# Post-Quantum Security of Key Encapsulation Mechanism against CCA Attacks with a Single Decapsulation Query

Haodong Jiang[1], Zhi Ma[1], and Zhenfeng Zhang[2]

[1] Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, 450001, Henan, China

[2] TCA Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing,100190, China

hdjiang13@gmail.com, mzh2830@163.com, zhenfeng@iscas.ac.cn

**Abstract.** Recently, in post-quantum cryptography migration, it has been shown that an IND-1-CCA-secure key encapsulation mechanism (KEM) is required for replacing an ephemeral Diffie-Hellman (DH) in widely-used protocols, e.g., TLS, Signal, and Noise. IND-1-CCA security is a notion similar to the traditional IND-CCA security except that the adversary is restricted to one single decapsulation query. At EUROCRYPT 2022, based on CPA-secure public-key encryption (PKE), Huguenin-Dumittan and Vaudenay presented two IND-1-CCA KEM constructions called $T_{CH}$ and $T_H$, which are much more efficient than the widely-used IND-CCA-secure Fujisaki-Okamoto (FO) KEMs. The security of $T_{CH}$ was proved in both random oracle model (ROM) and quantum random oracle model (QROM). However, the QROM proof of $T_{CH}$ relies on an additional ciphertext expansion. While, the security of $T_H$ was only proved in the ROM, and the QROM proof is left open.

In this paper, we prove the security of $T_H$ and $T_{RH}$ (an implicit variant of $T_H$) in both ROM and QROM with much tighter reductions than Huguenin-Dumittan and Vaudenay's work. In particular, our QROM proof will not lead to ciphertext expansion. Moreover, for $T_{RH}$, $T_H$ and $T_{CH}$, we also show that a $O(1/q)$ ($O(1/q^2)$, resp.) reduction loss is unavoidable in the ROM (QROM, resp.), and thus claim that our ROM proof is optimal in tightness. Finally, we make a comprehensive comparison among the relative strengths of IND-1-CCA and IND-CCA in the ROM and QROM.

**Keywords:** quantum random oracle model · key encapsulation mechanism · 1CCA security · tightness · KEM-TLS

## 1 Introduction

With the gradual advancement of NIST post-quantum cryptography (PQC) standardization, research on migration from the existing protocols to post-quantum protocols with new standardized algorithms has been a hot topic. For ephemeral key establishment, one has to move the current Diffie-Hellman (DH) key-exchange to post-quantum key encapsulation mechanisms (KEMs).

The security goal required for such a substitutive KEM has been thoroughly analyzed for TLS 1.3 [15, 21], KEM-TLS [37, 38], Signal [9] and Noise [2]. In general, the security of these DH-based protocols is proved based on the PRF-ODH assumption [10]. But, when one uses KEM to replace DH, IND-1-CCA security is required instead, see post-quantum TLS [15, 21, 37, 38], post-quantum Signal [9] and post-quantum Noise [2]. In addition, Huguenin-Dumittan and Vaudenay [21] pointed out that IND-1-CCA KEMs are also used in Ratcheting [4, 25, 32]. Roughly speaking, IND-1-CCA security says that the adversary is required to distinguish an honestly generated key from a randomly generated key by making at most a *single* decapsulation query.

IND-1-CCA security is obviously implied by IND-CCA security that has been widely studied in [16, 17, 35, 22–24, 6, 26, 19, 14]. In general, IND-CCA-secure KEMs are obtained by applying Fujisaki-Okamoto-like (FO-like) transform to a OW/IND-CPA-secure public-key encryption (PKE). In particular, all the KEM candidates to be standardized and Round-4 KEM submissions [30] adopted FO-like construction. The current implementations of KEM-TLS [37, 38], post-quantum TLS 1.3 [31] and post-quantum Noise framework [2] directly take IND-CCA-secure KEMs as IND-1-CCA-secure KEMs. However, FO-like IND-CCA-secure KEMs require re-encryption of the decrypted plaintext in decapsulation, making it an expensive operation. For instance, as shown in [21], when re-encryption is removed, there will be a 2.17X and 6.11X speedup over decapsulation in CRYSTALS-Kyber [8] and FrodoKEM [28] respectively. Moreover, the re-encryption makes the KEM more vulnerable to side-channel attacks and almost all the NIST-PQC Round-3 KEMs are affected, see [39, 3]. Meanwhile, the side-channel protection of re-encryption will significantly increase deployment costs and thus complicate the integration of NIST-PQC KEMs [27]. Therefore, designing a dedicated IND-1-CCA-secure KEM without re-encryption was taken as an open problem raised by Schwabe, Stebila and Wiggers [37].

This problem was recently studied by Huguenin-Dumittan and Vaudenay [21]. They found that simple modification of the current FO-like KEMs can achieve an IND-1-CCA-secure KEM without re-encryption. In detail, they presented two constructions. One construction (called $T_{CH}$) is that an additional hash value of message and ciphertext is appended to the original ciphertext (usually called key-confirmation). The security of $T_{CH}$ was proved in the random oracle model (ROM) with tightness $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}$, and in the quantum random oracle model (QROM) with tightness $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}^2$, where $\epsilon_R$ ($\epsilon_{\mathcal{A}}$, resp.) is the advantage of the reduction $R$ ( adversary $\mathcal{A}$, resp.) breaking the security of the underlying PKE (the resulting KEM, resp.), and $q$ is the number of $\mathcal{A}$'s queries to the random oracle (RO). Different from ROM, QROM allows the adversary to make quantum queries to the RO. To prove the post-quantum security of cryptosystem, one has to prove in the QROM [7]. Unfortunately, the QROM proof of $T_{CH}$ in [21] relies on key-confirmation (i.e., an additional length-preserving hash is required)[3], which will leads to a ciphertext expansion.

[3] The length-preserving property of the additional hash is implicitly required by the QROM proof in [21] and will increase the ciphertext size by $|ct| + |m|$, where $|ct|$

The second construction given in [21] is $T_H$, where ciphertext $c$ is obtained by encrypting a randomly message $m$, the key is derived by $H(m, c)$. In decapsulation, if $m' = Dec(sk, c) = \perp$, $\perp$ is returned, otherwise $H(m', c)$ is returned, where $Dec$ is the decryption algorithm of PKE, and $sk$ is the secret key. In fact, $T_H$ is the same as $U^{\perp}$ in [17]. Note that both $T_{CH}$ and $T_H$ do not require re-encryption. But, compared with $T_{CH}$, $T_H$ will not lead to ciphertext expansion. However, Huguenin-Dumittan and Vaudenay [21] only gave the ROM proof of $T_H$ with tightness $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}$. The QROM proof is left open due to the challenge that a lot of RO programming property is used[4].

### 1.1 Our Contributions

Our contributions are as follows.

1. First, we prove the security of $T_H$ and its implicit variant $T_{RH}$ in both ROM and QROM. $T_{RH}$ is the same as the $T_H$ except that in decapsulation a pseudorandom value $H(\star, c)$ is returned instead of an explicit $\perp$ for an invalid ciphertext $c$ such that $Dec(sk, c) = \perp$. In particular, our QROM proof will not lead to ciphertext expansion. In the ROM, our reduction has tightness $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}$, which is much tighter than $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}$ given by [21] for $T_H$. In the QROM, our reduction achieves tightness $\epsilon_R \approx O(1/q^2)\epsilon_{\mathcal{A}}^2$, which is tighter than $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}^2$ given by Huguenin-Dumittan and Vaudenay in [21] for $T_{CH}$ (with ciphertext expansion).
2. Then, for $T_H$, $T_{RH}$ and $T_{CH}$, we show that if the underlying PKE meets malleability property, a $O(1/q)$ ($O(1/q^2)$, resp.) loss is unavoidable in the ROM (QROM, resp.). That is, our ROM reduction is optimal in general. Roughly speaking, the malleability property says that an adversary can efficiently transform a ciphertext into another ciphertext which decrypts to a related plaintext. In particular, such a malleability property is met by real-world PKE schemes, e.g., ElGamal, FrodoKEM.PKE [28], CRYSTALS–Kyber.PKE [8], etc..
3. Finally, we compare the relative strengths of IND-1-CCA and IND-CCA in the ROM and QROM, see Fig 1. For each pair of notions A, B $\in$\{IND-1-CCA ROM, IND-CCA ROM, IND-1-CCA QROM, IND-CCA QROM\}, we show either an implication or a separation, so that no relation remains open.

---

is the PKE ciphertext size and $|m|$ is the message size. Very recently, Huguenin-Dumittan and Vaudenay [20] updated their ePrint version and presented a new proof for $T_{CH}$ using the extractable RO technique [14] with improved bound $\epsilon_R \approx O(1/q^2)\epsilon_{\mathcal{A}}^2 - O(q^3/2^n) - O(q/\sqrt{2^n})$ ($n$ is the RO-output length), which removes the length-preserving requirement. But, the additional key-confirmation is still required.

[4] At EUROCRYPT 2022, Huguenin-Dumittan and Vaudenay [21] conjectured that the popular compressed oracle technique proposed by Zhandry [42] might be of use in the QROM proof. Surprisingly, in our QROM proof, only the other two well-known techniques called one-way to hiding (O2H) [1, 6] and measure-and-reprogram [12] are used.

*Remark 1.* Our construction $T_{RH}$ is essentially the construction $U^{\not\perp}$ in [17], except that the secret seed $s$ in decapsulation is replaced by a public value $\star$ ($\star$ can be any fixed message). In fact, our proof can work for both secret seed and public value thanks to the newly introduced decapsulation simulation technique, while the current IND-CCA proofs for implicit FO-KEMs (e.g., see [17, 22]) can only work for secret seed. We choose to replace secret seed by public value since it reduces the secret key size and makes the construction more concise. Morerover, from a high-assurance implementation (i.e., side-channel protected) point of view, public value is also preferable to secure seed, see comments by Schneider at NIST pqc-forum [36].

Table 1: Reduction tightness in the ROM/QROM.

| Transformation | Reduction tightness | Ciphertext expansion | Re-encryption | ROM or QROM |
|---|---|---|---|---|
| *FO* [17] | $\epsilon_R \approx \epsilon_{\mathcal{A}}$ | N | Y | ROM |
| $T_{CH}$ [21] | $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}$ | Y | N | ROM |
| $T_H$ [21] | $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}$ | N | N | ROM |
| Our $T_{RH}$ and $T_H$ | $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}$ | N | N | ROM |
| *FO* [24, 6] | $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}^2$ | N | Y | QROM |
| $T_{CH}$ [21] | $\epsilon_R \approx O(1/q^3)\epsilon_{\mathcal{A}}^2$ | Y | N | QROM |
| Our $T_{RH}$ and $T_H$ | $\epsilon_R \approx O(1/q^2)\epsilon_{\mathcal{A}}^2$ | N | N | QROM |

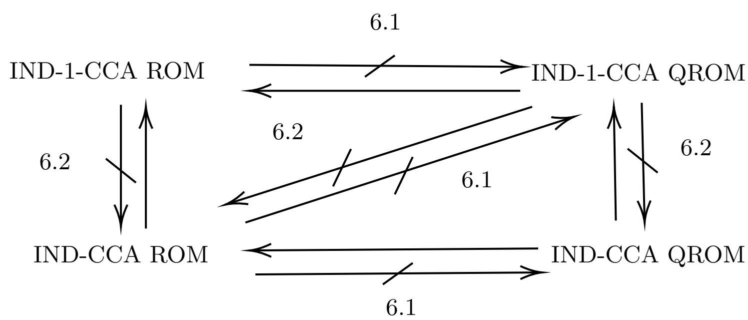


Fig. 1: The relations among notions of security for KEM. An arrow is an implication, and there is a path from A to B if and and only A $\Rightarrow$ B. The hatched arrows represent separations actually we prove. The number on an hatched arrow refers to the theorem in this paper which establishes this relationship.

### 1.2 Practical Impact

An IND-1-CCA KEM is sufficient to replace Diffie-Hellman in the post-quantum migration of the widely-deployed protocols, such as TLS 1.3, Signal and Noise. Our results show that IND-1-CCA-secure KEMs can be constructed in the ROM and QROM without re-encryption and cipher-expansion. Compared with IND-CCA-secure KEMs based on FO transform, such as CRYSTALS-Kyber, the IND-1-CCA-secure KEMs based on $T_H$ and $T_{RH}$ do not require the re-encryption in decapsulation. The re-encryption is highly vulnerable to attacks and its side-channel protection will significantly increase deployment costs. Thus, from a practical point of view, removing the re-encryption of FO-like KEMs will improve the performance of embedded side-channel secure implementations. Therefore, according to our results, one can easily transform CRYSTALSCKyber.PKE into an IND-1-CCA-secure KEM without re-encryption and cipher-expansion, and then establish post-quantum-secure variants of TLS 1.3, Signal and Noise with better performance in the embedded implementation.

### 1.3 Open Problem

We prove a $O(1/q)$ ($O(1/q^2)$, resp.) loss is unavoidable in the ROM (QROM, resp.) for the IND-1-CCA KEMs in this paper and [21]. Our ROM proof essentially matches this loss. However, our QROM tightness does not match $O(1/q^2)$. Thus, a natural question is can our QROM reduction tightness be further improved, or can one find a new attack that matches the QROM proof in this paper.

### 1.4 Technique Overview

**Construction and reduction**. Re-encryption is the core feature of FO-like CCA-KEMs, which guarantees that only specific valid ciphertexts can be correctly decapsulated, and thus makes the decapsulation simulation in the ROM/QROM proof easy (see [16, 17, 35, 22–24, 6, 19, 14, 18]). However, on the other hand, as mentioned earlier, removing the re-encryption will bring a significant speed boost in decapsulation [37, 21] and reduce the risk of side-channel attacks [39, 3].

However, removing re-encryption makes the current decapsulation simulation for FO-like CCA-KEMs incompatible with the KEMs in this paper and [21]. So the key in the proof is the decapsulation simulation. We note that for a valid ciphertext $\bar{c}$ such that ($Dec(sk, \bar{c}) = \bar{m} \neq \perp$)[5], the decapsulation returns $H(\bar{m}, \bar{c})$. Thus, if we reprogram $H(\bar{m}, \bar{c})$ to a random $\bar{k}$, we can simulate the decapsulation of $\bar{c}$ using $\bar{k}$ without knowledge of $sk$. To guarantee the consistency between the outputs of $H$ and the simulated decapsulation, one needs to correctly guess when the adversary makes a query $(\bar{m}, \bar{c})$ to $H$, and perform a reprogram at that time. In the ROM, a randomly guess is correct with probability $1/q$.

[5] In the full proof of $T_{RH}$, the invalid case $Dec(sk, \bar{c}) = \perp$ is integrated into the valid case $Dec(sk, \bar{c}) \neq \perp$. while, the security of $T_H$ is directly reduced to the security of $T_{RH}$.

In the QROM, due to adversary's superposition RO-query, it is hard to define when the adversary makes a query $(\bar{m}, \bar{c})$. Therefore, in the QROM, we argue in a different way. We find that the consistency between $H$ and the simulated decapsulation can be guaranteed if the predicate $Decap(sk, \bar{c}) = H(\bar{m}, \bar{c})$ is satisfied. Don, Fehr, Majenz, and Schaffner [13, 12] showed that a random measure-and-reprogram can keep the predicate satisfied with a high probability. However, the measure-and-reprogram in [13, 12] cannot be directly applied to our case. This is due to the fact that the random measure in [13, 12] is performed for all the $H$-queries while in our case there is an implicit (classical) $H$-query used in the real decapsulation that will be removed in the simulated decapsulation and thus can not be measured. In this paper, extending the measure-and-reprogram technique in [13, 12], we derive a variant of measure-and-reprogram (see Lemma 3.1), which is suitable for our case. With this new measure-and-reprogram, the QROM adversary can accept the simulation of both $H$ and the decapsulation oracle with probability at least $O(1/q^2)$.

When embedding the instance of the underlying security experiment into the IND-1-CCA instance, we successfully embed an IND-CPA instance without reduction loss in the ROM. While in [21] a OW-CPA instance is embedded with a $O(1/q)$ loss in the ROM. In the QROM, the instance embedding is very tricky. We extend the double-sided O2H technique (see Lemma 2.3) to argue the QROM instance embedding, more details please refer to the proof of Theorem 4.2.

We also remark that one can easily extend the results in this paper to the IND-q-CCA KEM case for any arbitrary constant $q$. But, as aforementioned, IND-1-CCA KEM is sufficient in practical protocols, e.g., TLS 1.3, KEM-TLS.

