(Tightly) QCCA-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model

Keita Xagawa and Takashi Yamakawa

October 19, 2018
NTT Secure Platform Laboratories
3-9-11, Midori-cho uMsashino-shi, Tokyo 180-8585 Japan
{xagawa.keita, yamakawa.takashi}@lab.ntt.co.jp

Abstract. This paper shows the security against *quantum* chosen-ciphertext attacks (QCCA security) of the KEM in Saito, Yamakawa, and Xagawa (EUROCRYPT 2018) in the QROM. The proof is very similar to that for the CCA security in the QROM, easy to understand, and as tight as the original proof.
keywords: Tight security, quantum chosen-ciphertext security, post-quantum cryptography, KEM.

1 Introduction

Quantum Superposition Attacks: Quantum superposition attacks are worth being considered (if we can mount them in the future). Theoretically speaking, we already know quantum superposition attacks that break classically-secure cryptographic primitives: Kuwakado and Morii [KM12] presented a quantum chosen-plaintext attack against the Even-Monsour construction of a block cipher if the inner permutation is publicly available as quantum oracle, which employed Simon's algorithm neatly. Kaplan, Leurent, Leverrier, and Naya-Plasencia [KLLNP16] also studied quantum superposition attacks against several block ciphers and modes. (On the other hand, Anand, Targhi, Tabia, and Unruh [ATTU16] showed some modes are secure if the underlying block cipher is quantumly-secure PRF.) Boneh and Zhandry [BZ13] also gave an example of a block cipher that is secure against chosen-plaintext-and-ciphertext attacks but vulnerable against quantum chosen-ciphertext attacks.

Security of PKE/KEM against Quantum Chosen-Ciphertext Attacks: Boneh and Zhandry [BZ13] introduced the quantum-chosen-ciphertext (QCCA) security for public-key encryption (PKE), which is security against adversaries that make decryption queries in quantum superpositions.

Boneh and Zhandry [BZ13] showed that a PKE scheme obtained by applying the Canetti-Halevi-Katz conversion [BCHK07] to an ID-based encryption (IBE) scheme and one-time signature is IND-QCCA-secure if the underlying IBE scheme is selectively-secure against quantum chosen-ID queries and the underlying one-time signature scheme is (classically) strongly, existentially unforgeable against chosen-message attacks. They also showed that if there exists an IND-CCA-secure PKE, then there exists an ill-formed PKE that is IND-CCA-secure but not IND-QCCA-secure [BZ13].

As far as we know, this is the only known PKE scheme that is proven to be IND-QCCA secure (excluding the concurrent work by Zhandry [Zha18, 2018-08-14 ver.]).

1.1 Our Contribution

We show that a key encapsulation mechanism (KEM) in Saito, Xagawa, and Yamakawa [SXY18] is also IND-QCCA-secure in the quantum random oracle model (QROM) if the underlying deterministic PKE is perfectly correct and disjoint-simulatable.

Our idea is very simple: At the last step in the security proof of the IND-CCA security, the challenger should simulate the decapsulation oracle on a query of any ciphertext c except the challenge ciphertext c^*. Roughly speaking, we observe that, if this simulation is "history-free," i.e., if the simulation does not depend on previously made queries at all, this procedure can be quantumly simulated by implementing this procedure in the quantum way. For example, in the last step of the game hopping in [SXY18], the decapsulation oracle on input c returns $K = \mathsf{H}_q(c)$ if $c \neq c^*$, where H_1 is a random function chosen by the reduction algorithm. We observe this procedure is "history-free" and can be implemented quantumly. [1]

[1] Boneh et al. [BDF+11] defined the history-free property of reduction for signature scheme, but they gave no definition of the history-free property of reduction for encryption schemes.

1.2 Concurrent Works

Zhandry [Zha18, 2018-08-14 ver.] showed that the PKE scheme obtained by applying the Fujisaki-Okamoto conversion [FO13] to a PKE scheme PKE and a DEM scheme DEM is IND-qCCA-secure in the QROM, if PKE is OW-CPA-secure and well-spread, DEM is OT-secure [2]. Zhandry proposed recording and testing techniques to simulate the decryption oracles. We note that his security proof is non-tight unlike ours.

2 Preliminaries

2.1 Notation

A security parameter is denoted by κ. We use the standard O-notations: O, Θ, Ω, and ω. DPT and PPT stand for deterministic polynomial time and probabilistic polynomial time. A function $f(\kappa)$ is said to be *negligible* if $f(\kappa) = \kappa^{-\omega(1)}$. We denote a set of negligible functions by $\mathsf{negl}(\kappa)$. For two finite sets $\mathcal{X}$ and $\mathcal{Y}$, $\mathrm{Map}(\mathcal{X}, \mathcal{Y})$ denote a set of all functions whose domain is $\mathcal{X}$ and codomain is $\mathcal{Y}$.

For a distribution χ, we often write "$x \leftarrow \chi$," which indicates that we take a sample x from χ. For a finite set S, $U(S)$ denotes the uniform distribution over S. We often write "$x \leftarrow S$" instead of "$x \leftarrow U(S)$." For a set S and a deterministic algorithm A, $\mathsf{A}(S)$ denotes the set $\{\mathsf{A}(x) \mid x \in S\}$.

If inp is a string, then "$\mathsf{out} \leftarrow \mathsf{A}(\mathsf{inp})$" denotes the output of algorithm A when run on input inp. If A is deterministic, then out is a fixed value and we write "$\mathsf{out} := \mathsf{A}(\mathsf{inp})$." We also use the notation "$\mathsf{out} := \mathsf{A}(\mathsf{inp}; r)$" to make the randomness r explicit.

For the Boolean statement P, $\mathrm{boole}(P)$ denotes the bit that is 1 if P is true, and 0 otherwise. For example, $\mathrm{boole}(b' \stackrel{?}{=} b)$ is 1 if and only if $b' = b$.

2.2 Quantum Computation

We refer to [NC00] for basic of quantum computation.

Quantum Random Oracle Model. Roughly speaking, the quantum random oracle model (QROM) is an idealized model where a hash function is modeled as a publicly and quantumly accessible random oracle. See [BDF+11] for a more detailed description of the model.

