probability. When there are more than one message or when $\mathsf{c}_i = \mathsf{c}$, we define $\mathsf{m}_i :=\perp$. The random variable entails the view of $\mathcal{A}$ and messages $\mathsf{m}_1, \ldots, \mathsf{m}_m$.*

$\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$: *The simulator S receives an auxiliary input z and generates m commitments $\mathsf{c}_1, \ldots, \mathsf{c}_m$. As previously, for all $i \in [m]$, we define m_i as the unique committed message in c_i except if it is not unique or no such message exists. In that case, it is defined as $\mathsf{m}_i :=\perp$. In addition, S can also set any $\mathsf{m}_i :=\perp$.*

*We call a commitment scheme ε-*concurrent non-malleable with respect to commitments *if for any PPT adversary $\mathcal{A}$ there exists a PPT simulator S such that for any PPT distinguisher D, message $\mathsf{m} \in \mathsf{M}$, polynomial $m \in \mathbb{N}$ and any polynomial size auxiliary input z,*

$$|\Pr[\mathsf{D}(\mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \mathsf{m})) = 1] - \Pr[\mathsf{D}(\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z) = 1)]| \leq \varepsilon.$$

A commitment scheme that is non-malleable is also computationally hiding, since otherwise an adversary could extract some information about m and a simulator which is independent of m could not simulate the view of such an adversary, which would break non-malleability.

We extend Definition 2.9 to commitments that are not statistically binding. This allows to formalize that $H(r, \mathsf{m})$ is still non-malleable in the sense that it should be hard to change a commitment $H(r, \mathsf{m})$ to a commitment $H(r, \mathsf{m}')$ for a related message m'.

Definition 2.10 (weak Concurrent Non-Malleability)**.** *Define the random variables* $\mathsf{wmim}^{\mathcal{A}}_{\mathsf{com}}(z, \mathsf{m})$ *and* $\mathsf{wsim}^{\mathsf{S}}_{\mathsf{com}}(z)$ *as* $\mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \mathsf{m})$ *and* $\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$ *with the difference that they include all messages $\mathsf{m}_{i,j}$ for which there exists an opening $\mathsf{o}_{i,j}$ such that c_i opens to $\mathsf{m}_{i,j}$.*

*We call a commitment scheme ε-*weak-concurrent non-malleable with respect to commitments *if for any PPT adversary $\mathcal{A}$ there exists a PPT simulator S such that for any PPT distinguisher D, message $\mathsf{m} \in \mathsf{M}$, polynomial $m \in \mathbb{N}$ and any polynomial size auxiliary input z,*

$$|\Pr[\mathsf{D}(\mathsf{wmim}^{\mathcal{A}}_{\mathsf{com}}(z, \mathsf{m})) = 1] - \Pr[\mathsf{D}(\mathsf{wsim}^{\mathsf{S}}_{\mathsf{com}}(z) = 1)]| \leq \varepsilon.$$

Definition 2.10 is weaker than Definition 2.9 because it does not cover that an adversary can generate a commitment to a related message by simply copying the commitment. More specifically, a commitment c could be a commitment for m and m'. Clearly, these two messages are related messages in the sense that given $\mathsf{c} = \mathsf{c}(\mathsf{m}') = \mathsf{c}(\mathsf{m})$, m cannot take every value in M unless the commitment is statistically hiding. Thus, unless it is hiding, a simulator that has no access to m could not simulate such a commitment. Definition 2.10 ignores this issue since the distinguisher receives $\perp$ instead of the committed messages in c and therefore does not offer security for this case. Nevertheless, just copying the commitment does not seem to be a significant attack against the intuitive notion of malleability, and by the computationally binding property of the commitment, an adversary would not be able to open the commitment to any other message m'. Due to this fact, we can use the same reasoning that non-malleability with respect to commitments implies non-malleability with respect to openings [DIO98, FF00] to argue that weak non-malleability with respect to commitments together with computational binding implies non-malleability with respect to openings.

Random-Oracle Based Commitments. For commitment schemes whose security properties rely on modeling their underlying hash functions as random oracles, the corresponding definitions of hiding, binding and non-malleability need to be modified accordingly in the QROM, i.e., we additionally need to give the involved parties (i.e., adversaries, simulators, and distinguishers) quantum access to the random oracle(s) associated with the commitment scheme.

2.3 Other Basic Cryptographic Primitives

Definition 2.11 (Pseudorandom Functions)**.** *A pseudorandom function (PRF) is a function family* $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ *with* $\mathcal{K}$ *being the key-space, and* $\mathcal{X}$ *and* $\mathcal{Y}$ *being the domain and range respectively. Additionally,* PRF *is said to be post-quantum (respectively, quantum) secure if no quantum polynomial-time adversary* $\mathcal{A}$ *making classical (respectively, quantum) queries can distinguish between a truly random function and the function* $\mathsf{PRF}(k, \cdot)$ *for a random key* k*. More formally, for every such adversary* $\mathcal{A}$*, we have*

$$\left| \Pr_{k \leftarrow \mathcal{K}}[\mathcal{A}^{\mathsf{PRF}(k,\cdot)}() = 1] - \Pr_{H \leftarrow \mathcal{Y}^{\mathcal{X}}}[\mathcal{A}^{H}() = 1] \right| \leq \mathsf{negl}.$$

Definition 2.12 (Signatures)**.** *A signature scheme is a tuple of PPT algorithms* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *with the following syntax.*

Gen**:** *Takes as input* 1^κ *and generates a public/secret key pair* $(\mathsf{pk}, \mathsf{sk})$.

Sign**:** *Takes as input the secret key* sk *and a message* m *and outputs a signature* σ *on it.*

Ver**:** *Takes as input the public key* pk*, a message* m *and a signature* σ*, and outputs* acc *or* rej *such that*

$$\mathsf{Ver}(\mathsf{pk}, \mathsf{m}, \mathsf{Sign}(\mathsf{sk}, \mathsf{m})) = \mathsf{acc}.$$

To define security, we will use the standard chosen-message attack (CMA) game:

- *The challenger generates* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$ *and sends* pk *to* $\mathcal{A}$*.*
- $\mathcal{A}$ *can make signature queries on messages* m_i *to which the challenger responds with* $\mathsf{Sign}(\mathsf{sk}, \mathsf{m}_i)$.
- $\mathcal{A}$ *produces a forgery candidate* (m, σ).

$\mathcal{A}$ *is said to win the game if* $\mathsf{m} \neq \mathsf{m}_i$ *for any* i *and* $\mathsf{Ver}(\mathsf{pk}, \mathsf{m}, \sigma) = \mathsf{acc}$*. The signature scheme* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *is said to be (post-quantum[2])* existentially unforgeable*, aka. (post-quantum)* EUF-CMA secure*, if for all (respectively, quantum) PPT adversaries* $\mathcal{A}$*, the winning probability in the above game is negligible in* κ*.*

[2]Note the distinction between "*post-quantum*" secure signatures and "*quantum*" secure signatures; in the former security notion, the adversary can only make *classical* signature queries, whereas in the latter, the adversary can ask for signatures of *quantum* superpositions of messages. This distinction also applies to encryption schemes with respect to classical/quantum decryption queries. See [BZ13] for the precise quantum security definitions for signatures and encryption schemes.

Definition 2.13 (Trapdoor Permutations)**.** *A trapdoor permutation (TDP) is a tuple of PPT algorithms* $(\mathsf{Gen}, \mathsf{f}, \mathsf{f}^{-1})$ *where:*

Gen**:** *Takes as input* 1^κ *and generates a public/secret key pair* $(\mathsf{pk}, \mathsf{sk})$.

f**:** *Takes as input the public key* pk *and an element* $x \in \{0,1\}^\kappa$ *and returns* $y \in \{0,1\}^\kappa$ *such that* $\mathsf{f}(\mathsf{pk}, \cdot)$ *is a bijection over* $\{0,1\}^\kappa$.

f^{-1}**:** *Takes as input the secret key* sk *and an element* $y \in \{0,1\}^\kappa$ *and returns* $x \in \{0,1\}^\kappa$ *such that* $\mathsf{f}(\mathsf{pk}, x) = y$.