**Attack and tightness**. Re-encryption in the FO-like KEMs will guarantee that only the ciphertexts generated by derandomization are identified as valid. That is, any ciphertext obtained by transforming another valid ciphertext can be identified as invalid by re-encryption check. However, for the IND-1-CCA KEMs in this paper and [21], the re-encryption check is removed. Thus, given a challenge ciphertext $c^* \leftarrow Enc(pk, m^*)$ to distinguish $K_0 = H(m^*, c^*)$ from a random $K_1$, if an adversary $\mathcal{B}$ can efficiently transform $c^*$ into another ciphertext $c'$ such that $Dec(sk, c') = f(m^*)$ for some specific function $f$ (this property is defined as malleability), then $\mathcal{B}$ can derive a hash value $tag = Decap(sk, c') = H(f(m^*), c^*)$. Thus, $\mathcal{B}$ can search for $m^*$ such that $tag = H(f(m^*), c^*)$ from the message $\mathcal{M}$ by querying the random oracle $H$, and finally use $H(m^*, c^*)$ to distinguish $K_0$ from $K_1$. By detailed analysis, we show $\mathcal{B}$ can achieve advantage at least $O(q/2^\lambda)$ in the ROM ($O(q^2/2^\lambda)$ in the QROM). For a $\lambda$-bit secure PKE, any PPT adversary breaks the security of PKE with advantage at most $O(1/2^\lambda)$. Thus, we can claim that a $O(1/q)$ ($O(1/q^2)$, resp.) loss is unavoidable in the ROM (QROM, resp.) for the IND-1-CCA KEMs in this paper and [21].

**Implication and separation**. By introducing a proof of quantum access to random oracle given in [40], we construct a KEM that is provably IND-CCA-secure (hence also IND-1-CCA secure) in the ROM, but cannot achieve IND-1-CCA security (hence also IND-CCA security) in the QROM. In addition, we show that applying our $H_{RU}$ to lattice-based PKE, e.g., FrodoPKE [28], can derive an IND-1-CCA ROM (and also QROM) secure KEM. However, such a KEM cannot achieve IND-CCA security in the ROM (hence QROM). The other implication relations can be trivially obtained.

### 1.5 Related Work

The tranformations in [21] and our paper are similar to U-transformation which is originally proposed in [11] and converts a OW-PCA-secure/deterministic PKE into an IND-CCA-secure KEM. The U-transformation has various variants, including $U^{\perp}_m$, $U^{\not\perp}_m$, $HU^{\perp}_m$, $HU^{\perp}$,$QU^{\perp}_m$, $QU^{\not\perp}_m$, $U^{\perp}$, $U^{\not\perp}$[6]. For $QU^{\perp}_m$ and $QU^{\not\perp}_m$, Hofheinz, Hövelmanns and Kiltz [17] showed that the IND-CCA security of KEM can be reduced to the OW-PCA security of PKE with tightness $\epsilon_R \approx O(1/q^2)\epsilon^2_{\mathcal{A}}$. The OW-PCA security is the same as the OW-CPA security except that the adversary can additionally access a plaintext-checking oracle that judges whether decryption of a given ciphertext is equal to a given plaintext. For implicit transformations $U^{\not\perp}_m$ and $U^{\not\perp}$, Jiang, Zhang, Chen, Wang and Ma [22] showed that the IND-CCA security of KEM can be reduced to the quantum variant of OW-PCA security of PKE or OW-CPA security of deterministic PKE (DPKE) with tightness $\epsilon_R \approx O(1/q^2)\epsilon^2_{\mathcal{A}}$, which is further improved to $\epsilon_R \approx O(1/q)\epsilon^2_{\mathcal{A}}$ by Jiang, Zhang and Ma [24], improved to $\epsilon_R \approx \epsilon^2_{\mathcal{A}}$ by Bindel, Hamburg, Hövelmanns, Hülsing and Persichetti [6], and improved to $\epsilon_R \approx O(1/q)\epsilon_{\mathcal{A}}$ by Kuchta, Sakzad, Stehlé, Steinfeld and Sun [26]. In particular, Saito, Xagawa, and Yamakawa [35] gave a tight reduction for $U^{\not\perp}_m$ from a newly introduced security (called disjoint simulatability) of DPKE to the IND-CCA security of KEM. This tight result was subsequently extended for the explicit $HU^{\perp}_m$ by Jiang, Zhang and Ma [23]. For $HU^{\perp}_m$ and $HU^{\perp}$, Bindel, Hamburg, Hövelmanns, Hülsing and Persichetti [6] showed that the same QROM results can be achieved as the implicit variants. Recently, Don, Fehr, Majenz and Schaffner [14] first proved the QROM security of $U^{\perp}_m$[7]. Note that all the U-transformations require re-encryption in decapsulation except $U^{\perp}$ and $U^{\not\perp}$ (see [17, 22]). However, the proofs for $U^{\perp}$ and $U^{\not\perp}$ in [17, 22] require the underlying PKE satisfies OW-PCA security, which is usually obtained by using de-randomization and re-encryption.

## 2 Preliminaries

**Symbol description.** A security parameter is denoted by $\lambda$. The set $\{0, \cdots, q\}$ is denoted by $[q]$. The abbreviation PPT stands for probabilistic polynomial time. $\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$ and $\mathcal{R}$ are denoted as key space, message space, ciphertext space and

[6] The symbol $\perp$ ($\not\perp$) means explicit (implicit) rejection, $m$ (without $m$) means $K = H(m)$ ($K = H(m, c)$), $H$ ($Q$) means an additional (length-preserving) hash value is appended into the ciphertext. In this paper, $U^{\perp}_m$ and $U^{\not\perp}_m$ are referred to transformations with re-encryption in decapsulation.

[7] Strictly speaking, they proved the security of $FO^{\perp}_m$ in the QROM. But, their proof can be translated into a proof for $U^{\perp}_m$.

randomness space, respectively. Given a finite set $X$, we denote the sampling of a uniformly random element $x$ by $x \leftarrow_{\$} X$. Denote the sampling from some distribution $D$ by $x \leftarrow D$. $x = ?y$ is denoted as an integer that is 1 if $x = y$, and otherwise 0. $\Pr[P : G]$ is the probability that the predicate $P$ holds true where free variables in $P$ are assigned according to the program in $G$. Denote deterministic (probabilistic, resp.) computation of an algorithm $A$ on input $x$ by $y = A(x)$ ($y \leftarrow A(x)$, resp.). Let $|X|$ be the cardinality of set $X$. $A^H$ ($A^{|H\rangle}, resp.$) means that algorithm $A$ gets classical (quantum, resp.) access to the oracle $H$. We present the cryptographic primitives in Supporting Material A.

### 2.1 Quantum Random Oracle Model

We refer the reader to [29] for basic of quantum computation. Random oracle model (ROM) [5] is an idealized model, where a hash function is modeled as a publicly accessible random oracle. Quantum adversary can off-line evaluate the hash function on an arbitrary superposition of inputs. As a result, quantum adversary should be allowed to query the random orale with quantum state. We call this quantum random oracle model (QROM) [7].

### 2.2 One-way to Hiding and its Double-sided Variant

**Lemma 2.1 (One-way to hiding (O2H)[1, Theorem 3]).** *Let $S \subseteq \mathcal{X}$ be random. Let $G$, $H$ be oracles such that $\forall x \notin S$. $G(x) = H(x)$. Let $z$ be a random bitstring. ($S, G, H, z$ may have arbitrary joint distribution.) Let $A$ be quantum oracle algorithm that makes at most $q$ queries (not necessarily unitary). Let $B^{|H\rangle}$ be an oracle algorithm that on input $z$ does the following: pick $i \in [q-1]$, run $A^{|H\rangle}(z)$ until (just before) the $(i+1)$-th query, measure all query input registers in the computational basis, output the set $T$ of measurement outcomes. Then*

$$\left|\Pr[1 \leftarrow A^{|H\rangle}(Z)] - \Pr[1 \leftarrow A^{|G\rangle}(Z)]\right| \leq 2q\sqrt{\Pr[S \cap T \neq \emptyset : T \leftarrow B^{|H\rangle}(z)]}.$$

**Lemma 2.2 ((Adapted) Double-sided O2H [6, Lemma 5]).** *Let $G$, $H : \mathcal{X} \to \mathcal{Y}$ be oracles such that $\forall x \neq x^*$. $G(x) = H(x)$. Let $z$ be a random bitstring. ($x^*, G, H, z$ may have arbitrary joint distribution.) Let $A$ be quantum oracle algorithm that makes at most $q$ queries (not necessarily unitary). Then, there is an another double-sided oracle algorithm $B^{|G\rangle,|H\rangle}(z)$ such that $B$ runs in about the same amount of time as $A$, and*

$$\left|\Pr[1 \leftarrow A^{|H\rangle}(z)] - \Pr[1 \leftarrow A^{|G\rangle}(z)]\right| \leq 2\sqrt{\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)]}.$$

*In particular, the double-sided oracle algorithm $B^{|G\rangle,|H\rangle}(z)$ runs $A^{|H\rangle}(z)$ and $A^{|G\rangle}(z)$ in superposition, and the probability $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)]$ is exactly $\left\| |\psi_H^q\rangle - |\psi_G^q\rangle \right\|^2 /4$, where $|\psi_H^q\rangle$ ($|\psi_G^q\rangle$, resp.) is the final state of $A^{|H\rangle}(z)$ ($A^{|G\rangle}(z), resp.$).*

## 2.3 Search in Double-sided Oracle

In the proof of our main theorem 4.2, we need to bound the advantage of searching a reprogramming point in a double-sided oracle. Thus, we develop the following lemma.

**Lemma 2.3 (Search in Double-sided Oracle).** *Let $G$, $H : \mathcal{X} \to \mathcal{Y}$ be oracles such that $\forall x \neq x^*$ $G(x) = H(x)$. Let $z$ be a random bitstring. Let $A$ be quantum oracle algorithm that makes at most $q$ queries (not necessarily unitary). Let $B^{|G\rangle,|H\rangle}(z)$ be a double-sided oracle algorithm such that $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)] = \left\| |\psi_H^q\rangle - |\psi_G^q\rangle \right\|^2 /4$, where $|\psi_H^q\rangle$ ($|\psi_G^q\rangle$, resp.) be the final state of $A^{|H\rangle}(z)$ ($A^{|G\rangle}(z)$, resp.). Let $C^{|H\rangle}(z)$ be an oracle algorithm that picks $i \leftarrow_{\$} \{1, 2, \ldots, q\}$, runs $A^{|H\rangle}(z)$ until (just before) the $i$-th query, measures the query input registers in the computational basis, and outputs the measurement outcome. Thus, we have*

$$\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)] \leq q^2 \Pr[x^* = x' : x' \leftarrow C^{|H\rangle}(z)].$$

*In particular, if $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$, $x^* = (x_1^*, x_2^*)$, $x_1^*$ is uniform and independent of $H$ and $z$, then we further have $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)] \leq q^2/ |\mathcal{X}_1|$.*

*Proof.* Let $|\psi_0\rangle$ be an initial state that depends on $z$ (but not on $G$, $H$ or $x^*$), $O_H : |x, y\rangle \to |x, y \oplus H(x)\rangle$, and $U_i$ is $A$'s state transition operation after the $i$-th query. (And analogously for $A^{|G\rangle}$.) We define $|\psi_H^i\rangle$ as $U_i O_H \cdots U_1 O_H |\psi_0\rangle$, and similarly $|\psi_G^i\rangle$. Thus, $|\psi_H^q\rangle$ ($|\psi_G^q\rangle$, resp.) be the final states of $A^{|H\rangle}(z)$ ($A^{|G\rangle}(z)$, resp.). Let $P_{x^*} = |x^*\rangle\langle x^*|$, $D_i = \left\| |\psi_H^i\rangle - |\psi_G^i\rangle \right\|$. Then, for $i \geq 1$, we have

$$\begin{aligned} D_i &= \left\| U_i O_H |\psi_H^{i-1}\rangle - U_i O_G |\psi_G^{i-1}\rangle \right\| \\ &= \left\| O_H |\psi_H^{i-1}\rangle - O_G |\psi_H^{i-1}\rangle + O_G |\psi_H^{i-1}\rangle - O_G |\psi_G^{i-1}\rangle \right\| \\ &\overset{*}{\leq} \left\| (O_H - O_G) |\psi_H^{i-1}\rangle \right\| + \left\| O_G (|\psi_H^{i-1}\rangle - \psi_G^{i-1}\rangle) \right\| \\ &\overset{**}{=} D_{i-1} + \left\| (O_H - O_G) P_{x^*} |\psi_H^{i-1}\rangle \right\| \\ &\overset{***}{=} D_{i-1} + 2 \left\| P_{x^*} |\psi_H^{i-1}\rangle \right\| \end{aligned} \tag{1}$$

Here, the inequation $(*)$ uses the triangle inequality. The equation $(**)$ uses that $(O_H - O_G) P_{x^*} = O_H - O_G$ since $G(x) = H(x)$ for $\forall x \neq x^*$. The inequation $(***)$ uses the fact that $(O_H - O_G)$ has operator norm $\leq 2$. Note that $D_0 = \left\| |\psi_0\rangle - |\psi_0\rangle \right\| = 0$. From (1), we get $D_i \leq D_{i-1} + 2 \left\| P_{x^*} |\psi_H^{i-1}\rangle \right\|$. This implies $D_q \leq 2 \sum_{i=0}^{q-1} \left\| P_{x^*} |\psi_H^i\rangle \right\|$. Using Jensen's inequality, we get $\sum_{i=0}^{q-1} \left\| P_{x^*} |\psi_H^i\rangle \right\| \leq q \sqrt{\sum_{i=0}^{q-1} 1/q \left\| P_{x^*} |\psi_H^i\rangle \right\|^2}$.

Note that $\Pr[x^* = x' : x' \leftarrow C^{|H\rangle}(z)]$ is $\sum_{i=0}^{q-1} 1/q \left\| P_{x^*} |\psi_H^i\rangle \right\|^2$. Thus, we have $D_q \leq 2q \sqrt{\Pr[x^* = x' : x' \leftarrow C^{|H\rangle}(z)]}$. Since $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)]$ is exactly $\left\| |\psi_H^q\rangle - |\psi_G^q\rangle \right\|^2 /4 = D_q^2/4$, we have $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)] \leq q^2 \Pr[x^* = x' : x' \leftarrow C^{|H\rangle}(z)]$. In particular, if $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$, $x^* = (x_1^*, x_2^*)$, $x_1^*$ is uniform and independent of $H$ and $z$, then $\Pr[x^* = x' : x' \leftarrow C^{|H\rangle}(z)] \leq 1/ |\mathcal{X}_1|$. Thus, we have $\Pr[x^* = x' : x' \leftarrow B^{|G\rangle,|H\rangle}(z)] \leq q^2/ |\mathcal{X}_1|$. $\square$

## 3 Extended Measure-and-reprogram Technique

Measure-and-reprogram introduced by [13, 12] shows how to reprogram the quantum random oracle adaptively at one input. In detail, for any oracle algorithm $A^{|H\rangle}$ that makes at most $q$ queries to $H$ and outputs a pair $(x,z)$ such that some predicate $V(x,H(x),z)$ is satisfied, the measure-and-reprogram technique shows that there exists an another algorithm $S^A$ that simulates $H$, extracts $x$ from $A^H$ by randomly measuring one of $A$'s queries to $H$, and then reprograms $H(x)$ to a given value $\Theta$ so that $z$ output by $A^H$ satisfies $V(x,\Theta,z)$ with a multiplicative $O(q^2)$ loss in probability.

As we discussed in Sec. 1.4, the standard measure-and-reprogram technique in [13, 12] cannot be directly applied to our case. In the proof of our main theorem 4.2, an implicit classical $H$-query (this is exactly $x$) cannot be measured, while the random measure in [13, 12] is required to be performed for all the $H$-queries. Thus, we extend the standard measure-and-reprogram technique and give the following lemma.

**Lemma 3.1 ((Single-classical-query) Measure-and-reprogram).** *Let $A^{|H\rangle}$ be an arbitrary oracle quantum algorithm that makes $q$ queries to a uniformly random $H:\mathcal{X}\to\mathcal{Y}$, and outputs some classical $x\in\mathcal{X}$ and a (possibly quantum) output $z$. In particular, $A$'s $i^*$-th query input state is exactly $|x\rangle$ (this is a classical state and identical with the $x$ output by $A^{|H\rangle}$).*

*Let $S^A(\Theta)$ be an oracle algorithm that randomly picks a pair $(i,b_0)\in([q-1]\setminus\{i^*-1\}\times\{0,1\})\cup\{(q,0)\}$, runs $A^{|H_i^{i^*}\rangle}$ to output $z$, where $H_i^{i^*}$ is an oracle that returns $\Theta$ for $A$'s $i^*$-th $H$-query, measures $A$'s $(i+1)$-th $H$-query input to obtain $x$, returns $A$'s $l$-th $H$-query using $H$ for $l<(i+1+b_0)$ and $l\neq i^*$, and returns $A$'s $l$-th $H$-query using $H_{x\Theta}$ ($H_{x\Theta}(x)=\Theta$ and $H_{x\Theta}(x')=H(x')$ for all $x'\neq x$) for $l\geq(i+1+b_0)$ and $l\neq i^*$.*

*Let $S_1^A(\Theta)$ be an oracle algorithm that randomly picks a pair $(j,b_1)\in(\{i^*,\cdots,q-1\}\times\{0,1\})\cup\{(q,0)\}\cup\{(i^*-1,1)\}$, runs $A^{|H_j\rangle}$ to output $z$, where $H_j$ is an oracle that measures $A$'s $(j+1)$-th $H$-query input to obtain $x$, returns $A$'s $l$-th $H$-query using $H$ for $l<(j+1+b_1)$, and returns $A$'s $l$-th $H$-query using $H_{x\Theta}$ for $l\geq(j+1+b_1)$.*

*Thus, for any $x_0\in X$, $i^*\in\{1,\cdots,q\}$ and any predicate $V$:*

$$\Pr_H[x=x_0\wedge V(x,H(x),z)=1:(x,z)\leftarrow A^{|H\rangle}]\leq 2(2q-1)^2\Pr_{H,\Theta}[x=x_0\wedge V(x,\Theta,z)=1:(x,z)\leftarrow S^A]+8q^2\Pr_{H,\Theta}[x=x_0\wedge V(x,\Theta,z)=1:(x,z)\leftarrow S_1^A],$$

*where the subscript $\{H,\Theta\}$ in $\Pr_H$ and $\Pr_{H,\Theta}$ denotes that the probability is averaged over a random choice of $H$ and $\Theta$. Moreover, if $V=V_1\wedge V_2$ such that $V_1(x,y,z)=1$ iff $y$ is returned for $A$'s $i^*$-th query, then $\sum x_0\Pr_{H,\Theta}[x=x_0\wedge V(x,\Theta,z)=1:(x,z)\leftarrow S_1^A]\leq\frac{1}{|\mathcal{Y}|}$.*

*Proof.* Let $|\phi_0\rangle$ be an initial state that is independent of $H$ and $\Theta$[8]. $O_H : |x, y\rangle \to |x, y \oplus H(x)\rangle$. Let $A_i$ be $A$'s state transition operation after the $i$-th H-query ($i \in \{1, \cdots, q\}$).