Lemma. We review useful lemmas regarding the quantum oracles.

Lemma 2.1. *Let ℓ be an integer. Let $\mathsf{H}\colon \{0,1\}^\ell \times \mathcal{X} \to \mathcal{Y}$ and $\mathsf{H}'\colon \mathcal{X} \to \mathcal{Y}$ be two independent random oracles. If an unbounded time quantum adversary $\mathcal{A}$ makes a query to H at most q_H times, then we have*

$$\left|\Pr[\mathcal{A}^{\mathsf{H},\mathsf{H}(s,\cdot)}() \to 1 \mid s \leftarrow \{0,1\}^\ell] - \Pr[\mathcal{A}^{\mathsf{H},\mathsf{H}'}() \to 1]\right| \leq q_\mathsf{H} \cdot 2^{\frac{-\ell+1}{2}}$$

where all oracle accesses of $\mathcal{A}$ can be quantum.

Though this seems to be a folklore, Saito et al. [SXY18] and Jiang et al. [JZC+18] gave the proof.

The second one is the hardness of generic search problem. If the oracle F rarely returns 1, then it is hard to distinguish F from the zero oracle N.

Lemma 2.2 (Generic Search Problem ([ARU14, Lemma 37], [HRS16, Thm.1], [JZC+18])). *Let $\gamma \in [0,1]$. Let $\mathcal{Z}$ be a finite set. Let $F\colon \mathcal{Z} \to \{0,1\}$ be the following function: For each z, $F(z) = 1$ with probability p_z at most γ and $F(z) = 0$ else. Let N be the zero function, that is, $N(z) = 0$ for any $z \in \mathcal{Z}$. If an oracle algorithm $\mathcal{A}$ makes at most Q quantum queries to F (or N), then*

$$\left|\Pr[\mathcal{A}^F() \to 1] - \Pr[\mathcal{A}^N() \to 1]\right| \leq 2q\sqrt{\gamma}.$$

Particularly, the probability that $\mathcal{A}$ finds a z satisfying $F(z) = 1$ is at most $2q\sqrt{\gamma}$.

[2] any efficient adversary cannot distinguish $E(k, m_0)$ from $E(k, m_1)$ even if it chooses m_0 and m_1 with $|m_0| = |m_1|$.

Simulation of Random Oracle. In the original quantum random oracle model introduced by Boneh et al. [BDF+11], they do not allow a reduction algorithm to access a random oracle, so it has to simulate a random oracle by itself. In contrast, in this paper, we give a random oracle access to a reduction algorithm. We remark that this is just a convention and not a modification of the model since we can simulate a random oracle against quantum adversaries in several ways; 1) $2q$-wise independent hash function [Zha12], 2) quantumly-secure PRF [BDF+11], and 3) hash function modeled as quantum random oracle [KLS18]. In addition, Zhandry proposed a new technique to simulate the quantum random oracle, the compressed oracle technique [Zha18]. His new simulation of the quantum random oracle is perfect even for *unbounded* number of queries. In what follows, we use t_{RO} to denote a time needed to simulate a quantum random oracle.

3 Definitions

3.1 Public-Key Encryption

The model for PKE schemes is summarized as follows:

Definition 3.1. *A PKE scheme* PKE *consists of the following triple of polynomial-time algorithms* (Gen, Enc, Dec).

- $\mathsf{Gen}(1^\kappa; r_g) \to (ek, dk)$*: a key-generation algorithm that on input* 1^κ*, where* κ *is the security parameter, outputs a pair of keys* (ek, dk)*.* ek *and* dk *are called the encryption key and decryption key, respectively.*
- $\mathsf{Enc}(ek, m; r_e) \to c$*: an encryption algorithm that takes as input encryption key* ek *and message* $m \in \mathcal{M}$ *and outputs ciphertext* $c \in C$*.*
- $\mathsf{Dec}(dk, c) \to m/\bot$*: a decryption algorithm that takes as input decryption key* dk *and ciphertext* c *and outputs message* $m \in \mathcal{M}$ *or a rejection symbol* $\bot \notin \mathcal{M}$*.*

Definition 3.2. *We say a PKE scheme* PKE *is deterministic if* Enc *is deterministic. DPKE stands for deterministic public key encryption.*

Definition 3.3 (Correctness). *We say* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has* perfect correctness *if for any* (ek, dk) *generated by* Gen *and for any* $m \in \mathcal{M}$ *,we have that*

$$\Pr[\mathsf{Dec}(dk, c) = m \mid c \leftarrow \mathsf{Enc}(ek, m)] = 1.$$

We also review δ correctness in HHK17.

Definition 3.4 (δ-Correctness). *Let* $\delta = \delta(\kappa)$*. We say that* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* δ-correct *if*

$$\mathrm{Ex}_{(ek,dk)\leftarrow \mathsf{Gen}(1^\kappa)}\left[\max_{m\in\mathcal{M}} \Pr[\mathsf{Dec}(dk, c) = m \mid c \leftarrow \mathsf{Enc}(ek, m)]\right] \leq \delta(\kappa).$$

In particular, we just say perfeclty correct if $\delta = 0$*.*

We say that a key pair (ek, dk) is accurate if $\Pr[\mathsf{Dec}(dk, c) = m \mid c \leftarrow \mathsf{Enc}(ek, m)] = 1$ for any $m \in \mathcal{M}$.

Remark 3.1. We observe that if PKE is deterministic, then δ-correctness implies that

$$\mathrm{Ex}_{(ek,dk)\leftarrow \mathsf{Gen}(1^\kappa)}[ek \text{ is inaccurate}] \leq \delta(\kappa).$$

In other words, if PKE is deterministic and δ-correct, then a key pair is accurate with probability $\geq 1 - \delta$. We finally stress that, if PKE is deterministic but derandomized by the random oracle, then we cannot apply the above argument.

Security Notions: We define onewayness under chosen-plaintext attacks (OW-CPA), indistinguishability under chosen-plaintext attacks (IND-CPA), and indistinguishability under chosen-ciphertext attacks (IND-CCA) for a PKE.