A TDP $(\mathsf{Gen}, \mathsf{f}, \mathsf{f}^{-1})$ *is said to be (post-quantum)* one-way *if for any (respectively, quantum) PPT adversary* $\mathcal{A}$*,*

$$\Pr[\mathcal{A}(\mathsf{pk}, \mathsf{f}(\mathsf{pk}, x)) = x] \leq \mathsf{negl},$$

where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$ *and* $x \leftarrow \{0,1\}^\kappa$.

3 Non-Observable Quantum Random Oracle Model

We follow the outline of the NO ROM of Ananth and Bhaskar [AB13] and make some adaptations to allow for queries in superpositions. For the sake of simplicity, we ignore that a random oracle could also be adaptively programmed during a reduction.[3] In addition, we simply use a random function or random permutation [IR90] to describe the model rather than using a stateful Turing machine as [AB13]. We remark that the quantum indistinguishability of random functions and random permutations has been implicitly shown in [Zha15]. During a security game, the reduction might replace this random function or random permutation with a different function that is indistinguishable for an adversary with query access. Such a function might be for example a polynomial, where the degree of the polynomial depends on the maximum amount of adversarial queries. We allow this by adding a setup phase in which the oracle can be programmed. In Figure 1, we describe the setup and query phase. During the query phase, an oracle algorithm can send its queries and receives a response. In our setting with random permutations, the oracle is not answering queries for the inverse permutation which separates this model from an ideal cipher model.

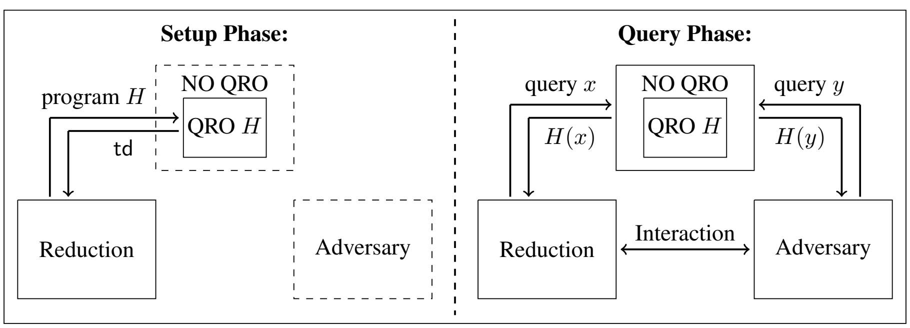

Figure 1: The figure shows two phases, during the setup phase a reduction can program the quantum random oracle and might receive a polynomial size trapdoor information td. During the query phase, the reduction and adversary can query the quantum random oracle. The reduction cannot observe queries made by the adversary or measure them. We omit the case of adaptive programming, in which the reduction can program H during the query phase.

Following [BDF+11], a query can be a superposition over the domain of the oracle. Upon receiving a query for quantum state $|\phi\rangle := \sum \alpha_{x,y}|x, y\rangle$ the oracle responds with $\sum \alpha_{x,y}|x, y + H(x)\rangle$. We remark that an adversary does not actually need to send his quantum state. It can locally evaluate oracle H as long as it does not violate the only black-box access requirement of the model. In the following, we will consider non-uniform adversaries. To provide

[3] To the best of our knowledge it is unclear how useful an adaptive progammability of a ROM is if queries cannot be observed. We are not aware of any protocol or primitive in which adaptive programming is necessary during the reduction but observing the adversarial random oracle queries is not.

security against such adversaries we assume that H is rerandomized using a key or a salt. In addition, when working with the NO QROM, we can leverage the Lemmas 2.1, 2.2, 2.4, 2.6, and 2.7 since they do not require observing any query. This is crucial to establish our results.

4 Extractable Non-Malleable Commitments in the NO QROM

We revisit the definition of the standard hash-based commitment scheme.

Definition 4.1 (Standard Hash-based Commitment)**.** *Let $\ell \in \mathbb{N}$, and let R/M be the randomness/message space. For a hash function $H : \mathsf{R} \times \mathsf{M} \to \{0,1\}^\ell$, the standard hash-based commitment scheme is defined as follows.*

$\mathsf{Com}(1^\kappa, \mathsf{m})$**:** *Sample $r \leftarrow \mathsf{R}$. Compute and output $\mathsf{c} := H(r, \mathsf{m})$, $\mathsf{o} := (r, \mathsf{m})$.*

$\mathsf{Open}(\mathsf{c}, \mathsf{o})$**:** *Parse $\mathsf{o} = (r, \mathsf{m})$ and output m if $\mathsf{c} = H(r, \mathsf{m})$ and otherwise output $\perp$.*

We now prove the computational and statistical binding properties with respect to different parameters of the commitment schemes defined above.

Lemma 4.2 (Binding)**.** *The standard hash-based commitment above is computationally (respectively, statistically) binding for $\ell \geq \omega(\log \kappa)$ (respectively $\ell \geq 2\log|\mathsf{M}| + 2\log|\mathsf{R}| + \omega(\log \kappa)$).*

Proof. We start with computationally binding. An unbounded algorithm $\mathcal{A}$ making at most q quantum queries to the random oracle H breaking the binding property would output a commitment c such that there exist two openings o_0 and o_1 with $\mathsf{o}_0 \neq \mathsf{o}_1$. This implies that $H(\mathsf{o}_0) = \mathsf{c} = H(\mathsf{o}_1)$ and thus breaking the collision-resistance of H. However from Lemma 2.1, the latter probability is bounded by $O(q^3/2^\ell)$ which is negligible for $\ell \geq \omega(\log \kappa)$.

We now consider the statistical binding property. The commitments are determined by the randomness r and message m. Thus there are at most $|\mathsf{M}| \cdot |\mathsf{R}|$ many commitments. Therefore, the probability that there exists an r_0, r_1, m_0 and m_1 such that it results in the same commitment is bounded by $|\mathsf{R}|^2 \cdot |\mathsf{M}|^2 \cdot 2^{-\ell}$ which is negligible for $\ell \geq 2\log|\mathsf{M}| + 2\log|\mathsf{R}| + \omega(\log \kappa)$. ☐

When we use random permutations instead of random functions, we get better bounds on ℓ for the case of statistical binding. In addition, since random permutations are indistinguishable from random functions all other properties such as extractability, hiding, and non-malleability still hold. When replacing the permutation with a degree $2q-1$ polynomial, we might lose statistical binding since there might be up to $2q-1$ preimages per output. Our extractor does this replacement and therefore unique extractability requires $\ell \geq \omega(\log \kappa)$ to prevent collisions of the $2q-1$ preimages with overwhelming probability.

Lemma 4.3 (Statistical Binding for Permutations)**.** *Let H be the hash function in Definition 4.1 and let H be defined as $H(r, \mathsf{m}) = P(r, \mathsf{m}) || H'(r, \mathsf{m})$ where P is a random permutation and $H' : \mathsf{R} \times \mathsf{M} \to \{0,1\}^{\ell'}$. Then, the standard hashed-based commitment is statistically binding.*

Proof. The proof is almost identical to the proof of Lemma 4.2. The difference is that we get a much better bound on preventing a collision than the birthday bound due to the definition of a permutation which does not have such collisions. Therefore, such a collision can only happen with respect to the oracle H'. However, the image of P uniquely defines r, m and therefore we can ignore collisions in the image of H'. ☐

We now consider extractability of the commitent scheme. We first adapt extractability for a commitment scheme to the NO QROM described in Section 3. We allow an extractor similar to a reduction to program H during the setup phase. In this process, the extractor obtains a trapdoor information td which allows it to extract the message from a commitment.