We set $A^H_{i\to j} = A_j O_H \cdots A_{i+1} O_H$ for $0 \le i < j \le q$ and $A^H_{i\to j} = \mathbb{I}$ for $i \ge j$. Let $|\phi^H_i\rangle = A^H_{0\to i}|\phi_0\rangle$ be the state of $A$ right before the $(i+1)$-th query. The final state $|\phi^H_q\rangle$ is considered to be a state over registers X, Z and E.

Let quantum predicate $V$ be a family of projections $\{\Pi_{x,\Theta}\}_{x,\Theta}$ with $x \in \mathcal{X}$ and $\Theta \in \mathcal{Y}$. Set $G^\Theta_x = |x\rangle\langle x| \otimes \Pi_{x,\Theta}$, where $X = |x\rangle\langle x|$ acts on register X, and $\Pi_{x,\Theta}$ acts on register Z.

Then, we have

$$\Pr[x = x_0 \wedge V(x, H(x), z) = 1 : (x, z) \leftarrow A^{|H\rangle}] = \left\| G^{H(x_0)}_{x_0} |\phi^H_q\rangle \right\|^2 .$$

Since $H_{x\Theta}(x') = H(x')$ for all $x' \neq x$, we have $(A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})(\mathbb{I} - X)|\phi^H_i\rangle = (A^{H_{x\Theta}}_{i\to q})(\mathbb{I} - X)|\phi^H_i\rangle$. Thus, $(A^{H_{x\Theta}}_{i+1\to q})|\phi^H_{i+1}\rangle$

$$\begin{aligned}
&= (A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})(\mathbb{I} - X)|\phi^H_i\rangle + (A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})X|\phi^H_i\rangle \\
&= (A^{H_{x\Theta}}_{i\to q})(\mathbb{I} - X)|\phi^H_i\rangle + (A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})X|\phi^H_i\rangle \\
&= (A^{H_{x\Theta}}_{i\to q})|\phi^H_i\rangle - (A^{H_{x\Theta}}_{i\to q})X|\phi^H_i\rangle + (A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})X|\phi^H_i\rangle.
\end{aligned}$$

Applying $G^\Theta_x$ and using the triangle equality, we have $\left\| G^\Theta_x (A^{H_{x\Theta}}_{i\to q})|\phi^H_i\rangle \right\| \le$

$$\left\| G^\Theta_x (A^{H_{x\Theta}}_{i+1\to q})|\phi^H_{i+1}\rangle \right\| + \left\| G^\Theta_x (A^{H_{x\Theta}}_{i\to q})X|\phi^H_i\rangle \right\| + \left\| G^\Theta_x (A^{H_{x\Theta}}_{i+1\to q})(A^H_{i\to i+1})X|\phi^H_i\rangle \right\| .$$

Summing up the above inequality over $i = 0, \cdots, q-1$, we get

$$\left\| G^\Theta_x |\phi^{H_{x\Theta}}_q\rangle \right\| \le \left\| G^\Theta_x |\phi^H_q\rangle \right\| + \sum_{0 \le i < q, b \in \{0,1\}} \left\| G^\Theta_x (A^{H_{x\Theta}}_{i+b\to q})(A^H_{i\to i+b})X|\phi^H_i\rangle \right\| \quad (2)$$

Note that $A$'s $i^*$-th query is classical and the query input is $|x\rangle$. Then, $X|\phi^H_{(i^*-1)}\rangle = |\phi^H_{(i^*-1)}\rangle$. Thus, there is a specific term

$$\left\| G^\Theta_x (A^{H_{x\Theta}}_{(i^*-1)\to q})X|\phi^H_{(i^*-1)}\rangle \right\| = \left\| G^\Theta_x (A^{H_{x\Theta}}_{(i^*-1)\to q})|\phi^H_{(i^*-1)}\rangle \right\| \quad (3)$$

on the right hand side of inequality (2).

Set $B^H_{j\to k} = A_{i^*+k} O_H \cdots A_{i^*+j+1} O_H$ for $k \ge (j+1)$ ($B^H_{j\to k} = \mathbb{I}$ for $k \le j$.), $|\psi_0\rangle = (A^{H_{x\Theta}}_{(i^*-1)\to i^*})\ |\phi^H_{(i^*-1)}\rangle$, and $|\psi^H_j\rangle = B^H_{0\to j}|\psi_0\rangle$. Then,

$$\left\| G^\Theta_x (A^{H_{x\Theta}}_{(i^*-1)\to q})|\phi^H_{(i^*-1)}\rangle \right\| = \left\| G^\Theta_x |\psi^{H_{x\Theta}}_{q-i^*}\rangle \right\| = \left\| G^\Theta_x B^{H_{x\Theta}}_{0\to(q-i^*)}|\psi_0\rangle \right\| .$$

[8] This initial state can be seen as an additional input to $A$. In [12, Theorem 2], it is also implicitly required that the initial state is independent of $H$ and $\Theta$.

Since $H_{x\Theta}(x') = H(x')$ for all $x' \neq x$, we have

$$(B^{H}_{j\to(j+1)})(\mathbb{I}-X)|\psi^{H}_{j}\rangle = (B^{H_{x\Theta}}_{j\to(j+1)})(\mathbb{I}-X)|\psi^{H}_{j}\rangle.$$

Thus, we can write $(B^{H_{x\Theta}}_{j+1\to(q-i^*)})|\psi^{H}_{j+1}\rangle$

$$\begin{aligned}
&= (B^{H_{x\Theta}}_{j+1\to(q-i^*)})(B^{H}_{j\to j+1})(\mathbb{I}-X)|\psi^{H}_{j}\rangle + (B^{H_{x\Theta}}_{j+1\to(q-i^*)})(B^{H}_{j\to j+1})X|\psi^{H}_{j}\rangle \\
&= (B^{H_{x\Theta}}_{j\to(q-i^*)})(\mathbb{I}-X)|\psi^{H}_{j}\rangle + (B^{H_{x\Theta}}_{j+1\to(q-i^*)})(B^{H}_{j\to j+1})X|\psi^{H}_{j}\rangle \\
&= (B^{H_{x\Theta}}_{j\to(q-i^*)})|\psi^{H}_{j}\rangle - (B^{H_{x\Theta}}_{j\to(q-i^*)})X|\psi^{H}_{j}\rangle + (B^{H_{x\Theta}}_{j+1\to(q-i^*)})(B^{H}_{j\to j+1})X|\psi^{H}_{j}\rangle.
\end{aligned}$$

Rearranging terms, applying $G^{\Theta}_{x}$ and using the triangle equality, we have $\left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j\to(q-i^*)})|\psi^{H}_{j}\rangle\right\| \leq \left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j+1\to(q-i^*)})|\psi^{H}_{j+1}\rangle\right\| +$

$$\left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j\to(q-i^*)})X|\psi^{H}_{j}\rangle\right\| + \left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j+1\to(q-i^*)})(B^{H}_{j\to j+1})X|\psi^{H}_{j}\rangle\right\|.$$

Summing up the inequality over $j = 0, \cdots, q-i^*-1$, we get

$$\begin{aligned}
\left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{(i^*-1)\to q})|\phi^{H}_{(i^*-1)}\rangle\right\| = \ &\left\|G^{\Theta}_{x}B^{H_{x\Theta}}_{0\to(q-i^*)}|\psi_0\rangle\right\| \leq \left\|G^{\Theta}_{x}|\psi^{H}_{q-i^*}\rangle\right\| + \\
\sum_{0\leq j<(q-i^*),b\in\{0,1\}} &\left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j+b\to(q-i^*)})(B^{H}_{j\to j+b})X|\psi^{H}_{j}\rangle\right\| \qquad (4)
\end{aligned}$$

According to equalities (2), (3) and (4), we get

$$\left\|G^{\Theta}_{x}|\phi^{H_{x\Theta}}_{q}\rangle\right\| \leq Term0 + Term1, \qquad (5)$$

$$\begin{aligned}
Term0 \ &= \sum_{\substack{0\leq i<(i^*-1)\\ b_0\in\{0,1\}}} \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{i+b_0\to q})(A^{H}_{i\to i+b_0})X|\phi^{H}_{i}\rangle\right\| + \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{(i^*-1)\to q})X|\phi^{H}_{(i^*-1)}\rangle\right\| \\
&= \sum_{0\leq i<(i^*-1),b_0\in\{0,1\}} \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{i+b_0\to q})(A^{H}_{i\to i+b_0})X|\phi^{H}_{i}\rangle\right\| \\
&\quad + \left\|G^{\Theta}_{x}|\psi^{H}_{q-i^*}\rangle\right\| + \sum_{0\leq j<(q-i^*),b_0\in\{0,1\}} \left\|G^{\Theta}_{x}(B^{H_{x\Theta}}_{j+b_0\to(q-i^*)})(B^{H}_{j\to j+b_0})X|\psi^{H}_{j}\rangle\right\| \\
&= \sum_{0\leq i<(i^*-1),b_0\in\{0,1\}} \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{i+b_0\to q})(A^{H}_{i\to i+b_0})X|\phi^{H}_{i}\rangle\right\| \\
&\quad + \left\|G^{\Theta}_{x}(A^{H}_{i^*\to q})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^{H}_{(i^*-1)}\rangle\right\| \\
&\quad + \sum_{\substack{i^*\leq i<q\\ b_0\in\{0,1\}}} \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{(i+b_0)\to q})(A^{H}_{i\to(i+b_0)})X(A^{H}_{i^*\to i})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^{H}_{(i^*-1)}\rangle\right\| \\
Term1 \ &= \left\|G^{\Theta}_{x}|\phi^{H}_{q}\rangle\right\| + \sum_{\substack{i^*\leq i<q\\ b_1\in\{0,1\}}} \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{i+b_1\to q})(A^{H}_{i\to i+b_1})X|\phi^{H}_{i}\rangle\right\| \\
&\quad + \left\|G^{\Theta}_{x}(A^{H_{x\Theta}}_{i^*\to q})(A^{H}_{(i^*-1)\to i^*})X|\phi^{H}_{(i^*-1)}\rangle\right\|.
\end{aligned}$$

According to inequality (5), we have

$$\left\|G_x^{\Theta}|\phi_q^{H_{x\Theta}}\rangle\right\|^2 \leq 2Term0^2 + 2Term1^2.$$

Since $G_x^{\Theta} = G_x^{\Theta}X$, we get $G_x^{\Theta}(A^H_{i^*\to q})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^H_{(i^*-1)}\rangle = G_x^{\Theta}(A^{H_{x\Theta}}_{(i+b_0)\to q})(A^H_{i\to(i+b_0)})X(A^H_{i^*\to i})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^H_{(i^*-1)}\rangle$ with $i = q$ and $b_0 = 0$ and $G_x^{\Theta}|\phi_q^H\rangle = G_x^{\Theta}X|\phi_q^H\rangle = G_x^{\Theta}(A^{H_{x\Theta}}_{i+b_1\to q})(A^H_{i\to i+b_1})X|\phi_i^H\rangle$ with $i = q$ and $b_1 = 0$. Then, using Jensen's inequality, we have

$$\begin{aligned}
Term0^2 &\leq (2q-1)\Big(\sum_{0\leq i<(i^*-1), b_0\in\{0,1\}} \left\|G_x^{\Theta}(A^{H_{x\Theta}}_{i+b_0\to q})(A^H_{i\to i+b_0})X|\phi_i^H\rangle\right\|^2 \\
&\quad + \left\|G_x^{\Theta}(A^H_{i^*\to q})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^H_{(i^*-1)}\rangle\right\|^2 \\
&\quad + \sum_{\substack{i^*\leq i<q\\ b_0\in\{0,1\}}} \left\|G_x^{\Theta}(A^{H_{x\Theta}}_{(i+b_0)\to q})(A^H_{i\to(i+b_0)})X(A^H_{i^*\to i})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^H_{(i^*-1)}\rangle\right\|^2\Big) \\
&= (2q-1)^2\,\mathbb{E}_{i,b_0}\left[\left\|\delta_{i<(i^*-1)}T_0\right\|^2 + \left\|\delta_{i\geq i^*}T_1\right\|^2\right],
\end{aligned}$$

where $T_0 = (G_x^{\Theta}(A^{H_{x\Theta}}_{i+b_0\to q})(A^H_{i\to i+b_0})X|\phi_i^H\rangle)$, $T_1 = G_x^{\Theta}(A^{H_{x\Theta}}_{(i+b_0)\to q})(A^H_{i\to(i+b_0)})X(A^H_{i^*\to i})(A^{H_{x\Theta}}_{(i^*-1)\to i^*})|\phi^H_{(i^*-1)}\rangle$, $\delta_{i<(i^*-1)} = 1$ if $i < (i^*-1)$ otherwise 0, $\delta_{i\geq i^*} = 1$ if $i \geq i^*$ otherwise 0, the expectation in $Term0^2$ is over uniform $(i, b_0) \in ([q-1]\setminus\{i^*-1\}\times\{0,1\})\cup\{(q,0)\}$.

Thus, the probability of $S$ outputting $(x, z)$ such that $V(x, \Theta, z) = 1$ is exactly $\mathbb{E}_{i,b_0}\left[\left\|\delta_{i<(i^*-1)}T_0\right\|^2 + \left\|\delta_{i\geq i^*}T_1\right\|^2\right]$.

Likewise, using Jensen's inequality, we get

$$\begin{aligned}
Term1^2 &\leq (2q-2i^*+2)\Big(\left\|G_x^{\Theta}|\phi_q^H\rangle\right\|^2 + \sum_{\substack{i^*\leq i<q\\ b_1\in\{0,1\}}} \left\|G_x^{\Theta}(A^{H_{x\Theta}}_{i+b_1\to q})(A^H_{i\to i+b_1})X|\phi_i^H\rangle\right\|^2 \\
&\quad + \left\|G_x^{\Theta}(A^{H_{x\Theta}}_{i^*\to q})(A^H_{(i^*-1)\to i^*})X|\phi^H_{(i^*-1)}\rangle\right\|^2\Big) \\
&= (2q-2i^*+2)^2\,\mathbb{E}_{j,b_1}\left[\left\|G_x^{\Theta}(A^{H_{x\Theta}}_{j+b_1\to q})(A^H_{j\to j+b_1})X|\phi_j^H\rangle\right\|^2\right]
\end{aligned}$$

where the expectation in $Term1^2$ is over uniform $(j, b_1) \in (\{i^*, \cdots, q-1\}\times\{0,1\})\cup\{(q,0)\}\cup\{(i^*-1,1)\}$.

Thus, the probability of $S_1$ outputting $(x, z)$ such that $V(x, \Theta, z) = 1$ is exactly $\mathbb{E}_{j,b_1}\left[\left\|G_x^{\Theta}(A^{H_{x\Theta}}_{j+b_1\to q})(A^H_{j\to j+b_1})X|\phi_j^H\rangle\right\|^2\right]$.

