UNIVERSITY OF TARTU
Institute of Computer Science
Computer Science Curriculum

Reelika Tõnisson

Tighter post-quantum secure encryption schemes using semi-classical oracles

Master's Thesis (30 ECTS)

Supervisor: Dominique Peer Ghislain Unruh, PhD

Tartu 2019

Tighter post-quantum secure encryption schemes using semi-classical oracles

Abstract: The random oracle model (ROM) has been widely used for analyzing cryptographic schemes. In the real world, a quantum adversary equipped with a quantum computer can execute hash functions on an arbitrary superposition of inputs. Therefore, one needs to analyze the post-quantum security in the quantum random oracle model (QROM). Unfortunately, working in the QROM is quite difficult because many proof techniques in the ROM have no analogue in the QROM. A technique that can help solve this problem is the One-Way to Hiding (O2H) Theorem, which was first proven in 2015 by Unruh. In 2018, Ambainis, Hamburg and Unruh presented an improved version of the O2H Theorem which uses so called semi-classical oracles and has higher flexibility and tighter bounds. This improvement of the O2H Theorem should allow us to derive better security bounds for most schemes that used the old version. We take one paper that used the old version of the O2H Theorem to prove the security of different schemes in the QROM and give new proofs using semi-classical oracles.

Keywords: Post-quantum cryptography, random oracle model, public-key encryption, semi-classical oracles

CERCS: P170 - Computer science, numerical analysis, systems, control

Tihedamad postkvant turvalised krüpteerimisprotokollid poolklassikaliste oraaklite abil

Lühikokkuvõte: Krüpteerimisprotokollide analüüsimiseks kasutatakse tihti juhusliku oraakli mudelit (JOM), aga postkvant turvaliste protokollide analüüs tuleb läbi viia kvant juhusliku oraakli mudelis (KJOM). Kuna paljudel tõestamise tehnikatel ei ole kvant juhusliku oraakli mudelis analoogi, on KJOMis raske töötada. Seda probleemi aitab lahendada *One-Way to Hiding* (O2H) Teoreem, mille Unruh tõestas 2015. aastal. Ambainis, Hamburg ja Unruh esitasid teoreemi täiustatud versiooni 2018. aastal. See kasutab poolklassikalisi oraakleid, millel on suurem paindlikkus ja tihedamad piirid. Täiustatud versioon võimaldab tugevdada kõigi protokollide turvalisust, mis kasutasid vana versiooni. Me võtame ühe artikli, kus kasutati vana O2H Teoreemi versiooni, ja tõestame protokollide turvalisuse uuesti kasutades poolklassikalisi oraakleid.

Võtmesõnad: Postkvantkrüptograafia, juhusliku oraakli mudel, avaliku võtme krüptograafia, poolklassikalised oraaklid

CERCS: P170 - Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Contents

1 Introduction

The random oracle model (ROM) has been widely used for analyzing cryptographic schemes. In the random oracle model, instead of using a hash function $H : M \to N$, we model the hash function as a uniformly randomly chosen function out of the space of all functions from M to N. Generic constructions for an efficient IND-CCA-secure KEM in the ROM have renewed interest in the post quantum setting. In the real world, a quantum adversary equipped with a quantum computer can execute hash functions on an arbitrary superposition of inputs [JZM19a]. Therefore, one needs to analyze the post-quantum security in the quantum random oracle model (QROM). In the quantum random oracle model, quantum adversaries are given quantum access to the random oracles and classical access to all other oracles. Unfortunately, working in the QROM is quite difficult because many proof techniques in the ROM have no analogue in the QROM [Bon+11].

A technique that can help solve this problem is One-Way to Hiding (O2H) Theorem, which was first proven by Unruh [Unr15b]. Since the O2H Theorem gives a generic reduction from a hiding-style property to a one-wayness-style property, the Theorem was used in many security proofs after its first release. In 2018, Ambainis, Hamburg and Unruh [AHU19] presented an improved version of the O2H Theorem which uses so called semi-classical oracles (see subsection 3.2.1) and has higher flexibility and tighter bounds.

The improvement of the O2H Theorem should allow us to derive better security bounds for most schemes that used the old version. In addition to explaining the improved version of the Theorem, Ambainis et al. [AHU19] showed the advantage gained by the new version in a *Quantum Security of the Fujisaki-Okamoto and OAEP Transforms* [TU16]. Similar security proof improvements were later made by Hövelmanns et al. [HKSU18] and Jiang et al. [JZM19a]. We take one more paper [HHK17] that used the old version of the O2H Theorem to prove the security of different schemes in the QROM and give new proofs using semi-classical oracles. We distinguish query number and query depth and give proofs with different assumptions about the underlying public key encryption scheme to get better bounds.

In the second section we give an overview of techniques and definitions that we use. In the third section we introduce the original One-Way to Hiding Theorem, define semi-classical oracles and show the improved version of the O2H Theorem. Subsection 3.3 focuses on the impact of the O2H Theorem to existing cryptosystems. In section 4 we define three transformations and prove the security of these transformations in the quantum random oracle model using the improved version of the O2H Theorem.

2 Background

In this section we give an overview of techniques and definitions that we are going to use. We expect the reader to have some knowledge of cryptography and quantum computing. Since we work with theorems from different authors, we need to fix one notion that we use throughout this thesis to not confuse the reader. For basics of quantum computing, we refer to a standard textbook such as [NC00].

For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$. For a set S, denote the cardinality of set S by $|S|$. For a finite set S, we denote the sampling of a uniformly random element x by $x \overset{\$}{\leftarrow} S$ and we denote the sampling according to some distribution $\mathcal{D}$ by $x \leftarrow \mathcal{D}$. By $[\![B]\!]$ we denote the bit that is 1 if the boolean statement B is true, and otherwise 0. For a polynomial $p(X)$, $\mathsf{Roots}(p)$ denotes the set of (complex) roots of p.

Algorithms. We denote the deterministic computation of an algorithm A on input x by $y := A(x)$ and the probabilistic computation by $y \leftarrow A(x)$. We denote algorithms with access to an oracle $\mathcal{O}$ by $A^{\mathcal{O}}$.

Quantum computing. A quantum accessible oracle $\mathcal{O}$ for a function $f : X \to Y$ is modelled as a unitary transformation U_f operating on two registers: an input register Q and an output register R (with space $\mathbb{C}^X$ and $\mathbb{C}^Y$ respectively), where $U_f : |q, r\rangle \mapsto |q, r \oplus f(x)\rangle$. Here $\oplus$ is a involutive group operation like XOR for a set of bitstrings.

A quantum oracle algorithm can perform classical and quantum computations, and query classical and/or quantum-accessible oracles. We allow an oracle algorithm A to perform oracle queries in parallel. We say that A is a q-query algorithm if it performs at most q oracle queries (counting parallel queries as separate queries), and has query depth d if it invokes the oracle at most d times (counting parallel queries as one query). For example, if A performs 4 parallel queries followed by 3 parallel queries, we have $q = 7$ and $d = 2$.

2.1 Security

The notion of indistinguishability against chosen-cicphertext attacks ($\mathsf{IND\text{-}CCA}$) is widely known as the standard security notion for asymmetric encryption schemes. Intuitively, $\mathsf{IND\text{-}CCA}$ security requires that no efficient adversary, who has access to decryption oracle, can recognize which of the two messages was encrypted in a given ciphertext, even if the adversary chooses the candidate messages himself. In a similar but weaker notion of indistinguishability against chosen-plaintext attacks ($\mathsf{IND\text{-}CPA}$), adversary is not given access to a decryption oracle. [HHK17]

IND-CCA is usually the desired notion of security. Unfortunately, the security is often much more difficult to prove than IND-CPA security for example. Thus, multiple transformations have been suggested for turning a weaker public-key encryption (PKE) scheme into an IND-CCA one. For example, Fujisaki and Okamoto [FO13] combined a one-way (OW-CPA) secure asymmetric encryption scheme with a one-time secure symmetric encryption scheme. OW-CPA security requires that no efficient adversary can find the encrypted message based on only the ciphertext and public key. The resulting hybrid scheme was IND-CCA secure in the random oracle model (see below).

Okamoto and Pointcheval [OP01] and Coron et al. [Cor+02] also proposed two more generic transformations that were considerably simpler. These however required the underlying asymmetric scheme to be one-way against plaintext checking attacks (OW-PCA), that is a non-standard security notion that provides the adversary with a plaintext checking oracle $Pco(c, m)$. Pco returns 1 if and only if decryption of ciphertext c yields the original message m.

Although many generic transformations for reaching IND-CCA security (or some other required security) have been proposed, using newer techniques may give tighter security reductions. We call a security reduction non-tight in the random oracle model if it loses a factor q_{G} (the number of random oracle queries). For example, the security reduction FO transformation in [FO13] is not tight and this results in considerably less efficient schemes.

2.2 Random oracle model

In many cases, the security of cryptosystems that use hash functions is very difficult or even impossible to prove based on simple assumptions about the hash function (such as collision-resistance). Instead, we would like to use the fact that a hash function behaves like a totally random function. This is called analyzing protocols in the Random Oracle Model (ROM). So, instead of using a hash function $H : M \to N$, we model the hash function as a uniformly randomly chosen function out of the space of all functions from M to N. This randomly chosen function is called a random oracle. Using a ROM as a proof technique in a cryptographic setting was first introduced in [BR93].

Since many existing public-key systems are proven insecure in the quantum setting, the interest in post-quantum secure cryptosystems has increased. Boneh et al. [Bon+11] state that to prove post-quantum security one needs to prove security in the quantum-accessible random oracle model (QROM). That is a model where the adversary can query the random oracle with quantum state.

If the adversary has *classical* access to the random oracle, the adversary is given oracle access to a random hash function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ and it can learn the value $\mathcal{O}(x)$ only by querying the oracle $\mathcal{O}$ at the classical state x. However, in a concrete system, the random oracle is replaced with a concrete hash function. This enables a quantum attacker to evaluate this hash function. Therefore, in the QROM, the adversary is allowed to evaluate the random oracle "in superposition". This means that the adversary can submit quantum sates $|\varphi\rangle = \sum |x, y\rangle$ to the oracle $\mathcal{O}$ and receive the evaluated state $\sum |x, y \oplus \mathcal{O}(x)\rangle$. This is called a *quamtum(-accessible) random oracle model.* [Bon+11]

While quantum adversaries are given quantum access to the random oracles involved, access to all other oracles (e.g., plaintext checking or decapsulation oracles) remains classical [HHK17].

2.3 Public-key encryption

A public-key encryption scheme $\mathsf{PKE} = (Gen, Enc, Dec)$ consists of three algorithms and a finite message space $\mathcal{M}$. The message space could be infinite in general, but in we consider only finite message spaces. The key generation algorithm Gen outputs a key pair (pk, sk). The encryption algorithm Enc outputs an encryption $c \leftarrow Enc(pk, m)$ of m under the public key pk. The decryption algorithm Dec outputs either a message $m = Dec(sk, c) \in M$ or a special symbol $\perp \notin M$ to indicate that c is not a valid ciphertext. [HHK17]

```
GAME COR
$(pk, sk) \leftarrow Gen$
$m \leftarrow A(sk, pk)$
$c \leftarrow Enc(pk, m)$
return $[\![Dec(sk, c) \neq m]\!]$
```

```
GAME COR-RO
$(pk, sk) \leftarrow Gen$
$m \leftarrow A^G(sk, pk)$
$c \leftarrow Enc(pk, m)$
return $[\![Dec(sk, c) \neq m]\!]$
```

```
GAME COR-QRO
$(pk, sk) \leftarrow Gen$
$m \leftarrow A^{\mathsf{H}}(sk, pk)$
$c \leftarrow Enc(pk, m)$
return $[\![Dec(sk, c) \neq m]\!]$
```

Figure 1: Correctness games COR for PKE in the standard model, COR-RO for PKE defined relative to a random oracle G and COR-QRO for PKE defined relative to a quantum random oracle H.

The δ-correctness of a public-key encryption scheme PKE means, that for all (possibly unbounded) adversaries A,

$$\Pr[\mathsf{COR}^A_{\mathsf{PKE}} \Rightarrow 1\,] \leq \delta.$$

The correctness game COR is defined in Figure 1.

If PKE is defined relative to a random oracle G, then the correctness bound might depend on the number of queries to G. We call a public-key encryption scheme PKE $\delta(g_{\mathsf{G}})$-correct in the random oracle model if for all (possibly unbounded) adversaries A, making at most q_{G} queries to the random oracle G,

$$\Pr[\mathsf{COR}^{A}_{\mathsf{PKE}} \Rightarrow 1\,] \leq \delta(g_{\mathsf{G}}).$$

The correctness game $\mathsf{COR\text{-}RO}$ is defined in Figure 1.