Definition 4.4 (Extractability in the NO QROM)**.** *We call a commitment scheme* online-extractable in the NO QROM *if there exists a PPT algorithm E which programs QRO H during the setup phase and might receive a polynomial length trapdoor information td within the process. During the query phase, E receives commitment c and outputs m, i.e., $\mathsf{m} \leftarrow \mathsf{E}(\mathsf{td}, \mathsf{c})$, such that there exists an opening o with $\mathsf{Open}(\mathsf{c}, \mathsf{o}) = \mathsf{m}$. Otherwise, E outputs $\perp$.*

We now present two extraction techniques for the standard hash-based commitment scheme in the NO QROM. Both techniques follow a similar approach, but they allow different parameter, security, and extraction probability trade-offs. In the first technique, at a high-level, the corresponding extractor simulates the QROs using polynomials over finite fields with a sufficiently large degree, thanks to Lemma 2.2, and then it utilizes an efficient *root-finding* algorithm over related polynomials to compute valid openings for a given commitment – *without* observing the queries made to the QROs.

We start with showing *perfect online-extractability* in the NO QROM based on finding roots of polynomials.

Theorem 4.5 (Extraction via Roots Finding)**.** *As per Definition 4.1, let H be modeled as a QRO with the structure $H(r,\mathsf{m}) = H'(r,\mathsf{m})||H''(r,\mathsf{m})$, where $H' : \mathsf{R}\times\mathsf{M} \to \mathsf{R}\times\mathsf{M}$, $H'' : \mathsf{R}\times\mathsf{M} \to \{0,1\}^{\ell'}$ are QROs such that $\ell' = \ell - \log|\mathsf{M}| - \log|\mathsf{R}|$. Then the standard hash-based commitment from Definition 4.1 is perfectly online-extractable in the NO QROM.*

Proof. We describe a PPT extractor E with respect to an adversary $\mathcal{A}$ which makes at most q queries to the QROs. In the setup phase, E replaces the true random oracle H' with an oracle f evaluating a uniformly random polynomial of degree $2q-1$ over the finite field $\mathbb{F}_{2^\nu}$, where $\{0,1\}^\nu = \mathsf{R}\times\mathsf{M}$. From Lemma 2.2, the oracle f is *perfectly* indistinguishable from the QRO H' in $\mathcal{A}$'s view. E retains the (polynomial sized) description of f as the trapdoor information td.

Upon receiving a commitment $\mathsf{c} = (\mathsf{c}_1,\mathsf{c}_2) = (H'(r,\mathsf{m}), H''(r,\mathsf{m}))$ from $\mathcal{A}$ in the query phase, E first computes a set of roots S of the polynomial $f(x) - \mathsf{c}_1$. This can be done efficiently using the algorithm in [Ben81]. Since the polynomial is of degree $2q-1$, there are at most $2q-1$ roots. For each of the roots (r,m), E makes a classical query to H'' and checks whether $H''(r,\mathsf{m}) = \mathsf{c}_2$. If there exists such a root (r,m), E picks one of them and outputs m as the result of its extraction, i.e., $\mathsf{m} \leftarrow \mathsf{E}(\mathsf{td},\mathsf{c})$. Otherwise, E returns $\perp$. It's not hard to see that when E outputs $\mathsf{m} \neq \perp$, then there exists an opening o such that $\mathsf{Open}(\mathsf{c},\mathsf{o}) = \mathsf{m}$, namely $\mathsf{o} = (r,\mathsf{m}) \in S$. On the other hand, when E outputs $\perp$, there exists no valid opening for c. $\square$

Note that the first approach comes with the disadvantage that extraction is possible if the commitment size at least matches the message plus randomness size. Our second approach requires much less overhead for the commitment size. However, it has the shortcoming that extraction needs superpolynomial space for a negligible distinguishability advantage between the normal and the extraction mode.

In the second approach, the extractor simulates the QROs using *small-range distributions* (described in Lemma 2.4) and then (efficiently) iterates over the small output space of the QROs in order to compute valid openings for a given commitment – again while not observing any queries made to the QROs. For this approach, we first define a "small range mode" which allows extraction. In the small range mode, we replace oracle access to H with oracle access to $\hat{H}_{\mathsf{E}.\eta}$, which is a special oracle since it outputs the message m and masks it with an element from the small range set SR_η. More precisely, we denote the oracle in extraction mode (with parameter η) with $\hat{H}_{\mathsf{E}.\eta} : \mathsf{R}\times\mathsf{M} \to \{0,1\}^\ell$ where $\ell \geq \log|\mathsf{M}| + \log\eta$ and for any $r \in \mathsf{R}$, $\mathsf{m} \in \mathsf{M}$, we set $\hat{H}_{\mathsf{E},\eta}(r,\mathsf{m}) := \mathsf{SR}_\eta(r,\mathsf{m}) + (\mathsf{m}||0^{\ell'})$ where $\ell' := \ell - \log|\mathsf{M}|$.

Lemma 4.6. *Let $\hat{H}_{\mathsf{E},\eta}$ be the oracle in extraction mode with parameter η, and let H be the oracle in the standard NO QROM mode. Then, for any unbounded distinguisher D making at most q queries,*

$$|\Pr[D^H = 1] - \Pr[D^{\hat{H}_{\mathsf{E},\eta}} = 1]| \leq \frac{14q^3}{\eta}.$$

Proof. Let $\tilde{H} : \mathsf{R}\times\mathsf{M} \to \{0,1\}^\ell$ be defined as $\tilde{H}(r,\mathsf{m}) := H(r,\mathsf{m}) + (\mathsf{m},0^{\ell'})$ for all $r \in \mathsf{R}$, $\mathsf{m} \in \mathsf{M}$, where H is the QRO. Due to the uniformity of $H(r,\mathsf{m})$, the oracles H and $\tilde{H}$ are identically distributed. By Lemma 2.4, we can replace $\hat{H}$ with SR_η and this can be distinguished at most with probability $14q^3/\eta$. $\square$

Theorem 4.7 (Extraction via Small Range Distributions)**.** *Let $H : \mathsf{R}\times\mathsf{M} \to \{0,1\}^\ell$ be modeled as a QRO and $\ell \geq \log|\mathsf{M}| + \log\eta$. Then the standard hash-based commitment from Definition 4.1 is perfectly online-extractable in the NO QROM extraction mode and E runs in time polynomial in η.*

Proof. Our extractor E is defined as follows. During the setup phase, E sets up the oracle such that it is in extraction mode, i.e., $\hat{H}_{\mathsf{E},\eta}$. E receives set $\mathbb{I}_\eta$ of SR_η as trapdoor information which has size at most η.

During the query phase, E receives a commitment $\mathsf{c} = (\mathsf{c}_1, \mathsf{c}_2) \in \mathsf{M} \times \{0,1\}^{\ell'}$. For any element $(\tilde{\mathsf{m}}, x) \in \mathbb{I}_\eta$, E checks whether $x = \mathsf{c}_2$. If this is the case, E outputs $\mathsf{m} = \mathsf{c}_1 - \tilde{\mathsf{m}}$. If no such x exists, E outputs $\perp$.