Since the initial state is independent of $H$ and $\Theta$, we have $\Pr_{H,\Theta}[\left\|G_x^{\Theta}|\phi_q^{H_{x\Theta}}\rangle\right\|^2]$ $= \Pr_{H,\Theta}[\left\|G_x^{H(x)}|\phi_q^H\rangle\right\|^2]$. Thus, for any $x_0 \in X$ and predicate $V$, we have

$$\Pr_H[x = x_0 \wedge V(x, H(x), z) = 1 : (x,z) \leftarrow A^{|H\rangle}] \leq 2(2q-1)^2 \Pr_{H,\Theta}[x = x_0 \wedge V(x, \Theta, z) = 1 : (x,z) \leftarrow S^A] + 8q^2 \Pr_{H,\Theta}[x = x_0 \wedge V(x,\Theta,z) = 1 : (x,z) \leftarrow S_1^A],$$

as desired. Set $V_1(x,y,z) = 1$ iff $y$ is returned for $A$'s $i^*$-th query. When $V = V_1 \wedge V_2$, we get

$$\sum x_0 \Pr_{H,\Theta}[x = x_0 \wedge V(x,\Theta,z) = 1 : (x,z) \leftarrow S_1^A] \leq \Pr[H(x) = \Theta] = \frac{1}{|\mathcal{Y}|}.$$

# 4 IND-1-CCA-secure KEM without Re-encryption and Ciphertext Expansion

To a public-key encryption PKE$'$=($Gen'$, $Enc'$, $Dec'$) and a random oracle $H$ ($H : \mathcal{M} \times \mathcal{C} \to \mathcal{K}$), we associate $\text{KEM}_H = T_H[\text{PKE}', H]$ and $\text{KEM}_{RH} = T_{RH}[\text{PKE}', H]$ as in Fig. 2. The only difference between $\text{KEM}_H$ and $\text{KEM}_{RH}$ is the return value for invalid ciphertexts. In detail, when a ciphertext decrypts to $\perp$, such a ciphertext will decapsulate to $\perp$ in $\text{KEM}_H$, and to $H(\star, c)$ in $\text{KEM}_{RH}$. Here, $\star$ can be any fixed public value. In the following, Theorems 4.1 and 4.2 show the IND-1-CCA security of $\text{KEM}_{RH}$ in the (Q)ROM. In particular, Theorems 4.1 and 4.2 works for both $\star \in \mathcal{M}$ and $\star \notin \mathcal{M}$. Then, we will show that the IND-1-CCA security of $\text{KEM}_H$ can be reduced to the IND-1-CCA security of $\text{KEM}_{RH}$ by Theorem 4.3.

| *Gen* | *Encaps(pk)* | *Decaps(sk, c)* |
|---|---|---|
| 1 : $(pk, sk) \leftarrow Gen'$ | 1 : $m \leftarrow_\$ \mathcal{M}$ | 1 : $m' := Dec'(sk, c)$ |
| 2 : **return** $(pk, sk)$ | 2 : $c \leftarrow Enc'(pk, m)$ | 2 : **if** $m' = \perp$ |
| | 3 : $K := H(m, c)$ | 3 : **return** $\perp$ $//T_H$ |
| | 4 : **return** $(K, c)$ | 4 : **return** $K := H(\star, c)$ $//T_{RH}$ |
| | | 5 : **else return** $K := H(m', c)$ |

Fig. 2: $\text{KEM}_H = T_H[\text{PKE}', H]$ and $\text{KEM}_{RH} = T_{RH}[\text{PKE}', H]$

**Theorem 4.1 (ROM security of $T_{RH}$).** *If PKE$'$ is $\delta$-*correct*, for any adversary $\mathcal{B}$ against the IND-1-CCA security of KEM$_{RH}$ $= T_{RH}[\text{PKE}', H]$ in Fig. 2, issuing at most a single (classical) query to the decapsulation oracle* DECAPS *and at most $q_H$ queries to the random oracle $H$, there exists a OW-CPA adversary $\mathcal{A}$ and an IND-CPA adversary $\mathcal{D}$ against PKE$'$ such that* $\text{Time}(\mathcal{A}) \approx \text{Time}(\mathcal{D}) \approx$

$\mathrm{Time}(\mathcal{B}) + O(q_H^2)$ *and*

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) \leq q_H(q_H+1)\mathtt{Adv}^{\text{OW}-\text{CPA}}_{\text{PKE}'}(\mathcal{A}) \tag{6}$$
$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) \leq 2(q_H+1)\mathtt{Adv}^{\text{IND}-\text{CPA}}_{\text{PKE}'}(\mathcal{D}) + 2q_H(q_H+1)/\left|\mathcal{M}\right|.$$

*If the PKE is deterministic, the bound (6) can be improved as*

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) \leq (q_H+1)\mathtt{Adv}^{\text{OW}-\text{CPA}}_{\text{PKE}'}(\mathcal{A}) + \delta,$$

*where* $\mathrm{Time}(\mathcal{A}) \approx \mathrm{Time}(\mathcal{B}) + O(q_H^2) + O(q_H \cdot \mathrm{Time}(Enc'))$.

*Proof.* Let $\mathcal{B}$ be an adversary against the IND-CCA security of $\text{KEM}_{RH}$, issuing (exactly) one classical query to DECAPS (by introducing a dummy query if necessary), and at most $q_H$ queries (excluding the queries implicitly made in DECAPS) to $H$. Let $\Omega_H$ be the sets of all functions $H : \mathcal{M} \times \mathcal{C} \to \mathcal{K}$. Consider the games in Fig. 3.

GAME $G_0$. This is exactly the IND-1-CCA game, thus $\left|\Pr[G_0^{\mathcal{B}} \Rightarrow 1] - 1/2\right| = \mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B})$.

GAME $G_1$. In game $G_1$, $k_0^* := H(m^*, c^*)$ is replaced by $k_0^* \leftarrow_\$ \mathcal{K}$. Thus, in $G_1$, the bit $b$ is independent of $\mathcal{B}$'s view, thus $\Pr[G_1^{\mathcal{B}} \Rightarrow 1] = 1/2$. Define QUERY as the event that $(m^*, c^*)$ is queried to $H$. Then, $G_1$ is identical with $G_0$ in $\mathcal{B}$'s view unless the event QUERY happens. Thus, we have

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) = \left|\Pr[G_0^{\mathcal{B}} \Rightarrow 1] - \Pr[G_1^{\mathcal{B}} \Rightarrow 1]\right| \leq \Pr[\text{QUERY} : G_1].$$

GAME $G_2$. In game $G_2$, we make two changes. First, we modify the DECAPS oracle, and replace $K := H(\bar{m}, \bar{c})$ by $K := \bar{k}$. Second, we reprogram the random oracle $H$ conditional a uniform $i$ over $[q_H]$. In particular, reprogram $H$ to $H_1^i$ (given by Fig. 3) when $\mathcal{B}$ makes the $(i+1)$-th $H$-query $(0 \leq i \leq (q_H - 1))$, and then answer $\mathcal{B}$ with $H_1^i$ for $\mathcal{B}$'s $j$-th query $(j \geq (i+1))$. Let $(m_i, c_i)$ be $\mathcal{B}$'s $i$-th $H$-query input. $H_1^i(m, c)$ returns $\bar{k}$ when $(m, c) = (m_{i+1}, c_{i+1})$ and $H_1(m, c)$ otherwise. Let $(i^* + 1)$ be the number of $\mathcal{B}$'s first query to $H$ with $(\bar{m}, \bar{c})$, where $i^* \in [q_H - 1]$. We also denote $i^* = q_H$ as the event that $\mathcal{B}$ makes no query to $H$ with $(\bar{m}, \bar{c})$. Note that $G_2$ has the same distribution as $G_1$ in $\mathcal{B}$'s view when the event $i^* = i$ happens. Thus, we have

$$\Pr[\text{QUERY} : G_1] \leq (q_H + 1)\Pr[\text{QUERY} : G_2].$$

Let $(pk, sk) \leftarrow Gen'$, $m^* \leftarrow_\$ \mathcal{M}$, $c^* \leftarrow Enc(pk, m^*)$. Then, we construct an adversary $\mathcal{A}'(pk, c^*)$ that simulates $\mathcal{B}$'s view as in game $G_2$ and returns $\mathcal{B}$'s $H$-query list H-List, see Fig. 4. Note that a $q_H$-wise independent function is perfectly indistinguishable from a true random function for any distinguisher that makes at most $q_H$ queries [41]. Thus, the probability of the H-List returned by $\mathcal{A}'$ contains $(m^*, c^*)$ is exactly $\Pr[\text{QUERY} : G_2]$.

Now, we construct an adversary $\mathcal{A}$ against the OW-CPA security of the underlying PKE. If the underlying PKE is probabilistic, $\mathcal{A}$ runs $\mathcal{A}'$, and randomly selects one message in H-List as a return. Then, we have $\mathtt{Adv}^{\mathrm{OW-CPA}}_{\mathrm{PKE}'}(\mathcal{A}) \geq 1/q_H \Pr[\textsc{Query} : G_2]$. Therefore, for probabilistic PKE, we have

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\mathrm{KEM}_{RH}}(\mathcal{B}) \leq q_H(q_H+1)\mathtt{Adv}^{\mathrm{OW-CPA}}_{\mathrm{PKE}'}(\mathcal{A}).$$

Next, we consider the case of the deterministic PKE.

GAMES $G_0 - G_2$ and $G_1^A - G_2^A$

$(pk, sk) \leftarrow Gen', j = 0, i \leftarrow_\$ [q_H]$
$\textsc{Query} = \textbf{false}\ , H_1 \leftarrow_\$ \Omega_H$
$\bar{k}, k_1^* \leftarrow_\$ \mathcal{K}, b \leftarrow_\$ \{0,1\}$
$m^* \leftarrow_\$ \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$
**if** COLL **return** $\perp // G_1^A - G_2^A$
$k_0^* = H(m^*, c^*) \quad //G_0$
$k_0^* \leftarrow_\$ \mathcal{K} // G_1 - G_2, G_1^A - G_2^A$
$b' \leftarrow \mathcal{B}^{H,\textsc{Decaps}}(pk, c^*, k_b^*)$
**return** $b' =? b$

$H_1^i(m,c)$

**if** $(m,c) = (m_{i+1}, c_{i+1})$
  **return** $\bar{k}$
**else return** $H_1(m,c)$

$H(m,c)$

**if** $(m,c) = (m^*, c^*)$
  $\textsc{Query} = \textbf{true}$
**if** $j \geq i$ **return** $H_1^i(m,c) \quad //G_2, G_2^A$
$j = j+1 \quad //G_2, G_2^A$
**return** $H_1(m,c)$

$\textsc{Decaps}\ (sk, \bar{c} \neq c^*)$

**if** more than 1 query **return** $\perp$
**return** $K := \bar{k} \quad //G_2, G_2^A$
$m' := Dec'(sk, \bar{c})$
**if** $m' = \perp$ **do** $\bar{m} = \star$
**else do** $\bar{m} = m'$
**return** $K := H(\bar{m}, \bar{c})$

Fig. 3: Games for the proof of Theorem 4.1

$\mathcal{A}'(pk,\ c^*)$

$k^*, \bar{k} \leftarrow_\$ \mathcal{K}, j = 0, i \leftarrow_\$ [q_H]$
Pick a $q_H$-wise functions $H_1$
$b' \leftarrow \mathcal{B}^{H,\textsc{Decaps}}(pk, c^*, k^*)$
**return** H-List

$H_1^i(m,c)$

**if** $(m,c) = (m_{i+1}, c_{i+1})$ **return** $\bar{k}$
**else return** $H_1(m,c)$

$H(m,c)$

**if** $i = q_H$ **return** $H_1(m,c)$
**if** $j \geq i$ **return** $H_1^i(m,c)$
$j = j+1$
**return** $H_1(m,c)$

$\textsc{Decaps}\ (\bar{c} \neq c^*)$

**return** $\bar{k}$

Fig. 4: Adversary $\mathcal{A}'$ for the proof of Theorem 4.1

Game $G_1^A$. Define COLL as the event that there is a messages $m \neq m^*$ such that $Enc'(pk, m) = c^* = Enc'(pk, m^*)$. $G_1^A$ is the same as $G_1$ except that $\perp$ is returned if COLL happens. Note that $G_1$ and $G_1^A$ have the same distribution when COLL doe not happen (implied by the $\delta$-correctness). Thus, we have

$$\Pr[\textsc{Query} : G_1] \le \Pr[\textsc{Query} : G_1^A] + \delta.$$

Game $G_2^A$. $G_2^A$ is the same as $G_1^A$ except that oracles Decaps and $H$ are modified as in $G_2$. Then, arguing in the same way as in $G_2$, we have

$$\Pr[\textsc{Query} : G_1^A] \le (q_H + 1)\Pr[\textsc{Query} : G_2^A].$$

Now, we construct an adversary $\mathcal{A}$ against deterministic PKE. $\mathcal{A}$ runs $\mathcal{A}'$, selects a $(m', c')$ from H-List such that $c' = c^*$ and $Enc(pk, m') = c^*$, and returns $m'$. Note that if COLL does not happen, $\mathcal{A}$ returns $m^*$ with probability $\Pr[\textsc{Query} : G_2^A]$. Thus, $\mathtt{Adv}_{\mathrm{PKE}'}^{\mathrm{OW-CPA}}(\mathcal{A}) \ge \Pr[\textsc{Query} : G_2^A]$. Therefore, putting the inequalities together, we have

$$\mathtt{Adv}_{\mathrm{KEM}_{RH}}^{\mathrm{IND\text{-}1\text{-}CCA}}(\mathcal{B}) \le (q_H + 1)\mathtt{Adv}_{\mathrm{PKE}'}^{\mathrm{OW-CPA}}(\mathcal{A}) + \delta.$$

When the underlying PKE satisfies IND-CPA security, we can construct an IND-CPA adversary $\mathcal{D}$, and derive a tighter bound. In particular, $\mathcal{D}(pk)$ samples two uniform messages $m_0^*$ and $m_1^*$ from $\mathcal{M}$, i.e., $m_0^*, m_1^* \leftarrow_{\$} \mathcal{M}$. The IND-CPA challenger chooses a bit $b$, generates the challenge ciphertext $c^* \leftarrow Enc(pk, m_b^*)$ and sends $c^*$ to $\mathcal{D}$. Then, $\mathcal{D}$ runs $\mathcal{A}'(pk, c^*)$, get $\mathcal{B}$'s H-List. If $(m_{b'}^*, *)$ is in H-List and $(m_{1-b'}^*, *)$ is not in H-List, $\mathcal{D}$ returns $b'$. For other cases, $\mathcal{D}$ returns a uniform $b'$, i.e., $b' \leftarrow_{\$} \{0, 1\}$. Let BAD be the event that $\mathcal{B}$ queries $(m_{1-b}^*, *)$ (that is, $(m_{1-b}^*, *)$ is in H-List). Note that $m_{1-b}^*$ is uniformly distributed and independent from $\mathcal{B}$'s view. Thus, the events BAD and Query are independent, and $\Pr[\mathrm{BAD}] \le q_H/|\mathcal{M}|$. Note that if BAD does not happen, then $\mathcal{D}$ makes a correct guess of $b$ with probability 1 when Query happens, and with probability 1/2 when Query does not happen. Thus, we have $\mathtt{Adv}_{\mathrm{PKE}'}^{\mathrm{IND-CPA}}(\mathcal{D}) = |\Pr[b' = b] - 1/2|$

$$\begin{aligned}
&= |\Pr[b' = b \wedge \mathrm{BAD}] + \Pr[b' = b \wedge \neg\mathrm{BAD}] - 1/2(\Pr[\mathrm{BAD}] + \Pr[\neg\mathrm{BAD}])| \\
&\ge |\Pr[b' = b \wedge \neg\mathrm{BAD}] - 1/2\Pr[\neg\mathrm{BAD}]| - \Pr[\mathrm{BAD}]\,|\Pr[b' = b|\mathrm{BAD}] - 1/2| \\
&\ge |\Pr[b' = b \wedge \neg\mathrm{BAD}] - 1/2\Pr[\neg\mathrm{BAD}]| - 1/2\Pr[\mathrm{BAD}] \\
&= |\Pr[b' = b \wedge \neg\mathrm{BAD} \wedge \textsc{Query}] - 1/2\Pr[\neg\mathrm{BAD} \wedge \textsc{Query}]| - 1/2\Pr[\mathrm{BAD}] \\
&= 1/2\Pr[\neg\mathrm{BAD} \wedge \textsc{Query}] - 1/2\Pr[\mathrm{BAD}] \\
&\ge 1/2\Pr[\textsc{Query}] - \Pr[\mathrm{BAD}] \\
&\ge 1/2\Pr[\textsc{Query}] - q_H/|\mathcal{M}| = 1/2\Pr[\textsc{Query} : G_2] - q_H/|\mathcal{M}|.
\end{aligned}$$

Putting the bounds together, we have

$$\mathtt{Adv}_{\mathrm{KEM}_{RH}}^{\mathrm{IND\text{-}1\text{-}CCA}}(\mathcal{B}) \le 2(q_H + 1)\mathtt{Adv}_{\mathrm{PKE}'}^{\mathrm{IND-CPA}}(\mathcal{D}) + 2q_H(q_H + 1)/|\mathcal{M}|.$$

□

**Theorem 4.2 (QROM security of $T_{RH}$).** *If PKE′ is $\delta$-correct, for any adversary $\mathcal{B}$ against the IND-1-CCA security of KEM$_{RH}$ $= T_{RH}[\mathrm{PKE}', H]$ in Fig. 2, issuing at most one single (classical) query to the decapsulation oracle* Decaps *and at most $q_H$ queries to the quantum random oracle $H$, there exists a OW-CPA adversary $\mathcal{A}$ and an IND-CPA adversary $\mathcal{D}$ against PKE′ such that* $\mathrm{Time}(\mathcal{A}) \approx \mathrm{Time}(\mathcal{D}) \approx \mathrm{Time}(\mathcal{B}) + O(q_H^2)$ *and*

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\mathrm{KEM}_{RH}}(\mathcal{B}) \leq 6(q_H+1)^2\sqrt{\mathtt{Adv}^{\mathrm{OW-CPA}}_{\mathrm{PKE}'}(\mathcal{A}) + 1/|\mathcal{K}|}.$$

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\mathrm{KEM}_{RH}}(\mathcal{B}) \leq 6(q_H+1)\sqrt{4\mathtt{Adv}^{\mathrm{IND-CPA}}_{\mathrm{PKE}'}(\mathcal{D}) + 2(q_H+1)^2/|\mathcal{M}| + 1/|\mathcal{K}|}.$$

*If the PKE is deterministic, the bound can be improved as*

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\mathrm{KEM}_{RH}}(\mathcal{B}) \leq 6(q_H+1)\sqrt{\mathtt{Adv}^{\text{OW-CPA}}_{\mathrm{PKE}'}(\mathcal{A}) + 1/|\mathcal{K}| + \delta},$$

*where* $\mathrm{Time}(\mathcal{A}) \approx \mathrm{Time}(\mathcal{B}) + O(q_H^2) + O(q_H \cdot \mathrm{Time}(Enc'))$.