$\mathsf{Expt}^{\text{ow-cpa}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{A}}(\kappa)$	$\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$	$\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$	$\textsc{Dec}_a(c)$
$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$b \leftarrow \{0,1\}$	$b \leftarrow \{0,1\}$	if $c = a$, return $\bot$
$m^* \leftarrow \mathcal{D}_\mathcal{M}$	$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$m := \mathsf{Dec}(dk, c)$
$c^* \leftarrow \mathsf{Enc}(ek, m^*)$	$(m_0, m_1, st) \leftarrow \mathcal{A}_1(ek)$	$(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\textsc{Dec}_\bot(\cdot)}(ek)$	**return** m
$m' \leftarrow \mathcal{A}(ek, c^*)$	$c^* \leftarrow \mathsf{Enc}(ek, m_b)$	$c^* \leftarrow \mathsf{Enc}(ek, m_b)$	
return $\mathsf{boole}(m' \stackrel{?}{=} \mathsf{Dec}(dk, c^*))$	$b' \leftarrow \mathcal{A}_2(c^*, st)$	$b' \leftarrow \mathcal{A}_2^{\textsc{Dec}_{c^*}(\cdot)}(c^*, st)$	
	return $\mathsf{boole}(b' \stackrel{?}{=} b)$	**return** $\mathsf{boole}(b' \stackrel{?}{=} b)$	

Fig. 1: Games for PKE schemes

Definition 3.5 (Security notions for PKE). *Let $\mathcal{D}_\mathcal{M}$ be a distribution over the message space $\mathcal{M}$. For any adversary $\mathcal{A}$, we define its* OW-CPA, IND-CPA, *and* IND-CCA *advantages against a PKE scheme* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *as follows:*

$$\begin{aligned} \mathsf{Adv}^{\text{ow-cpa}}_{\mathcal{A},\mathcal{D}_\mathcal{M},\mathsf{PKE}}(\kappa) &:= \Pr[\mathsf{Expt}^{\text{ow-cpa}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{A}}(\kappa) = 1], \\ \mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{A}}(\kappa) &:= \left|\Pr[\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{A}}(\kappa) = 1] - 1/2\right|, \\ \mathsf{Adv}^{\text{ind-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa) &:= \left|\Pr[\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa) = 1] - 1/2\right|, \end{aligned}$$

where $\mathsf{Expt}^{\text{ow-cpa}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{A}}(\kappa)$, $\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$, *and* $\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$ *are experiments described in Figure 1. For* GOAL-ATK $\in$ {OW-CPA, IND-CPA, IND-CCA}, *we say that* PKE *is* GOAL-ATK*-secure if* $\mathsf{Adv}^{\text{goal-atk}}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ *is negligible for any PPT adversary $\mathcal{A}$. We omit $\mathcal{D}_\mathcal{M}$ from* OW-CPA *security if $\mathcal{D}_\mathcal{M}$ is the uniform distribution over $\mathcal{M}$.*

Disjoint Simulatability Saito et al. defined *disjoint simulatability* of DPKE [SXY18]. Intuitively speaking, a DPKE scheme is disjoint simulatable if there exists a simulator that is only given a public key and generates a "fake ciphertext" that is indistinguishable from a real ciphertext of a random message. Moreover, we require that a fake ciphertext falls in a valid ciphertext space with negligible probability. The formal definition is as follows.

Definition 3.6 (Disjoint simulatability [SXY18]). *Let $\mathcal{D}_\mathcal{M}$ denote an efficiently sampleable distribution on a set $\mathcal{M}$. A deterministic PKE scheme* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with plaintext and ciphertext spaces $\mathcal{M}$ and $\mathcal{C}$ is $\mathcal{D}_\mathcal{M}$-*disjoint simulatable *if there exists a PPT algorithm $\mathcal{S}$ that satisfies the following.*

– *(Statistical disjointness:)*

$$\mathsf{Disj}_{\mathsf{PKE},\mathcal{S}}(\kappa) := \max_{(ek,dk)\in\mathsf{Gen}(1^\kappa;\mathcal{R})} \Pr[c \in \mathsf{Enc}(ek, \mathcal{M}) \mid c \leftarrow \mathcal{S}(ek)]$$

is negligible, where $\mathcal{R}$ denotes a randomness space for Gen.

– *(Ciphertext-indistinguishability:) For any PPT adversary $\mathcal{A}$,*

$$\mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE},\mathcal{D}_\mathcal{M},\mathcal{A},\mathcal{S}}(\kappa) := \left| \begin{array}{l} \Pr\left[\mathcal{A}(ek, c^*) \to 1 \,\middle|\, \begin{array}{c} (ek, dk) \leftarrow \mathsf{Gen}(1^\kappa); m^* \leftarrow \mathcal{D}_\mathcal{M}; \\ c^* := \mathsf{Enc}(ek, m^*) \end{array} \right] \\ - \Pr\left[\mathcal{A}(ek, c^*) \to 1 \mid (ek, dk) \leftarrow \mathsf{Gen}(1^\kappa); c^* \leftarrow \mathcal{S}(ek)\right] \end{array} \right|$$

is negligible.

IND-QCCA In [BZ13], Boneh and Zhandry showed that we cannot quantumize the challenge oracle; They showed that indistinguishability against fully-quantum chosen-plaintext attack (IND-fqCPA) and indistinguishability against fully-quantum chosen-left-right-plaintext attack (IND-fqlrCPA) is impossible. (For the details, see their paper.) Thus, we do not quantumize the challenge oracle, but quantumize decryption oracle.