Since $|\{0,1\}^{\ell'}| \geq \eta = |\mathsf{SR}_\eta|$, E extracts the correct message and only outputs $\perp$ if c is not a valid commitment and therefore E is a correct extractor. □

After establishing the (computational and statistical) binding and (perfect online) extractability properties of the standard hash-based commitment scheme in the NO QROM, we turn our attention towards proving their respective computational hiding properties. As discussed in Section 2, it suffices to show their *non-malleability* in the NO QROM instead because non-malleable commitments are also computationally hiding. We prove that they are computationally hiding in the settings when the schemes are statistically (respectively, computationally) binding by showing that they satisfy concurrent (respectively, *weak* concurrent) non-malleability in the NO QROM.

Theorem 4.8 (Non-Malleability when Statistically Binding). *Let the standard hash-based commitment (Definition 4.1) be set up such that it is statistically binding. Then, it is ε-concurrent non-malleable with respect to commitments in the NO QROM for $\varepsilon \leq \mathsf{negl}$ as long as $\log |\mathsf{R}| \geq \omega(\log \kappa)$.*

Proof. We can use the approach of puncturing the random oracle and make the commitment to m independent of H and therefore uniform. Though there is one subtlety in the definition of non-malleable commitments. After the adversary sends its commitments, there is an exponential time routine that brute forces the commitments to extract the unique message. After the puncturing, it could happen that a commitment that was previously valid becomes invalid and instead of outputting the actual message, the brute force routine forwards $\perp$ to the distinguisher. Clearly, a distinguisher could then easily distinguish the punctured setting from the normal setting. Fortunately, for the standard hash-based commitment, the puncturing only affects a single commitment since we puncture H on point r, m which uniquely defines c. Moreover, if the adversary copies this commitment, the brute force routine forwards $\perp$ by default to the distinguisher so that it does not help to distinguish the punctured setting from the normal setting during the brute force routine.

We use a domain separation to define $H_{\hat{\mathsf{m}}}$ for message $\hat{\mathsf{m}} \in \mathsf{M}$ such that for all $r \in \mathsf{R}$, $H_{\hat{\mathsf{m}}}(r) := H(r, \hat{\mathsf{m}})$. We sample $\hat{r} \leftarrow \mathsf{R}$, $\hat{y} \leftarrow \{0,1\}^\ell$ and define $\hat{G}_{\hat{\mathsf{m}}}$ as follows. $\hat{G}_{\hat{\mathsf{m}}}(\hat{r}) := \hat{y}$. For all other $r \in \mathsf{R} \backslash \{\hat{r}\}$, we set $\hat{G}_{\hat{\mathsf{m}}}(r) := H_{\hat{\mathsf{m}}}(r)$.

To prove non-malleability, we define the following simple simulator. The simulator samples a random string $\hat{y} \leftarrow \{0,1\}^\ell$ and sends $\hat{y}$ to $\mathcal{A}$ as commitment. $\mathcal{A}$ then outputs commitments $\mathsf{c}_1, \ldots, \mathsf{c}_m$. For any $i \in [m]$ for which $\mathsf{c}_i = \hat{y}$, sim sets $\mathsf{m}_i := \perp$. The random variable $\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$ is generated from the view of $\mathcal{A}$ and the messages $\mathsf{m}_1, \ldots, \mathsf{m}_m$, where m_i is either $\perp$ or the unique message committed in c_i.

Afterwards, we use the puncturing technique to argue that the distinguisher cannot distinguish between $\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$ and $\mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \hat{m})$. The reduction uses D to distinguish between $\tilde{H}_{\hat{\mathsf{m}}} = H_{\hat{\mathsf{m}}}$ and $\tilde{H}_{\hat{\mathsf{m}}} = \hat{G}_{\hat{\mathsf{m}}}$. During the setup, the reduction programs H such that for a query $r, \hat{\mathsf{m}}$ it outputs $\tilde{H}_{\hat{\mathsf{m}}}(r)$. For all other messages $\mathsf{m} \in \mathsf{M} \setminus \{\hat{\mathsf{m}}\}$, the reduction does not change H. In addition, the reduction receives trapdoor information $\hat{y}$. During the query phase, the reduction sends $\hat{y}$ to $\mathcal{A}$ and uses $\mathcal{A}$'s view and commitments to define random variable X. If for a commitment we have $\mathsf{c}_i = \hat{y}$, it defines $\mathsf{m}_i := \perp$.

When $\tilde{H}_{\hat{\mathsf{m}}} = \hat{G}_{\hat{\mathsf{m}}}$, $\hat{y}$ is a valid (and the only) commitment for $\hat{\mathsf{m}}$ with randomness $\hat{r}$. In this case, $\mathsf{X} = \mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \hat{\mathsf{m}})$. When $\tilde{H}_{\hat{\mathsf{m}}} = H_{\hat{\mathsf{m}}}$, $\hat{y}$ is statistically uniform and independent of $\hat{\mathsf{m}}$. Moreover, due to the fact that the input $\hat{r}, \hat{\mathsf{m}}$ to $\hat{H}$ defines a unique commitment, the puncturing of point $\hat{r}$ for $H_{\hat{\mathsf{m}}}$ does not affect any commitment with $\mathsf{m} \neq \hat{\mathsf{m}}$ or $r \neq \hat{r}$. Therefore, during the exponential time brute force routine, there is no message m_i that gets invalidated (due to the puncturing) except for messages derived from $\hat{y}$ which are in any case set to $\perp$. Thus, in this case $\mathsf{X} = \mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$. When D distinguishes $\mathsf{mim}^{\mathcal{A}}_{\mathsf{com}}(z, \hat{\mathsf{m}})$ from $\mathsf{sim}^{\mathsf{S}}_{\mathsf{com}}(z)$ it implicitly distinguishes $H_{\hat{\mathsf{m}}}$ from $\hat{G}_{\hat{\mathsf{m}}}$ which is bounded by $4q\sqrt{2^{-\kappa}}$ by Lemma 2.7, where q is the number of NO QRO queries of D and $\mathcal{A}$. □

Theorem 4.9 (Weak Non-Malleability when Computationally Binding). *Let the standard hash-based commitment from Definition 4.1 be set up such that it is computationally binding. Then it is ε-weak-concurrent non-malleable with respect to commitments in the NO QROM for $\varepsilon \leq \mathsf{negl}$ as long as $\log |\mathsf{R}| \geq \omega(\log \kappa)$ and $|\mathsf{c}| \geq \omega(\log \kappa)$.*

Proof. The proof follows essentially from the proof of Theorem 4.8 and we can use exactly the same simulator. We outline the differences. A string $\hat{\mathsf{c}}$ received by $\mathcal{A}$ when generating wmim might be a commitment that has valid openings for multiple messages $\hat{\mathsf{m}}_1, \ldots, \hat{\mathsf{m}}_j$. Due to the definition of the experiment, $\hat{\mathsf{m}}_1, \ldots, \hat{\mathsf{m}}_j$ are not contained in wmim and replaced with $\perp$. The puncturing of $\hat{\mathsf{c}}$ again only affects $H(\hat{\mathsf{m}}, \hat{r})$ as before. Though there is another subtlety when considering the unbounded procedure that extracts the messages for the distinguisher. Using a uniformly random $\hat{y}$ instead of $\hat{\mathsf{c}}$ could lead to replacing a different set of messages with $\perp$ such that wmim and wsim are distinguishable. However, this is only possible when collisions occur. Due to $|\mathsf{c}| \geq \omega(\log \kappa)$ and Lemma 2.1, this happens at most with probability $q^3 2^{-\omega(\log \kappa)}$ which is negligible. $\square$

5 Signature Schemes in the NO QROM

In this section, we establish the post-quantum security of certain generic classes of signatures in the NO QROM. First we consider signature schemes whose proofs of security in the classical ROM involve so-called *history-free reductions* as defined in [BDF$^+$11]; examples of such schemes include the lattice-based signature in [GPV08] and *Fiat-Shamir* signatures analyzed in [KLS18]. Then we shift our attention to the well-known generic *full domain hash* (FDH) signatures of Bellare and Rogaway [BR93] in the NO QROM.

