QCCA-Secure Generic Key Encapsulation Mechanism with Tighter Security in the Quantum Random Oracle Model

Xu Liu[1,2] and Mingqiang Wang[1,2](✉)

[1] School of Mathematics, Shandong University, Jinan, China
liuxu17@mail.sdu.edu.cn, wangmingqiang@sdu.edu.cn
[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

Abstract. Xagawa and Yamakawa (PQCrypto 2019) proved the transformation SXY can tightly turn DS secure PKEs into IND-qCCA secure KEMs in the quantum random oracle model (QROM). But transformations such as KC, TPunc that turn PKEs with standard security (OW-CPA or IND-CPA) into DS secure PKEs still suffer from quadratic security loss in the QROM. In this paper, we give a tighter security reduction for the transformation KC that turns OW-CPA secure deterministic PKEs into modified DS secure PKEs in the QROM. We use the Measure-Rewind-Measure One-Way to Hiding Lemma recently introduced by Kuchta et al. (EUROCRYPT 2020) to avoid the square-root advantage loss. Moreover, we extend it to the case that underlying PKEs are not perfectly correct. Combining with other transformations, we finally obtain a generic KEM from any IND-CPA secure PKE. Our security reduction has roughly the same tightness as the result of Kuchta et al. without any other assumptions and we achieve the stronger IND-qCCA security. We also give a similar result for another KEM transformation achieving the same security notion from any OW-CPA secure deterministic PKE.

Keywords: Key encapsulation mechanism · Quantum chosen ciphertext security · Quantum random oracle model

1 Introduction

Key encapsulation mechanism (KEM) is a foundational cryptography primitive. It can be used to construct efficient hybrid encryption using the KEM/DEM paradigm [8]. Indistinguishability under chosen ciphertext attacks (IND-CCA) is widely used as the desired security notion for KEM and public-key encryption (PKE). With the development of quantum computer, we need to develop cryptographic schemes that would be secure against both quantum and classical computers. In this paper, we consider the indistinguishability under quantum chosen ciphertext attacks (IND-qCCA) for KEM in the quantum random oracle model (QROM).

J. A. Garay (Ed.): PKC 2021, LNCS 12710, pp. 3–26, 2021.
https://doi.org/10.1007/978-3-030-75245-3_1

In the quantum world, one can deal with superposition states, which brings more capabilities to the adversaries. To achieve the security against quantum adversaries, we have to base our cryptographic constructions on quantum-resistant assumptions. But it is not sufficient if adversaries can interact with honest parties using quantum communication. Boneh et al. [6] argued that quantum random oracle model should be used instead of random oracle model (ROM) [4]. In the QROM, hash functions are modeled as public oracles similarly as ROM but with quantum access. Furthermore, Boneh and Zhandry [7] introduced the IND-qCCA security notion for PKE, where adversaries can make quantum queries to the decryption oracle. Their goal is to construct classical systems that remain secure even when implemented on a quantum computer, thereby potentially giving the attacker the ability to issue quantum queries. Following it, Xagawa and Yamakawa [22] considered the IND-qCCA security for KEM, where adversaries can make quantum queries to the decapsulation oracle. Note that different from PKE, there is no challenge messages queried by the adversary in the IND-CCA game for KEM. All interactions with the adversary use quantum communication. Therefore, the corresponding IND-qCCA security in the QROM is the security notion against fully quantum adversaries for KEM.

To achieve the IND-CCA security, generic transformations such as Fujisaki-Okamoto (FO) transformation [10,11] are usually used. They can transform a weakly secure (one-wayness under chosen plaintext attacks (OW-CPA) or indistinguishability under chosen plaintext attacks (IND-CPA)) PKE to a IND-CCA one. Dent [9] gave the KEM version of FO. Hofheinz, Hövelmanns and Kiltz [12] analyzed it in a modular way, decomposing it into two transformations named T and $\mathsf{U}^{\not\perp}$. They also introduced some variants of transformation $\mathsf{U}^{\not\perp}$ named $\mathsf{U}^{\not\perp}_m$, $\mathsf{U}^{\perp}$ and $\mathsf{U}^{\perp}_m$, and they gave a detailed result about them in the classical setting. Subsequent works [5,13,15–18] are devoted to the analysis in the quantum setting. The core tool used in these analysis is the One-Way to Hiding (O2H) Lemma [21] and its variants [2,5,12,18]. Roughly speaking, the O2H lemma can be used to construct a one-wayness adversary from a distinguisher.