We will need to define the result of $m \oplus \bot$, where $\bot \notin \mathcal{M}$. In order to do so, we encode $\bot$ as a bit string not in the message space.

$$
\begin{array}{ll}
\underline{\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{PKE},\mathcal{A}}(\kappa)} & \underline{\text{QDEC}_a(\sum_{c,z}\phi_{c,z}\,|c,z\rangle)} \\
b \leftarrow \{0,1\} & \textbf{return } \sum_{c,z}\phi_{c,z}\,|c, z \oplus f_a(c)\rangle \\
(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa) & \\
(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\text{QDEC}_\perp(\cdot)}(ek) & \underline{f_a(c)} \\
c^* \leftarrow \mathsf{Enc}(ek, m_b) & m := \mathsf{Dec}(dk, c) \\
b' \leftarrow \mathcal{A}_2^{\text{QDEC}_{c^*}(\cdot)}(c^*, st) & \text{if } c = a, \text{ set } m := \perp \\
\textbf{return } \mathsf{boole}(b' \stackrel{?}{=} b) & \textbf{return } m
\end{array}
$$

Fig. 2: More Games for PKE schemes

Definition 3.7 (IND-QCCA for PKE [BZ13]). *For any adversary $\mathcal{A}$, we define its* IND-QCCA *advantages against a PKE scheme* PKE = (Gen, Enc, Dec) *as follows:*

$$\mathsf{Adv}^{\text{ind-qcca}}_{\mathsf{PKE},\mathcal{A}}(\kappa) := \left|\Pr[\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{PKE},\mathcal{A}}(\kappa) = 1] - 1/2\right|,$$

where $\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$ is an experiment described in Figure 2. We say that PKE *is* IND-QCCA*-secure if $\mathsf{Adv}^{\text{ind-qcca}}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ is negligible for any PPT adversary $\mathcal{A}$.*

3.2 Key Encapsulation

The model for KEM schemes is summarized as follows:

Definition 3.8. *A KEM scheme* KEM *consists of the following triple of polynomial-time algorithms* (Gen, Encaps, Decaps)*:*

- $\mathsf{Gen}(1^\kappa; r_g) \to (ek, dk)$*: a key-generation algorithm that on input 1^κ, where κ is the security parameter, outputs a pair of keys (ek, dk). ek and dk are called the encapsulation key and decapsulation key, respectively.*
- $\mathsf{Encaps}(ek; r_e) \to (c, K)$*: an encapsulation algorithm that takes as input encapsulation key ek and outputs ciphertext $c \in C$ and key $K \in \mathcal{K}$.*
- $\mathsf{Decaps}(dk, c) \to K/\perp$*: a decapsulation algorithm that takes as input decapsulation key dk and ciphertext c and outputs key K or a rejection symbol $\perp \notin \mathcal{K}$.*

Definition 3.9 (Correctness). *We say* KEM = (Gen, Encaps, Decaps) *has* perfect correctness *if for any (ek, dk) generated by* Gen*, we have that*

$$\Pr[\mathsf{Decaps}(dk, c) = K : (c, K) \leftarrow \mathsf{Encaps}(ek)] = 1.$$

Security: We define indistinguishability under chosen-plaintext and chosen-ciphertext attacks (denoted by IND-CPA and IND-CCA) for KEM, respectively.

Definition 3.10. *For any adversary $\mathcal{A}$, we define its* IND-CPA *and* IND-CCA *advantages against a KEM scheme* KEM = (Gen, Encaps, Decaps) *as follows:*

$$\mathsf{Adv}^{\text{ind-cpa}}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \left|\Pr[\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1] - 1/2\right|,$$
$$\mathsf{Adv}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \left|\Pr[\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1] - 1/2\right|,$$

where $\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ and $\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ are experiments described in Figure 3.

For ATK ∈ {CPA, CCA}*, we say that* KEM *is* IND-ATK*-secure if $\mathsf{Adv}^{\text{ind-atk}}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ is negligible for any PPT adversary $\mathcal{A}$.*

$\mathsf{Expt}^{\text{ind-cpa}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$	$\mathsf{Expt}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$	$\textsc{Dec}_{c^*}(c)$
$b \leftarrow \{0,1\}$	$b \leftarrow \{0,1\}$	if $c = c^*$, return $\bot$
$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	$K := \mathsf{Decaps}(dk, c)$
$(c^*, K_0^*) \leftarrow \mathsf{Encaps}(ek)$;	$(c^*, K_0^*) \leftarrow \mathsf{Encaps}(ek)$;	**return** K
$K_1^* \leftarrow \mathcal{K}$	$K_1^* \leftarrow \mathcal{K}$	
$b' \leftarrow \mathcal{A}(ek, c^*, K_b^*)$	$b' \leftarrow \mathcal{A}^{\textsc{Dec}_{c^*}(\cdot)}(ek, c^*, K_b^*)$	
return $\mathsf{boole}(b' \stackrel{?}{=} b)$	**return** $\mathsf{boole}(b' \stackrel{?}{=} b)$	

Fig. 3: Games for KEM schemes

$\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$	$\textsc{qDec}_a(\sum_{c,z} \phi_{c,z} \lvert c, z\rangle)$
$b \leftarrow \{0,1\}$	**return** $\sum_{c,z} \phi_{c,z} \lvert c, z \oplus f_a(c)\rangle$
$(ek, dk) \leftarrow \mathsf{Gen}(1^\kappa)$	
$(c^*, K_0^*) \leftarrow \mathsf{Encaps}(ek)$;	$f_a(c)$
$K_1^* \leftarrow \mathcal{K}$	$K := \mathsf{Decaps}(dk, c)$
$b' \leftarrow \mathcal{A}^{\textsc{qDec}_{c^*}(\cdot)}(ek, c^*, K_b^*)$	if $c = a$, set $K := \bot$
return $\mathsf{boole}(b' \stackrel{?}{=} b)$	**return** K

Fig. 4: More Games for KEM schemes

IND-qCCA We also define indistinguishability under *quantum chosen-ciphertext attacks* (denoted by IND-qCCA) for KEM by follwoing [BZ13].

Definition 3.11 (IND-qCCA for KEM). *For any adversary $\mathcal{A}$, we define its* IND-qCCA *advantage against a KEM scheme* KEM = (Gen, Encaps, Decaps) *as follows:*

$$\mathsf{Adv}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \left|\Pr[\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1] - 1/2\right|,$$

where $\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ is an experiment described in Figure 4.