5.1 Signatures with History-Free Reductions

Boneh *et al.* [BDF$^+$11] showed that if the security proof of a signature scheme in the classical ROM follows a specific structure known as a *history-free reduction*, then the scheme is also provably secure in the QROM. At a high-level, in a history-free reduction, the responses to an adversary's random oracle queries are determined *independently* of the responses to previous queries. A more formal definition of a history-free reduction follows (taken from [BDF$^+$11]):

Definition 5.1 (History-Free Reductions). *A random oracle signature scheme $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ has a history-free reduction from a hard problem P if the proof of security uses a classical PPT adversary $\mathcal{A}$ against S^H to construct a classical PPT algorithm $\mathcal{B}$ to solve problem P such that:*

- *$\mathcal{B}$ contains four classical algorithms:* START, RAND^{H_c}, SIGN^{H_c} *and* FINISH^{H_c}*; the latter three algorithms have access to a shared classical random oracle H_c. These algorithms are used as follows:*
  - *Given an instance x for problem P, $\mathcal{B}$ first runs* START(x) *to get $(\mathsf{pk}, \mathsf{st})$ where pk is a public key of S^H and st is some private state to be used by $\mathcal{B}$. Then $\mathcal{B}$ simulates the standard CMA security game (Definition 2.12) with respect to S^H by first forwarding pk to $\mathcal{A}$.*
  - *When $\mathcal{A}$ makes a classical RO query $H(r)$, $\mathcal{B}$ responds with* RAND$^{H_c}(r, \mathsf{st})$. *Note here that* RAND^{H_c} *is only given the current query r as input, and in particular, is unaware of previous queries and responses.*
  - *When $\mathcal{A}$ makes a signature query $\mathsf{Sign}^H(\mathsf{sk}, \mathsf{m})$, where sk is the secret key corresponding to pk, $\mathcal{B}$ responds with* SIGN$^{H_c}(\mathsf{m}, \mathsf{st})$.
  - *When $\mathcal{A}$ outputs a forgery candidate (m, σ), $\mathcal{B}$ outputs* FINISH$^{H_c}(\mathsf{m}, \sigma, \mathsf{st})$.
- *There is an efficiently computable function* INSTANCE(pk) *which generates an instance x for problem P such that* START$(x) = (\mathsf{pk}, \mathsf{st})$ *for some st. We also need the following distribution of x to be negligibly close to the original distribution of x considered in problem P: first generate $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$ and compute $x =$* INSTANCE(pk).
- *Consider the classical oracle $O(r) =$* RAND$^{H_c}(r, \mathsf{st})$*, for a fixed st. Define the corresponding quantum oracle O_q which maps $|r\rangle |s\rangle \mapsto |r\rangle |s \oplus O(r)\rangle$. We require O_q to be (quantum) computationally indistinguishable from a truly random oracle.*
- SIGN^{H_c} *either generates a valid signature relative to the oracle $O(r) =$* RAND$^{H_c}(r, \mathsf{st})$ *with a distribution negligibly close to the correct signing algorithm, or it aborts (hence making $\mathcal{B}$ abort as well). The probability that none of $\mathcal{A}$'s signature queries result in an abort is non-negligible.*
- *If the output (m, σ) of $\mathcal{A}$ is a valid signature forgery with respect to the received public key pk and oracle $O(r) =$* RAND$^{H_c}(r, \mathsf{st})$*, then the output* FINISH$^{H_c}(\mathsf{m}, \sigma, \mathsf{st})$ *of B solves the problem P with respect to instance x with non-negligible probability.*

After defining history-free reductions for signature schemes, Boneh *et al.* proved a general lifting theorem from ROM security to QROM security for such reductions [BDF+11, Theorem 1]. In the following, we extend their lifting theorem to show that signature schemes with history-free reductions are in fact secure in the *weaker* NO QROM.

Theorem 5.2. *Let* $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ *be a random oracle signature scheme with a history-free reduction from a problem* P *assumed to be hard for polynomial-time quantum algorithms. Assuming that post-quantum one-way functions exist,* S^H *is post-quantum* EUF-CMA secure *when* H *is modeled in the NO QROM.*

The following proof essentially follows a similar strategy as the one by Boneh *et al.* for "history-free signatures" in the plain QROM [BDF+11, Theorem 1] (however we provide a sketch for the sake of completeness). In addition, we adapt their proof in our NO QROM framework when it comes to simulating the responses to an adversary's quantum random oracle queries in the reduction.

Proof Sketch. As per Definition 5.1, recall that the history-free reduction for signature $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ above involves the classical algorithms START, RAND, SIGN, FINISH, and INSTANCE. Towards a contradiction, assume there is a quantum PPT adversary $\mathcal{A}$ that breaks the EUF-CMA security of S^H with non-negligible probability ε. The proof proceeds by a sequence of game-hybrids. Namely, let G_0 be the standard CMA game with respect to S^H.

Now let the game G_1 be the following modification of G_0: after the challenger generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, it computes $x = \text{INSTANCE}(\mathsf{pk})$ and $(\mathsf{pk}, \mathsf{st}) \leftarrow \text{START}(x)$. Then instead of using a truly random oracle to answer $\mathcal{A}$'s quantum queries to H, the challenger uses the quantum oracle O_q which maps $|r\rangle\,|s\rangle \mapsto |r\rangle\,|s \oplus \text{RAND}^{H_c}(r, \mathsf{st})\rangle$; here H_c is a truly random quantum oracle which is not directly accessible to $\mathcal{A}$. From Definition 5.1, we have O_q to be quantum computationally indistinguishable from a truly random oracle. Hence, we have the winning probability of $\mathcal{A}$ in G_1 to be negligibly close to that in G_0.

Let G_2 be the following modification of G_1: instead of generating $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$ and computing $x = \text{INSTANCE}(\mathsf{pk})$, the challenger samples x from the *original* instance distribution with respect to problem P; it then uses the latter x to obtain $(\mathsf{pk}, \mathsf{st}) \leftarrow \text{START}(x)$ before forwarding pk to $\mathcal{A}$. Furthermore, when $\mathcal{A}$ makes a signature query on m, the challenger responds with $\text{SIGN}^{H_c}(\mathsf{m}, \mathsf{st})$. From the property of INSTANCE in Definition 5.1, we have the distributions of x in games G_1 and G_2 to be negligibly close. Also from the property of SIGN^{H_c}, we have with a non-negligible probability that all of $\mathcal{A}$'s signing queries are answered successfully (i.e., without aborting) with the corresponding signatures having a distribution negligibly close to the actual signatures in G_1. Hence as argued in the proof of [BDF+11, Theorem 1], it's not hard to see that $\mathcal{A}$'s winning probability in G_2 (i.e., probability of outputting a valid forgery) is non-negligible.

Finally let G_3 be the following modification of G_2: instead of using a truly random quantum oracle for evaluating H_c internally, the challenger uses a quantum-secure pseudorandom function PRF (Definition 2.11). Specifically, the challenger first samples a random PRF key k. Then it replaces H_c with the quantum oracle $|\mathsf{PRF}(k, \cdot)\rangle$ which maps $|r\rangle\,|s\rangle \mapsto |r\rangle\,|s \oplus \mathsf{PRF}(k, r)\rangle$. Because of the quantum-security of PRF, it's not hard to see that the winning probabilities of $\mathcal{A}$ in games G_2 and G_3 are negligibly close. Hence we have the latter probability to be non-negligible as well. Also note that quantum-secure pseudorandom functions can be constructed (in a black-box manner) from post-quantum one-way functions, as shown by Zhandry [Zha12a].