Recently, Kuchta et al. [18] introduced a new O2H variant named Measure-Rewind-Measure One-Way to Hiding (MRM O2H) Lemma. It is the first variant to get rid of the square-root advantage loss, and using this lemma, they gave a security proof for FO from IND-CPA security to IND-CCA security without the square-root advantage loss for the first time. Their security proof is nearly tight for low query depth attacks. The case of (relatively) low query depth attacks tends to be of high practical interest, since it corresponds, for instance, to massively parallelized attacks, which are the standard approach to deal with high computation costs in practical cryptanalysis. However, their proof doesn't apply to the IND-qCCA security. As argued in [7,22], in order to be immune to quantum superposition attacks, quantum chosen ciphertext security is worth investigating. On the other hand, Saito, Xagawa and Yamakawa [20] introduced a new security notion named disjoint simulatability (DS). Intuitively, disjoint simulatability means that we can efficiently sample "fake ciphertexts" that are computationally indistinguishable from real ciphertexts ("simulatability"), while the set of

possible fake ciphertexts is required to be (almost) disjoint from the set of real ciphertexts ("disjointness"). In addition, they gave a transformation named SXY which can tightly turn DS secure PKEs into IND-CCA secure KEMs. Furthermore, they find it can be easily extended to the stronger IND-qCCA security tightly also [22]. However, transformations KC and TPunc introduced in [20] from standard secure (OW-CPA or IND-CPA) PKEs to DS secure PKEs still suffer from quadratic security loss, so is the KEM combined with transformation SXY.

Our Contributions. In this paper, we analyze two generic KEMs and we prove that they achieve IND-qCCA security from standard security without quadratic security loss in the QROM. At the heart of our result is a tighter security reduction for the transformation KC. We modify the definition of DS and we use the MRM O2H lemma to prove that the transformation KC can transform a OW-CPA secure deterministic PKE (dPKE) into a modified DS secure PKE without the square-root advantage loss. Moreover, we don't require the underlying PKE to be perfectly correct as before.

The first KEM we analyzed is SXY ∘ KC ∘ T and the second KEM is SXY ∘ KC. We give an overview in Fig. 1. The upper part and the lower part of Fig. 1 are the two KEMs respectively. The second KEM is relatively simple, and it is the combination of transformation KC and transformation SXY. Xagawa and Yamakawa has already proved transformation SXY can tightly turn δ-correct DS secure dPKEs into IND-qCCA secure KEMs in the QROM (Lemma 5 [22]).

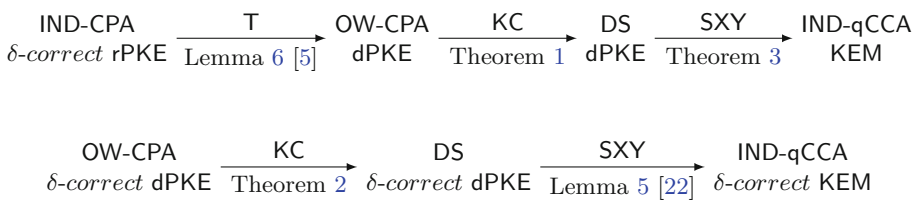

Fig. 1. Overview of KEMs.

In the previous security proofs of KC [17,20], some variants of O2H lemmas are used. However, they all incur a quadratic loss of security. The MRM O2H lemma doesn't suffer from it, but it requires the simulator can simulate both G and H. In our case, the simulator doesn't know the $m^* \in S$, however, the simulator can simulate G (or H) that should be reprogrammed at m^* by testing whether the queried m satisfies $\mathsf{Enc}(pk, m) = c^*$ or not instead. With a detailed analysis, the MRM O2H lemma can be applied to prove the second property of DS even if the underlying PKE is not perfectly correct. But it is difficult to satisfy the first requirement of DS with imperfectly correct underlying PKEs in KC. However, we find that the DS notion in [20] is slightly stronger, so we make a modification to its definition to relax the requirement. With this new DS notion, we get rid of the perfectly correctness requirement in KC. And finally we prove that the transformation KC can turn δ-correct OW-CPA secure

dPKEs into δ-correct DS secure dPKEs without the square-root advantage loss in Theorem 2.[1]