Similarly, if $\mathsf{PKE} = \mathsf{PKE}^{\mathsf{H}}$ is defined relative to a quantum random oracle H, then the correctness bound might also depend on the number of queries to H. We call a public-key encryption scheme PKE in the quantum random oracle model $\delta(g_{\mathsf{H}})$-correct if for all (possibly unbounded) adversaries A, making at most q_{H} queries to the quantum random oracle H,

$$\Pr[\mathsf{COR} - \mathsf{QRO}^{A}_{\mathsf{PKE}} \Rightarrow 1\,] \leq \delta(g_{\mathsf{H}}).$$

The correctness game $\mathsf{COR\text{-}QRO}$ is also defined in Figure 1. [HHK17]

Security. We also define security notions for public-key encryption. Definitions are adapted from [HHK17].

First four security notions for public-key encryption are:

- $\mathsf{OW\text{-}CPA}$ stands for one-wayness under chosen plaintext attacks. $\mathsf{OW\text{-}CPA}$ security requires that no efficient adversary can find the encrypted message based on only the ciphertext and public key.

- $\mathsf{OW\text{-}PCA}$ stands for one-wayness under plaintext checking attacks. $\mathsf{OW\text{-}PCA}$ is a non-standard security notion that provides the adversary with a plaintext checking oracle $Pco(c, m)$. Pco returns 1 if and only if decryption of ciphertext c yields the original message m.

- $\mathsf{OW\text{-}VA}$ stands for one-wayness under validity checking attacks. $\mathsf{OW\text{-}VA}$ is a non-standard security notion that provides the adversary with a validity checking oracle $Cvo(c)$. Cvo returns 1 if and only if decryption of ciphertext c yields a valid message (that is $m \in \mathcal{M}$).

- $\mathsf{OW\text{-}PCVA}$ stands for one-wayness under plaintext and validity checking attacks. $\mathsf{OW\text{-}PCVA}$ is a non-standard security notion that provides the adversary with both a plaintext checking oracle $Pco(c, m)$ and a validity checking oracle $Cvo(c)$.

```
GAME OW-ATK
  $(pk, sk) \leftarrow Gen$
  $m^* \leftarrow \mathcal{M}$
  $c^* \leftarrow Enc(pk, m)$
  $m' \leftarrow A^{\mathcal{O}_{\mathsf{ATK}}}(pk, c^*)$
  return $Pco(m', c^*)$

$Pco(m \in \mathcal{M}, c)$
  return $[\![Dec(sk, c) = m]\!]$

$Cvo(c \neq c^*)$
  $m := Dec(sk, c)$
  return $[\![m \in \mathcal{M}]\!]$
```

Figure 2: Games OW-ATK for PKE, $\mathcal{O}_{\mathsf{ATK}}$ is defined in Definition 2.1.

Definition 2.1. *(*OW-ATK *for* PKE*). Let* PKE $= (Gen, Enc, Dec)$ *be a public-key encryption scheme with message space $\mathcal{M}$. For* ATK $\in \{$CPA, PCA, VA, PCVA$\}$*, we define* OW-ATK *games as in Figure 2, where*

$$\mathcal{O}_{\mathsf{ATK}} := \begin{cases} - & \mathsf{ATK} = \mathsf{CPA} \\ Pco(\cdot,\cdot) & \mathsf{ATK} = \mathsf{PCA} \\ Cvo(\cdot) & \mathsf{ATK} = \mathsf{VA} \\ Pco(\cdot,\cdot),\, Cvo(\cdot) & \mathsf{ATK} = \mathsf{PCVA} \end{cases},$$

We define the OW-ATK *advantage function of an adversary A against* PKE *as*

$$Adv^{\mathsf{OW\text{-}ATK}}_{\mathsf{PKE}}(A) := Pr[\mathsf{OW\text{-}ATK}^{A}_{\mathsf{PKE}} \Rightarrow 1].$$

The next security notion is indistinguishability under chosen plaintext attacks (IND-CPA). Intuitively, IND-CPA security requires that no efficient adversary can recognize which of the two messages was encrypted in a given ciphertext, even if the adversary chooses the candidate messages himself.

```
GAME IND-CPA
  $(pk, sk) \leftarrow Gen$
  $b \xleftarrow{\$} \{0,1\}$
  $(m_0^*, m_1^*, st) \leftarrow A_1(pk)$
  $c^* \leftarrow Enc(pk, m_b^*)$
  $b' \leftarrow A_2(pk, c^*, st)$
  return $[\![b' = b]\!]$

GAME IND-CCA
  $(pk, sk) \leftarrow Gen$
  $b \xleftarrow{\$} \{0,1\}$
  $(K_0^*, c^*) \leftarrow Encaps(pk)$
  $K_1^* \xleftarrow{\$} \mathcal{K}$
  $b' \leftarrow A^{Decaps}(c^*, K_b^*)$
  return $[\![b' = b]\!]$

$Decaps(c \neq c^*)$
  $K := Decaps(sk, c)$
  return $K$
```

Figure 3: Games IND-CPA for PKE and IND-CCA for KEM.

Definition 2.2. *(*$\mathsf{IND\text{-}CPA}$ *for* PKE*). Let* $\mathsf{PKE} = (Gen, Enc, Dec)$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. We define* $\mathsf{IND\text{-}CPA}$ *game as in Figure 3, and the* $\mathsf{IND\text{-}CPA}$ *advantage function of an adversary* $A = (A_1, A_2)$ *against* PKE *(s.t.* A_2 *has binary output) as*

$$Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(A) := \left| Pr[\mathsf{IND\text{-}CPA}^{A} \Rightarrow 1] - \frac{1}{2} \right|$$

It is well known that $\mathsf{IND\text{-}CPA}$ security of PKE (with sufficiently large message space) implies its $\mathsf{OW\text{-}CPA}$ security. This is summarized in the following lemma from [HHK17]:

Lemma 2.1. *For any adversary* B *there exists and adcersary* A *with the same running time as* B *such that*

$$Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(B) \leq Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(A) + \frac{1}{|\mathcal{M}|}.$$

2.4 Key encapsulation mechanism (KEM)

A key encapsulation mechanism is a probabilistic algorithm that produces a random symmetric key and an asymmetric encryption of that key. KEMs are useful because any $\mathsf{IND\text{-}CCA}$ secure KEM can be combined with any chosen-ciphertext secure symmetric encryption scheme to obtain a $\mathsf{IND\text{-}CCA}$ secure public-key encryption scheme [CS98]. Since KEMs are efficient and versatile, in practice one often works with hybrid encryption schemes derived from a KEM.

A key encapsulation mechanism $\mathsf{KEM} = (Gen, Encaps, Decaps)$ consists of three algorithms. The key generation algorithm Gen outputs a key pair (pk, sk), here pk also defines the finite key space $\mathcal{K}$. The encapsulation algorithm $Encaps(pk)$ outputs a tuple (K, c), where c is said to be the encapsulation of key $K \in \mathcal{K}$. The deterministic decapsulation algorithm $Decaps(sk, c)$ outputs either a key $K = Decaps(sk, c) \in \mathcal{K}$ or a special symbol $\perp \notin \mathcal{K}$ to indicate that c is not a valid encapsulation. [HHK17]

The next security notion is indistinguishability under chosen ciphertext attacks ($\mathsf{IND\text{-}CCA}$). Intuitively, $\mathsf{IND\text{-}CCA}$ security requires that no efficient adversary, who has access to decryption oracle, can recognize which of the two messages was encrypted in a given ciphertext, even if the adversary chooses the candidate messages himself.

Definition 2.3. *(*IND-CCA *for* KEM*). Let* KEM $= (Gen, Encaps, Decaps)$ *be a key encapsulation mechanism with key space* $\mathcal{K}$*. We define* IND-CCA *game as in Figure 3, and the* IND-CCA *advantage function of an adversary* A *against* KEM *as*

$$Adv_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(A) := \left| \textit{Pr}[\mathsf{IND\text{-}CCA}^{A} \Rightarrow 1] - \frac{1}{2} \right|.$$

3 One-Way to Hiding Theorem

The random oracle model has been widely used for analyzing cryptographic schemes. Generic constructions for an efficient IND-CCA-secure KEM in the ROM like in [HHK17] have renewed interest in the post quantum setting. In the real world, a quantum adversary equipped with a quantum computer can execute hash functions on an arbitrary superposition of inputs [JZM19a]. Therefore, one needs to analyze the post-quantum security in the quantum random oracle model (QROM), first introduced by Boneh et al. [Bon+11].

Unfortunately, working in the QROM is quite difficult because many proof techniques in the ROM have no analogue in the QROM [Bon+11]. One example of such technique is programming of the random oracle, where we run the adversary with access to a random oracle but change the answer to certain queries during the execution. Here, the proof goes through if the adversary does not notice the programming. This is achieved by showing that the probability of changing a queried value is negligible. But in the quantum setting the adversary could query the superposition of all inputs in the first query. Now the proof would not go through because programming would change a value that the adversary already queried.

A technique that can solve this problem is the One-Way to Hiding (O2H) Theorem, which was first proven by Unruh [Unr15b]. Since the O2H Theorem gives a generic reduction from a hiding-style property to a one-wayness-style property, the theorem was used in many security proofs after its first release. In 2018, Ambainis, Hamburg and Unruh [AHU19] presented an improved version of the O2H Theorem that has higher flexibility and tighter bounds.

3.1 Original O2H Theorem

Unruh's "one-way to hiding" (O2H) Theorem from [Unr15b] is used in most post-quantum security analyses. The O2H Theorem was first used to prove that a timed-release encryption that is (revocably) one-way can be transformed it into one that is (revocably) hiding in the random oracle model [Unr15b]. The theorem was given as follows:

Theorem 3.1 (One-way to hiding from [Unr15b]). *Let $H : \{0,1\}^n \to \{0,1\}^m$ be a random oracle. Consider an algorithm A that makes at most q oracle queries. Let $B^H(x)$ do the following: pick $i \xleftarrow{\$} \{1,\dots,q\}$ and $y \xleftarrow{\$} \{0,1\}^m$, run $A^H(x,y)$ until (just before) the i-th query, measure the argument of the query in the computational basis,* *output the outcome. Let*

$$\begin{aligned}
&P_A^1 := \Pr[b' = 1 : x \leftarrow \{0,1\}^n, b' \leftarrow A^H(x, H(x))] \\
&P_A^2 := \Pr[b' = 1 : x \leftarrow \{0,1\}^n, y \leftarrow \{0,1\}^m, b' \leftarrow A^H(x, y)] \\
&P_B := \Pr[x = x' : x \leftarrow \{0,1\}^n, x' \leftarrow B^H(x)]
\end{aligned} \tag{1}$$

Then $|P_A^1 - P_A^2| \leq 2q\sqrt{P_B}$.

Here, $|P_A^1 - P_A^2|$ shows the probability that the adversary distinguishes between the original oracle and the reprogrammed oracle. On the other hand, P_B shows the probability that the adversary guesses the location where the oracle was reprogrammed. This type of game is often called ”guessing game“.

3.2 New approach

In 2018, Ambainis, Hamburg and Unruh [AHU19] presented an improved version of the O2H Theorem. This improves the theorem in many aspects:

- **Non-uniform random oracles.** Instead of a uniformly random function, any distribution of oracles is allowed.
- **Multiple reprogrammed points.** Instead of allowing to reprogram only a single point, an entire set S of positions can be reprogrammed.
- **Arbitrary joint distributions.** The distribution of reprogrammed locations and of the adversary’s input can be arbitrarily correlated with the distribution of the random oracle.
- **Tighter bounds.** Theorem gives better bounds compared to the original one.
- **Query depth.** Theorem distinguishes between the number of queries q and query depth d.

3.2.1 Semi-classical oracles

One major difference from the original O2H theorem is the use of ”semi-classical oracles“. We know that quantum oracles do not measure their input or output, but classical oracles measure everything. Semi-classical oracles [AHU19] are defined to only measure the input. Formally, a semi-classical oracle $\mathcal{O}_f^{SC}$ for a function $f : X \rightarrow Y$ is queried with two registers: an input register Q and an output register R (with space $\mathbb{C}^X$ and $\mathbb{C}^Y$ respectively).

When the oracle is queried with a value $|x\rangle$ in Q, the oracle performs a measurement of $f(x)$ and initializes the R register to $|y\rangle$ for the measured y. In the paper by Ambainis et al. [AHU19], f is always the indicator function f_S for a set S. This means: $f_s(x) = 1$ if $x \in S$ and $f_s(x) = 0$ if $x \notin S$. Let us call a semi-classical oracle with this index function $\mathcal{O}_S^{SC}$.

Define event Find as follows: $\mathcal{O}_S^{SC}$ returns $|1\rangle$ during the execution of a quantum algorithm $A^{\mathcal{O}_S^{SC}}$. This event is called Find because if it occurs during the execution, the simulator could stop and measure the input register Q to "find" an element $x \in S$.

If $H : X \to Y$ is some other quantum-accessible oracle, $H \setminus S$ ("H punctured on S") is defined as an oracle which on input x first queries $\mathcal{O}_S^{SC}(x)$ and then $H(x)$. It is called "puncturing" because when Find doesn't occur, the outcome of $A^{H\setminus S}$ is independent of $H(x)$ for all $x \in S$, as shown in the following lemma.