We say that KEM *is* IND-qCCA*-secure if $\mathsf{Adv}^{\text{ind-qcca}}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ is negligible for any PPT adversary $\mathcal{A}$.*

3.3 Data Encapsulation

The model for DEM schemes is summarized as follows:

Definition 3.12. *A DEM scheme* DEM *consists of the following triple of polynomial-time algorithms* (E, D) *with key space $\mathcal{K}$ and message space $\mathcal{M}$:*

- $\mathsf{E}(K, m) \rightarrow d$*: an encapsulation algorithm that takes as input key K and data m and outputs ciphertext d.*
- $\mathsf{D}(K, d) \rightarrow m/\bot$*: a decapsulation algorithm that takes as input key K and ciphertext c and outputs data m or a rejection symbol $\bot \notin \mathcal{M}$.*

Definition 3.13 (Correctness). *We say* DEM = (E, D) *has* perfect correctness *if for any $K \in \mathcal{K}$ and any $m \in \mathcal{M}$, we have that*

$$\Pr[\mathsf{D}(K, c) = m : d \leftarrow \mathsf{E}(K, m)] = 1.$$

Boneh and Zhandry [BZ13] defined the IND-qCCA security of DEM. They also showed that a combination of two quantumly-secure PRFs yields IND-qCCA-secure DEM. Thus, in the QROM, we easily have IND-qCCA-secure DEM using two quantum random oracles.

Soukharev, Jao, and Seshadri [SJS16] studied the Encrypt-then-Mac construction in quantum setting and showed that DEM = EtM[SKE, MAC] is IND-qCCA-secure if SKE is IND-qCPA-secure and MAC is SUF-qCMA-secure, which is left as open problem in Boneh and Zhandry [BZ13].

3.4 Hybrid Encryption

It is obvious that IND-qCCA-secure KEM and IND-qCCA-secure DEM yield IND-qCCA-secure PKE. That is, the proof of Cramer and Shoup [CS03] goes through even for the quantum setting. We omit the detail.

4 IND-qCCA Security of SXY

$\underline{\mathsf{Gen}(1^\kappa)}$	$\underline{\mathsf{Enc}(ek')}$	$\underline{\mathsf{Dec}(dk, c)}$, where $dk = (dk', ek', s)$
$(ek', dk') \leftarrow \mathsf{Gen}_1(1^\kappa)$	$m \leftarrow \mathcal{D}_\mathcal{M}$	$m := \mathsf{Dec}_1(dk', c)$
$s \leftarrow \{0,1\}^\ell$	$c := \mathsf{Enc}_1(ek', m)$	**if** $m = \bot$, **return** $K := \mathsf{H}'(s, c)$
$dk \leftarrow (dk', ek', s)$	$K := \mathsf{H}(m)$	**if** $c \neq \mathsf{Enc}_1(ek', m)$, **return** $K := \mathsf{H}'(s, c)$
return (ek', dk)	**return** (K, c)	**else return** $K := \mathsf{H}(m)$

Fig. 5: $\mathsf{KEM} := \mathsf{SXY}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$.

We show that $\mathsf{KEM} := \mathsf{SXY}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$ is IND-qCCA-secure if the underlying PKE_1 is a disjoint simulatable DPKE. Let $\mathsf{PKE}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ be a deterministic PKE scheme and let $\mathsf{H}\colon \mathcal{M} \to \mathcal{K}$ and $\mathsf{H}'\colon \{0,1\}^\ell \times \mathcal{C} \to \mathcal{K}$ be random oracles. We review the conversion SXY in Figure 5.

Theorem 4.1 (Security of SXY in the ROM (an adapted version of [HHK17, Theorem 3.6])). *Let PKE_1 be a perfectly correct DPKE scheme. For any IND-CCA adversary $\mathcal{A}$ against KEM issuing q_H and $q_{\mathsf{H}'}$ quantum random oracle queries to H and H' and $q_{\overline{\mathsf{Dec}}}$ decryption queries, there exists an OW-CPA adversary $\mathcal{B}$ against PKE_1, such that*

$$\mathsf{Adv}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) \leq \mathsf{Adv}^{\text{ow-cpa}}_{\mathsf{PKE}_1,\mathcal{B}}(\kappa) + q_{\mathsf{H}'} \cdot 2^{-\ell}$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q_\mathsf{H} \cdot \mathsf{Time}(\mathsf{Enc}_1) + (q_\mathsf{H} + q_{\mathsf{H}'} + q_{\overline{\mathsf{Dec}}}) \cdot t_{\mathsf{CRO}}$, where t_{CRO} is the running time to simulate the classical random oracle.

Theorem 4.2 (IND-CCA **Security of** SXY **in the QROM [SXY18]).** *Let PKE_1 be a perfectly correct DPKE scheme that satisfies the $\mathcal{D}_\mathcal{M}$-disjoint simulatability with a simulator $\mathcal{S}$. For any IND-CCA quantum adversary $\mathcal{A}$ against KEM issuing q_H and $q_{\mathsf{H}'}$ quantum random oracle queries to H and H' and $q_{\overline{\mathsf{Dec}}}$ decryption queries, there exists an adversary $\mathcal{B}$ against the disjoint simulatability of PKE_1 such that*

$$\mathsf{Adv}^{\text{ind-cca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) \leq \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1,\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{B}}(\kappa) + \mathsf{Disj}_{\mathsf{PKE}_1,\mathcal{S}}(\kappa) + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}}$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q_\mathsf{H} \cdot \mathsf{Time}(\mathsf{Enc}_1) + (q_\mathsf{H} + q_{\mathsf{H}'} + q_{\overline{\mathsf{Dec}}}) \cdot t_{\mathsf{RO}}$.

Theorem 4.3 (IND-qCCA **security of** SXY **in the QROM).** *Let PKE_1 be a δ-correct DPKE scheme that satisfies the $\mathcal{D}_\mathcal{M}$-disjoint simulatability with a simulator $\mathcal{S}$. For any IND-qCCA quantum adversary $\mathcal{A}$ against KEM issuing q_H and $q_{\mathsf{H}'}$ quantum random oracle queries to H and H' and $q_{\overline{\mathsf{Dec}}}$ decryption queries, there exists an adversary $\mathcal{B}$ against the disjoint simulatability of PKE_1 such that*

$$\mathsf{Adv}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) \leq \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1,\mathcal{D}_\mathcal{M},\mathcal{S},\mathcal{B}}(\kappa) + \mathsf{Disj}_{\mathsf{PKE}_1,\mathcal{S}}(\kappa) + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} + 2\delta$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q_\mathsf{H} \cdot \mathsf{Time}(\mathsf{Enc}_1) + (q_\mathsf{H} + q_{\mathsf{H}'} + q_{\overline{\mathsf{Dec}}}) \cdot t_{\mathsf{RO}}$.