After defining games $\mathsf{G}_0 - \mathsf{G}_3$ with respect to adversary $\mathcal{A}$, we now construct a polynomial-time quantum algorithm $\mathcal{B}$ that solves the underlying hard problem P in the NO QROM with non-negligible probability. Upon receiving an instance x with respect to problem P, $\mathcal{B}$ computes $(\mathsf{pk}, \mathsf{st}) \leftarrow \text{START}(x)$. Then in the "setup phase" of the NO QROM (Section 3), $\mathcal{B}$ samples a random PRF key k and programs the quantum random oracle H as:

$$H(r) := \text{RAND}^{|\mathsf{PRF}(k,\cdot)\rangle}(r, \mathsf{st}),$$

as in game G_3. $\mathcal{B}$ also forwards pk to $\mathcal{A}$, and acts as the CMA-challenger in game G_3. Specifically in the "query phase" of the NO QROM:

- When $\mathcal{A}$ makes a signature query on message m, $\mathcal{B}$ responds with the value $\text{SIGN}^{|\mathsf{PRF}(k,\cdot)\rangle}(\mathsf{m}, \mathsf{st})$.
- When $\mathcal{A}$ returns a forgery candidate (m, σ), $\mathcal{B}$ outputs $\text{FINISH}^{|\mathsf{PRF}(k,\cdot)\rangle}(m, \sigma, \mathsf{st})$.

It's not hard to see that $\mathcal{B}$ perfectly simulates the game G_3 towards $\mathcal{A}$, while importantly, also executing a valid reduction in the NO QROM. This is because $\mathcal{B}$ never has to observe the quantum queries made by $\mathcal{A}$ to the random oracle H after the setup phase (also the above two steps in query phase can be seen as the "Interaction" in Figure 1). Now since we have the winning probability of $\mathcal{A}$ in G_3 to be non-negligible, it follows that the probability of $\mathcal{A}$ returning a valid forgery candidate (m, σ) to $\mathcal{B}$ in the above query phase is also non-negligible. So from the property of the FINISH algorithm in Definition 5.1, we note that the output $\text{FINISH}^{|\mathsf{PRF}(k,\cdot)\rangle}(m, \sigma, \mathsf{st})$ of $\mathcal{B}$ solves the problem P with respect to given instance x with a non-negligible probability. This contradicts our starting assumption that P is hard for polynomial-time quantum algorithms, which in turn implies the EUF-CMA security in the NO QROM. ☐

Following the results on history-free reductions [BDF+11], many works started devising "history-free versions" of classical ROM security proofs of important signature schemes to establish their post-quantum security in the QROM. Examples of such schemes include the lattice-based signature of [GPV08], as analyzed in [BDF+11], and Fiat-Shamir signatures as analyzed in [KLS18]. So a consequence of our lifting theorem (i.e., Theorem 5.2) above is that these classes of signature schemes are also provably secure in the weaker NO QROM, i.e., we explicitly establish that *weaker* heuristics – which do not require observing an adversary's quantum random oracle queries – are sufficient to prove post-quantum security of the aforementioned signature schemes.

5.2 FDH-based Signature Schemes

We first recall the definition of FDH signatures as follows.

Definition 5.3 (FDH Signatures)**.** *Let* $\mathsf{F} = (\mathsf{Gen}, \mathsf{f}, \mathsf{f}^{-1})$ *be a trapdoor permutation, and let* H *be a hash function that maps messages to the co-domain of* f. *Let* $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ *be a signature scheme where:*

- $\mathsf{Sign}^H(\mathsf{sk}, \mathsf{m}) = \mathsf{f}^{-1}(\mathsf{sk}, H(\mathsf{m}))$
- $\mathsf{Ver}^H(\mathsf{pk}, \mathsf{m}, \sigma) = \begin{cases} \mathsf{acc} & \text{if } \mathsf{f}(\mathsf{pk}, \sigma) = H(m) \\ \mathsf{rej} & \text{otherwise} \end{cases}$

In the classical setting, Bellare and Rogaway [BR93] proved the EUF-CMA security of FDH signatures in the *classical* ROM while relying on one-wayness of the underlying TDP. At a high level, in their proof (via a reduction), the "TDP adversary" $\mathcal{B}$ randomly guesses which of the random oracle queries the "signature adversary" $\mathcal{A}$ will use to produce a forgery with respect to the FDH scheme. $\mathcal{B}$ then *embeds* y into the response for this oracle query, and if the guess is correct and $\mathcal{A}$ produces a valid forgery, then $\mathcal{B}$ will be able to find a preimage for y.

However, as observed by Zhandry [Zha12b], the approach above will not work in the QROM setting because each of $\mathcal{A}$'s random oracle queries might be a superposition of exponentially many inputs; this makes it hard for $\mathcal{B}$ to meaningfully embed its challenge y into the oracle responses. Nevertheless, Zhandry [Zha12b] was able to overcome this barrier by introducing a class of oracle distributions called *Semi-Constant Distributions* (Definition 2.5) which allows for a specific random value to be embedded into a small but significant fraction of oracle inputs, while at the same time, ensuring that it is in some sense hard for a quantum algorithm to distinguish between this semi-constant oracle and a uniformly random oracle (Lemma 2.6). This allowed Zhandry to translate the above embedding-based argument of Bellare and Rogaway to the quantum setting in order to show the EUF-CMA security of FDH signatures in the plain QROM based on the one-wayness of the underlying TDP against *quantum* adversaries.

However, upon a closer inspection of Zhandry's proof, note that nowhere in the reduction is the "TDP adversary" $\mathcal{B}$ required to observe the "signature adversary" $\mathcal{A}$'s quantum queries to the random oracle. In other words, by adapting Zhandry's proof in [Zha12b], the FDH signature scheme can be shown to be EUF-CMA secure in the *weaker* heuristic model of NO QROM – while still relying on the (post-quantum) one-wayness of the underlying TDP – wherein $\mathcal{B}$ would still have to (non-adaptively) program the random oracle by replacing it with a semi-constant oracle in the *setup phase* (see Section 3).

Theorem 5.4. *Let* $\mathsf{F} = (\mathsf{Gen}, \mathsf{f}, \mathsf{f}^{-1})$ *be a (post-quantum) one-way TDP. Then the corresponding FDH signature scheme* $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ *is post-quantum* EUF-CMA secure *when* H *is modeled in the NO QROM.*

The proof below mirrors the one given by Zhandry [Zha12b] for FDH signatures in the plain QROM. Here we adapt his proof to fit within our NO QROM framework, as described in Section 3.

Proof Sketch. Towards a contradiction, assume there is a quantum PPT adversary $\mathcal{A}$ that breaks the FDH signature scheme $\mathsf{S}^H = (\mathsf{Gen}, \mathsf{Sign}^H, \mathsf{Ver}^H)$ with non-negligible probability ε. The proof proceeds by a sequence of hybrids. Let G_0 be the standard CMA game with respect to S^H. Namely, the challenger generates the pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$ and sends pk to $\mathcal{A}$. The adversary $\mathcal{A}$ can make *classical* signature queries on messages m_i to which the challenger responds with $\mathsf{Sign}^H(\mathsf{sk}, \mathsf{m}_i)$, and *quantum* hash queries to the oracle H. $\mathcal{A}$ wins if it produces a pair (m, σ) such that $\mathsf{m} \neq \mathsf{m}_i$ for all i and $\mathsf{Ver}^H(\mathsf{pk}, \mathsf{m}, \sigma) = \mathsf{acc}$. Also suppose $\mathcal{A}$ makes q_H hash queries and q_S signature queries.