**Proof sketch:** Our proof mainly consists of two steps. One is the underlying security game embedding via replacing the real key $H(m^*, c^*)$ with a random key (i.e., reprogramming $H$). We argue the impact of such a reprogramming by different O2H variants. When the underlying PKE is OW-CPA-secure, we follow previous proofs for $U^{\not\perp}$ in [22, 6], and use general O2H (Lemma 2.1) for probabilistic PKE and double-sided O2H (Lemma 2.2) for deterministic PKE. When the underlying PKE is IND-CPA-secure, we also adopt double-sided O2H (Lemma 2.2) to argue the reprogramming impact. Since the embedded IND-CPA game is decisional, an additional game that searches a reprogramming point in double-sided oracle is introduced and we use Lemma 2.3 to argue this advantage. The other is simulation of the Decaps oracle. As discussed in Sec. 1.4, we adopt a new Decaps simulation that directly replaces the output $H(\bar{m}, \bar{c})$ with a random key $\bar{k}$. Intuitionally, this simulation is perfect if $H(\bar{m}, \bar{c})$ is reprogrammed to be $\bar{k}$ when the adversary first makes a query $(\bar{m}, \bar{c})$. However, in the QROM, it is hard to define the first time to query $(\bar{m}, \bar{c})$. Thus, in the QROM, we argue this in a different way. We find the simulation is perfect if the predicate $\textsc{Decaps}(sk, \bar{c}) = H(\bar{m}, \bar{c})$ is satisfied. Since in the simulation of Decaps, an implicit (classical) $H$-query $(\bar{m}, \bar{c})$ made in the real implementation is removed and thus this specific query can not be measured. Therefore, we use a refined optional-query measure-and-reprogram technique in Lemma 3.1 to argue the simulation impact.

*Proof.* Let $\Omega_H$ be the sets of all functions $H : \mathcal{M} \times \mathcal{C} \to \mathcal{K}$. Let $\mathcal{B}$ be an IND-CCA adversary against KEM$_{RH}$, issuing a single classical query to Decaps (if none, introduce a dummy one), and at most $q_H$ quantum queries (excluding the queries implicitly made in Decaps) to $H$. Consider the games in Fig. 5.

| GAMES $G_0 - G_2$ | DECAPS $(sk, \bar{c} \neq c^*)$ $//G_0 - G_2$ |
|---|---|
| $(pk, sk) \leftarrow Gen', H \leftarrow_\$ \Omega_H$ | $m' := Dec'(sk, \bar{c})$ |
| $k, k_1^* \leftarrow_\$ \mathcal{K}, b \leftarrow_\$ \{0,1\}$ | **if** more than 1 query **return** $\perp$ |
| $m^* \leftarrow_\$ \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$ | **if** $m' = \perp$ **do** $\bar{m} = \star$ |
| $k_0^* = H(m^*, c^*)$ $//G_0 - G_1$ | **else do** $\bar{m} = m'$ |
| $k_0^* \leftarrow_\$ \mathcal{K}$ $//G_2$ | **return** $K := H(\bar{m}, \bar{c})$ |
| $b' \leftarrow \mathcal{B}^{\vert H\rangle, \text{DECAPS}}(pk, c^*, k_b^*)$ $//G_0, G_2$ | $H'(m, c)$ |
| $b' \leftarrow \mathcal{B}^{\vert H'\rangle, \text{DECAPS}}(pk, c^*, k_b^*)$ $//G_1$ | **if** $(m, c) = (m^*, c^*)$ **return** $k$ |
| **return** $b' =?b$ | **return** $H(m, c)$ |

Fig. 5: Games $G_0$-$G_2$ for the proof of Theorem 4.2

GAME $G_0$. Since game $G_0$ is exactly the IND-1-CCA game, $\left|\Pr[G_0^{\mathcal{B}} \Rightarrow 1] - 1/2\right| = \mathtt{Adv}_{\text{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B})$.

GAME $G_1$. In game $G_1$, the random oracle $H$ accessed by $\mathcal{B}$ is replaced by an oracle $H'$ given by Fig. 5. It is easy to see that $G_1$ can be rewritten as game $G_2$.

GAME $G_2$. The game $G_2$ is the same as game $G_0$ except that $k_0^* := H(m^*, c^*)$ is replaced by $k_0^* \leftarrow_\$ \mathcal{K}$. Thus, in $G_2$, the bit $b$ is independent of $\mathcal{B}$'s view, thus $\Pr[G_2^{\mathcal{B}} \Rightarrow 1] = 1/2$. Note that games $G_1$ and $G_2$ have the same distribution. Thus, $\Pr[G_1^{\mathcal{B}} \Rightarrow 1] = \Pr[G_2^{\mathcal{B}} \Rightarrow 1] = 1/2$. Therefore, we have

$$\mathtt{Adv}_{\text{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) = \left|\Pr[G_0^{\mathcal{B}} \Rightarrow 1] - \Pr[G_1^{\mathcal{B}} \Rightarrow 1]\right|. \tag{7}$$

**Lemma 4.1.** *There exists an adversary $\mathcal{A}$ against the OW-CPA of probabilistic* PKE$'$ *such that* Time$(\mathcal{A}) \approx$ Time$(\mathcal{B}) + O(q_H^2)$*and* $\mathtt{Adv}_{\text{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) \leq 6(q_H + 1)^2\sqrt{\mathtt{Adv}_{\text{PKE}'}^{\text{OW-CPA}}(\mathcal{A}) + 1/|\mathcal{K}|}$.

The proof of Lemma 4.1. Define games $G_{3A}$ and $G_{4A}$ as in Fig. 6.

Let $z1 = (pk, sk, c^*, k_b^*, b)$. Let $A^O$ $(O \in H, H')$ be an oracle algorithm that runs $\mathcal{B}^{|O\rangle, \text{DECAPS}}(pk, c^*, k_b^*)$ to obtain $b'$, and returns $b' =?b$. Thus, we have $\Pr[G_0^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|H\rangle}(z1)]$ and $\Pr[G_1^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|H'\rangle}(z1)]$. Let $B(z1)$ be an algorithm that randomly samples $j \in [q_H - 1]$, runs $A^{|H'\rangle}$ until (just before) the $(j+1)$-th query (In game $G_{3A}$, $H'$ is rewritten to be $H$), measures the query input registers in the computational basis, and outputs measurement outcomes. Thus, we have $\Pr[G_{3A}^{\mathcal{B}} \Rightarrow 1] = \Pr[(m^*, *) \leftarrow B^{|H\rangle}(z1)] \geq \Pr[(m^*, c^*) \leftarrow B^{|H\rangle}(z1)]$. Therefore, according to Lemma 2.1, we have

$$\left|\Pr[G_0^{\mathcal{B}} \Rightarrow 1] - \Pr[G_1^{\mathcal{B}} \Rightarrow 1]\right| \leq 2(q_H + 1)\sqrt{\Pr[G_{3A}^{\mathcal{B}} \Rightarrow 1]}.$$

Let $C^{|H\rangle}$ be an oracle algorithm that samples $pk, sk, k^*, j, m^*, c^*$, and runs $\mathcal{B}^{|H\rangle, \text{DECAPS}}$ as in game $G_{3A}$. Let $\bar{c}$ be $\mathcal{B}$'s query to the DECAPS oracle. Let $\bar{m} = \star$

if $\bar{m}' = \perp$, and $\bar{m} = \bar{m}'$ if $\bar{m}' \neq \perp$, where $\bar{m}' = Dec'(sk, \bar{c})$. Let $x = (\bar{m}, \bar{c})$, $y = H(x)$, and $z = (z_1, z_2, z_3) = (\textsc{Decaps}(sk, \bar{c}), m^*, m')$. $C$ outputs $(x, z)$. Let $V_1(x, y, z) = (y = ?z_1)$ and $V_2 = (z_2 = ?z_3)$. Instantiating the predicate $V$ in Lemma 3.1 by $V = V_1 \wedge V_2$. Note that in $G_{3A}$ the return of the Decaps oracle is exactly $H(x)$. That is, $V_1 = 1$ is always satisfied. Thus, we have $\Pr[G_{3A}^{\mathcal{B}} \Rightarrow 1] = \sum x_0 \Pr_H[x = x_0 \wedge V(x, H(x), z) = 1 : (x, z) \leftarrow C^{|H\rangle}]$.

GAMES $G_{3A} - G_{4A}$

$(pk, sk) \leftarrow Gen', H \leftarrow_{\$} \Omega_H, k^*, \bar{k} \leftarrow_{\$} \mathcal{K}, m^* \leftarrow_{\$} \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$

$l = 0, j \leftarrow_{\$} [q_H - 1], (i, b) \leftarrow_{\$} ([q_H - 1] \times \{0, 1\}) \cup \{(q_H, 0)\}$

Run $\mathcal{B}^{|H\rangle, \textsc{Decaps}}(pk, c^*, k^*)$ until the $(j+1)$-th query $|\psi\rangle$ $//G_{3A}$

Run $\mathcal{B}^{|H_1^i\rangle, \textsc{Decaps}}(pk, c^*, k^*)$ until the $(j+1)$-th query state$|\psi\rangle$ $//G_{4A}$

$(m', c') \leftarrow M|\psi\rangle$

// Make a standard measure $M$ on $\mathcal{B}$'s $(j+1)$-th query input register

**return** $m^* = ?m'$

Decaps $(sk, \bar{c} \neq c^*)$ $//G_{3A} - G_{4A}$

**if** more than 1 query **return** $\perp$

**return** $\bar{k}$ $//G_{4A}$

$\bar{m}' := Dec'(sk, \bar{c})$

**if** $\bar{m}' = \perp$ **do** $\bar{m} = \star$

**else do** $\bar{m} = \bar{m}'$

**return** $K := H(\bar{m}, \bar{c})$

$H_1^i(m, c)$

**if** $l \geq (i + b) \wedge (m, c) = (m_{i+1}, c_{i+1})$

// $(m_{i+1}, c_{i+1})$ is the measurement outcome

// on $\mathcal{B}$'s $(i+1)$-th query input register

**return** $\bar{k}$

**else return** $H(m, c)$

$l = l + 1$

Fig. 6: Games $G_{3A}$-$G_{4A}$ for the proof of Lemma 4.1

Note that $C$ needs to implicitly query $H(\bar{m}, \bar{c})$ to simulate the Decaps oracle. That is, $C$ makes $q_H + 1$ $H$-queries in total. In the following, unless otherwise specified, the $H$-queries we mentioned does not include this implicit $H$-query. Let $S^C(\Theta)$ be an oracle algorithm that always returns $\Theta$ for $C$'s implicit classical $H$-query $H(\bar{m}, \bar{c})$. $S$ samples a uniform $(i, b) \leftarrow_{\$} ([q_H - 1] \times \{0, 1\}) \cup \{(q_H, 0)\}$, runs $C^{|H\rangle}$ until the $C$'s $(i+1)$-th query (excluding the implicit $H$-query), measures the query input registers to obtain $x$, continues to run $C^{|H\rangle}$ until the $(i + b + 1)$-th $H$-query, reprogram $H$ to $H_{x\Theta}$ ($H_{x\Theta}(x) = \Theta$ and $H_{x\Theta}(x') = H(x')$ for all $x' \neq x$), and runs $A^{|H_{x\Theta}\rangle}$ until the end to output $z$. Let $x = (\bar{m}, \bar{c})$, $y = \Theta$, and $z = (z_1, z_2, z_3) = (\textsc{Decaps}(sk, \bar{c}), m^*, m')$. $S^C$ outputs $(x, z)$. Note that $V_1(x, y, z) = (y = ?z_1) = 1$ for $S^C$. Sample $\Theta = \bar{k} \leftarrow_{\$} \mathcal{K}$ and $H \leftarrow_{\$} \Omega_H$. Then, $S^C(\Theta)$ perfectly simulates game $G_{4A}$ and we have $\Pr[G_{4A}^{\mathcal{B}} \Rightarrow 1] = \sum x_0 \Pr_{H,\Theta}[x = x_0 \wedge V(x, \Theta, z) = 1 : (x, z) \leftarrow S^C]$.

According to Lemma 3.1, $\sum x_0 \Pr_H[x = x_0 \wedge V(x, H(x), z) = 1 : (x, z) \leftarrow C^{|H\rangle}] \leq 2(2q_H + 1)^2 \sum x_0 \Pr_{H,\Theta}[x = x_0 \wedge V(x, \Theta, z) = 1 : (x, z) \leftarrow S^C] + 8(q_H +$

$1)^2 \frac{1}{|\mathcal{K}|}$. Therefore, we get

$$\Pr[G_{3A}^{\mathcal{B}} \Rightarrow 1] \leq 8(q_H+1)^2(\Pr[G_{4A}^{\mathcal{B}} \Rightarrow 1] + 1/|\mathcal{K}|).$$

Now, we can construct a OW-CPA adversary $\mathcal{A}(pk, c^*)$ against PKE$'$, where $(pk, sk) \leftarrow Gen', m^* \leftarrow_{\$} \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$. $\mathcal{A}$ samples $k^*, \bar{k}, j, i, b$ as in game $G_{4A}$, picks a $2q_H$-wise independent function $H$ (undistinguishable from a random function for a $q_H$-query adversary according to [41, Theorem 6.1]), runs $\mathcal{B}^{|H_1^i\rangle, \textsc{Decaps}}(pk, c^*, k^*)$ (the simulations of $H_1^i$, $\textsc{Decaps}$ are the same as the ones in game $G_{4A}$) until the $(j+1)$-th query, measures $\mathcal{B}$'s query input register to obtain $(m', c')$, finally outputs $m'$ as a return. It is obvious that the advantage of $\mathcal{A}$ against the OW-CPA security of PKE$'$ is exactly $\Pr[G_{4A}^{\mathcal{B}} \Rightarrow 1]$. Putting everything together, we have

$$\mathtt{Adv}_{\mathrm{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) \leq 6(q_H+1)^2\sqrt{\mathtt{Adv}_{\mathrm{PKE}'}^{\mathrm{OW-CPA}}(\mathcal{A}) + 1/|\mathcal{K}|}.$$

**Lemma 4.2.** *There exists an adversary $\mathcal{A}$ against the OW-CPA security of deterministic* PKE$'$ *such that* $\mathrm{Time}(\mathcal{A}) \approx \mathrm{Time}(\mathcal{B}) + O(q_H^2) + O(q_H \cdot \mathrm{Time}(Enc'))$ *and* $\mathtt{Adv}_{\mathrm{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) \leq 6(q_H+1)\sqrt{\mathtt{Adv}_{\mathrm{PKE}'}^{\text{OW-CPA}}(\mathcal{A}) + 1/|\mathcal{K}| + \delta}$.

The proof of Lemma 4.2. Define games $G_{3B}$, $G_{4B}$ and $G_{5B}$ as in Fig. 7. Let $z1 = (pk, sk, c^*, k_0^*)$, where $(pk, sk) \leftarrow Gen'$, $k_0^* \leftarrow_{\$} \mathcal{K}$, $m^* \leftarrow_{\$} \mathcal{M}$, and $c^* \leftarrow Enc(pk, m^*)$. Sample $G \leftarrow_{\$} \Omega_H$. Let $G'$ be an oracle such that $G'(m^*, c^*) = k_0^*$, and $G'(x) = G(x)$ for $x \neq (m^*, c^*)$. Let $A^{|O\rangle}(z1)$ $(O \in G, G')$ be an oracle algorithm that first samples $k_1^* \leftarrow_{\$} \mathcal{K}$, $b \leftarrow_{\$} \{0,1\}$, then runs $\mathcal{B}^{|O\rangle, \textsc{Decaps}}(pk, c^*, k_b^*)$ to obtain $b'$ (simulating $\textsc{Decaps}$ as in games $G_0$ and $G_1$), finally returns $b' =?b$. Thus, we have $\Pr[G_0^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|G'\rangle}(z1)]$ and $\Pr[G_1^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|G\rangle}(z1)]$.