We note that the proof of Theorem 4.3 is essentially equivalent to that of Theorem 4.2 except at the final game we require quantum simulation of decapsulation oracle.

Remark 4.1. We can relax the perfect correctness into the δ-correctness for some negligible $\delta = \delta(\kappa)$ even in the case of Theorem 4.2. Recall that if DPKE is δ-correct, then a key pair is accurate with probability $\geq 1 - \delta$. We can eliminate those inaccurate keys by introducing an additional game.

Table 1: Summary of Games for the Proof of Theorem 4.3

Game	H	c^*	K_0^*	K_1^*	Decryption of valid c	Decryption of invalid c	justification
Game_0	$\mathsf{H}(\cdot)$	$\mathsf{Enc}_1(ek', m^*)$	$\mathsf{H}(m^*)$	random	$\mathsf{H}(m)$	$\mathsf{H}'(s, c)$	
Game_1	$\mathsf{H}(\cdot)$	$\mathsf{Enc}_1(ek', m^*)$	$\mathsf{H}(m^*)$	random	$\mathsf{H}(m)$	$\mathsf{H}_q(c)$	Lemma 2.1
$\mathsf{Game}_{1.5}$	$\mathsf{H}'_q(\mathsf{Enc}_1(ek', \cdot))$	$\mathsf{Enc}_1(ek', m^*)$	$\mathsf{H}(m^*)$	random	$\mathsf{H}(m)$	$\mathsf{H}_q(c)$	Perfect correctness
Game_2	$\mathsf{H}_q(\mathsf{Enc}_1(ek', \cdot))$	$\mathsf{Enc}_1(ek', m^*)$	$\mathsf{H}(m^*)$	random	$\mathsf{H}(m)$	$\mathsf{H}_q(c)$	Conceptual
Game_3	$\mathsf{H}_q(\mathsf{Enc}_1(ek', \cdot))$	$\mathsf{Enc}_1(ek', m^*)$	$\mathsf{H}_q(c^*)$	random	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	Perfect correctness
Game_4	$\mathsf{H}_q(\mathsf{Enc}_1(ek', \cdot))$	$\mathcal{S}(ek')$	$\mathsf{H}_q(c^*)$	random	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	DS-IND

Security Proof. We use game-hopping proof. The overview of all games is given in Table 1.

Game_0*:* This is the original game, $\mathsf{Expt}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$.

Game_1*:* This game is the same as Game_0 except that $\mathsf{H}'(s, c)$ in the decryption oracle is replaced with $\mathsf{H}_q(c)$ where $\mathsf{H}_q : C \to \mathcal{K}$ is another random oracle. We remark that $\mathcal{A}$ is not given direct access to H_q.

$\mathsf{Game}_{1.5}$*:* This game is the same as Game_1 except that the random oracle $\mathsf{H}(\cdot)$ is simulated by $\mathsf{H}'_q(\mathsf{Enc}_1(ek, \cdot))$ where H'_q is yet another random oracle. We remark that a decryption oracle and generation of K_0^* also use $\mathsf{H}'_q(\mathsf{Enc}_1(ek, \cdot))$ as $\mathsf{H}(\cdot)$ and that $\mathcal{A}$ is not given direct access to H'_q.

Game_2*:* This game is the same as $\mathsf{Game}_{1.5}$ except that the random oracle $\mathsf{H}(\cdot)$ is simulated by $\mathsf{H}_q(\mathsf{Enc}_1(ek, \cdot))$ instead of $\mathsf{H}'_q(\mathsf{Enc}_1(ek, \cdot))$. We remark that the decryption oracle and generation of K_0^* also use $\mathsf{H}_q(\mathsf{Enc}_1(ek, \cdot))$ as $\mathsf{H}(\cdot)$.

Game_3*:* This game is the same as Game_2 except that K_0^* is set as $\mathsf{H}_q(c^*)$ and the decryption oracle always returns $\mathsf{H}_q(c)$ as long as $c \neq c^*$. We denote the modified decryption oracle by $\textsc{qDec}$'.

Game_4*:* This game is the same as Game_3 except that c^* is set as $\mathcal{S}(ek')$.

The above completes the descriptions of games. We clearly have

$$\mathsf{Adv}^{\text{ind-qcca}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = |\Pr[\mathsf{Game}_0 = 1] - 1/2|$$

by the definition. We upperbound this by the following lemmas.

Lemma 4.1. *We have*

$$|\Pr[\mathsf{Game}_0 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}}.$$

Proof. This is obvious from Lemma 2.1. □

Lemma 4.2. *Let* Acc *denote the event that the key pair* (ek', dk') *is accurate. We have*

$$|\Pr[\mathsf{Game}_1 = 1] - 1/2| \leq |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] - 1/2| + \delta.$$

Proof. By the definition, we have

$$\Pr[\overline{\mathsf{Acc}} \text{ happens in } \mathsf{Game}_1] \leq \delta.$$

We have

$$\begin{aligned}
|\Pr[\mathsf{Game}_1 = 1] - 1/2| &= \left|\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] + \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \overline{\mathsf{Acc}}] - 1/2\right| \\
&\leq \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \overline{\mathsf{Acc}}] + |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] - 1/2| \\
&\leq \Pr[\overline{\mathsf{Acc}}] + |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] - 1/2| \\
&\leq |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] - 1/2| + \delta
\end{aligned}$$

as we wanted.