Lemma 3.1 (from [AHU19]). *Let $S \subseteq X$ be random. Let $G, H : X \to Y$ be random functions satisfying $\forall x \notin S : G(x) = H(x)$. Let z be a random bitstring. (S, G, H, z may have arbitrary joint distribution.)*

Let A be a quantum oracle algorithm (not neccesarily unitary).

Let E be an arbitrary (classical) event.

Then

$$\Pr[E \wedge \neg\mathsf{Find} : x \leftarrow A^{H\setminus S}(z)] = \Pr[E \wedge \neg\mathsf{Find} : x \leftarrow A^{G\setminus S}(z)].$$

3.2.2 Semi-classical O2H Theorem

Semi-classical oracles allow us to split the original O2H Theorem into two parts. The first part shows how much adversary's behavior changes when a random oracle is punctured on S:

Theorem 3.2 (Semi-classical O2H from [AHU19]). *Let $S \subseteq X$ be random. Let $G, H : X \to Y$ be random functions satisfying $\forall x \notin S : G(x) = H(x)$. Let z be a random bitstring. (S, G, H, z may have arbitrary joint distribution.)*

Let A be an oracle algorithm of query depth d (not necessarily unitary).

Let

$$\begin{aligned} P_{\mathit{left}} &:= \Pr[b = 1 : b \leftarrow A^H(z)] \\ P_{\mathit{right}} &:= \Pr[b = 1 : b \leftarrow A^G(z)] \\ P_{\mathit{find}} &:= \Pr[\mathsf{Find} : A^{G\setminus S}(z)] = \Pr[\mathsf{Find} : A^{H\setminus S}(z)] \end{aligned} \tag{2}$$

Then

$$|P_{\mathit{left}} - P_{\mathit{right}}| \leq 2\sqrt{(d+1)\cdot P_{\mathit{find}}} \quad \textit{and} \quad |\sqrt{P_{\mathit{left}}} - \sqrt{P_{\mathit{right}}}| \leq 2\sqrt{(d+1)\cdot P_{\mathit{find}}}.$$

The theorem also holds with bound $\sqrt{(d+1)\cdot P_{\mathit{find}}}$ for the following alternative definitions of P_{right}:

$$P_{right} := \Pr[b = 1 : b \leftarrow A^{H\setminus S}(z)] \tag{3}$$
$$P_{right} := \Pr[b = 1 \wedge \neg\mathsf{Find} : b \leftarrow A^{H\setminus S}(z)] \tag{4}$$
$$P_{right} := \Pr[b = 1 \wedge \neg\mathsf{Find} : b \leftarrow A^{G\setminus S}(z)] \tag{5}$$
$$P_{right} := \Pr[b = 1 \wedge \mathsf{Find} : b \leftarrow A^{H\setminus S}(z)] \tag{6}$$
$$P_{right} := \Pr[b = 1 \wedge \mathsf{Find} : b \leftarrow A^{G\setminus S}(z)] \tag{7}$$

In Theorem 3.2, A is given access to a single oracle (G or H). In many cases (Theorem 4.2 for example), A must have access to additional oracles. In that case, additional oracles can just be encoded as part of z. The Theorem still holds because there were no assumptions on the runtime of A, the size of z or the number of queries to additional oracles. The proof of Theorem 3.2 is given in [AHU19].

The second part of O2H Theorem relates the probability of event Find to the guessing probability:

Theorem 3.3 (Search in semi-classical oracle from [AHU19]). *Let A be any quantum oracle algorithm making at most q queries to a semi-classical oracle with domain X. Let $S \subseteq X$ and $z \in \{0,1\}^*$. (S, z may have arbitrary joint distribution.)*

Let B be an algorithm that on input z chooses $i \overset{\$}{\leftarrow} \{1,\ldots,d\}$; runs $A^{\mathcal{O}_{\varnothing}^{SC}}(z)$ until (just before) the i-th query; then measures all query input registers in the computational basis and outputs the set T of measurement outcomes.

Then

$$\Pr[\mathsf{Find} : A^{\mathcal{O}_S^{SC}}(z)] \leq 4d \cdot \Pr[S \cap T \neq \varnothing : T \leftarrow B(z)]. \tag{8}$$

The proof of Theorem 3.3 is also given in [AHU19]. The next Corollary shows what happens in the common case that the input of A is independent of S:

Corollary 3.1 (from [AHU19]). *Suppose that S and z are independent and that A is a q-query algorithm. Let $P_{\max} := \max_{x\in X} \Pr[x \in S]$. Then*

$$\Pr[\mathsf{Find} : A^{\mathcal{O}_S^{SC}}(z)] \leq 4q \cdot P_{\max}. \tag{9}$$

For uniform $x \in \{1,\ldots,N\}$, $A^{\mathcal{O}_{\{x\}}^{SC}}$ finds x with probability less than $\frac{4\cdot q}{N}$.

3.3 Impact

After the first release of the O2H Theorem [Unr15b], Unruh gave two more variants of the Theorem. In a paper called *Quantum position verification in the random oracle model* [Unr14] Unruh introduced an adaptive version, which allows to reprogram the random oracle at a location that is influenced by the adversary. This was used for analyzing a quantum verification protocol. The third variant of the O2H Theorem published in *Non-interactive zero-knowledge proofs in the quantum random oracle model* [Unr15a] was even more adaptive and was used for the design of non-interactive zero-knowledge proof systems.

The Theorem was also widely used by other authors. Here, we give a list of papers with authors that used one of the three variants of the O2H Theorem in security proofs:

- Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, Dominique Unruh. *Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation* [ATTU16]

- Ehsan Ebrahimi Targhi, Dominique Unruh. *Quantum Security of the Fujisaki-Okamoto and OAEP Transforms* [TU16].

- Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger. *Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives** [Cha+17].

- Dennis Hofheinz, Kathrin Hövelmanns, Eike Kiltz. *A Modular Analysis of the Fujisaki-Okamoto Transformation* [HHK17].

- Fang Song, Aaram Yun. *Quantum Security of NMAC and Related Constructions* [SY17].

- Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, Zhi Ma. *IND-CCA-secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited* [Jia+18].

- Sungsook Kim, Jeeun Lee, Rakyong Cho, Kwangjo Kim. *Validating IGE Mode of Block Cipher from Quantum Adversaries* [KLCK18].

- Alan Szepieniec, Reza Reyhanitabar, Bart Preneel. *Key Encapsulation from Noisy Key Agreement in the Quantum Random Oracle Model* [SRP18].

- Tsunekazu Saito, Keita Xagawa, Takashi Yamakawa. *Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model* [SXY18].
- Anne Broadbent, Sebastien Lord. *Uncloneable Quantum Encryption via Random Oracles* [BL19].
- Haodong Jiang, Zhenfeng Zhang, Zhi Ma. *Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model* [JZM19b].

These are the results that are public and that we are aware of. We do not claim, that this list is complete. Since the release of the improved O2H Theorem, which uses semi-classical oracles [AHU19], some authors have already used this new version:

- Kathrin Hövelmanns, Eike Kiltz, Sven Schäge, Dominique Unruh. *Generic Authenticated Key Exchange in the Quantum Random Oracle Model* [HKSU18].
- Haodong Jiang, Zhenfeng Zhang, Zhi Ma. *Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model* [JZM19a]
- Haodong Jiang, Zhenfeng Zhang, Zhi Ma. *Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model* [JZM19b].

In *Quantum security proofs using semi-classical oracles* [AHU19], the authors also improved the security proof from *Quantum Security of the Fujisaki-Okamoto and OAEP Transforms* [TU16].

The comparison of the old and new bounds is summarized in Figure 4. Since it is difficult to compare the various formulas, in the column ”queries“, we summarize the relationship between the number of queries and attack probability: Say ε is the advantage against the underlying public-key encryption scheme. We assume that the terms that involve ε dominate all other terms and find how many queries does one have to make to break the scheme (with constant probability). Take the advantage $q\varepsilon^{1/2}$ for example. We need $q \approx \varepsilon^{-1/2}$ queries for a successful attack, so we get $q^2 \approx 1/\varepsilon$ queries.

The bounds for the first three papers ([TU16], [HKSU18] and [JZM19a]) were given by Ambainis, Hamburg and Unruh [AHU19]. There is a small difference in the bound for Jiang-Zhang-Ma, new O2H, IND-CPA: the second and third summands $q2^{-n/2} + \frac{q}{2^{n'}}$ were omitted by accident in [AHU19]. But to be consistent with the other bounds, we included it here.

Setting	**Security**	**Bound**	**Queries**
Targhi-Unruh [TU16]			
old O2H, OW-CPA	IND-CCA	$\varepsilon_{sym} + q^{9/5}2^{-\gamma/5} + q^{3/2}\varepsilon^{1/4} + q^{3/2}2^{-n_1/4}$	$q^6 \approx 1/\varepsilon$
new O2H, IND-CPA	IND-CCA	$\varepsilon_{sym} + q^{9/5}2^{-\gamma/5} + qq_{\text{dec}}^{1/2}\varepsilon^{1/2} + q^{3/2}q_{\text{dec}}2^{-n/2}$	$q^2 q_{\text{dec}} \approx 1/\varepsilon$
new O2H, OW-CPA	IND-CCA	$\varepsilon_{sym} + q^{9/5}2^{-\gamma/5} + q^{3/2}q_{\text{dec}}\varepsilon^{1/2}$	$q^3 q_{\text{dec}}^2 \approx 1/\varepsilon$
Hövelmanns-Kiltz-Schäge-Unruh [HKSU18]			
old O2H, IND-CPA	IND-CCA	$q\varepsilon^{1/2} + q2^{-n/2}$	$q^2 \approx 1/\varepsilon$
new O2H, IND-CPA	IND-CCA	$q^{1/2}\varepsilon^{1/2} + q2^{-n/2}$	$q \approx 1/\varepsilon$
Jiang-Zhang-Ma [JZM19a]			
old O2H, OW-CPA	IND-CCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, OW-CPA	IND-CCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, IND-CPA	IND-CCA	$q^{1/2}\varepsilon^{1/2} + q2^{-n/2} + q2^{-n'}$	$q \approx 1/\varepsilon$
Hofheinz-Hövelmanns-Kiltz [HHK17]			
old O2H, OW-CPA	OW-PCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, OW-CPA	OW-PCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, IND-CPA	OW-PCA	$q^{1/2}\varepsilon^{1/2} + q2^{-n/2}$	$q \approx 1/\varepsilon$
old O2H, OW-PCA	IND-CCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, OW-PCA	IND-CCA	$q\varepsilon^{1/2}$	$q^2 \approx 1/\varepsilon$
new O2H, IND-PCA	IND-CCA	$q^{1/2}\varepsilon^{1/2} + q2^{-n/2}$	$q \approx 1/\varepsilon$
old O2H, OW-CPA	IND-CCA	$q^{3/2}\varepsilon^{1/4}$	$q^6 \approx 1/\varepsilon$
new O2H, OW-CPA	IND-CCA	$q^{3/2}\varepsilon^{1/4}$	$q^6 \approx 1/\varepsilon$
new O2H, IND-CPA	IND-CCA	$q^{5/4}\varepsilon^{1/4} + q^{3/2}2^{-n/4}$	$q^5 \approx 1/\varepsilon$

The ”setting“ column says whether the proof uses the old or the new O2H Theorem and which security of the underlying public-key encryption scheme was used.
The ”bound“ column gives the bound on the advantage of the adversary against the security in ”security“ column, up to constant factor. In [TU16] a hybrid public-key encryption scheme is constructed, in the other cases for IND-CCA security, a KEM. If the security is OW-PCA [HHK17], the resulting scheme is a public-key encryption scheme. ε is the advantage of the reduced adversary against the one-wayness or IND-CPA security of the underlying public-key scheme. ε_{sym} is the advantage against the underlying symmetric encryption scheme. q is the number of queries (random oracle and decryption queries), but q_{dec} only the decryption queries. γ is the min-entropy of ciphertexts and n is the length of the plaintext of the underlying public-key scheme. n' is the length of an additional hash appended to the ciphertext in [JZM19a].
The column ”queries“ summarizes the relationship between the number of queries and attack probability. Here, we treat all advantages (ε, ε_{sym}) as the same.
For simplicity, all the bounds are given for the case that no decryption errors occur.

Figure 4: Security bounds of different Fujisaki-Okamoto variants using the old and the new O2H Theorems.

We added the bounds for *A Modular Analysis of the Fujisaki-Okamoto Transformation* [HHK17] to this Figure. Note that for the lines with "Setting“ in bold, the security proof from [HHK17] was modified by us (see Section 4) so that it uses the improved version of the O2H Theorem. In Section 4 we consider adversaries that might execute parallel oracle invocations and therefore we differentiate between query depth d and query number q. In Figure 4 we use the upper bound $q \geq d$ to make the comparison between different papers easier.

Since the original analysis was modular (OW-CPA secure PKE was turned into and IND-CCA secure KEM in two steps), we decided to include transformations from OW-CPA to OW-PCA and from OW-PCA to IND-CCA separately. This allows us to see the improvement in bounds on each transformation. We also combined these two transformations to get the same setting that the other three papers had (that is from OW-CPA to IND-CCA).