The underlying PKE of above KEM is dPKE. If we want to let the underlying PKE be a rPKE (randomized PKE), we can apply the transformation T first. And this yields the first KEM. Although there exists results of transformation T that it can turn δ-correct IND-CPA secure rPKEs into OW-CPA secure dPKEs (Lemma 6 [5]), we cannot simply append it to the proof of the second KEM. The reason is that the concept of δ-correct doesn't apply to the resulting dPKE of T directly, though the resulting dPKE is not perfectly correct. So actually, Theorem 1 and Theorem 3 are different from corresponding Theorem 2 and Lemma 5 [22]. In the proof of Theorem 3, we use the method in [12,15] to deal with it. In the proof of Theorem 1, we make a direct analysis to get a better result. Specifically, we use a different Bad event than that in the proof of Theorem 2 to separate the case that a "bad" message is chosen.

Here we give a comparison of KEM transformations from IND-CPA secure PKEs in the QROM in Table 1. Kuchta et al.'s [18] proof of $\mathsf{FO}^{\not\perp}$ achieves the best known security bound of KEMs from IND-CPA security to IND-CCA security in the QROM. Xagawa and Yamakawa [22] gave the first KEM to achieve the stronger IND-qCCA security. And Jiang et al. [17] improved the security bound of Tpunc. But the security bound of the combination scheme is still larger than the first one in certain settings. Our proof of $\mathsf{KEM} := \mathsf{SXY} \circ \mathsf{KC} \circ \mathsf{T}$ achieves the IND-qCCA security with tighter security bound than the second one, roughly the same as the first one. What's more, it doesn't need any other requirements.

Table 1. Comparison of KEM transformations from IND-CPA secure PKEs in the QROM. The "Security bound" column shows the dependence of the approximate upper bound on attacker's advantage $\mathsf{Adv}(\mathcal{A})$ against the KEM in terms of the attacker advantage ϵ against the underlying PKE, and $\mathcal{A}$'s total query number q or query depth d to quantum random oracles.

Transformation	Underlying security	Achieved security	Security bound	Other requirements
$\mathsf{FO}^{\not\perp} := \mathsf{U}^{\not\perp} \circ \mathsf{T}$[18]	IND-CPA	IND-CCA	$d^2\epsilon$	$\mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ is η-injective.
$\mathsf{SXY} \circ \mathsf{TPunc}$[17,22]	IND-CPA	IND-qCCA	$\sqrt{q\epsilon}$	PKE is perfectly correct.
$\mathsf{SXY} \circ \mathsf{KC} \circ \mathsf{T}$ [This work]	IND-CPA	IND-qCCA	$d^2\epsilon$	-

2 Preliminaries

2.1 Notation

For a finite set S, $|S|$ denotes the cardinality of S, and we denote the sampling of a uniformly random element x from S by $x \xleftarrow{\$} S$, while we denote the sampling

[1] In the main body of the paper, Theorem 2 actually follows Theorem 1. Here we reverse the order of introduction.

according to some distribution $\mathcal{D}$ by $x \leftarrow \mathcal{D}$. $\mathcal{U}_S$ denotes the uniform distribution over S. By $[\![B]\!]$ we denote the bit that is 1 if the Boolean statement B is true, and otherwise 0.

We denote deterministic computation of an algorithm A on input x by $y := \mathsf{A}(x)$. We denote algorithms with access to an oracle O by A^O. Unless stated otherwise, we assume all our algorithms to be probabilistic and denote the computation by $y \leftarrow \mathsf{A}(x)$. We also use the notation $y := \mathsf{A}(x; r)$ to make the randomness r explicit. By $\mathsf{Time}(\mathsf{A})$ we denote the running time of A.

Some algorithms such as Gen need a security parameter $\lambda \in \mathbb{N}$ as input. However, we usually omit it for simplicity. We say a function is *negligible* in λ if $f(\lambda) = \lambda^{-\omega(1)}$. PPT stands for probabilistic polynomial time.

2.2 Quantum Computation

We refer to [19] for basic of quantum computation. In this subsection we mainly present several useful lemmas.

Quantum Random Oracle Model. Following [3,6], we review a quantum oracle O as a mapping

$$|x\rangle\,|y\rangle \to |x\rangle\,|y \oplus O(x)\rangle\,,$$

where $O : \{0,1\}^n \to \{0,1\}^m, x \in \{0,1\}^n$ and $y \in \{0,1\}^m$. 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, while adversaries are only given classical oracle access in the classical random oracle model (ROM).