Lemma 4.3. *We have*

$$\Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] = \Pr[\mathsf{Game}_{1.5} = 1 \mid \mathsf{Acc}].$$

Proof. Since we assume that the key pair (ek', dk') of PKE_1 is accurate, $\mathsf{Enc}_1(ek', \cdot)$ is injective. Therefore, if $\mathsf{H}'_q(\cdot)$ is a random function, then $\mathsf{H}'_q(\mathsf{Enc}_1(ek, \cdot))$ is also a random function. Remarking that access to H'_q is not given to $\mathcal{A}$, it causes no difference from the view of $\mathcal{A}$ if we replace $\mathsf{H}(\cdot)$ with $\mathsf{H}'_q(\mathsf{Enc}_1(ek, \cdot))$. □

Lemma 4.4. *We have*

$$\Pr[\mathsf{Game}_{1.5} = 1 \mid \mathsf{Acc}] = \Pr[\mathsf{Game}_2 = 1 \mid \mathsf{Acc}].$$

Proof. We call a ciphertext c valid if we have $\mathsf{Enc}_1(ek', \mathsf{Dec}_1(dk', c)) = c$ and invalid otherwise. We remark that H_q is used only for decrypting an invalid ciphertext c as $\mathsf{H}_q(c)$ in $\mathsf{Game}_{1.5}$. This means that a value of $\mathsf{H}_q(c)$ for a valid c is not used at all in $\mathsf{Game}_{1.5}$. On the other hand, any output of $\mathsf{Enc}_1(ek', \cdot)$ is valid due to the perfect correctness of PKE_1. Since H'_q is only used for evaluating an output of $\mathsf{Enc}(ek', \cdot)$, a value of $\mathsf{H}_q(c)$ for a valid c is not used at all in $\mathsf{Game}_{1.5}$. Hence, it causes no difference from the view of $\mathcal{A}$ if we use the same random oracle H_q instead of two independent random oracles H_q and H'_q. □

Lemma 4.5. *We have*

$$\Pr[\mathsf{Game}_2 = 1 \mid \mathsf{Acc}] = \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}].$$

Proof. Since we set $\mathsf{H}(\cdot) := \mathsf{H}_q(\mathsf{Enc}_1(ek', \cdot))$, for any valid c and $m := \mathsf{Dec}_1(dk', c)$, we have $\mathsf{H}(m) = \mathsf{H}_q(\mathsf{Enc}_1(ek', m)) = \mathsf{H}_q(c)$. Therefore, responses of the decryption oracle are unchanged. We also have $\mathsf{H}(m^*) = \mathsf{H}_q(c^*)$ for a similar reason. □

Lemma 4.6. *We have*

$$|\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}] - 1/2| \le |\Pr[\mathsf{Game}_3 = 1] - 1/2| + \delta.$$

Proof. We have

$$\begin{aligned}
|\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}] - 1/2| &\le \left| \begin{matrix} \Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}] + \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \overline{\mathsf{Acc}}] \\ - \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \overline{\mathsf{Acc}}] - 1/2 \end{matrix} \right| \\
&\le \left| \Pr[\mathsf{Game}_3 = 1] - \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \overline{\mathsf{Acc}}] - 1/2 \right| \\
&\le |\Pr[\mathsf{Game}_3 = 1] - 1/2| + \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \overline{\mathsf{Acc}}] \\
&\le |\Pr[\mathsf{Game}_3 = 1] - 1/2| + \Pr[\overline{\mathsf{Acc}}] \\
&\le |\Pr[\mathsf{Game}_3 = 1] - 1/2| + \delta.
\end{aligned}$$

In the third inequality, we invoke Lemma A.1 by setting $a = \Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}]$, $b = 1/2$ and $c = \Pr[\overline{\mathsf{Acc}}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \overline{\mathsf{Acc}}]$. □

Lemma 4.7. *There exists an adversary $\mathcal{B}$ such that*

$$|\Pr[\mathsf{Game}_3 = 1] - \Pr[\mathsf{Game}_4 = 1]| \le \mathrm{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1, \mathcal{D}_\mathcal{M}, \mathcal{S}, \mathcal{B}}(\kappa).$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q_\mathsf{H} \cdot \mathsf{Time}(\mathsf{Enc}_1) + (q_\mathsf{H} + q_{\mathsf{H}'} + q_{\overline{\mathsf{Dec}}}) \cdot t_\mathsf{RO}$.

Proof. We construct an adversary $\mathcal{B}$, which is allowed to access two random oracles H_q and H', against the disjoint simulatability as follows [3].

$\mathcal{B}^{\mathsf{H}_q, \mathsf{H}'}(ek', c^*)$: It picks $b \leftarrow \{0, 1\}$, sets $K_0^* := \mathsf{H}_q(c^*)$ and $K_1^* \leftarrow \mathcal{K}$, and invokes $b' \leftarrow \mathcal{A}^{\mathsf{H}, \mathsf{H}', \mathsf{qDec}'}(ek', c^*, K_b^*)$ where $\mathcal{A}$'s oracles are simulated as follows.

- $\mathsf{H}(\cdot)$ is simulated by $\mathsf{H}_q(\mathsf{Enc}_1(ek', \cdot))$.
- H' can be simulated because $\mathcal{B}$ has access to an oracle H'.

[3] We allow a reduction algorithm to access the random oracles. See subsection 2.2 for details.

– $\textsc{qDec}'(\cdot)$ is simulated by filtering c^* and forwarding to $\mathsf{H}_q(\cdot)$; that is, on input $\sum_{c,z} \phi_{c,z} |c, z\rangle$, $\mathcal{B}$ returns $\sum_{c \neq c^*, z} \phi_{c,z} |c, z \oplus \mathsf{H}_q(c)\rangle + \sum_z \phi_{c^*,z} |c^*, z \oplus \bot\rangle$.

Finally, $\mathcal{B}$ returns boole$(b \stackrel{?}{=} b')$.

This completes the description of $\mathcal{B}$. It is easy to see that $\mathcal{B}$ perfectly simulates Game_3 if $c^* = \mathsf{Enc}_1(ek, m^*)$ and Game_4 if $c^* = \mathcal{S}(ek')$. Therefore, we have

$$|\Pr[\mathsf{Game}_3 = 1] - \Pr[\mathsf{Game}_4 = 1]| \leq \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1, \mathcal{D}_\mathcal{M}, \mathcal{S}, \mathcal{B}}(\kappa)$$

as wanted. Since $\mathcal{B}$ invokes $\mathcal{A}$ once, H is simulated by one evaluation of Enc_1 plus one evaluation of a random oracle, and H' and $\textsc{qDec}'$ are simulated by one evaluation of random oracles, we have $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A}) + q_\mathsf{H} \cdot \mathsf{Time}(\mathsf{Enc}_1) + (q_\mathsf{H} + q_{\mathsf{H}'} + q_{\overline{\mathsf{Dec}}}) \cdot t_\mathsf{RO}$. □