Lemma 2.2 states that there exists an oracle algorithm $\bar{B}^{|G\rangle, |G'\rangle}(z1)$ such that $|\Pr[1 \leftarrow A^{|G\rangle}(z1)] - \Pr[1 \leftarrow A^{|G'\rangle}(z1)| \leq 2\sqrt{\Pr[(m^*, c^*) \leftarrow \bar{B}^{|G\rangle, |G'\rangle}(z1)]}$. Define game $G_{3B}$ as in Fig. 7, where $\hat{B}$ is the same as $\bar{B}$ except that $\hat{B}$ simulates $\mathcal{B}$'s $\textsc{Decaps}$ query using a given $\textsc{Decaps}$ oracle (implemented as in $G_0$ and $G_1$). Thus, it is obvious that $\Pr[(m^*, c^*) \leftarrow \bar{B}^{|G\rangle, |G'\rangle}(z1)] \leq \Pr[G_{3B}^{\hat{B}} \Rightarrow 1]$. Thus, we have

$$\mathtt{Adv}_{\mathrm{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) \leq 2\sqrt{\Pr[G_{3B}^{\hat{B}} \Rightarrow 1]}.$$

Game $G_{4B}$ is identical to game $G_{3B}$ except the simulation of $G'$. In game $G_{4B}$, the judgement condition $(m, c) = (m^*, c^*)$ is replaced by $c = c^* \wedge Enc'(pk, m) = c^*$ without knowledge of $m^*$. Define COLL as an event that there is a message $m \neq m^*$ such that $Enc'(pk, m) = c^* = Enc'(pk, m^*)$. Note that if COLL does not happen (implied by the injectivity of DPKE), then $G_{4B}$ and $G_{3B}$ have the same distribution. Thus, we have

$$\left|\Pr[G_{3B}^{\hat{B}} \Rightarrow 1] - \Pr[G_{4B}^{\hat{B}} \Rightarrow 1]\right| \leq \delta.$$

$G_{3B} - G_{5B}$

$(pk, sk) \leftarrow Gen', G \leftarrow_\$ \Omega_H, k_0^*, \bar{k} \leftarrow_\$ \mathcal{K}, m^* \leftarrow_\$ \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$
$l = 0, (i, b) \leftarrow_\$ ([q_H - 1] \times \{0,1\}) \cup \{(q_H, 0)\}$
$(m', c') \leftarrow \hat{B}^{|G\rangle, |G'\rangle, \text{DECAPS}}(pk, c^*, k_0^*) \quad //G_{3B}, G_{4B}$
$(m', c') \leftarrow \hat{B}^{|G_1^i\rangle, |G'\rangle, \text{DECAPS}}(pk, c^*, k_0^*) \quad //G_{5B}$
**return** $m^* =?m'$

DECAPS $(sk, \bar{c} \neq c^*)$

**if** more than 1 query **return** $\perp$
**return** $\bar{k} \quad //G_{5B}$
$\bar{m}' := Dec'(sk, \bar{c})$
**if** $\bar{m}' = \perp$ **do** $\bar{m} = \star$
**else do** $\bar{m} = \bar{m}'$
**return** $K := G(\bar{m}, \bar{c})$

$G_1^i(m, c)$

**if** $l \geq (i + b) \wedge (m, c) = (m_{i+1}, c_{i+1})$
// $(m_{i+1}, c_{i+1})$ is the measurement outcome
// on $\hat{B}$'s $(i+1)$-th query input register
  **return** $\bar{k}$
**else return** $G(m, c)$
$l = l + 1$

$G'(m, c)$

**if** $(m, c) = (m^*, c^*) \quad //G_{3B}$
**if** $c = c^* \wedge Enc'(pk, m) = c^* \quad //G_{4B} - G_{5B}$
  **return** $k_0^* // G_{3B} - G_{5B}$
**return** $G(m, c) // G_{3B} - G_{4B}$
**return** $G_1^i(m, c) // G_{5B}$

Fig. 7: Games $G_{3B} - G_{5B}$ for the proof of Lemma 4.2

In game $G_{5B}$, DECAPS is modified to output a random $\Theta = \bar{k}$ for the single query $\bar{c}$, and the random oracle $G$ is correspondingly reprogrammed conditioned on $(i, b)$, where $(i, b) \leftarrow_\$ ([q_H - 1] \times \{0,1\}) \cup \{(q_H, 0)\}$. Using Lemma 3.1 in the same way as in Lemma 4.1, we have

$$\Pr[G_{4B}^{\hat{B}} \Rightarrow 1] \leq 8(q_H + 1)^2 (\Pr[G_{5B}^{\hat{B}} \Rightarrow 1] + 1/|\mathcal{K}|).$$

Now, we can construct a OW-CPA adversary $\mathcal{A}(pk, c^*)$ against deterministic PKE$'$, where $(pk, sk) \leftarrow Gen', m^* \leftarrow_\$ \mathcal{M}, c^* \leftarrow Enc(pk, m^*)$. $\mathcal{A}$ samples $k_0^*, \bar{k}, i, b$ as in game $G_{5B}$, picks a $2q_H$-wise function $G$, runs $\hat{B}^{|G_1^i\rangle, |G'\rangle, \text{DECAPS}}(pk, c^*, k^*)$ (the simulations of $G_1^i, G', \text{DECAPS}$ are the same as in game $G_{5B}$) to obtain $(m', c')$, finally outputs $m'$ as a return. It is obvious that the advantage of $\mathcal{A}$ against the OW-CPA security of deterministic PKE$'$ is exactly $\Pr[G_{5B}^{\hat{B}} \Rightarrow 1]$. Thus, we have

$$\begin{aligned} \mathtt{Adv}_{\text{KEM}_{RH}}^{\text{IND-1-CCA}}(\mathcal{B}) &\leq 2\sqrt{8(q_H+1)^2(\mathtt{Adv}_{\text{PKE}'}^{\text{OW-CPA}}(\mathcal{A}) + 1/|\mathcal{K}|) + \delta} \\ &\leq 6(q_H+1)\sqrt{\mathtt{Adv}_{\text{PKE}'}^{\text{OW-CPA}}(\mathcal{A}) + 1/|\mathcal{K}| + \delta}. \end{aligned}$$

**Lemma 4.3.** *There exists an adversary $\mathcal{D}$ against the IND-CPA security of probabilistic* PKE$'$ *such that* $\mathrm{Time}(\mathcal{D}) \approx \mathrm{Time}(\mathcal{B}) + O(q_H^2)$ *and* $\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) \leq 6(q_H+1)\sqrt{4\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}'}(\mathcal{D}) + 2(q_H+1)^2/|\mathcal{M}| + 1/|\mathcal{K}|}$.

The proof of Lemma 4.3. Define games $G_{3C} - G_{6C}$ as in Fig. 8.

Let $z1 = (pk, sk, c^*, k_0^*)$, where $(pk, sk) \leftarrow Gen'$, $k_0^* \leftarrow_\$ \mathcal{K}$, $m_0^*, m_1^* \leftarrow_\$ \mathcal{M}$, $\bar{b} \leftarrow_\$ \{0,1\}$ and $c^* \leftarrow Enc(pk, m_{\bar{b}}^*)$. Sample $G \leftarrow_\$ \Omega_H$. Let $G'$ be an oracle such that $G'(m_{\bar{b}}^*, c^*) = k_0^*$, and $G'(x) = G(x)$ for $x \neq (m_{\bar{b}}^*, c^*)$. Let $A^{|O\rangle}(z1)$ ($O \in G, G'$) be an oracle algorithm that first samples $k_1^* \leftarrow_\$ \mathcal{K}$, $\tilde{b} \leftarrow_\$ \{0,1\}$, then runs $\mathcal{B}^{|O\rangle,\textsc{Decaps}}(pk, c^*, k_{\tilde{b}}^*)$ to obtain $\tilde{b}'$ (simulating $\textsc{Decaps}$ as in games $G_0$ and $G_1$), finally returns $\tilde{b}' =? \tilde{b}$. Thus, we have $\Pr[G_0^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|G'\rangle}(z1)]$ and $\Pr[G_1^{\mathcal{B}} \Rightarrow 1] = \Pr[1 \leftarrow A^{|G\rangle}(z1)]$.

GAMES $G_{3C} - G_{6C}$

$(pk, sk) \leftarrow Gen', G \leftarrow_\$ \Omega_H, l = 0, (i, b) \leftarrow_\$ ([q_H - 1] \times \{0,1\}) \cup \{(q_H, 0)\}$
$k_0^*, \bar{k} \leftarrow_\$ \mathcal{K}, \bar{b} \leftarrow_\$ \{0,1\}, m_0^*, m_1^* \leftarrow_\$ \mathcal{M}, c^* \leftarrow Enc(pk, m_{\bar{b}}^*)$
$(m', c') \leftarrow \hat{B}^{|G\rangle,|G'\rangle,\textsc{Decaps}}(pk, c^*, k_0^*) \quad //G_{3C}$
$(m', c') \leftarrow \hat{B}^{|G_1^i\rangle,|G'\rangle,\textsc{Decaps}}(pk, c^*, k_0^*) \quad //G_{4C} - G_{6C}$
**return** $(m_{\bar{b}}^*, c^*) =? (m', c') // G_{3C} - G_{4C}$
**return** $(m_{1-\bar{b}}^*, c^*) =? (m', c') // G_{5C}$
**if** $(m_0^*, c^*) = (m', c')$ **then** $\tilde{b}' = 0$ **else then** $\tilde{b}' = 1 // G_{6C}$
**return** $\tilde{b}' =? \bar{b} // G_{6C}$

$\textsc{Decaps}$ $(sk, \bar{c} \neq c^*)$ $//G_{3C} - G_{6C}$

**if** more than 1 query **return** $\perp$
**return** $\bar{k} \quad //G_{4C} - G_{6C}$
$\bar{m}' := Dec'(sk, \bar{c})$
**if** $\bar{m}' = \perp$ **do** $\bar{m} = \star$
**else do** $\bar{m} = \bar{m}'$
**return** $K := G(\bar{m}, \bar{c})$

$G_1^i(m, c)$

**if** $l \geq (i + b) \wedge (m, c) = (m_{i+1}, c_{i+1})$
// $(m_{i+1}, c_{i+1})$ is the measurement outcome
// on $\mathcal{B}$'s $(i+1)$-th query input register
  **return** $\bar{k}$
**else return** $G(m, c)$
$l = l + 1$

$G'(m, c)$

**if** $(m, c) = (m_{\bar{b}}^*, c^*) \quad //G_{3C} - G_{4C}$
**if** $(m, c) = (m_{1-\bar{b}}^*, c^*) \quad //G_{5C}$
**if** $(m, c) = (m_0^*, c^*) \quad //G_{6C}$
  **return** $k_0^* // G_{3C} - G_{6C}$
**return** $G(m, c) // G_{3C}$
**return** $G_1^i(m, c) // G_{4C} - G_{6C}$

Fig. 8: Games $G_{3C}$-$G_{6C}$ for the proof of Lemma 4.3

Lemma 2.1 states that there exists an oracle algorithm $\bar{B}^{|G\rangle,|G'\rangle}(z1)$ such that $|\Pr[1 \leftarrow A^{|G\rangle}(z1)] - \Pr[1 \leftarrow A^{|G'\rangle}(z1)| \leq 2\sqrt{\Pr[(m^*_{\bar{b}}, c^*) \leftarrow \bar{B}^{|G\rangle,|G'\rangle}(z1)]}$. Define game $G_{3C}$ as in Fig. 8, where $\hat{B}$ is the same as $\bar{B}$ except that $\hat{B}$ simulates $\mathcal{B}$'s DECAPS query using a given DECAPS oracle (implemented as in $G_0$ and $G_1$). Thus, it is obvious that $\Pr[(m^*_{\bar{b}}, c^*) \leftarrow \bar{B}^{|G\rangle,|G'\rangle}(z1)] \leq \Pr[G^{\hat{B}}_{3C} \Rightarrow 1]$. Thus, we have

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) \leq 2\sqrt{\Pr[G^{\hat{B}}_{3C} \Rightarrow 1]}.$$

In game $G_{4C}$, DECAPS is modified to output a random $\Theta = \bar{k}$ for the single query $\bar{c}$, and the random oracle $H$ is correspondingly reprogrammed conditioned on $(i, b)$, where $(i, b) \leftarrow_{\$} ([q_H - 1] \times \{0, 1\}) \cup \{(q_H, 0)\}$. Then, using Lemma 3.1 in the same way as in Lemma 4.1, we have

$$\Pr[G^{\hat{B}}_{3C} \Rightarrow 1] \leq 8(q_H + 1)^2(\Pr[G^{\hat{B}}_{4C} \Rightarrow 1] + 1/|\mathcal{K}|).$$

Game $G_{5C}$ is identical to game $G_{4C}$ except that $G'(m^*_{\bar{b}}, c^*) = k^*_0$ is replaced by $G'(m^*_{1-\bar{b}}, c^*) = k^*_0$, and correspondingly $(m^*_{1-\bar{b}}, c^*) =?(m', c')$ is returned instead of $(m^*_{\bar{b}}, c*) =?(m', c')$.

Note that game $G_{4C}$ conditioned on $\bar{b} = 1$ has the same output distribution as game $G_{4C}$ conditioned on $\bar{b} = 0$. Thus, we have $\Pr[G^{\hat{B}}_{4C} \Rightarrow 1 : \bar{b} = 0] = \Pr[G^{\hat{B}}_{4C} \Rightarrow 1 : \bar{b} = 1] = \Pr[G^{\hat{B}}_{4C} \Rightarrow 1]/2$. Analogously, we have $\Pr[G^{\hat{B}}_{5C} \Rightarrow 1 : \bar{b} = 1] = \Pr[G^{\hat{B}}_{5C} \Rightarrow 1]/2$. Note that $m^*_{1-\bar{b}}$ is independent of $pk$, $c^*$, $k^*_0$ and $G$. Thus, according to Lemma 2.3, we have

$$\Pr[G^{\hat{B}}_{5C} \Rightarrow 1 : \bar{b} = 1] \leq (q_H + 1)^2/|\mathcal{M}|.$$

Define game $G_{6C}$ as in Fig. 8. Thus, $\Pr[G^{\hat{B}}_{6C} \Rightarrow 1]$

$$\begin{aligned}
&= 1/2\Pr[(m^*_0, c^*) = (m', c') : \bar{b} = 0] + 1/2\Pr[(m^*_0, c^*) \neq (m', c') : \bar{b} = 1] \\
&= 1/2\Pr[(m^*_0, c^*) = (m', c') : \bar{b} = 0] + 1/2 - 1/2\Pr[(m^*_0, c^*) = (m', c') : \bar{b} = 1] \\
&= 1/2 + 1/2\Pr[G^{\hat{B}}_{4C} \Rightarrow 1 : \bar{b} = 0] - 1/2\Pr[G^{\hat{B}}_{5C} \Rightarrow 1 : \bar{b} = 1] \\
&= 1/2 + 1/4(\Pr[G^{\hat{B}}_{4C} \Rightarrow 1] - \Pr[G^{\hat{B}}_{5C} \Rightarrow 1])
\end{aligned}$$

Now, we can construct an IND-CPA adversary $\mathcal{D}(pk)$ against PKE$'$, where $(pk, sk) \leftarrow Gen'$. $\mathcal{D}$ samples $m^*_0, m^*_1 \leftarrow_{\$} \mathcal{M}$, receives challenge ciphertext $c^* \leftarrow Enc(pk, m^*_{\bar{b}})$ ($\bar{b} \leftarrow_{\$} \{0, 1\}$), samples $k^*_0, \bar{k}, i, b$ as in game $G_{6C}$, picks a $2q_H$-wise independent function $H$, runs $\hat{B}^{|G^i_1\rangle,|G'\rangle,\text{DECAPS}}(pk, c^*, k^*_0)$ (the simulations of $G^i_1, G'$, DECAPS are the same as in game $G_{6C}$) to obtain $(m', c')$, finally outputs 0 if $(m^*_0, c^*) = (m', c')$, and returns 1 otherwise. Thus, apparently,

$$\left|\Pr[G^{\hat{B}}_{6C} \Rightarrow 1] - 1/2\right| = \mathtt{Adv}^{\text{IND}-\text{CPA}}_{\text{PKE}'}(\mathcal{D})$$

Putting everything together, we have

$$\begin{aligned}
\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) &\leq 2\sqrt{8(q_H + 1)^2(4\mathtt{Adv}^{\text{IND}-\text{CPA}}_{\text{PKE}'}(\mathcal{D}) + 2(q_H + 1)^2/|\mathcal{M}| + 1/|\mathcal{K}|)} \\
&\leq 6(q_H + 1)\sqrt{4\mathtt{Adv}^{\text{IND}-\text{CPA}}_{\text{PKE}'}(\mathcal{D}) + 2(q_H + 1)^2/|\mathcal{M}| + 1/|\mathcal{K}|}.
\end{aligned}$$

□

**Theorem 4.3** **($T_H \to T_{RH}$).** *For any adversary $\mathcal{B}'$ against the IND-1-CCA security of $KEM_H = T_H[\mathrm{PKE}', H]$, issuing $q_H$ queries to the random oracle $H$, there exists an IND-1-CCA adversary $\mathcal{B}$ against $KEM_{RH} = T_{RH}[\mathrm{PKE}', H]$[9] that makes $q_H + 1$ queries to $H$ such that* $\mathrm{Time}(\mathcal{B}') \approx \mathrm{Time}(\mathcal{B})$ *and*

$$\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_H}(\mathcal{B}') \leq \mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}_{RH}}(\mathcal{B}) + \epsilon_{\text{coll}},$$

*where $\epsilon_{\text{coll}}$ is an advantage bound of an algorithm searching a collision of the random oracle $H$ with $q_H$ queries. In particular, $\epsilon_{\text{coll}} = q_H^2/|\mathcal{K}|$ in the ROM, and $\epsilon_{\text{coll}} = q_H^3/|\mathcal{K}|$ in the QROM [42, Corollary 2].*

*Proof.* Let $\mathcal{B}'^{H,\textsc{Decaps}_{T_H}}(pk, c^*, k_b^*)$ be an adversary against the IND-1-CCA security of $T_H[\mathrm{PKE}', H]$. Construct an adversary $\mathcal{B}^{H,\textsc{Decaps}_{T_{RH}}}(pk, c^*, k_b^*)$ that runs $\mathcal{B}'^{H,\textsc{Decaps}'}(pk, c^*, k_b^*)$, and returns $\mathcal{B}'$'s return. The oracle $\textsc{Decaps}'$ is simulated by querying $\textsc{Decaps}_{T_{RH}}$. In detail, $\textsc{Decaps}'(\bar{c})$ returns $\perp$ if $\textsc{Decaps}_{T_{RH}}(\bar{c}) = H(\star, \bar{c})$. For other cases, $\textsc{Decaps}'(\bar{c})$ just returns $\textsc{Decaps}_{RH}(\bar{c})$. Note that when $\textsc{Decaps}_{T_H}(\bar{c}) = \perp$, $\textsc{Decaps}'(\bar{c})$ returns $\perp$ with probability 1. When $\textsc{Decaps}_{T_H}(\bar{c}) \neq \perp$, $\Pr[\textsc{Decaps}_{RH}(\bar{c}) = H(\star, \bar{c})] \leq \epsilon_{\text{coll}}$ since $\star \notin \mathcal{M}$. Thus $\textsc{Decaps}'(\bar{c})$ returns $\textsc{Decaps}_H(\bar{c})$ with probability at least $(1 - \epsilon_{\text{coll}})$. That is, for any $\bar{c}$, $\textsc{Decaps}_{T_H}(\bar{c}) = \textsc{Decaps}'(\bar{c})$ with probability at least $1 - \epsilon_{\text{coll}}$. Thus, we have $\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}}(\mathcal{B}') \leq \mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}}(\mathcal{B}) + \epsilon_{\text{coll}}$.