The security proofs were restated under the assumption that the underlying public-key encryption scheme is one-way and that it is IND-CPA (or IND-PCA) secure. No matter which of the assumptions is used, the resulting bounds are essentially the same in the original proof. However, the resulting bounds are much better when we used IND-CPA (or IND-PCA) security with the new O2H Theorem.

From Figure 4 we can see that the bounds are essentially the same with the old and the new O2H if we use the same security assumption. But if we used IND-CPA (or IND-PCA), the dependence on the query number changed from square to linear. After combining transformations IND-CPA to OW-PCA and from OW-PCA to IND-CCA , the dependence on the query number changed from the sixth power to fifth.

The improvement would be even greater if we could use both transformations from IND-CPA to OW-PCA and from IND-PCA to IND-CCA. But that requires an additional transformation in the middle: from OW-PCA to IND-PCA. With a tight transformation from OW-PCA to IND-PCA, we could combine the bounds for transformations from IND-CPA to OW-PCA and from IND-PCA to IND-CCA. The resulting scheme would have $q^{3/4}\varepsilon^{1/4}+q2^{-n/4}$ in the "Bound“ column and $q^3 \approx 1/\varepsilon$ in the "Queries“ column. This means that the the dependence on the query number would change from the sixth power to cubic. This result would be similar to the improvement on Targhi-Unruh [TU16]. We view it as an open problem to find such transformation from OW-PCA to IND-PCA, because this could significantly improve the bound.

4 Transformations

In this section we use semi-classical oracles to improve on security proofs that used O2H Theorem from [Unr15b]. To make comparison between the old and new proof easier, we use the same notation and reproduce text verbatim (in the parts where the proof does not change). The parts of the proofs that we changed have a shaded box around them (this does not include minor changes like a change in the game number).

4.1 T: from $\mathsf{OW\text{-}CPA}$ to $\mathsf{OW\text{-}PCA}$ security in the QROM

T transforms an $\mathsf{OW\text{-}CPA}$ secure public-key encryption scheme into an $\mathsf{OW\text{-}PCA}$ secure one [HHK17].

```
$\underline{Enc_1^{\mathsf{G}}(pk, m)}$
$c := Enc(pk, m; \mathsf{G}(m))$
return $c$

$\underline{Dec_1^{\mathsf{G}}(sk, c)}$
$m' := Dec(sk, c)$
if $m' = \bot$ or $Enc(pk, m'; \mathsf{G}(m')) \neq c$
    return $\bot$
else return $m'$
```

Figure 5: $\mathsf{OW\text{-}PCA}$-secure encryption scheme $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$. We write $^{\mathsf{G}}$ to emphasize that Enc_1 and Dec_1 use the oracle G.

Take $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$, where the public-key encryption scheme $\mathsf{PKE} = (Gen, Enc, Dec)$ has message space $\mathcal{M}$, randomness space $\mathcal{R}$ and a random oracle $\mathsf{G} : \mathcal{M} \to \mathcal{R}$. The algorithms of $\mathsf{PKE}_1 = (Gen, Enc_1^{\mathsf{G}}, Dec_1^{\mathsf{G}})$ are defined in Figure 5. Note that the resulting encryption is deterministic (it produces the same ciphertext for a given message and public key).

The following theorem establishes that $\mathsf{OW\text{-}PCA}$ security of PKE_1 reduces to the $\mathsf{OW\text{-}CPA}$ security of PKE in the QROM. We first state a lemma that is used in the proof.

Lemma 4.1 (from [HHK17]). *Assume* PKE *to be δ-correct. Then* $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ *is δ_1-correct in the quantum random oracle model, where* $\delta_1 = \delta_1(q_{\mathsf{G}}) \leq 8 \cdot (q_{\mathsf{G}} + 1)^2 \cdot \delta$.

The proof of this lemma can be found in [HHK17].

Theorem 4.1 (PKE $\mathsf{OW\text{-}CPA}$ ($\mathsf{IND\text{-}CPA}$) $\xrightarrow{QROM}$ PKE_1 $\mathsf{OW\text{-}PCA}$)**.** *Assume* PKE *to be δ-correct. Then, for any* $\mathsf{OW\text{-}PCA}$ *quantum adversary B that issues at most q_{G} queries to the quantum random oracle* G *with query depth d_{G} and q_{P} (classical) queries to a plaintext checking oracle Pco with query depth d_{P},* *(a) there exist* OW-CPA *quantum adversaries C and E such that*

$$\begin{aligned} Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(B) \leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(C)} \\ + (4d_{\mathsf{G}} + 4d_{\mathsf{P}} + 4) \cdot \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E)}. \end{aligned}$$

and the running time of B is about that of C and E.

(b) there exist IND-CPA *quantum adversaries G and F such that*

$$\begin{aligned} Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(B) \leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(G) + \frac{1}{|\mathcal{M}|}} \\ + (2\sqrt{d_{\mathsf{G}} + d_{\mathsf{P}} + 1}) \cdot \sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(F) + \frac{4(d_{\mathsf{G}} + d_{\mathsf{P}})}{|\mathcal{M}|}}. \end{aligned}$$

and the running time of B is about that of G and F.

The original bound from [HHK17] is

$$Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(B) \leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + (1 + 2q_{\mathsf{G}}) \cdot \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(A)}.$$

Note that Theorem 4.1 distinguishes query depth d_{G} and query number q_{G} while the original theorem from [HHK17] only used query number q_{G}. This change is introduced because [AHU19] considers adversaries that might execute parallel oracle invocations. For comparison, we also give the bound for q_{G} in the end of the proof.

In the original proof [HHK17], the random oracle was modeled as a $2q_{\mathsf{G}}$-wise independent hash function. Zhandry [Zha12] proved that no quantum algorithm A^f, issuing at most q quantum queries to f, can distinguish between a random function f and a $2q$-wise independent function. We assume that simulating random oracles takes unit cost and that random oracle is just a random function as common in literature. This ensures that the running time of B is about that of C and D.

Proof. Let B be an adversary against the OW-PCA security of PKE_1, issuing at most q_{G} queries to G with query depth d_{G} and at most q_{P} queries to Pco with query depth q_{P}. We write Pco^{G} to emphasize that the random oracle used for randomness in the encryption is G. Consider the games given in Figure 6.

```
GAME $G_0$-$G_3$
$(pk, sk) \leftarrow Gen$
$m^* \xleftarrow{\$} \mathcal{M}$
$\mathsf{G} \xleftarrow{\$} (\mathcal{M} \to \mathcal{R})$
$r^* := \mathsf{G}(m^*)$                                  $/\!\!/ G_0$-$G_1$
$r^* \xleftarrow{\$} \mathcal{R}$                          $/\!\!/ G_2$-$G_3$
$c^* := Enc(pk, m^*; r^*)$
$m' \leftarrow B^{\mathsf{G}, Pco^{\mathsf{G}}}(pk, c^*)$   $/\!\!/ G_0, G_1, G_3$
$\mathsf{H} := \mathsf{G}(m^* := r^*)$                     $/\!\!/ G_2$
$m' \leftarrow B^{\mathsf{H}, Pco^{\mathsf{H}}}(pk, c^*)$   $/\!\!/ G_2$
return $[\![m' = m^*]\!]$

$Pco^{\mathsf{G}}(m \in \mathcal{M}, c)$
$m' := Dec(sk, c)$                                        $/\!\!/ G_0$
return $[\![m' = m \wedge Enc(pk, m'; \mathsf{G}(m')) = c]\!]$   $/\!\!/ G_0$
return $[\![Enc(pk, m; \mathsf{G}(m)) = c]\!]$            $/\!\!/ G_1$-$G_5$

GAME $G_4, G_5$
FIND := false
$(pk, sk) \leftarrow Gen$
$m^* \xleftarrow{\$} \mathcal{M}$
$\mathsf{G} \xleftarrow{\$} (\mathcal{M} \to \mathcal{R})$
$r^* \xleftarrow{\$} \mathcal{R}$
$c^* := Enc(pk, m^*; r^*)$                                $/\!\!/ G_4$
$c^* := Enc(pk, 0; r^*)$                                  $/\!\!/ G_5$
$B^{\mathsf{G} \setminus \{m^*\}, Pco^{\mathsf{G} \setminus \{m^*\}}}(pk, c^*)$
return FIND

$\mathsf{G} \setminus \{m^*\} |\psi, \phi\rangle$
$|\psi', b\rangle := \mathcal{O}^{SC}_{\{m^*\}} |\psi, 0\rangle$
if $b = 1$
    FIND := true
return $\mathsf{G}|\psi', \phi\rangle$
```

Figure 6: Games G_0-G_5 for the proof of Theorem 4.1.

GAME G_0. Since game G_0 is the original OW-PCA game for PKE_1,

$$\Pr[G_0^B \Rightarrow 1] = Adv_{\mathsf{PKE}_1}^{\textsf{OW-PCA}}(B).$$

GAME G_1. In game G_1 the plaintext checking oracle Pco^{G} is replaced with a simulation that does not make use of the secret key anymore. We claim

$$|\Pr[G_1^B \Rightarrow 1] - \Pr[G_0^B \Rightarrow 1]| \leq 8 \cdot (q_{\mathsf{G}} + 1)^2 \cdot \delta. \tag{10}$$

To show Equation (10), first note that both Game G_0 and Game G_1 proceed identically until the event that B submits a Pco^{G} query (m, c) such that $c = Enc(pk, m; \mathsf{G}(m))$ and $Dec(sk, c) \neq m$. We call this event BADR. Since both Game G_0 and Game G_1 proceed identically conditioned on the event that BADR does not happen,

$$|\Pr[G_1^B \Rightarrow 1] - \Pr[G_0^B \Rightarrow 1]| \leq \Pr[\text{BADR}].$$

One can show that there exists an adversary F against COR-QRO that perfectly simulates games G_0 and G_1 and wins iff BADR happens. COR-QRO is defined in Figure 1. Applying Lemma 4.1, we see that

$$\Pr[\text{BADR}] \leq \Pr[\textsf{COR-QRO}^F] \leq 8 \cdot (q_{\mathsf{G}} + 1)^2 \cdot \delta.$$

GAME G_2. In game G_2, replace oracle access to G with oracle access to H in line 9. H is defined as follows: pick a uniformly random r^* in line 5, let $\mathsf{H}(m) := \mathsf{G}(m)$ for all $m \neq m^*$ and let $\mathsf{H}(m^*) = r^*$. Since G is uniformly random, replacing it everywhere with $\mathsf{H} := \mathsf{G}(m^* := r^*)$ does not change the distribution. Replacing $\mathsf{G}(m^*)$ by r^* does not change the game either because r^* is the output of $\mathsf{G}(m^*)$. We have shown that

$$\Pr[G_2^B \Rightarrow 1] = \Pr[G_1^B \Rightarrow 1].$$

```
$\hat{B}^{\mathsf{H}}(pk, c^*, m^*)$
$m' \leftarrow B^{\mathsf{H}, Pco^{\mathsf{H}}}(pk, c^*)$
return $[\![m' = m^*]\!]$
```

Figure 7: Adversary $\hat{B}$ for the proof of Theorem 4.1.

GAME G_3. In game G_3, we switch back to oracle access to G from H. Define $\hat{B}^{\mathsf{H}}(pk, c^*, m^*)$ as in Figure 7. Note that $\hat{B}$ simulates Pco itself. For $z := (pk, c^* := Enc(pk, m^*; r^*), m^*)$ and $S := \{m^*\}$, where $(pk, sk) \leftarrow Gen$, $m^* \xleftarrow{\$} \mathcal{M}$ and $r^* \xleftarrow{\$} \mathcal{R}$, we can write:

$$P_{\mathit{left}} := \Pr[b = 1 : b \leftarrow \hat{B}^{\mathsf{H}}(z)] = \Pr[G_2^B \Rightarrow 1]$$
$$P_{\mathit{right}} := \Pr[b = 1 : b \leftarrow \hat{B}^{\mathsf{G}}(z)] = \Pr[G_3^B \Rightarrow 1]$$
$$P_{\mathit{find}} := \Pr[\mathsf{Find} : \hat{B}^{\mathsf{G} \setminus S}(z)] = \Pr[G_4^B \Rightarrow 1]$$

From the O2H Theorem (3.2) with $A := \hat{B}$ we get

$$|\Pr[G_3^B \Rightarrow 1] - \Pr[G_2^B \Rightarrow 1]| \leq 2 \cdot \sqrt{(d_{\mathsf{G}} + d_{\mathsf{P}} + 1) \cdot \Pr[G_4^B \Rightarrow 1]}.$$

Now that r^* is uniformly random and not used anywhere except as the randomness for Enc in line 6 we trivially construct an adversary C in Figure 8 against the OW-CPA security of the original encryption scheme PKE simulating game G_3 for B that outputs $m' = m^*$ if B wins in game G_3.

$$\Pr[G_3^B \Rightarrow 1] = Adv_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(C).$$

```
$\underline{C(pk, c^*)}$
$\mathsf{G} \xleftarrow{\$} (\mathcal{M} \to \mathcal{R})$
$m' \leftarrow B^{\mathsf{G}, Pco^{\mathsf{G}}}(pk, c^*)$
return $m'$
```

```
$\underline{D^{\mathcal{O}^{SC}}(pk, c^*)}$
$\mathsf{G} \xleftarrow{\$} (\mathcal{M} \to \mathcal{R})$
$m' \leftarrow B^{\mathcal{O}^{SC} \circ \mathsf{G}, Pco^{\mathcal{O}^{SC} \circ \mathsf{G}}}(pk, c^*)$
return $m'$
```

Figure 8: Adversaries C (left) and D (right) for the proof of Theorem 4.1.