Lemma 1 ([20, Lemma 2.2])**.** *Let l be an integer. Let $\mathsf{H} : \{0,1\}^l \times X \to Y$ and $\mathsf{H}' : X \to Y$ 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*

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

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

Lemma 2 (Generic Distinguishing Problem with Bounded Probabilities [1,13,14])**.** *Let X be a finite set, and let $\lambda \in [0,1]$. $\mathsf{F}_1 : X \to \{0,1\}$ is the following function: For each $x \in X$, $\mathsf{F}_1(x) = 1$ with probability λ_x ($\lambda_x \leq \lambda$), and $\mathsf{F}_1(x) = 0$ else. F_2 is the constant zero function. Then, for any algorithm A issuing at most q quantum queries to F_1 or F_2, $|\Pr[1 \leftarrow \mathsf{A}^{\mathsf{F}_1}] - \Pr[1 \leftarrow \mathsf{A}^{\mathsf{F}_2}]| \leq 8q^2\lambda$.*

Lemma 3 (Measure-Rewind-Measure One-Way to Hiding [18, Lemma 3.3])**.** *Let $G, H : X \to Y$ be random functions, z be a random value, and $S \subseteq X$ be a random set such that $G(x) = H(x)$ for every $x \notin S$. The tuple (G, H, S, z) may have arbitrary joint distribution. Furthermore, let $\mathcal{A}^O$ be a quantum oracle*

algorithm which queries oracle O with query depth d. Then we can construct an algorithm $\mathcal{D}^{G,H}(z)$ such that $\mathsf{Time}(\mathcal{D}^{G,H}) \approx 2 \cdot \mathsf{Time}(\mathcal{A}^O)$[2] *and*

$$\mathsf{Adv}(\mathcal{A}^O) \leq 4d \cdot \mathsf{Adv}(\mathcal{D}^{G,H}).$$

Here $\mathsf{Adv}(\mathcal{A}^O) := |P_{\mathsf{left}} - P_{\mathsf{right}}|$ *with*

$$P_{\mathsf{left}} := \Pr_{H,z}[1 \leftarrow \mathcal{A}^H(z)], \ P_{\mathsf{right}} := \Pr_{G,z}[1 \leftarrow \mathcal{A}^G(z)],$$

and

$$\mathsf{Adv}(\mathcal{D}^{G,H}) := \Pr_{G,H,S,z}[T \cap S \neq \varnothing | T \leftarrow \mathcal{D}^{G,H}(z)].$$

2.3 Public-Key Encryption

Definition 1 (PKE). *A* (randomized) *public-key encryption scheme* ((r)PKE) *is defined over a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, a public key space $\mathcal{PK}$ and a secret key space $\mathcal{SK}$. It consists of a triple of algorithms* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *defined as follows.*

- $\mathsf{Gen} \rightarrow (pk, sk)$ *is a randomized algorithm that returns a public key $pk \in \mathcal{PK}$ and a secret key $sk \in \mathcal{SK}$.*
- $\mathsf{Enc}(pk, m) \rightarrow c$ *is a randomized algorithm that takes as input a public key pk and a message $m \in \mathcal{M}$, and outputs a ciphertext $c \in \mathcal{C}$. If necessary, we make the used randomness of* Enc *explicit by writing $c := \mathsf{Enc}(pk, m; r)$, where $r \xleftarrow{\$} \mathcal{R}$ and $\mathcal{R}$ is the randomness space.*
- $\mathsf{Dec}(sk, c) \rightarrow m/\perp$ *is a deterministic algorithm that takes as input a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{C}$ and returns either a message $m \in \mathcal{M}$ or a failure symbol $\perp \notin \mathcal{M}$.*

A deterministic *public-key encryption scheme* (dPKE) *is defined the same way, except that* Enc *is a deterministic algorithm.*

Definition 2 (Correctness [12]**).** *A public-key encryption scheme* PKE *is δ-correct if*

$$\mathrm{E}\left[\max_{m \in \mathcal{M}} \Pr[\mathsf{Dec}(sk, c) \neq m | c \leftarrow \mathsf{Enc}(pk, m)]\right] \leq \delta,$$

where the expectation is taken over $(pk, sk) \leftarrow \mathsf{Gen}$. We say the PKE *is perfectly correct if $\delta = 0$.*

Remark 1. Above correctness definition is in the standard model, there is no random oracle relative to the PKE. But we still use this definition in the random oracle model if random oracles have no effect on it.