*Remark 2.* The proof of Theorem 4.3 requires $\star \notin \mathcal{M}$. Theorems 4.1 and 4.2 for $\text{KEM}_{RH}$ works for both $\star \in \mathcal{M}$ and $\star \notin \mathcal{M}$. Thus, combing Theorems 4.1, 4.2, 4.3, we can directly obtain the (Q)ROM security proofs of $\text{KEM}_H = T_H[\mathrm{PKE}', H]$ with the same tightness as $\text{KEM}_{RH} = T_{RH}[\mathrm{PKE}', H]$.

## 5 Tightness of the Reductions

In this section, we will show that for $KEM = T_{RH}[\mathrm{PKE}', H]$, a $O(q)$-ROM-loss (and $q^2$-loss) is unavoidable in general.

**Theorem 5.1.** *Let $\mathrm{PKE}' = (Gen', Enc', Dec')$ be a PKE with malleability property. Let $\mathcal{M} = \{0,1\}^n$ be the message space of $\mathrm{PKE}'$. Then, there exists a ROM (QROM, resp.) adversary $\mathcal{B}$ against the IND-1-CCA security of $KEM = T_{RH}[\mathrm{PKE}', H]$ such that the advantage $\mathtt{Adv}^{\text{IND-1-CCA}}_{\text{KEM}}(\mathcal{B})$ is about $(1/e)\frac{q}{|\mathcal{M}|}$ ($(q+1)^2/|\mathcal{M}|$, resp.), where $q$ is the number of queries to $H$ such that $1/\sqrt{|\mathcal{M}|} \leq \sin(\frac{\pi}{6q+3})$ and $q \leq |\mathcal{K}|$ ($\mathcal{K}$ is the key space).*

*Proof.* Let $(pk, sk) \leftarrow Gen'$, $m^* \leftarrow_\$ \mathcal{M}$, $c^* \leftarrow Enc(pk, m^*)$, $k_0^* = H(m^*, c^*)$, $k_1^* \leftarrow_\$ \mathcal{K}$, and $b \leftarrow_\$ \{0,1\}$. Since $\mathrm{PKE}'$ satisfies the malleability property, there

[9] In Theorem 4.3, the return value $\star$ for invalid ciphertext in decapsulation of $\text{KEM}_{RH}$ is required not in message space (i.e., $\star \notin \mathcal{M}$).

exists an algorithm $\bar{B}$ that on input $(pk, c^*)$ outputs $(f, c')$ such that (1) $f(m^*) = Dec(sk, c') \neq \perp$; (2)$f(\tilde{m}) \neq Dec(sk, c')$ for any $\tilde{m} \in \mathcal{M}$ and $\tilde{m} \neq m$.

Define the function $g^H_{c,k} : \mathcal{M} \to \{0, 1\}$ as

$$g^H_{c,k}(m) = \begin{cases} 1 & H(f(m), c) = k \\ 0 & \text{Otherwise} \end{cases}$$

First, we consider the ROM case. Let $\mathcal{B}^{H,\textsc{Decaps}}(pk, c^*, k^*_b)$ be a ROM adversary as follows.

1. Run $\bar{B}$ to obtain $(f, c')$;
2. Query the Decaps oracle with $c'$ and obtain $k'$;
3. Randomly pick $m_1, \ldots, m_q$ from $\mathcal{M}$, and compute $g^H_{c',k'}(m_i)$ for each $i \in \{1, \ldots, q\}$ by querying $H$;
4. If there exists an $m_i$ such that $g^H_{c',k'}(m_i) = 1$, return $1 - (H(m_i, c^*) =?k^*_b)$, else return $\perp$.

Note that $g^H_{c',k'}(m^*) = 1$ with probability 1, and $g^H_{c',k'}(\tilde{m}) = 1$ with negligible probability $1/|\mathcal{K}|$ for $\tilde{m} \neq m^*$. We also note that $\Pr[m^* \in \{m_1, \ldots, m_q\}] = \frac{q}{\mathcal{M}}$. Thus, the ROM advantage of $\mathcal{B}$ is at least $\frac{q}{\mathcal{M}}(1 - 1/|\mathcal{K}|)^{q-1} \gtrapprox (1/e)\frac{q}{\mathcal{M}}$ since $q \leq |\mathcal{K}|$.

Next, we consider the QROM case. Let $\mathcal{B}^{|H\rangle,\textsc{Decaps}}(pk, c^*, k^*_b)$ be a QROM adversary as follows.

1. Run $\bar{B}$ to obtain $(f, c')$;
2. Query the Decaps oracle with $c'$ and obtain $k'$;
3. Use Grover's algorithm for $q$ steps to try to find $m^*$. In details, apply Grover iteration $q$ time on initial state $HGate^{\otimes n}|0^n\rangle$ and make a standard measurement to derive $\bar{m}$, where Grover iteration is composed of oracle query $O_g$ that turns $|m\rangle$ into $(-1)^{g^H_{c',k'}(m)}|m\rangle$, and diffusion operator $U = HGate^{\otimes n}(2|0^n\rangle\langle 0^n| - I_n)HGate^{\otimes n}$;
4. Return $1-(H(\bar{m}, c^*) =?k^*_b)$, where $\bar{m}$ is the outcome obtained using Grover's algorithm in step 3.

Note that $g^H_{c',k'}(m^*) = 1$ with probability 1, and $g^H_{c',k'}(\tilde{m}) = 1$ with negligible probability $1/|\mathcal{K}|$ for $\tilde{m} \neq m^*$. Let $p_0 = \Pr[g^H_{c',k'}(m) = 1 : m \in \mathcal{M}] \geq 1/|\mathcal{M}|$. By $q$ Grover iterations (requiring $q$ quantum queries to $H$), the probability $p_1$ of finding $m^*$ is $\sin^2((2q + 1)\theta)$, where $\sin^2(\theta) = p_0$.

When $1/\sqrt{|\mathcal{M}|} \leq \sin(\frac{\pi}{6q+3})$, we have $(2q + 1)\theta \leq \pi/3$. Thus, we have

$$\sin((2q + 1)\theta) \geq \sin(\theta) + \frac{2q \cdot \theta}{2} \geq (q + 1)\sin(\theta).$$

Therefore, we have $p_1 = \sin^2((2q + 1)\theta) \geq \frac{(q+1)^2}{|\mathcal{M}|}$. Note that when $m^*$ is obtained, one can derive $b^*$ with probability 1 by querying $H(\bar{m}, c^*)$. Thus, the QROM advantage of $\mathcal{B}$ is at least $\frac{(q+1)^2}{|\mathcal{M}|}$. $\square$

*Remark 3.* Most IND-CPA-secure PKEs has malleability property, e.g., ElGamal, FrodoKEM.PKE [28], Kyber.PKE [8], etc. Moreover, malleability property is inherent for a homomorphic PKE. Let PKE $= (Gen, Enc, Dec)$ be homomorphic in addition. That is, $Enc(pk, m_1 + m_2) = Enc(pk, m_1) + Enc(pk, m_2)$. Then, we can construct algorithm $\bar{B}(pk, c^*)$ ($c^* \leftarrow Enc(pk, m^*)$) that randomly picks $m \in \mathcal{M}$, computes $c' = c^* + Enc(pk, m)$, and defines $f(x) = x + m$. Note that $f(m^*) = Dec(sk, c')$ and $f(\tilde{m}) \neq Dec(sk, c')$ for $\tilde{m} \neq m$(We assume the PKE has perfect correctness for simplicity). Thus, the homomorphic property of a PKE implies the malleability property in this paper.

*Remark 4.* For a $\lambda$-bit IND-CPA-secure malleable public-key encryption PKE$'$ with message space $\mathcal{M} = 2^\lambda$ we require that any PPT adversary breaks the security of PKE$'$ with advantage at most $\frac{1}{2^\lambda}$. For example, such a PKE$'$ can be constructed based on the LWE assumption by a suitable parameter selection [34]. Theorem 5.1 shows that a ROM (QROM, resp.) adversary against the IND-1-CCA security of KEM $= T_{RH}[\text{PKE}', H]$ can achieve advantage at least $(1/e)\frac{q}{2^\lambda}$ ($\frac{(q+1)^2}{2^\lambda}$, resp.), where $q$ is the number of adversary's queries to $H$. That is, a $O(1/q)$ ($O(1/q^2)$, resp.) loss is unavoidable in the ROM (QROM, resp.) for $T_{RH}$.

*Remark 5.* We remark that the output of decapsulation for an invalid ciphertext $c$ is irrelevant to the attack given in Theorem 5.1. Thus, the aforementioned tightness results can also be applied to $T_H$. We also remark that such a tightness result can also be extended to the IND-1-CCA KEM construction $T_{CH}$ given in [21], where there is tag $tag = H'(m^*, c_0^*)$ in the ciphertext ($c_0^* \leftarrow Enc(pk, m^*)$), and the key is computed by $K = H(m^*)$. The idea is that the adversary against KEM can first search $m^*$ such that $tag = H'(m^*, c_0^*)$ by querying $H'$, and then query $H$ with $m^*$, thus break the key indistinguishability. Following the same analysis in Theorem 5.1, one can easily derive the same tightness result for $T_{CH}$.

## 6 Relations among Notions of CCA Security for KEM

In this section, we will compare the relative strengths of notions of IND-1-CCA security and IND-CCA security in ROM and QROM. In detail, we works out the relations among four notions. For each pair of notions $\text{A}, \text{B} \in \{$ IND-1-CCA ROM, IND-1-CCA QROM, IND-CCA ROM, IND-CCA QROM $\}$, we show one of the following:

- A $\Rightarrow$ B: A proof that if a KEM meets the notion of security A then it also meets the notion of security B.
- A $\not\Rightarrow$ B: There is a KEM construction that provably meets the notion of security A but does not meet the notion of security B.

First, according to the security definitions, one can trivially derive the relations IND-CCA QROM $\Rightarrow$ IND-1-CCA QROM $\Rightarrow$ IND-1-CCA ROM, and IND-CCA QROM $\Rightarrow$ IND-CCA ROM $\Rightarrow$ IND-1-CCA ROM. Next, we show the other nontrivial relations.

**Theorem 6.1.** *If the LWE assumption (Definition B.1) holds, then we have IND-1-CCA ROM$\not\Rightarrow$ IND-1-CCA QROM, IND-CCA ROM$\not\Rightarrow$IND-1-CCA QROM and IND-CCA ROM $\not\Rightarrow$IND-CCA QROM.*

*Proof.* First, if the LWE assumption holds, we can have a KEM=$(Gen, Encaps, Decaps)$ that satisfies the IND-CCA ROM security. For example, FrodoKEM [28] is such a KEM whose IND-CCA ROM security can be reduced to the LWE assumption. Let PoQRO=$(Setup, Prove, Verify)$ (Definition C.1) be a proof of quantum access to random oracle $H$, whose existence is based on the LWE assumption, see Lemma C.1. Here, $H$ is independent of the KEM.

Construct a new KEM$'$=$(Gen', Encaps', Decaps')$ as in Fig. 9. Note that any efficient ROM adversary cannot find a $c_2$ such that $Verify^H(sk_2, c_2) = 1$ (otherwise the soundness of the PoQRO is broken). Thus, for an efficient ROM adversary, querying oracle $Decaps'$ is equivalent to querying oracle $Decaps$. Thus, KEM$'$ also meets the IND-CCA ROM security.

| $Gen'$ | $Encaps'(pk)$ | $Decaps'(sk, c)$ |
|---|---|---|
| $(pk_1, sk_1) \leftarrow Gen$ | **parse** $pk = (pk_1, pk_2)$ | **parse** $sk = (sk_1, sk_2)$ |
| $(pk_2, sk_2) \leftarrow Setup$ | $(K, c_1) \leftarrow_{\$} Encaps(pk_1)$ | **parse** $c = (c_1, c_2)$ |
| $pk = (pk_1, pk_2)$ | $c = (c_1, \perp)$ | **if** $Verify^H(sk_2, c_2) = 1$ |
| $sk = (sk_1, sk_2)$ | **return** $(K, c)$ |     **return** $sk_1$ |
| **return** $(pk, sk)$ | | **return** $Decaps(sk_1, c_1)$ |

Fig. 9: Separation instance KEM$'$ for Theorem 6.1.

Meanwhile, a QROM adversary can find a $c_2$ such that $Verify^H(sk_2, c_2) = 1$. Thus, by querying oracle $Decaps'$ (only one time), a QROM adversary can obtain $sk_1$, hence break the IND-CCA security of KEM$'$. Therefore, KEM$'$ does not meet the IND-1-CCA QROM security (and also IND-CCA QROM security). Since KEM meets the IND-CCA ROM security, KEM is also IND-1-CCA-secure in the ROM. Hence, we have IND-1-CCA ROM$\not\Rightarrow$IND-1-CCA QROM, IND-CCA ROM$\not\Rightarrow$IND-1-CCA QROM and IND-CCA ROM$\not\Rightarrow$IND-CCA QROM. $\square$

**Theorem 6.2.** *If the LWE assumption holds, then we have IND-1-CCA ROM $\not\Rightarrow$IND-CCA ROM, IND-1-CCA QROM$\not\Rightarrow$IND-CCA QROM, and IND-1-CCA QROM$\not\Rightarrow$IND-CCA ROM.*

*Proof.* Let $(Gen, Enc, Dec)$ be the key-generation, encryption and decryption algorithms of FrodoPKE [28], whose IND-CPA security can be reduced to the LWE assumption. Then, according to Theorems 4.1 and 4.2, KEM=$T_{RH}$[FrodoPKE, $H$] is IND-1-CCA secure in both ROM and QROM. Note that such a KEM is essentially a FO-KEM without re-encryption. Qin et al. [33] had shown such a KEM is vulnerable to key-mismatch attacks that can recover the secret key with only polynomial queries to the decapsulation oracle. That is, KEM=$T_{RH}$[FrodoPKE, $H$] is not IND-CCA-secure in ROM (and QROM). Hence, we have IND-1-CCA ROM$\not\Rightarrow$IND-CCA ROM, IND-1-CCA QROM$\not\Rightarrow$ IND-CCA QROM, and IND-1-CCA QROM $\not\Rightarrow$IND-CCA ROM. $\square$

***Acknowledgements.*** We thank anonymous reviewers for their insightful comments and suggestions. Haodong Jiang was supported by the National Key R&D Program of China (No. 2021YFB3100100), and the National Natural Science Foundation of China (Nos. 62002385). Zhi Ma was supported by the National Natural Science Foundation of China (No. 61972413).