In the original proof, an adversary D was constructed trivially against the $\mathsf{OW\text{-}CPA}$ security of PKE simulating game G_4. In our case, this is not possible, because in game G_4, the adversary has access to the oracle $\mathsf{G} \setminus \{m^*\}$ which might leak some information about m^*. We give two different proofs that eliminate this problem. The first proof assumes $\mathsf{OW\text{-}CPA}$ security of PKE (like in the original theorem statement) and the second proof assumes $\mathsf{IND\text{-}CPA}$ security of PKE.

(a) Proof using OW-CPA

Note that an oracle query to $\mathsf{G} \setminus \{m^*\}$ is equivalent to querying G and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Thus, we can define an adversary $D^{\mathcal{O}^{SC}}(pk, c^*)$ (see Figure 8) that simulates game G_4, using $\mathcal{O}^{SC}_{\{m^*\}}$ to simulate the queries to the punctured oracles, and c^* as the ciphertext $Enc(pk, m^*; r^*)$ where $(pk, sk) \leftarrow Gen$, $m^* \xleftarrow{\$} \mathcal{M}$ and $r^* \xleftarrow{\$} \mathcal{R}$. The oracle G is chosen by D. By writing $\mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{G}$ we mean querying G and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Then

$$\Pr[G_4^B \Rightarrow 1] = \Pr[\mathsf{Find} : D^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)]$$

where $c^* := Enc(pk, m^*; r^*)$ and m^* is uniform. By Theorem 3.3 (with $A := D$, $B := E$, $S = \{m^*\}$, $z := (pk, c^*)$ and $d := d_{\mathsf{G}} + d_{\mathsf{P}}$)

$$\Pr[\mathsf{Find} : D^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)] \leq 4(d_{\mathsf{G}} + d_{\mathsf{P}}) \cdot \Pr[m^* = E(pk, c^*)].$$

Here E is the adversary that stops D at a random query as in Theorem 3.3. The runtime of E is approximately the same as that of D. Then from the $\mathsf{OW\text{-}CPA}$ security of the original encryption scheme, we have

$$\Pr[m^* = E(pk, c^*)] \leq Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E)$$

and thus

$$\Pr[G_4^B \Rightarrow 1] \leq 4(d_{\mathsf{G}} + d_{\mathsf{P}}) \cdot Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E).$$

Collecting the probabilities gives us

$$
\begin{aligned}
Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}} + 1)^2 + \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(C)} \\
&\quad + (2\sqrt{d_{\mathsf{G}} + d_{\mathsf{P}}} \cdot 2\sqrt{d_{\mathsf{G}} + d_{\mathsf{P}} + 1}) \cdot \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E)}
\end{aligned}
$$

and further simplifying proves the theorem:

$$
\begin{aligned}
Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}} + 1)^2 + \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(C)} \\
&\quad + (4d_{\mathsf{G}} + 4d_{\mathsf{P}} + 4) \cdot \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E)}.
\end{aligned}
$$

(b) Proof using IND-CPA

Since r^* is uniformly random and not used anywhere except as the randomness for Enc, IND-CPA security implies that $Enc(pk, m^*; r^*)$ is indistinguishable from $Enc(pk, 0; r^*)$. If game G_5 is obtained from game G_4 by replacing $Enc(pk, m^*; r^*)$ with $Enc(pk, 0; r^*)$ on line 19 (see Figure 6), we have

$$
|\Pr[G_4^B \Rightarrow 1] - \Pr[G_5^B \Rightarrow 1]| \leq Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(F).
$$

F is defined as adversary against the IND-CPA security of PKE.

Note that an oracle query to $\mathsf{G} \setminus \{m^*\}$ is equivalent to querying G and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Thus, we can define an adversary $D^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)$ (see Figure 8) that simulates game G_5, using $\mathcal{O}^{SC}_{\{m^*\}}$ to simulate the queries to the punctured oracles, and c^* as the ciphertext $Enc(pk, 0; r^*)$ where $(pk, sk) \leftarrow Gen$ and $r^* \xleftarrow{\$} \mathcal{R}$. The oracle G is chosen by D. By writing $\mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{G}$ we mean querying G and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Then

$$
\Pr[G_5^B \Rightarrow 1] = \Pr[\mathsf{Find} : D^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)]
$$

where $c^* := Enc(pk, 0; r^*)$. By Corollary 3.1 (with $A := D$, $S = \{m^*\}$, $z := (pk, c^*)$ and $d := d_{\mathsf{G}} + d_{\mathsf{P}}$)

$$
\Pr[\mathsf{Find} : D^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)] \leq \frac{4(d_{\mathsf{G}} + d_{\mathsf{P}})}{|\mathcal{M}|}
$$

and thus

$$
\Pr[G_4^B \Rightarrow 1] \leq Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(F) + \frac{4(d_{\mathsf{G}} + d_{\mathsf{P}})}{|\mathcal{M}|}.
$$

Collecting the probabilities proves the theorem:

$$\begin{aligned} Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(C)} \\ &\quad + (2\sqrt{d_{\mathsf{G}}+d_{\mathsf{P}}+1}) \cdot \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(F) + \frac{4(d_{\mathsf{G}}+d_{\mathsf{P}})}{|\mathcal{M}|}}. \end{aligned}$$

It is well known that IND-CPA security of PKE (with sufficiently large message space) implies its OW-CPA security (see Lemma 2.1). This allows us to simplify the last bound:

$$\begin{aligned} \Pr[G_3^B \Rightarrow 1] = Adv_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(C) &\leq Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(G) + \frac{1}{|\mathcal{M}|} \\ &\leq \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(G) + \frac{1}{|\mathcal{M}|}} \end{aligned}$$

and thus

$$\begin{aligned} Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(G) + \frac{1}{|\mathcal{M}|}} \\ &\quad + (2\sqrt{d_{\mathsf{G}}+d_{\mathsf{P}}+1}) \cdot \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(F) + \frac{4(d_{\mathsf{G}}+d_{\mathsf{P}})}{|\mathcal{M}|}}. \end{aligned}$$

Results
Since the number of queries q_{G}, q_{P} is always larger or equal to the query depth d_{G}, d_{P} we get the following two bounds:

$$\begin{aligned} Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(C)} \\ &\quad + (4q_{\mathsf{G}}+4q_{\mathsf{P}}+4) \cdot \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(E)}. \\ Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(B) &\leq 8 \cdot \delta \cdot (q_{\mathsf{G}}+1)^2 + \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(G) + \frac{1}{|\mathcal{M}|}} \\ &\quad + (2\sqrt{q_{\mathsf{G}}+q_{\mathsf{P}}+1}) \cdot \sqrt{Adv_{\mathsf{PKE}}^{\mathsf{IND\text{-}CPA}}(F) + \frac{4(q_{\mathsf{G}}+q_{\mathsf{P}})}{|\mathcal{M}|}}. \end{aligned}$$

□

4.2 $\mathsf{QU}_m^{\perp}$: from $\mathsf{OW\text{-}PCA}$ to $\mathsf{IND\text{-}CCA}$ security in the QROM

$\mathsf{QU}_m^{\perp}$ transforms an $\mathsf{OW\text{-}PCA}$ secure public-key encryption scheme into an $\mathsf{IND\text{-}CCA}$ secure key encapsulation mechanism with explicit rejection [HHK17]. Explicit rejection (noted by $^{\perp}$ in $\mathsf{QU}_m^{\perp}$) means that decapsulation of an invalid ciphertext results in the rejection symbol $\perp$.

```
$QEnc_m^{\mathsf{H},\mathsf{H}'}(pk)$
$m \xleftarrow{\$} \mathcal{M}$
$c \leftarrow Enc_1(pk, m)$
$d := \mathsf{H}'(m)$
$K := \mathsf{H}(m)$
return $(K, (c, d))$
```

```
$QDec_m^{\perp \mathsf{H},\mathsf{H}'}(sk, (c, d))$
$m' := Dec_1(sk, c)$
if $m' = \perp$ or $\mathsf{H}'(m') \neq d$
    return $\perp$
else return $K := \mathsf{H}(m')$
```

Figure 9: $\mathsf{IND\text{-}CCA}$-secure key encapsulation mechanism $\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$. We write $^{\mathsf{H},\mathsf{H}'}$ to emphasize that $QEnc$ and $QDec$ use the oracles H and H'.

Take $\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$, where public-key encryption scheme $\mathsf{PKE}_1 = (Gen_1, Enc_1^{\mathsf{H}}, Dec_1^{\mathsf{H}})$ (see Figure 5) has message space $\mathcal{M} = \{0,1\}^n$, and random oracles $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ and $\mathsf{H}' : \{0,1\}^n \to \{0,1\}^n$. The algorithms of $\mathsf{QKEM}_m^{\perp} = (Gen_1, QEnc_m, QDec_m^{\perp})$ are defined in Figure 9.

The following theorem establishes that $\mathsf{IND\text{-}CCA}$ security of $\mathsf{QKEM}_m^{\perp}$ reduces to the $\mathsf{OW\text{-}PCA}$ security of PKE_1 in the QROM.

Theorem 4.2 (PKE_1 $\mathsf{OW\text{-}PCA}$ ($\mathsf{IND\text{-}PCA}$) $\xrightarrow{QROM}$ $\mathsf{QKEM}_m^{\perp}$ $\mathsf{IND\text{-}CCA}$)**.** *If* PKE_1 *is* δ_1*-correct, then so is* $\mathsf{QKEM}_m^{\perp}$*. For any* $\mathsf{IND\text{-}CCA}$ *quantum adversary* B *that issues at most* q_D *(classical) queries to the decapsulation oracle* $QDec_m^{\perp}$ *with query depth* d_{D}*, at most* q_{H} *queries to the quantum random oracle* H *with query depth* d_{H} *and at most* $q_{\mathsf{H}'}$ *queries to the quantum random oracle* H' *with query depth* $d_{\mathsf{H}'}$*,*

(a) there exist $\mathsf{OW\text{-}PCA}$ *quantum adversaries* E_0*,* E_1 *issuing* $2q_{\mathsf{D}}q_{\mathsf{H}'}$ *queries to oracle* Pco *such that*

$$Adv_{\mathsf{QKEM}_m^{\perp}}^{\mathsf{IND\text{-}CCA}}(B) \leq 2(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(E_0)} + 2(d_{\mathsf{H}'} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(E_1)}.$$

(b) there exists an $\mathsf{IND\text{-}PCA}$ *quantum adversary* A *issuing* $2q_{\mathsf{D}}q_{\mathsf{H}'}$ *queries to oracle* Pco *such that*

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq 2\sqrt{d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A)} + \frac{4(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1)}{\sqrt{n}}.$$

The original bound from [HHK17] is

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq (2q_{\mathsf{H}'} + q_{\mathsf{H}}) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(A)}.$$

Proof. Let B be an adversary against the $\mathsf{IND\text{-}CCA}$ security of $\mathsf{QKEM}^{\perp}_{m}$, issuing at most q_D queries to $QDec^{\perp}_{m}$ with query depth d_{D}, at most q_{H} queries to H with query depth d_{H} and at most $q_{\mathsf{H}'}$ queries to H' with query dept $d_{\mathsf{H}'}$. Consider the games given in Figure 10.

In the original proof in [HHK17], the games were given using double indices, for example game $G_{1,0}$. We use a single index for games to be consistent with the previous proof. For reference, games that had 0 as the second index in [HHK17] are now games with odd indices and games that had 1 as the second index now have even indices.

In the original proof [HHK17], the random oracle was modeled as a $2q_{\mathsf{G}}$-wise independent hash function. We assume that simulating random oracles takes unit cost and that the random oracle is just a random function as common in literature, unless stated otherwise.

In the proof we use the following notion for random oracles: $\mathsf{G} \times \mathsf{G}' : x \mapsto (\mathsf{G}(x), \mathsf{G}'(x))$.