Lemma 4.8. *We have*

$$|\Pr[\mathsf{Game}_4 = 1] - 1/2| \leq \mathsf{Disj}_{\mathsf{PKE}_1, \mathcal{S}}(\kappa).$$

Proof. Let Bad denote an event in which $c^* \in \mathsf{Enc}_1(ek', \mathcal{M})$ in Game_4. It is easy to see that we have

$$\Pr[\mathsf{Bad}] \leq \mathsf{Disj}_{\mathsf{PKE}_1, \mathcal{S}}(\kappa).$$

When Bad does not occur, i.e., $c^* \notin \mathsf{Enc}_1(ek', \mathcal{M})$, $\mathcal{A}$ obtains no information about $K_0^* = \mathsf{H}_q(c^*)$. This is because queries to H only reveal $\mathsf{H}_q(c)$ for $c \in \mathsf{Enc}_1(ek', \mathcal{M})$, and $\textsc{qDec}'(c)$ returns $\bot$ if $c = c^*$. Therefore, we have

$$\Pr[\mathsf{Game}_4 = 1 \mid \overline{\mathsf{Bad}}] = 1/2.$$

Combining the above, we have

$$\begin{aligned}
&|\Pr[\mathsf{Game}_4 = 1] - 1/2| \\
&= \left|\Pr[\mathsf{Bad}] \cdot (\Pr[\mathsf{Game}_4 = 1 \mid \mathsf{Bad}] - 1/2) + \Pr[\overline{\mathsf{Bad}}] \cdot (\Pr[\mathsf{Game}_4 = 1 \mid \overline{\mathsf{Bad}}] - 1/2)\right| \\
&\leq \Pr[\mathsf{Bad}] + \left|\Pr[\mathsf{Game}_4 = 1 \mid \overline{\mathsf{Bad}}] - 1/2\right| \\
&\leq \mathsf{Disj}_{\mathsf{PKE}_1, \mathcal{S}}(\kappa)
\end{aligned}$$

as we wanted. □

Proof (Proof of Theorem 4.3). Combining all lemmas in this section, we obtain the following inequality:

$$\begin{aligned}
\mathsf{Adv}^{\text{ind-qcca}}_{\mathsf{KEM}, \mathcal{A}}(\kappa) &= |\Pr[\mathsf{Game}_0 = 1] - 1/2| \\
&\leq |\Pr[\mathsf{Game}_1 = 1] - 1/2| + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&\leq |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_1 = 1 \mid \mathsf{Acc}] - 1/2| + \delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&= |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_{1.5} = 1 \mid \mathsf{Acc}] - 1/2| + \delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&= |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_2 = 1 \mid \mathsf{Acc}] - 1/2| + \delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&= |\Pr[\mathsf{Acc}] \cdot \Pr[\mathsf{Game}_3 = 1 \mid \mathsf{Acc}] - 1/2| + \delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&\leq |\Pr[\mathsf{Game}_3 = 1] - 1/2| + 2\delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&\leq |\Pr[\mathsf{Game}_4 = 1] - 1/2| + \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1, \mathcal{D}_\mathcal{M}, \mathcal{S}, \mathcal{B}}(\kappa) + 2\delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}} \\
&\leq \mathsf{Disj}_{\mathsf{PKE}_1, \mathcal{S}}(\kappa) + \mathsf{Adv}^{\text{ds-ind}}_{\mathsf{PKE}_1, \mathcal{D}_\mathcal{M}, \mathcal{S}, \mathcal{B}}(\kappa) + 2\delta + q_{\mathsf{H}'} \cdot 2^{\frac{-\ell+1}{2}}.
\end{aligned}$$

□

Acknowledgments

We would like to thank Haodong Jiang for insightful comments.

References

ARU14. Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th FOCS*, pages 474–483. IEEE Computer Society Press, October 2014. 2

ATTU16. Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the cbc, cfb, ofb, ctr, and XTS modes of operation. In Takagi [Tak16], pages 44–63. 1

BCHK07. Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007. 1

BDF+11. Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011. 1, 2, 3

BZ13. Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Heidelberg, August 2013. 1, 4, 5, 6

CS03. Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2003. 7

FO13. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, January 2013. 2

HHK17. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 341–371. Springer, Heidelberg, November 2017. 7

HRS16. Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016, Part I*, volume 9614 of *LNCS*, pages 387–416. Springer, Heidelberg, March 2016. 2

JZC+18. Haodong Jiang, Zhenfeng Zhang, Long Chen, Hong Wang, and Zhi Ma. Ind-cca-secure key encapsulation mechanism in the quantum random oracle model, revisited. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 96–125. Springer, 2018. 2

KLLNP16. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, Heidelberg, August 2016. 1

KLS18. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Heidelberg, April / May 2018. 3

KM12. Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012. 1

NC00. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000. 2

SJS16. Vladimir Soukharev, David Jao, and Srinath Seshadri. Post-quantum security models for authenticated encryption. In Takagi [Tak16], pages 64–78. 6

SXY18. Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, April / May 2018. 1, 2, 4, 7

Tak16. Tsuyoshi Takagi, editor. *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*. Springer, 2016. 11

Zha12. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012. 3

Zha18. Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. Cryptology ePrint Archive, Report 2018/276, 2018. https://eprint.iacr.org/2018/276. 1, 2, 3

A Simple Lemma

Lemma A.1. *For any reals a, b, and c with $c \geq 0$, we have*

$$|a - b - c| \leq |a - b| + c.$$

Proof. We consider the three cases below:

- Case $a - b \geq c \geq 0$: In this case, we have $a - b - c \geq 0$. Thus, we have $|a - b - c| = a - b - c \leq a - b + c = |a - b| + c$.
- Case $a - b \leq 0 \leq c$: In this case, we have $a - b - c \leq 0$. We have $|a - b - c| = -(a - b - c) = -(a - b) + c = |a - b| + c$.
- Case $0 \leq a - b \leq c$: Again, we have $a - b - c \leq 0$. We have $|a - b - c| = -(a - b - c) = -(a - b) + c \leq a - b + c = |a - b| + c$.

In all three cases, we have $|a - b - c| \leq |a - b| + c$ as we wanted. □