Let $0 \leq \lambda \leq 1$ be a parameter to be chosen later, and let M be the message space of S^H. We now construct a subset $\mathcal{X} \subseteq \mathsf{M}$ as follows: for each $\mathsf{m} \in \mathsf{M}$, put $\mathsf{m} \in \mathcal{X}$ with probability λ. Now let the game G_1 be the same as G_0 except that we modify the winning conditions as follows: if $\mathcal{A}$ asks for a signature on message $\mathsf{m}_i \in \mathcal{X}$ or if $\mathcal{A}$ attempts to forge the signature for a message $\mathsf{m} \notin \mathcal{X}$, we abort G_1 and $\mathcal{A}$ loses; other than this, the winning condition in G_0 applies to G_1 as well. It is not hard to see that G_1 does not abort with probability at least $\lambda(1 - \lambda q_S)$. Therefore, $\mathcal{A}$ wins G_1 with probability at least $\lambda(1 - \lambda q_S)\varepsilon \geq \lambda\varepsilon - q_S\lambda^2$.

Let G_2 be the same as G_1 except that we reprogram the random oracle H (only) on inputs in $\mathcal{X}$ as follows: fix a uniformly random value y in the co-domain of f and set $H(x) := y$ for all $x \in \mathcal{X}$. We can see that the modified H is now an oracle with a λ-constant distribution (Definition 2.5). As argued by Zhandry in [Zha12b, Claim 1] (based on Lemma 2.6) we have that the probability $\mathcal{B}$ wins in G_2 is at least $(\lambda\varepsilon - p(q_H, q_S)\lambda^2)$ for some polynomial $p(\cdot, \cdot)$.

After defining the games $\mathsf{G}_0 - \mathsf{G}_2$ with respect to adversary $\mathcal{A}$, we now construct a quantum PPT adversary $\mathcal{B}$ that breaks the underlying TDP $\mathsf{F} = (\mathsf{Gen}, \mathsf{f}, \mathsf{f}^{-1})$ in the NO QROM as follows. $\mathcal{B}$ first samples a $2(q_H + q_S + 1)$-wise independent function $O_1(\cdot)$ that maps M to the domain of f. Note that in the games $\mathsf{G}_0 - \mathsf{G}_2$, at most $(q_H + q_S + 1)$ queries are made to the quantum oracle H (q_H quantum hash queries, q_S classical queries via the signature queries $\mathsf{Sign}^H(\mathsf{sk}, \mathsf{m}_i)$ and one classical query for checking $\mathcal{A}$'s forgery $\mathsf{Ver}^H(\mathsf{pk}, \mathsf{m}, \sigma)$). From Lemma 2.2, we have that $O_1(\cdot)$ is perfectly indistinguishable from a uniformly random oracle mapping M to the domain of f in the view of $\mathcal{A}$. Similarly, $\mathcal{B}$ simulates an oracle $O_2 : \mathsf{M} \to \{0, 1\}$ such that for each $\mathsf{m} \in \mathsf{M}$, $O_2(\mathsf{m}) = 1$ with probability λ as follows (taken from [Zha12b, Section 6]): $\mathcal{B}$ approximates λ by a rational number a/b, with b being a prime power, and constructs a $2(q_H + q_S + 1)$-wise independent function $\hat{O}_2$ with range $\{1, \ldots, b\}$; it then constructs $O_2(\cdot)$ as

$$O_2(\mathsf{m}) = \begin{cases} 1 & \text{if } \hat{O}_2(\mathsf{m}) \leq a \\ 0 & \text{otherwise.} \end{cases}$$

Finally, $\mathcal{B}$ on input (pk, y) – for which it is supposed to find a preimage with respect to F – proceeds in the "setup phase" of the NO QROM by programming the quantum random oracle H as:

$$H(\mathsf{m}) = \begin{cases} y & \text{if } O_2(\mathsf{m}) = 1 \\ \mathsf{f}(\mathsf{pk}, O_1(\mathsf{m})) & \text{otherwise.} \end{cases}$$

$\mathcal{B}$ also sends pk to $\mathcal{A}$, playing the role of challenger in the game G_2. In the "query phase":

- When $\mathcal{A}$ makes a signature query on message m_i, $\mathcal{B}$ computes $O_2(\mathsf{m}_i)$ and aborts if the result is 1. Otherwise, $\mathcal{B}$ returns the response $O_1(\mathsf{m}_i)$.
- When $\mathcal{A}$ returns a forgery candidate (m, σ), $\mathcal{B}$ checks if $O_2(\mathsf{m}) = 1$ and $\mathsf{f}(\mathsf{pk}, \sigma) = y$. If satisfied, $\mathcal{B}$ returns the preimage σ. Otherwise, it aborts.

$\mathcal{B}$ perfectly simulating the game G_2 towards $\mathcal{A}$, while at the same time, implementing a valid reduction in the NO QROM; note that $\mathcal{B}$ never has to observe the quantum hash queries made by $\mathcal{A}$ to oracle H, and the above two steps in the query phase can be seen as part of the "Interaction" in Figure 1. Hence, by applying a similar analysis as that in [Zha12b, Theorem 5.1], we have $\mathcal{B}$'s advantage in breaking the underlying TDP F to be at least the non-negligible quantity $\frac{\varepsilon^2}{4p(q_H, q_S)}$, when we set $\lambda = \frac{\varepsilon}{2p(q_H, q_S)}$. This shows that S^H is indeed quantum EUF-CMA secure in the NO QROM, given that F is a (post-quantum) one-way TDP. ∎

6 Hinting PRGs in the NO QROM

In this section, we describe a simple and efficient construction of a cryptographic primitive in the NO QROM called *hinting* PRG [KW19]. This primitive is useful towards constructing CCA-secure encryption systems as will be detailed below. A hinting PRG is essentially a PRG with a stronger security property. It takes an n bit input $s \in \{0,1\}^n$ and outputs $(n+1)\cdot\ell$ bits $y_0, y_1, \ldots, y_n$ (where each y_i is an ℓ-bit string) such that the following two distributions $(r_0, (r_{i,0}, r_{i,1})_{i\in[n]})$ are computationally indistinguishable: in the first distribution, $r_0 = y_0$, $r_{i,s_i} = y_i$ and $r_{i,1-s_i}$ is chosen uniformly from $\{0,1\}^\ell$ (where s_i is the i-th bit of s) for $i \in [n]$. In the second distribution, r_0, $r_{i,0}$ and $r_{i,1}$ are all chosen uniformly at random from $\{0,1\}^\ell$ for $i \in [n]$. Note that in the first distribution, the relative "placement" of pseudorandom values y_i (for $i \in [n]$) in the tuple $(r_{i,0}, r_{i,1})$ depends on the i-th bit of seed s; hence in some sense, the values $(r_{i,0}, r_{i,1})_{i\in[n]}$ give away a "hint" about the seed. More formally, hinting PRGs are defined as follows:

Definition 6.1 (Hinting PRGs). *A hinting PRG is a deterministic polynomial-time algorithm* G *with parameters* n*,* ℓ*, such that* G *takes as input* 1^κ*, an* n *bit string* s*, and outputs an* $(n+1)\cdot\ell$ *bit string* y*. Moreover, it satisfies the following property for any ppt adversary* $\mathcal{A}$*:*

$$|\Pr[\mathcal{A}((y_0^0, (y_{i,0}^0, y_{i,1}^0)_{i\in[n]})) = 1] - \Pr[\mathcal{A}((y_0^1, (y_{i,0}^1, y_{i,1}^1)_{i\in[n]})) = 1]| \le \mathsf{negl}.$$

where $s = (s_1, \ldots, s_n)$*,* y_0^1*,* $(y_{i,0}^1, y_{i,1}^1)_{i\in[n]}$ *and* $(y_{i,1-s_i}^0)_{i\in[n]}$ *are uniformly distributed whereas* $(y_0^0, (y_{1,s_1}^0, y_{n,s_n}^0)_{i\in[n]})$ *is the output of* $\mathsf{G}(1^\kappa, s)$ *and* $s = (s_1, \ldots, s_n) \leftarrow \{0,1\}^n$*.*

Let $G : \{0,1\}^n \to \{0,1\}^{(n+1)\cdot\ell}$ be a hash function, or alternatively, an *extendable output function*. Our main observation is that by modeling G as a random oracle in the NO QROM, we get the above hinting property from G "*for free*." It's worth noting that recently, the work of [AP22] realized hinting PRGs using a random oracle albeit in a the *classical* setting.