GAMES G_0, G_1. Games G_0 and G_1 describe the $\mathsf{IND\text{-}CCA}$ game in its equivalent "left-or-right" style:

$$\begin{aligned} Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) &= \frac{1}{2} \cdot \left|\Pr\left[\mathsf{IND\text{-}CCA}^{B} \Rightarrow 0 | b = 0\right] - \Pr\left[\mathsf{IND\text{-}CCA}^{B} \Rightarrow 1 | b = 1\right]\right| \\ &= \frac{1}{2} \cdot \left|\Pr\left[G_0^B \Rightarrow 1\right] - \Pr\left[G_1^B \Rightarrow 1\right]\right| \end{aligned}$$

```
    GAMES $G_0$-$G_5$,
1   $(pk, sk) \leftarrow Gen_1$
2   $\mathsf{H} \xleftarrow{\$} (\{0,1\}^* \rightarrow \{0,1\}^n)$
3   $\mathsf{H}' \xleftarrow{\$} (\{0,1\}^n \rightarrow \{0,1\}^n)$
4   $m^* \xleftarrow{\$} \{0,1\}^n;\ c^* \leftarrow Enc_1(pk, m^*)$
5   $K^* := \mathsf{H}(m^*)$                                                  $/\!/G_0$
6   $K^* \xleftarrow{\$} \{0,1\}^n$                                            $/\!/G_1$-$G_5$
7   $d^* := \mathsf{H}'(m^*)$                                                 $/\!/G_0, G_1$
8   $d^* \xleftarrow{\$} \{0,1\}^n$                                            $/\!/G_2$-$G_5$
9   $b' \leftarrow B^{QDec_m^{\perp \mathsf{H},\mathsf{H}'}, \mathsf{H}\times\mathsf{H}'}(pk, (c^*, d^*), K^*)$   $/\!/G_0, G_1$
10  $\mathsf{G} := \mathsf{H}(m^* := K^*)$                                     $/\!/G_2$
11  $\mathsf{G}' := \mathsf{H}'(m^* := d^*)$                                   $/\!/G_2, G_3$
12  $b' \leftarrow B^{QDec_m^{\perp \mathsf{G},\mathsf{G}'}, \mathsf{G}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$   $/\!/G_2$
13  $b' \leftarrow B^{QDec_m^{\perp \mathsf{H},\mathsf{G}'}, \mathsf{H}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$   $/\!/G_3$
14  $b' \leftarrow B^{QDec_m^{\perp \mathsf{H},\mathsf{H}'}, \mathsf{H}\times\mathsf{H}'}(pk, (c^*, d^*), K^*)$   $/\!/G_4, G_5$
15  return $b'$

    $QDec_m^{\perp \mathsf{H},\mathsf{H}'}((c,d) \neq (c^*, d^*))$            $/\!/G_0$-$G_7$
16  $m' := Dec_1(sk, c)$
17  if $m' \neq \perp$ and $\mathsf{H}'(m') = d$
18      return $K := \mathsf{H}(m')$
19  else return $\perp$

    $(\mathsf{H} \times \mathsf{H}') \setminus \{m^*\}|\psi, \phi\rangle$
20  $|\psi', b\rangle := \mathcal{O}^{SC}_{\{m^*\}}|\psi, 0\rangle$
21  if $b = 1$
22      FIND := true
23  return $(\mathsf{H} \times \mathsf{H}')|\psi', \phi\rangle$

    GAMES $G_6$-$G_{10}$
24  FIND := false
25  $(pk, sk) \leftarrow Gen_1$
26  $\mathsf{H} \xleftarrow{\$} (\{0,1\}^* \rightarrow \{0,1\}^n)$
27  $\mathsf{H}' \xleftarrow{\$} (\{0,1\}^n \rightarrow \{0,1\}^n)$              $/\!/G_6, G_7$
28  $\mathsf{H}' = \mathsf{H}'(X) \xleftarrow{\$}$ polynomial of degree
            $\leq 2(q_\mathsf{H} + q_{\mathsf{H}'} + q_\mathsf{D})$ over $\mathbb{F}_{2^n}$   $/\!/G_8$-$G_{10}$
29  $m^* \xleftarrow{\$} \{0,1\}^n;\ c^* \leftarrow Enc_1(pk, m^*)$           $/\!/G_6$-$G_9$
30  $m^* \xleftarrow{\$} \{0,1\}^n;\ c^* \leftarrow Enc_1(pk, 0)$             $/\!/G_{10}$
31  $K^* \xleftarrow{\$} \{0,1\}^n$
32  $d^* \xleftarrow{\$} \{0,1\}^n$
33  $B^{QDec_m^{\perp \mathsf{H}\setminus\{m^*\},\mathsf{H}'\setminus\{m^*\}}, (\mathsf{H}\times\mathsf{H}')\setminus\{m^*\}}$
                $(pk, (c^*, d^*), K^*)$                                      $/\!/G_6, G_8$
34  $B^{QDec_m^{\perp \mathsf{H},\mathsf{H}'\setminus\{m^*\}}, \mathsf{H}\times(\mathsf{H}'\setminus\{m^*\})}$
                $(pk, (c^*, d^*), K^*)$                                      $/\!/G_7, G_9, G_{10}$
35  return FIND

    $QDec_m^{\perp \mathsf{H},\mathsf{H}'}((c,d) \neq (c^*, d^*))$            $/\!/G_8$-$G_{10}$
36  if $\exists m \in \mathsf{Roots}(\mathsf{H}'(X) - d)$ s.t.
            $Dec_1(sk, c) = m$
37      return $K := \mathsf{H}(m)$
38  else return $\perp$

    $\mathsf{H}' \setminus \{m^*\}|\psi, \phi\rangle$
39  $|\psi', b\rangle := \mathcal{O}^{SC}_{\{m^*\}}|\psi, 0\rangle$
40  if $b = 1$
41      FIND := true
42  return $\mathsf{H}'|\psi', \phi\rangle$
```

Figure 10: Games G_0 - G_{10} for the proof of Theorem 4.2

GAME G_2. In game G_2, starting from game G_0 replace oracle access to H with oracle access to G and H' with oracle access to G' in line 12. G is defined as follows: pick a uniformly random K^* in line 6, let $\mathsf{G}(m) := \mathsf{H}(m)$ for all $m \neq m^*$ and let $\mathsf{G}(m^*) = K^*$. G' is defined as follows: pick a uniformly random d^* in line 8, let $\mathsf{G}'(m) := \mathsf{H}'(m)$ for all $m \neq m^*$ and let $\mathsf{G}'(m^*) = d^*$. Since H and H' are uniformly random, replacing them everywhere with $\mathsf{G} := \mathsf{H}(m^* := K^*)$ and $\mathsf{G}' := \mathsf{H}'(m^* := d^*)$ does not change the distribution. Replacing $\mathsf{H}(m^*)$ by K^* and $\mathsf{H}'(m^*)$ by d^* does not change the game either because K^* is the output of $\mathsf{H}(m^*)$ and d^* is the output of $\mathsf{H}'(m^*)$. We have shown that

$$\Pr[G_2^B \Rightarrow 1] = \Pr[G_0^B \Rightarrow 1].$$

GAME G_3. In game G_3, starting from game G_1 replace oracle access to H' with oracle access to G' in line 13. G' is defined as follows: pick a uniformly random d^* in line 8, let $\mathsf{G}'(m) := \mathsf{H}'(m)$ for all $m \neq m^*$ and let $\mathsf{G}'(m^*) = d^*$. Since H' is uniformly random, replacing it everywhere with $\mathsf{G}' := \mathsf{H}'(m^* := d^*)$ does not change the distribution. Replacing $\mathsf{H}'(m^*)$ by d^* does not change the game either because d^* is the output of $\mathsf{H}'(m^*)$. We have shown that

$$\Pr[G_3^B \Rightarrow 1] = \Pr[G_1^B \Rightarrow 1].$$

```
$\hat{B}^{\mathsf{G}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$
$b' \leftarrow B^{QDec_m^{\perp\mathsf{G},\mathsf{G}'}, \mathsf{G}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$
**return** $b'$

$\hat{C}^{\mathsf{G}'}(pk, (c^*, d^*), K^*, \mathsf{H})$
$b' \leftarrow B^{QDec_m^{\perp\mathsf{H},\mathsf{G}'}, \mathsf{H}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$
**return** $b'$
```

Figure 11: Adversaries $\hat{B}$ and $\hat{C}$ for the proof of Theorem 4.2

GAME G_4. In game G_4, starting from game G_2 we switch back to oracle access to H from G and H' from G'. Define $\hat{B}^{\mathsf{G}\times\mathsf{G}'}(pk, (c^*, d^*), K^*)$ as in Figure 11. For $S := \{m^*\}$ and $z := (pk, (c^* = Enc_1(pk, m^*), d^*), K^*)$, where $(pk, sk) \leftarrow Gen_1$, $m^* \xleftarrow{\$} \{0,1\}^n$, $d^* \xleftarrow{\$} \{0,1\}^n$ and $K^* \xleftarrow{\$} \{0,1\}^n$, we can write

$$\begin{aligned} P_{left} &:= \Pr[b = 1 : b \leftarrow \hat{B}^{\mathsf{G}\times\mathsf{G}'}(z)] = \Pr[G_2^B \Rightarrow 1] \\ P_{right} &:= \Pr[b = 1 : b \leftarrow \hat{B}^{\mathsf{H}\times\mathsf{H}'}(z)] = \Pr[G_4^B \Rightarrow 1] \\ P_{find} &:= \Pr[\mathsf{Find} : \hat{B}^{\mathsf{H}\times\mathsf{H}'\setminus S}(z)] = \Pr[G_6^B \Rightarrow 1] \end{aligned}$$

From the O2H Theorem (3.2) with $\mathsf{H} := \mathsf{G}\times\mathsf{G}'$, $\mathsf{G} := \mathsf{H}\times\mathsf{H}'$ and $A := \hat{B}$ we get

$$\left|\Pr[G_4^B \Rightarrow 1] - \Pr[G_2^B \Rightarrow 1]\right| \leq 2 \cdot \sqrt{(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1) \cdot \Pr[G_6^B \Rightarrow 1]}.$$

GAME G_5. In game G_5, starting from game G_3 we switch back to oracle access to H' from G' . Define $\hat{C}^{\mathsf{G}'}(pk, (c^*, d^*), K^*, \mathsf{H})$ as in Figure 11. For $S := \{m^*\}$ and $z := (pk, (c^* = Enc_1(pk, m^*), d^*), K^*, \mathsf{H})$, where $(pk, sk) \leftarrow Gen_1$, $m^* \xleftarrow{\$} \{0,1\}^n$,

$d^* \xleftarrow{\$} \{0,1\}^n$ and $K^* \xleftarrow{\$} \{0,1\}^n$, we can write

$$P_{\mathit{left}} := \Pr[b = 1 : b \leftarrow \hat{C}^{\mathsf{G}'}(z)] = \Pr[G_3^B \Rightarrow 1]$$
$$P_{\mathit{right}} := \Pr[b = 1 : b \leftarrow \hat{C}^{\mathsf{H}'}(z)] = \Pr[G_5^B \Rightarrow 1]$$
$$P_{\mathit{find}} := \Pr[\mathsf{Find} : \hat{C}^{\mathsf{H}' \setminus S}(z)] = \Pr[G_7^B \Rightarrow 1]$$

Note that H in z is used for queries to $QDec_m^{\perp}$ and for queries to the random oracle H. All other random oracle queries are for the oracle that the game is given access to (G' in game G_2 and H' in games G_4 and G_6).

From the O2H Theorem (3.2) with $\mathsf{H} := \mathsf{G}'$, $\mathsf{G} := \mathsf{H}'$ and $A := \hat{C}$ we get

$$\left|\Pr[G_5^B \Rightarrow 1] - \Pr[G_3^B \Rightarrow 1]\right| \leq 2 \cdot \sqrt{(d_{\mathsf{H}'} + d_{\mathsf{D}} + 1) \cdot \Pr[G_7^B \Rightarrow 1]}.$$

Since $G_4 = G_5$, we obtain:

$$\begin{aligned}
&\left|\Pr[G_0^B \Rightarrow 1] - \Pr[G_1^B \Rightarrow 1]\right| \\
&\qquad \leq \left|\Pr[G_0^B \Rightarrow 1] - \Pr[G_4^B \Rightarrow 1]\right| + \left|\Pr[G_1^B \Rightarrow 1] - \Pr[G_5^B \Rightarrow 1]\right| \\
&\qquad \leq \left|\Pr[G_2^B \Rightarrow 1] - \Pr[G_4^B \Rightarrow 1]\right| + \left|\Pr[G_3^B \Rightarrow 1] - \Pr[G_5^B \Rightarrow 1]\right|.
\end{aligned}$$

GAMES G_8, G_9. In games G_8, G_9 the random oracle H' is replaced with a random polynomial of degree $2(q_{\mathsf{H}} + q_{\mathsf{H}'} + q_{\mathsf{D}})$ over $\mathbb{F}_{2^n}$. By Zhandry [Zha12] this polynomial is indistinguishable from a random function, so this change is only conceptual and does not change success probabilities.

The second change in games G_8, G_9 is that the oracle $QDec_m^{\perp}$ does not make use of the secret key any longer (except for line 36 by testing if $Dec_1(sk, c) = m$ for given c and messages m). Recall that $\mathsf{H}' = \mathsf{H}(X)$ is a random polynomial of degree $\leq 2(q_{\mathsf{H}} + q_{\mathsf{H}'} + q_{\mathsf{D}})$ over $\mathbb{F}_{2^n}$. Therefore, given that (c, d) is a valid encapsulation (i.e., $m' \in \mathcal{M}$ and $d = \mathsf{H}'(m')$, for $m' := Dec_1(sk, c)$), m' lies within the roots of $\mathsf{H}'(X) - d$. In order to show that $QDec_m^{\perp}$ returns the same output in games G_6 and G_8 (and in games G_7, G_9) for every query $(c, d) \neq (c^*, d^*)$, consider the following cases, where we define $m' := Dec_1(sk, c)$.