## A Supporting Material: Cryptographic Primitives

**Definition A.1 (Public-key encryption).** *A public-key encryption (PKE) scheme* PKE *consists of a triple of polynomial time (in the security parameter $\lambda$) algorithms and a finite message space $\mathcal{M}$. (1) $Gen(1^\lambda) \to (pk, sk)$: the key generation algorithm, is a probabilistic algorithm which on input $1^\lambda$ outputs a public/secret key-pair $(pk, sk)$. Usually, for brevity, we will omit the input of Gen. (2) $Enc(pk, m) \to c$: the encryption algorithm Enc, on input pk and a message $m \in \mathcal{M}$, outputs a ciphertext $c \leftarrow Enc(pk, m)$. (3) $Dec(sk, c) \to m$: the decryption algorithm Dec, is a deterministic algorithm which on input sk and a ciphertext c outputs a message $m := Dec(sk, c)$ or a rejection symbol $\perp \notin \mathcal{M}$.*

**Definition A.2 (Correctness [17]).** *A* PKE *is* $\delta$-correct *if* $E[\max_{m\in\mathcal{M}} \Pr[Dec(sk, c) \neq m : c \leftarrow Enc(pk, m)]] \leq \delta$, *where the expectation is taken over $(pk, sk) \leftarrow Gen$. We say a PKE is perfectly correct if $\delta = 0$.*

Note that this definition works for a deterministic or randomized PKE, but for a deterministic PKE[10] the term $\max_{m\in\mathcal{M}} \Pr[Dec(sk, c) \neq m : c = Enc(pk, m)]$ is either 0 or 1 for each keypair $(pk, sk)$.

**Definition A.3 (Injectivity of DPKE [6]).** *A deterministic PKE (DPKE) is* $\varepsilon$-injective *if* $\Pr[Enc(pk, *) \text{ is not injective } : (pk, sk) \leftarrow Gen] \leq \varepsilon$.

*Remark 6.* we observe that if DPKE is $\delta$-correct, then DPKE is injective with probability $\geq 1 - \delta$. That is, for DPKE, $\delta$-correctness implies $\delta$-injectivity.

**Definition A.4 (OW-CPA-secure PKE).** *Let* $\mathrm{PKE} = (Gen, Enc, Dec)$ *be a public-key encryption scheme with message space $\mathcal{M}$. Define* $\mathrm{OW-CPA}$ *game of PKE as in Fig. 10. Define the* $\mathrm{OW-CPA}$ *advantage function of an adversary $\mathcal{A}$ against PKE as* $\mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(\mathcal{A}) := \Pr[\text{OW-CPA}^{\mathcal{A}}_{\text{PKE}} = 1]$.

[10] A PKE is determinstic if *Enc* is deterministic

| Game OW-CPA | Game IND-CPA |
| --- | --- |
| $(pk, sk) \leftarrow Gen, m^* \xleftarrow{\$} \mathcal{M}$ | $(pk, sk) \leftarrow Gen, b \leftarrow_\$ \{0, 1\}$ |
| $c^* \leftarrow Enc(pk, m^*), m' \leftarrow \mathcal{A}(pk, c^*)$ | $(m_0, m_1) \leftarrow \mathcal{A}(pk)$ |
| **return** $m' =?m^*$ | $c^* \leftarrow Enc(pk, m_b), b' \leftarrow \mathcal{A}(pk, c^*)$ |
| | **return** $b' =?b$ |

Fig. 10: Game OW-CPA and game IND-CPA for PKE.

**Definition A.5 (IND-CPA-secure PKE).** *Let* $\mathrm{PKE} = (Gen, Enc, Dec)$ *be a PKE scheme. Define* $\mathrm{IND-CPA}$ *game of PKE as in Fig. 10, where* $m_0$ *and* $m_1$ *have the same length. Define the* $\mathrm{IND-CPA}$ *advantage function of an adversary* $\mathcal{A}$ *against PKE as* $\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(\mathcal{A}) := |\Pr[\text{IND-CPA}^{\mathcal{A}}_{\text{PKE}} = 1] - 1/2|$.

**Malleability.** In this paper, we say a $\mathrm{PKE} = (Gen, Enc, Dec)$ has a malleability property if for any $(pk, sk)$ generated by $Gen$, any $m \in \mathcal{M}$, and $c \leftarrow Enc(pk, m)$, there exists an algorithm $B$ that on input $(pk, c)$ outputs $(f, c')$ such that (1) $f(m) = Dec(sk, c')$ $(Dec(sk, c') \neq \perp)$ (2) $f(\tilde{m}) \neq Dec(sk, c')$ for any $\tilde{m} \in \mathcal{M}$ and $\tilde{m} \neq m$.

**Definition A.6 (Key encapsulation).** *A key encapsulation mechanism KEM consists of three algorithms. (1)* $Gen(1^\lambda) \rightarrow (pk, sk)$*: the key generation algorithm Gen outputs a key pair* $(pk, sk)$*. Usually, for brevity, we will omit the input of Gen. (2)* $Encaps(pk) \rightarrow (K, c)$*: the encapsulation algorithm Encaps, on input pk, outputs a tuple* $(K, c)$*, where* $K \in \mathcal{K}$ *and ciphertext c is said to be an encapsulation of the key* $K$*. (3)* $Decaps(sk, c) \rightarrow K$*: the deterministic decapsulation algorithm Decaps, on input sk and an encapsulation c, outputs either a key* $K := Decaps(sk, c) \in \mathcal{K}$ *or a rejection symbol* $\perp \notin \mathcal{K}$*.*

**Definition A.7 (IND-CCA-secure KEM).** *We define the* $\mathrm{IND-CCA}$ *game as in Fig. 11 and the advantage function of an adversary* $\mathcal{A}$ *against* KEM *as* $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}}(\mathcal{A}) := \left|\Pr[\text{IND-CCA}^{\mathcal{A}}_{\text{KEM}} = 1] - 1/2\right|$.

| Game IND-CCA | $\textsc{Decaps}(sk, c)$ |
| --- | --- |
| $(pk, sk) \leftarrow Gen, b \xleftarrow{\$} \{0, 1\}$ | **if** $c = c^*$ **return** $\perp$ |
| $(K_0^*, c^*) \leftarrow Encaps(pk), K_1^* \xleftarrow{\$} \mathcal{K}$ | **else return** |
| $b' \leftarrow \mathcal{A}^{\textsc{Decaps}}(pk, c^*, K_b^*)$ | $\quad K := Decaps(sk, c)$ |
| **return** $b' =?b$ | |

Fig. 11: IND-CCA game for KEM.

## B Supporting Material: Learning with Error (LWE)

**Definition B.1.** *Let* $n, m, q$ *be positive integers, and let* $\chi$ *be a distribution over* $\mathbb{Z}$*. The (decision) LWE problem is to distinguish between the distributions* $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}(\mathrm{mod} q))$ *and* $(\mathbf{A}, \mathbf{u})$*, where* $\mathbf{A} \leftarrow_\$ \mathbb{Z}_q^{n \times m}$*,* $\mathbf{s} \leftarrow_\$ \mathbb{Z}_q^n$*,* $\mathbf{e} \leftarrow \chi^m$*,* $\mathbf{u} \leftarrow_\$ \mathbb{Z}_q^m$*.*

In this paper, we refer the LWE assumption to that no quantum polynomial-time algorithm can solve the LWE problem with more than a negligible advantage.

## C Supporting Material: Proof of Quantum access to Random Oracle (PoQRO)

**Definition C.1 ([40]).** *A (non-interactive) proof of quantum access to a random oracle (PoQRO) consists of the following three algorithms. (1) Setup*$(1^\lambda)$*: This is a classical algorithm that takes the security parameter* $1^\lambda$ *as input and outputs a public key pk and a secret key sk. (2)* $Prove^{|H\rangle}(pk)$*: This is a quantum algorithm that takes a public key pk as input and given quantum access to a random oracle* $H$*, and outputs a proof* $\pi$[11]*. (3)* $Verify^H(sk, \pi)$*: This is a classical algorithm that takes a secret key sk and a proof* $\pi$ *as input and given classical access to a random oracle* $H$*, and outputs 1 indicating acceptance or 0 indicating rejection. PoQRO is required to satisfy the following properties.*
***Correctness.*** *We have* $\Pr[Verify^H(sk, \pi) = 0 : (pk, sk) \leftarrow Setep(1^\lambda), \pi \leftarrow Prove^{|H\rangle}(pk)] \leq \mathsf{negl}(\lambda)$.
***Soundness.*** *For any quantum polynomial-time adversary* $\mathcal{A}$ *that is given a classical oracle access to* $H$*, we have* $\Pr[Verify^H(sk, \pi) = 1 : Setep(1^\lambda), \pi \leftarrow \mathcal{A}^H(pk)] \leq \mathsf{negl}(\lambda)$.

**Lemma C.1 ([40, Theorem 3.3]).** *If the LWE assumption holds, then there exists a PoQRO.*

## References


1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019. LNCS, vol. 11693, pp. 269–295. Springer (2019), `https://doi.org/10.1007/978-3-030-26951-7\_10`
2. Angel, Y., Dowling, B., Hülsing, A., Schwabe, P., Weber, F.: Post quantum noise. In: ACM CCS 2022 (to appear) (2022), `https://eprint.iacr.org/2022/539`
3. Azouaoui, M., Bronchain, O., Hoffmann, C., Kuzovkova, Y., Schneider, T., Standaert, F.: Systematic study of decryption and re-encryption leakage: The case of kyber. In: Balasch, J., O'Flynn, C. (eds.) Constructive Side-Channel Analysis and Secure Design - 13th International Workshop, COSADE 2022. LNCS, vol. 13211, pp. 236–256. Springer (2022), `https://doi.org/10.1007/978-3-030-99766-3\_11`
4. Balli, F., Rösler, P., Vaudenay, S.: Determining the core primitive for optimally secure ratcheting. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020. LNCS, vol. 12493, pp. 621–650. Springer (2020), `https://doi.org/10.1007/978-3-030-64840-4\_21`
5. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 1993. pp. 62–73. ACM (1993)


[11] Here, $\pi$ is a classical value, and not a quantum state.

6. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography - 17th International Conference, TCC 2019. LNCS, vol. 11892, pp. 61–90. Springer (2019), https://doi.org/10.1007/978-3-030-36033-7_3
7. Boneh, D., Dagdelen, O., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology – ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer (2011)
8. Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In: EuroS&P 2018. pp. 353–367. IEEE (2018), https://doi.org/10.1109/EuroSP.2018.00032
9. Brendel, J., Fiedler, R., Günther, F., Janson, C., Stebila, D.: Post-quantum asynchronous deniable key exchange and the signal handshake. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) Public-Key Cryptography - PKC 2022. LNCS, vol. 13178, pp. 3–34. Springer (2022), https://doi.org/10.1007/978-3-030-97131-1_1
10. Brendel, J., Fischlin, M., Günther, F., Janson, C.: PRF-ODH: relations, instantiations, and impossibility results. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017. LNCS, vol. 10403, pp. 651–681. Springer (2017), https://doi.org/10.1007/978-3-319-63697-9_22
11. Dent, A.W.: A designer's guide to kems. In: Paterson, K.G. (ed.) Cryptography and Coding, 9th IMA International Conference. LNCS, vol. 2898, pp. 133–151. Springer (2003), https://doi.org/10.1007/978-3-540-40974-8_12
12. Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020. LNCS, vol. 12172, pp. 602–631. Springer (2020), https://doi.org/10.1007/978-3-030-56877-1_21
13. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019. LNCS, vol. 11693, pp. 356–383. Springer (2019), https://doi.org/10.1007/978-3-030-26951-7_13
14. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-extractability in the quantum random-oracle model. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022. LNCS, vol. 13277, pp. 677–706. Springer (2022), https://doi.org/10.1007/978-3-031-07082-2_24
15. Dowling, B., Fischlin, M., Günther, F., Stebila, D.: A cryptographic analysis of the TLS 1.3 handshake protocol. J. Cryptol. **34**(4), 37 (2021), https://doi.org/10.1007/s00145-021-09384-1
16. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) Advances in Cryptology – CRYPTO 1999. LNCS, vol. 99, pp. 537–554. Springer (1999)
17. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) Theory of Cryptography - 15th International Conference – TCC 2017. LNCS, vol. 10677, pp. 341–371. Springer (2017)
18. Hövelmanns, K., Hülsing, A., Majenz, C.: Failing gracefully: Decryption failures and the fujisaki-okamoto transform. In: Advances in Cryptology - ASIACRYPT 2022. Springer-Verlag (2022)

19. Hövelmanns, K., Kiltz, E., Schäge, S., Unruh, D.: Generic authenticated key exchange in the quantum random oracle model. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography - PKC 2020. LNCS, vol. 12111, pp. 389–422. Springer (2020), https://doi.org/10.1007/978-3-030-45388-6_14
20. Huguenin-Dumittan, L., Vaudenay, S.: On IND-qCCA security in the ROM and its applications - CPA security is sufficient for TLS 1.3. Cryptology ePrint Archive, Report 2021/844 (2022-12-16 version) (2021), https://eprint.iacr.org/2021/844.pdf
21. Huguenin-Dumittan, L., Vaudenay, S.: On IND-qCCA security in the ROM and its applications - CPA security is sufficient for TLS 1.3. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022. LNCS, vol. 13277, pp. 613–642. Springer (2022), https://doi.org/10.1007/978-3-031-07082-2_22
22. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018. LNCS, vol. 10993, pp. 96–125 (2018)
23. Jiang, H., Zhang, Z., Ma, Z.: Key encapsulation mechanism with explicit rejection in the quantum random oracle model. In: Lin, D., Sako, K. (eds.) Public-Key Cryptography - PKC 2019. LNCS, vol. 11443, pp. 618–645. Springer (2019), https://doi.org/10.1007/978-3-030-17259-6_21
24. Jiang, H., Zhang, Z., Ma, Z.: Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model. In: Ding, J., Steinwandt, R. (eds.) Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019. LNCS, vol. 11505, pp. 227–248. Springer (2019), https://doi.org/10.1007/978-3-030-25510-7_13
25. Jost, D., Maurer, U., Mularczyk, M.: Efficient ratcheting: Almost-optimal guarantees for secure messaging. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019. LNCS, vol. 11476, pp. 159–188. Springer (2019), https://doi.org/10.1007/978-3-030-17653-2_6
26. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.: Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020. LNCS, vol. 12107, pp. 703–728. Springer (2020), https://doi.org/10.1007/978-3-030-45727-3_24
27. Melissa Azouaoui, Joppe W. Bos, B.F.M.G.Y.K.J.R.T.S.C.v.V.O.B.C.H.F.X.S.: Surviving the fo-calypse: Securing pqc implementations in practice. RWC 2022 (2022), https://iacr.org/submit/files/slides/2022/rwc/rwc2022/48/slides.pdf
28. Naehrig, M. and Alkim, E. and Bos, J. and Ducas, L. and Easterbrook, K. and LaMacchia, B. and Longa, P. and Mironov, I. and Nikolaenko, V. and Peikert, C. and Raghunathan, A. and Stebila, D.: FrodoKEM Learning With Errors Key Encapsulatio. https://frodokem.org/files/FrodoKEM-specification-20210604.pdf
29. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. No. 2, Cambridge University Press (2000)
30. NIST: National institute for standards and technology. Post quantum crypto project (2017), https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

31. OQS: Open-quantum-safe OpenSSL (2021), https://github.com/open-quantum-safe/openssl
32. Poettering, B., Rösler, P.: Towards bidirectional ratcheted key exchange. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology - CRYPTO 2018. LNCS, vol. 10991, pp. 3–32. Springer (2018), https://doi.org/10.1007/978-3-319-96884-1_1
33. Qin, Y., Cheng, C., Zhang, X., Pan, Y., Hu, L., Ding, J.: A systematic approach and analysis of key mismatch attacks on lattice-based NIST candidate kems. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. LNCS, vol. 13093, pp. 92–121. Springer (2021), https://doi.org/10.1007/978-3-030-92068-5_4
34. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) Proceedings of the 37th Annual ACM Symposium on Theory of Computing. pp. 84–93. ACM (2005), https://doi.org/10.1145/1060590.1060603
35. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. LNCS, vol. 10822, pp. 520–551 (2018)
36. Schneider, T.: Implicit rejection in kyber. NIST pqc-forum (2022), https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3e210b6f-08d3-48f3-9689-1d048f9b3c58n\%40list.nist.gov
37. Schwabe, P., Stebila, D., Wiggers, T.: Post-quantum TLS without handshake signatures. In: Ligatti, J., Ou, X., Katz, J., Vigna, G. (eds.) ACM CCS 2020. pp. 1461–1480. ACM (2020), https://doi.org/10.1145/3372297.3423350
38. Schwabe, P., Stebila, D., Wiggers, T.: More efficient post-quantum KEMTLS with pre-distributed public keys. In: Bertino, E., Shulman, H., Waidner, M. (eds.) Computer Security - ESORICS 2021. LNCS, vol. 12972, pp. 3–22. Springer (2021), https://doi.org/10.1007/978-3-030-88418-5_1
39. Ueno, R., Xagawa, K., Tanaka, Y., Ito, A., Takahashi, J., Homma, N.: Curse of re-encryption: A generic power/em analysis on post-quantum kems. IACR Transactions on Cryptographic Hardware and Embedded Systems **2022**(1), 296C322 (Nov 2021), https://tches.iacr.org/index.php/TCHES/article/view/9298, artifact available at https://artifacts.iacr.org/tches/2022/a7,
40. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021. LNCS, vol. 12697, pp. 568–597. Springer (2021), https://doi.org/10.1007/978-3-030-77886-6_20
41. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology - CRYPTO 2012. LNCS
42. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019. LNCS, vol. 11693, pp. 239–268. Springer (2019), https://doi.org/10.1007/978-3-030-26951-7_9