Theorem 6.2. *The function* $G : \{0,1\}^n \to \{0,1\}^{(n+1)\cdot\ell}$ *is a hinting PRG in the NO QROM.*

Proof. Consider any PPT adversary $\mathcal{A}$ that has quantum access to the random oracle G in the setup phase (Section 3) and gets as input $y^0 = (y_0^0, (y_{i,0}^0, y_{i,1}^0)_{i\in[n]})$ where for a uniformly random seed $s = (s_1, \ldots, s_n) \leftarrow \{0,1\}^n$, we have $G(s) = (y_0^0, y_{1,s_1}^0, \ldots, y_{n,s_n}^0)$ and $y_{i,1-s_i}^0 \leftarrow \{0,1\}^\ell\ \forall i \in [n]$. Now we replace G with another random oracle $H : \{0,1\}^n \to \{0,1\}^{(n+1)\cdot\ell}$ in the setup phase such that $\forall x \in \{0,1\}^n \setminus \{s\}$, $H(x) = G(x)$ and $H(s) = \hat{y}$ for a uniformly random and independent $\hat{y} \leftarrow \{0,1\}^{(n+1)\cdot\ell}$.

In the context of applying Lemma 2.7, it's not hard to see that we have $\Pr[\mathcal{A}^H(y^0) = 1] = \Pr[\mathcal{A}^G(y^1) = 1]$, where $y^1 = (y_0^1, (y_{i,0}^1, y_{i,1}^1)_{i\in[n]})$ with the uniformly random values $y_0^1 \leftarrow \{0,1\}^\ell$ and $y_{i,b}^1 \leftarrow \{0,1\}^\ell\ \forall i \in [n], b \in \{0,1\}$; because in both cases, $\mathcal{A}$'s inputs y^0, y^1 have the same (uniformly random) distribution and are independent with respect to the oracle outputs $H(s), G(s)$ respectively. Hence if $\mathcal{A}$ makes at most q quantum oracle queries, then from Lemma 2.7 we have

$$\begin{aligned}
&|\Pr[\mathcal{A}^H(y^0) = 1] - \Pr[\mathcal{A}^G(y^0) = 1]| \\
&= |\Pr[\mathcal{A}^G(y^1) = 1] - \Pr[\mathcal{A}^G(y^0) = 1]| \le 4\sqrt{\frac{q(q+1)}{2^n}} = \mathsf{negl}.
\end{aligned}$$

□

CCA-secure Encryption in the NO QROM. Hinting PRGs allow constructing CCA-secure PKE schemes, and more advanced primitives such as CCA-secure *attribute-based encryption* (ABE) or CCA-secure *one-sided predicate encryption* schemes, from their CPA-secure counterparts in a black-box manner [KW19].

Hence, by replacing the hinting PRG in the constructions of [KW19] with a standard hash function/extendable output function – later modeled as a random oracle – we obtain the above CCA-secure encryption systems in the NO QROM; we can follow the proof strategies used in [KW19] with respect to their black-box constructions, in conjunction with Lemma 6.2 above, to prove CCA security of corresponding constructions in the NO QROM in a relatively straightforward fashion. We leave it as an open question to obtain more efficient constructions of the above CCA-secure primitives in the NO QROM.

References

[AB13] Prabhanjan Ananth and Raghav Bhaskar. Non observability in the random oracle model. In Willy Susilo and Reza Reyhanitabar, editors, *ProvSec 2013*, volume 8209 of *LNCS*, pages 86–103. Springer, Heidelberg, October 2013.

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 269–295. Springer, Heidelberg, August 2019.

[AP22] Navid Alamati and Sikhar Patranabis. Cryptographic primitives with hinting property. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part I*, volume 13791 of *LNCS*, pages 33–62. Springer, Heidelberg, December 2022.

[BBO07] Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 535–552. Springer, Heidelberg, August 2007.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.

[Ben81] Michael Ben-Or. Probabilistic algorithms in finite fields. In *22nd FOCS*, pages 394–398. IEEE Computer Society Press, October 1981.

[BGR+15] Hai Brenner, Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. Fast non-malleable commitments. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *ACM CCS 2015*, pages 1048–1057. ACM Press, October 2015.

[BLS22] Nir Bitansky, Huijia Lin, and Omri Shmueli. Non-malleable commitments against quantum attacks. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 519–550. Springer, Heidelberg, May / June 2022.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Heidelberg, August 2013.

[CCH+19] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. Fiat-Shamir: from practice to theory. In Moses Charikar and Edith Cohen, editors, *51st ACM STOC*, pages 1082–1090. ACM Press, June 2019.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited (preliminary version). In *30th ACM STOC*, pages 209–218. ACM Press, May 1998.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *23rd ACM STOC*, pages 542–552. ACM Press, May 1991.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

[DFMS22a] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Efficient NIZKs and signatures from commit-and-open protocols in the QROM. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 729–757. Springer, Heidelberg, August 2022.

[DFMS22b] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 677–706. Springer, Heidelberg, May / June 2022.

[DIO98] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Non-interactive and non-malleable commitment. In *30th ACM STOC*, pages 141–150. ACM Press, May 1998.

[FF00] Marc Fischlin and Roger Fischlin. Efficient non-malleable commitment schemes. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 413–431. Springer, Heidelberg, August 2000.

[FLR+10] Marc Fischlin, Anja Lehmann, Thomas Ristenpart, Thomas Shrimpton, Martijn Stam, and Stefano Tessaro. Random oracles with(out) programmability. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 303–320. Springer, Heidelberg, December 2010.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Heidelberg, August 1999.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

[HHM22] Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Failing gracefully: Decryption failures and the fujisaki-okamoto transform. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 414–443. Springer, Heidelberg, December 2022.

[IR90] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. Springer, Heidelberg, August 1990.

[JZC+18] Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 96–125. Springer, Heidelberg, August 2018.

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Heidelberg, April / May 2018.

[KW19] Venkata Koppula and Brent Waters. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 671–700. Springer, Heidelberg, August 2019.

[LMS22] Alex Lombardi, Fermi Ma, and Nicholas Spooner. Post-quantum zero knowledge, revisited or: How to do quantum rewinding undetectably. In *63rd FOCS*, pages 851–859. IEEE Computer Society Press, October / November 2022.

[LPV08] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. Concurrent non-malleable commitments from any one-way function. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 571–588. Springer, Heidelberg, March 2008.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, August 2019.

[NC00] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[PR05] Rafael Pass and Alon Rosen. Concurrent non-malleable commitments. In *46th FOCS*, pages 563–572. IEEE Computer Society Press, October 2005.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, June 2000.

[PS19] Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 89–114. Springer, Heidelberg, August 2019.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016.

[Unr16] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 497–527. Springer, Heidelberg, May 2016.

[YZ21] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021*, volume 12697 of *LNCS*, pages 568–597. Springer, 2021.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, October 2012.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Inf. Comput.*, 15(7&8):557–567, 2015.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Heidelberg, August 2019.

[Zha22] Mark Zhandry. Augmented random oracles. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 35–65. Springer, Heidelberg, August 2022.