- Case 1. $QDec_m^{\perp}(c, d)$ returns $\perp$ in games G_8, G_9, meaning that $m' \notin \mathsf{Roots}(\mathsf{H}'(X) - d)$. That latter happens iff $\mathsf{H}'(m') \neq d$ or $m' = \perp$, which is exactly the condition $QDec_m^{\perp}(c, d)$ returns $\perp$ in games G_6, G_7.
- Case 2. $QDec_m^{\perp}(c, d)$ does not return $\perp$ in games G_8, G_9, meaning that $m' \in$

$\mathsf{Roots}(\mathsf{H}'(X) - d)$ and $Dec_1(sk, c) = m'$. Consequently, $\mathsf{H}'(m') = d$ and $QDec_m^{\perp}(c, d)$ returns $K = \mathsf{H}(m')$ in games G_8, G_9. That latter is again exactly the condition $QDec_m^{\perp}(c, d)$ returns $K = \mathsf{H}(m')$ in games G_6, G_7.

It is easy to verify that the equivalence of $QDec_m^{\perp}$ in the games follows by negation and combining both cases. We have just shown

$$\Pr[G_6^B \Rightarrow 1] = \Pr[G_8^B \Rightarrow 1],$$
$$\Pr[G_7^B \Rightarrow 1] = \Pr[G_9^B \Rightarrow 1].$$

```
$A_b^{\mathcal{O}^{SC}_{\{m^*\}}, Pco}(pk, c^*)$
$d^* \xleftarrow{\$} \{0,1\}^n;\ K^* \xleftarrow{\$} \{0,1\}^n$
$\mathsf{H} \xleftarrow{\$} (\{0,1\}^n \to \{0,1\}^n)$
$\mathsf{H}' = \mathsf{H}'(X) \xleftarrow{\$}$ polynomial of degree $\leq 2(q_{\mathsf{H}} + q_{\mathsf{H}'} + q_D)$ over $\mathbb{F}_{2^n}$
$m' \leftarrow B^{QDec_m^{\perp \mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{H}, \mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{H}'}, \mathcal{O}^{SC}_{\{m^*\}} \circ (\mathsf{H} \times \mathsf{H}')}(pk, (c^*, d^*), K^*)$        $/\!/ b = 0$
$m' \leftarrow B^{QDec_m^{\perp \mathsf{H}, \mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{H}'}, \mathsf{H} \times (\mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{H}')}(pk, (c^*, d^*), K^*)$        $/\!/ b = 1$
return $m'$
```

Figure 12: Adversaries A_b against OW-PCA for the proof of Theorem 4.2. Oracle $QDec_m^{\perp}(c, d)$ is defined as in games G_8, G_9 of Figure 10. Note that the oracle $QDec_m^{\perp}$ uses sk in line 36 for decrypting c, but A_b does not have access to sk. This problem can be solved by using the plaintext checking oracle, because $Pco(m, c)$ returns 1 if and only if $Dec_1(sk, c) = m$.

In the original proof, the adversaries A_b were constructed trivially against the OW-PCA security of PKE_1 simulating games G_8 and G_9. In our case, this is not possible, because in game G_8, G_9, the adversary has access to the oracle $(\mathsf{H} \times \mathsf{H}') \setminus \{m^*\}$ or $\mathsf{H}' \setminus \{m^*\}$ which might leak some information about m^*. We give two different proofs that eliminate this problem. The first proof assumes OW-PCA security of PKE_1 (like in the original theorem statement) and the second proof assumes IND-PCA security of PKE_1. The proofs are almost identical for games G_8 and G_9, so we only give the proof for game G_9 (that is the proof for adversary A_1).

(a) Proof using OW-PCA

Note that an oracle query to $\mathsf{H}' \setminus \{m^*\}$ is equivalent to querying H' and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Thus, we can define an adversary $A_1^{\mathcal{O}^{SC}_{\{m^*\}}, Pco}(pk, c^*)$ (see Figure 12) that simulates game G_9, using $\mathcal{O}^{SC}_{\{m^*\}}$ to simulate the queries to the punctured oracles, and c^* as the ciphertext $Enc_1(pk, m^*)$ where $(pk, sk) \leftarrow Gen$ and $m^* \xleftarrow{\$} \{0,1\}^n$. By writing $\mathcal{O}^{SC}_{\{m^*\}} \circ \mathsf{H}'$ we mean querying H' and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Then

$$\Pr[G_9^B \Rightarrow 1] = \Pr[\mathsf{Find} : A_1^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)]$$

where $c^* := Enc_1(pk, m^*)$ and m^* is uniform. By Theorem 3.3 (with $A := A_1$, $B := E_1$, $S = \{m^*\}$, $z := (pk, c^*)$ and $d := d_{\mathsf{H}'} + d_{\mathsf{D}}$)

$$\Pr[\mathsf{Find} : A_1^{\mathcal{O}^{SC}_{\{m^*\}}}(pk, c^*)] \leq 4(d_{\mathsf{H}'} + d_{\mathsf{D}}) \cdot \Pr[m^* = E_1(pk, c^*)].$$

Here E_1 is the adversary that stops A_1 at a random query as in Theorem 3.3. The runtime of E_1 is approximately the same as that of A_1. Then from the OW-PCA security of the original encryption scheme, we have

$$\Pr[m^* = E_1(pk, c^*)] \leq Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)$$

and thus

$$\Pr[G_9^B \Rightarrow 1] \leq 4(d_{\mathsf{H}'} + d_{\mathsf{D}}) \cdot Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1).$$

Analogously, we get

$$\Pr[G_8^B \Rightarrow 1] \leq 4(d_{\mathsf{H}} + d_{\mathsf{H}'} + d_{\mathsf{D}}) \cdot Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0),$$

because $d := d_{\mathsf{H}} + d_{\mathsf{H}'} + d_{\mathsf{D}}$ if we use the O2H Theorem 3.3 in the A_0 case.

Collecting the probabilities gives us

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq \sqrt{d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1} \cdot \sqrt{4(d_{\mathsf{H}} + d_{\mathsf{H}'} + d_{\mathsf{D}}) Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0)}$$
$$+ \sqrt{d_{\mathsf{H}'} + d_{\mathsf{D}} + 1} \cdot \sqrt{4(d_{\mathsf{H}'} + d_{\mathsf{D}}) Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)}$$

and further simplifying proves the theorem:

$$\begin{aligned} Adv^{\textsf{IND-CCA}}_{\textsf{QKEM}^{\perp}_{m}}(B) \leq 2(d_{\textsf{H}'} + d_{\textsf{H}} + d_{\textsf{D}} + 1) \cdot \sqrt{Adv^{\textsf{OW-PCA}}_{\textsf{PKE}_1}(E_0)} \\ + 2(d_{\textsf{H}'} + d_{\textsf{D}} + 1) \cdot \sqrt{Adv^{\textsf{OW-PCA}}_{\textsf{PKE}_1}(E_1)}. \end{aligned}$$

(b) Proof using IND-PCA

IND-PCA security implies that $Enc_1(pk, m^*)$ is indistinguishable from $Enc_1(pk, 0)$. If game G_{10} is obtained from game G_9 by replacing $Enc_1(pk, m^*)$ with $Enc_1(pk, 0)$ on line 30, we have

$$\left|\Pr[G_9^B \Rightarrow 1] - \Pr[G_{10}^B \Rightarrow 1]\right| \leq Adv^{\textsf{IND-PCA}}_{\textsf{PKE}}(A).$$

A is defined as adversary against the IND-PCA security of $\textsf{PKE}_1$.

Note that an oracle query to $\textsf{H}' \setminus \{m^*\}$ is equivalent to querying $\textsf{H}'$ and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Thus, we can define an adversary $A_1^{\mathcal{O}^{SC},Pco}(pk, c^*)$ (see Figure 12) that simulates game G_{10}, using $\mathcal{O}^{SC}_{\{m^*\}}$ to simulate the queries to the punctured oracles, and c^* as the ciphertext $Enc_1(pk, 0)$ where $(pk, sk) \leftarrow Gen$. By writing $\mathcal{O}^{SC}_{\{m^*\}} \circ \textsf{H}'$ we mean querying $\textsf{H}'$ and $\mathcal{O}^{SC}_{\{m^*\}}$ consecutively. Then

$$\Pr[G_{10}^B \Rightarrow 1] = \Pr[\textsf{Find} : A_1^{\mathcal{O}^{SC}_{\{m^*\}},Pco}(pk, c^*)]$$

where $c^* := Enc_1(pk, 0)$. By Corollary 3.1 (with $A := A_1$, $S = \{m^*\}$, $z := (pk, c^*)$ and $d := d_{\textsf{H}'} + d_{\textsf{D}}$)

$$\Pr[\textsf{Find} : A_1^{\mathcal{O}^{SC}_{\{m^*\}},Pco}(pk, c^*)] \leq \frac{4(d_{\textsf{H}'} + d_{\textsf{D}})}{n}$$

and thus

$$\Pr[G_9^B \Rightarrow 1] \leq Adv^{\textsf{IND-PCA}}_{\textsf{PKE}_1}(A) + \frac{4(d_{\textsf{H}'} + d_{\textsf{D}})}{n}.$$

Analogously, we get

$$\Pr[G_8^B \Rightarrow 1] \leq Adv^{\textsf{IND-PCA}}_{\textsf{PKE}_1}(A) + \frac{4(d_{\textsf{H}'} + d_{\textsf{H}} + d_{\textsf{D}})}{n},$$

because $d := d_{\textsf{H}} + d_{\textsf{H}'} + d_{\textsf{D}}$ if we use the O2H Theorem 3.3 in the A_0 case.

Collecting the probabilities gives us

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq \sqrt{d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A) + \frac{4(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}})}{n}}$$
$$+ \sqrt{d_{\mathsf{H}'} + d_{\mathsf{D}} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A) + \frac{4(d_{\mathsf{H}'} + d_{\mathsf{D}})}{n}}$$

and further simplifying proves the theorem:

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq 2\sqrt{d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A)} + \frac{4(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1)}{\sqrt{n}}.$$

Results
Since the number of queries q is always larger or equal to the query depth d, we get the following two bounds:

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq 2(q_{\mathsf{H}'} + q_{\mathsf{H}} + q_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0)}$$
$$+ 2(q_{\mathsf{H}'} + q_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)}$$
$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq 2\sqrt{q_{\mathsf{H}'} + q_{\mathsf{H}} + q_{\mathsf{D}} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A)} + \frac{4(q_{\mathsf{H}'} + q_{\mathsf{H}} + q_{\mathsf{D}} + 1)}{\sqrt{n}}.$$

The original theorem statement from [HHK17] said that the running time of A is about that of B. Since A computes the roots of polynomials of degree $\leq 2q_{\mathsf{H}'}$, it is unlikely that the running time of A is linear to B . The same problem remains in our proof. But, if the running time of B is polynomial, then so is A, because finding roots of polynomials takes polynomial time [Ben81].

□

4.3 $\mathsf{QU}^{\not\perp}_{m}$: from OW-PCA to IND-CCA security in the QROM

$\mathsf{QU}^{\not\perp}_{m}$ transforms an OW-PCA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism with implicit rejection [HHK17]. Implicit rejection (noted by $\not\perp$ in $\mathsf{QU}^{\not\perp}_{m}$) means that decapsulation of an invalid ciphertext results in a pseudorandom key K.

```
$\underline{Gen^{\not\perp}}$
$(pk', sk') \leftarrow Gen_1$
$s \xleftarrow{\$} \mathcal{M}$
$sk := (sk', s)$
return $(pk', sk)$

$\underline{QEnc_m^{\mathsf{H},\mathsf{H}'}(pk)}$
$m \xleftarrow{\$} \mathcal{M}$
$c \leftarrow Enc_1(pk, m)$
$d := \mathsf{H}'(m)$
$K := \mathsf{H}'(m)$
return $(K, (c, d))$

$\underline{QDec_m^{\not\perp \mathsf{H},\mathsf{H}'}(sk' = (sk, s), (c, d))}$
$m' := Dec_1(sk, c)$
if $m' = \perp$ or $\mathsf{H}'(m') \neq d$
    return $K := \mathsf{H}(s, (c, d))$
else return $K := \mathsf{H}(m')$
```

Figure 13: IND-CCA-secure key encapsulation mechanism $\mathsf{QKEM}_m^{\not\perp} = \mathsf{QU}_m^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$. We write ${}^{\mathsf{H},\mathsf{H}'}$ to emphasize that $QEnc$ and $QDec$ use the oracles H and H′.

Take $\mathsf{QKEM}_m^{\not\perp} = \mathsf{QU}_m^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$, where public-key encryption scheme $\mathsf{PKE}_1 = (Gen_1, Enc_1, Dec_1$ has message space $\mathcal{M} = \{0,1\}^n$, and random oracles $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ and $\mathsf{H}' : \{0,1\}^n \to \{0,1\}^n$. The algorithms of $\mathsf{QKEM}_m^{\not\perp} = (Gen^{\not\perp}, QEnc_m, QDec_m^{\not\perp})$ are defined in Figure 13.

The following theorem establishes that IND-CCA security of $\mathsf{QKEM}_m^{\not\perp}$ reduces to the OW-PCA security of PKE_1 in the QROM.

Theorem 4.3 (PKE_1 OW-PCA (IND-PCA) $\xrightarrow{\textit{QROM}}$ $\mathsf{QKEM}_m^{\not\perp}$ IND-CCA)**.** *If* PKE_1 *is* δ_1*-correct, then so is* $\mathsf{QKEM}_m^{\not\perp}$*. For any* IND-CCA *quantum adversary* B *that issues at most* q_D *(classical) queries to the decapsulation oracle* $QDec_m^{\not\perp}$ *with query depth* d_D*, at most* q_H *queries to the quantum random oracle* H *with query depth* d_H *and at most* $q_{\mathsf{H}'}$ *queries to the quantum random oracle* H′ *with query depth* $d_{\mathsf{H}'}$*,*

(a) there exist OW-PCA *quantum adversaries* E_0*,* E_1 *issuing* $2q_\mathsf{D}q_{\mathsf{H}'}$ *queries to oracle* Pco *such that*

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}_m^{\not\perp}}(B) \leq 2(d_{\mathsf{H}'} + d_\mathsf{H} + d_\mathsf{D} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0)} + 2(d_{\mathsf{H}'} + d_\mathsf{D} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)}.$$

(b) there exists an IND-PCA *quantum adversary* A *issuing* $2q_\mathsf{D}q_{\mathsf{H}'}$ *queries to oracle* Pco *such that*

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}_m^{\not\perp}}(B) \leq 2\sqrt{d_{\mathsf{H}'} + d_\mathsf{H} + d_\mathsf{D} + 1} \cdot \sqrt{Adv^{\mathsf{IND\text{-}PCA}}_{\mathsf{PKE}_1}(A)} + \frac{4(d_{\mathsf{H}'} + d_\mathsf{H} + d_\mathsf{D} + 1)}{\sqrt{n}}.$$

The original bound from [HHK17] is

$$Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\not\perp}_m}(B) \le (2q_{\mathsf{H}'} + q_{\mathsf{H}}) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(A)}.$$

The proof is almost the same as the proof of Theorem 4.2. The difference is that in the proof of Theorem 4.2, the simulation of $QDec$ always knows if a given ciphertext is valid or not. If it is not valid, $\perp$ is returned. In the proof of Theorem 4.3 one can simply replace $\perp$ by $\mathsf{H}(s,(c,d))$.

4.4 The resulting KEMs

The transformations T and $\{\mathsf{QU}^{\perp}_m, \mathsf{QU}^{\not\perp}_m\}$ from previous sections can be combined to obtain two transformations $\mathsf{QKEM}^{\perp}_m$ and $\mathsf{QKEM}^{\not\perp}_m$. If we have public-key encryption scheme $\mathsf{PKE} = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ and randomness space $\mathcal{R}$, and random oracles $\mathsf{G} : \mathcal{M} \to \mathcal{R}$, $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ and $\mathsf{H}' : \{0,1\}^n \to \{0,1\}^n$, we get:

$$\begin{aligned}\mathsf{QKEM}^{\perp}_m &:= \mathsf{QU}^{\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H},\mathsf{H}'] = (Gen, QEnc_m, QDec^{\perp}_m)\\ \mathsf{QKEM}^{\not\perp}_m &:= \mathsf{QU}^{\not\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H},\mathsf{H}'] = (Gen^{\not\perp}, QEnc_m, QDec^{\not\perp}_m)\end{aligned}$$

Algorithms Gen, $QEnc$, $QDec$ are given if Figures 9 and 13.

Combining Theorems 4.1–4.3 gives us the concrete bounds of the IND-CCA security of these KEMs in the quantum random oracle model. $d_{\mathsf{H}'}, d_{\mathsf{H}}, d_{\mathsf{G}}, d_{\mathsf{P}}, d_{\mathsf{D}}$ are the query depths for quantum random oracles $\mathsf{H}', \mathsf{H}, \mathsf{G}$, the plaintext checking oracle Pco and the decapsulation oracle $QDec^{\perp}_m$, respectively. q_{G} is the number of queries to G. To simplify, we assume that $\sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(C)} = \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(E)} = \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(A)}$. We get the following bound:

$$\begin{aligned}&Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_m}(B) \le\\ &\le 2(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0)} + 2(d_{\mathsf{H}'} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)}\\ &\le (4d_{\mathsf{H}'} + 2d_{\mathsf{H}} + 4d_{\mathsf{D}} + 4) \cdot \sqrt{8 \cdot \delta \cdot (q_{\mathsf{G}} + 1)^2 + (4d_{\mathsf{G}} + 4d_{\mathsf{P}} + 5) \cdot \sqrt{Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(A)}}.\end{aligned}$$

Similarly, if we use a slightly stronger assumption of the IND-CPA-security of PKE and assume that $\sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(G)} = \sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(F)} = \sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(A)}$, we get a better bound:

$$\begin{aligned}
&Adv^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(B) \leq \\
&\leq 2(d_{\mathsf{H}'} + d_{\mathsf{H}} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_0)} + 2(d_{\mathsf{H}'} + d_{\mathsf{D}} + 1) \cdot \sqrt{Adv^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(E_1)} \\
&\leq (4d_{\mathsf{H}'} + 2d_{\mathsf{H}} + 4d_{\mathsf{D}} + 4) \cdot \\
&\quad \sqrt{8 \cdot \delta \cdot (q_{\mathsf{G}} + 1)^2 + (1 + 2\sqrt{d_{\mathsf{G}} + d_{\mathsf{P}} + 1}) \cdot \sqrt{Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(A) + \frac{4(d_{\mathsf{G}} + d_{\mathsf{P}})}{|\mathcal{M}|}}}.
\end{aligned}$$

The bounds for $\mathsf{QKEM}^{\not\perp}_{m}$ are the same.

5 Conclusion

With the intention to understand the impact of semi-classical One-Way to Hiding Theorem and to increase tightness of post-quantum secure encryption schemes, we gave on overview of the background in quantum cryptography and recreated proofs by Hofheinz et al. [HHK17] using semi-classical oracles. A detailed proof was given for two transformations T and $\mathsf{QU}_m^{\perp}$ that taken together yield an $\mathsf{IND\text{-}CCA}$ secure KEM from an $\mathsf{OW\text{-}CPA}$ secure public key encryption scheme. While the original analysis only assumed one-wayness from these two transformations, we showed that if we use slightly stronger assumption (that is $\mathsf{IND\text{-}CPA}$ and $\mathsf{IND\text{-}PCA}$ security, respectively), the tightness improves considerably.

Since the two transformations that gave the biggest improvement for tightness are incompatible (from $\mathsf{IND\text{-}CPA}$ to $\mathsf{OW\text{-}PCA}$ and $\mathsf{IND\text{-}PCA}$ to $\mathsf{IND\text{-}CCA}$), we view it as an open problem to find such transformation from $\mathsf{OW\text{-}PCA}$ to $\mathsf{IND\text{-}PCA}$ to possibly achieve even better bounds.

We also gave a list of papers that use the old version of the One-Way to Hiding Theorem. A similar analysis of recreating the security proofs with the improved version of the O2H Theorem could be carried out for all of these to improve the security bounds and possibly end up with tighter post-quantum secure encryption schemes.

References

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. "Quantum security proofs using semi-classical oracles". In: *Advances in Cryptology – CRYPTO 2019*. To appear. Springer Berlin Heidelberg, 2019. Full version at `https://eprint.iacr.org/2018/904`.

[ATTU16] Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. "Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation". In: *Post-Quantum Cryptography*. Cham: Springer International Publishing, 2016, pp. 44–63. Full version at `https://eprint.iacr.org/2016/197`.

[BR93] Mihir Bellare and Phillip Rogaway. *Random oracles are practical: A paradigm for designing efficient protocols.* V. Ashby, editor, ACM CCS 93, pages 62–73. ACM Press. 1993. DOI: `10.1145/168588.168596`.

[Ben81] Michael Ben-Or. "Probabilistic Algorithms in Finite Fields". In: *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*. SFCS '81. Washington, DC, USA: IEEE Computer Society, 1981, pp. 394–398. DOI: `10.1109/SFCS.1981.37`.

[Bon+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. "Random Oracles in a Quantum World". In: *Advances in Cryptology – ASIACRYPT 2011*. Springer Berlin Heidelberg, 2011, pp. 41–69. Full version at `https://eprint.iacr.org/2010/428`.

[BL19] Anne Broadbent and Sébastien Lord. *Uncloneable Quantum Encryption via Random Oracles*. Cryptology ePrint Archive, Report 2019/257. `https://eprint.iacr.org/2019/257`. 2019.

[Cha+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. *Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives*. Cryptology ePrint Archive, Report 2017/279. `https://eprint.iacr.org/2017/279`. 2017.

[Cor+02] Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen. "GEM: A Generic Chosen-Ciphertext Secure Encryption Method". In: *Topics in Cryptology — CT-RSA 2002*. Springer, 2002, pp. 263–276.

[CS98] Ronald Cramer and Victor Shoup. "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack". In: *Advances in Cryptology — CRYPTO '98*. Springer, 1998, pp. 13–25.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: vol. 26. 1. Jan. 2013, pp. 80–101. DOI: 10.1007/s00145-011-9114-1.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *Theory of Cryptography*. Cham: Springer International Publishing, 2017, pp. 341–371. Full version at https://eprint.iacr.org/2017/604.

[HKSU18] Kathrin Hövelmanns, Eike Kiltz, Sven Schäge, and Dominique Unruh. *Generic Authenticated Key Exchange in the Quantum Random Oracle Model*. Cryptology ePrint Archive, Report 2018/928. https://eprint.iacr.org/2018/928. 2018.

[Jia+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: *Advances in Cryptology – CRYPTO 2018*. Cham: Springer International Publishing, 2018, pp. 96–125. Full version at https://eprint.iacr.org/2017/1096.

[JZM19a] Haodong Jiang, Zhenfeng Zhang, and Zhi Ma. "Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model". In: *Public-Key Cryptography – PKC 2019*. Cham: Springer International Publishing, 2019, pp. 618–645. Full version at https://eprint.iacr.org/2019/052.

[JZM19b] Haodong Jiang, Zhenfeng Zhang, and Zhi Ma. *Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model*. Cryptology ePrint Archive, Report 2019/134. https://eprint.iacr.org/2019/134. 2019.

[KLCK18] Sungsook Kim, Jeeun Lee, Rakyong Choi, and Kwangjo Kim. "Validating IGE Mode of Block Cipher from Quantum Adversaries". In: 2018.

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

[OP01] Tatsuaki Okamoto and David Pointcheval. “REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform”. In: *Topics in Cryptology — CT-RSA 2001*. Springer, 2001, pp. 159–174.

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. “Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model”. In: *Advances in Cryptology – EUROCRYPT 2018*. Cham: Springer International Publishing, 2018, pp. 520–551. Full version at `https://eprint.iacr.org/2017/1005`.

[SY17] Fang Song and Aaram Yun. “Quantum Security of NMAC and Related Constructions”. In: *Advances in Cryptology – CRYPTO 2017*. Cham: Springer International Publishing, 2017, pp. 283–309. Full version at `https://eprint.iacr.org/2017/509`.

[SRP18] Alan Szepieniec, Reza Reyhanitabar, and Bart Preneel. *Key Encapsulation from Noisy Key Agreement in the Quantum Random Oracle Model*. Cryptology ePrint Archive, Report 2018/884. `https://eprint.iacr.org/2018/884`. 2018.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. “Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms”. In: *Theory of Cryptography*. Springer Berlin Heidelberg, 2016, pp. 192–216. Full version at `https://eprint.iacr.org/2015/1210`.

[Unr14] Dominique Unruh. “Quantum Position Verification in the Random Oracle Model”. In: *Advances in Cryptology – CRYPTO 2014*. Springer Berlin Heidelberg, 2014, pp. 1–18. Full version at `https://eprint.iacr.org/2014/118`.

[Unr15a] Dominique Unruh. “Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model”. In: *Advances in Cryptology - EUROCRYPT 2015*. Springer Berlin Heidelberg, 2015, pp. 755–784. Full version at `https://eprint.iacr.org/2014/587`.

[Unr15b] Dominique Unruh. “Revocable Quantum Timed-Release Encryption”. In: *J. ACM* 62.6 (Dec. 2015), 49:1–49:76. ISSN: 0004-5411. DOI: `10.1145/2817206`.

[Zha12] Mark Zhandry. “Secure Identity-Based Encryption in the Quantum Random Oracle Model”. In: *Advances in Cryptology – CRYPTO 2012*. Springer Berlin Heidelberg, 2012, pp. 758–775. Full version at `https://eprint.iacr.org/2012/076`.

Appendix

I. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Reelika Tõnisson**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Tighter post-quantum secure encryption schemes using semi-classical oracles,

supervised by Dominique Peer Ghislain Unruh.

2 I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3 I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4 I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Reelika Tõnisson
16.05.2019