[2] Actually, from the proof of lemma 3.2 and lemma 3.3 in [18], we have $\mathsf{Time}(\mathcal{D}^{G,H}) \approx \mathsf{Time}(\mathcal{B}_i^{G,H}) + \mathsf{Time}(\mathcal{C}_i^{G,H}) \approx \mathsf{Time}(\mathcal{B}_i^{G,H}) + \left(\mathsf{Time}(\mathcal{B}_i^{G,H}) + 2\left(\mathsf{Time}(\mathcal{A}_i^O) - \mathsf{Time}(\mathcal{B}_i^{G,H})\right)\right) \approx 2 \cdot \mathsf{Time}(\mathcal{A}^O)$.

Let $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme with message space $\mathcal{M}$. We now define three security notions for it. We say the PKE is GOAL-ATK secure if $\mathsf{Adv}^{\mathsf{GOAL}}_{\mathsf{PKE},\mathcal{A}}$-ATK is negligible for any PPT adversary $\mathcal{A}$.

Definition 3 (OW-CPA). *The One-Wayness under Chosen Plaintext Attacks* (OW-CPA) *game for* PKE *is defined in Fig. 2, and the* OW-CPA *advantage of an adversary* $\mathcal{A}$ *against* PKE *is defined as* $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}} := \Pr[\mathsf{OW\text{-}CPA}^{\mathcal{A}}_{\mathsf{PKE}} \Rightarrow 1]$.

GAME $\mathsf{OW\text{-}CPA}^{\mathcal{A}}_{\mathsf{PKE}}$	**GAME** $\mathsf{IND\text{-}CPA}^{\mathcal{A}}_{\mathsf{PKE}}$
$(pk, sk) \leftarrow \mathsf{Gen}$	$(pk, sk) \leftarrow \mathsf{Gen}$
$m^* \xleftarrow{\$} \mathcal{M}$	$b \xleftarrow{\$} \{0,1\}$
$c^* \leftarrow \mathsf{Enc}(pk, m^*)$	$(m_0^*, m_1^*, st) \leftarrow \mathcal{A}_1(pk)$
$m' \leftarrow \mathcal{A}(pk, c^*)$	$c^* \leftarrow \mathsf{Enc}(pk, m_b^*)$
return $[\![m' = m^*]\!]$	$b' \leftarrow \mathcal{A}_2(pk, c^*, st)$
	return $[\![b' = b]\!]$

Fig. 2. Games OW-CPA and IND-CPA for PKE.

Definition 4 (IND-CPA). *The Indistinguishability under Chosen Plaintext Attacks* (IND-CPA) *game for* PKE *is defined in Fig. 2, and the* IND-CPA *advantage of an adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *against* PKE *is defined as* $\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}} := 2|\Pr[\mathsf{IND\text{-}CPA}^{\mathcal{A}}_{\mathsf{PKE}} \Rightarrow 1] - 1/2|$.

Definition 5 (IND-qCCA [7]). *The Indistinguishability under quantum Chosen Ciphertext Attacks* (IND-qCCA) *game for* PKE *is defined in Fig. 3, and the* IND-qCCA *advantage of an adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *against* PKE *is defined as* $\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{PKE},\mathcal{A}} := |\Pr[\mathsf{IND\text{-}qCCA}^{\mathcal{A}}_{\mathsf{PKE}} \Rightarrow 1] - 1/2|$.

GAME $\mathsf{IND\text{-}qCCA}^{\mathcal{A}}_{\mathsf{PKE}}$	$\mathsf{Dec}_a(\sum_{c,m} \psi_{c,m} \lvert c, m\rangle)$
$(pk, sk) \leftarrow \mathsf{Gen}$	**return** $\sum_{c,m} \psi_{c,m} \lvert c, m \oplus f_a(c)\rangle$
$b \xleftarrow{\$} \{0,1\}$	
$(m_0^*, m_1^*, st) \leftarrow \mathcal{A}_1^{\mathsf{Dec}_\perp}(pk)$	$f_a(c)$
$c^* \leftarrow \mathsf{Enc}(pk, m_b^*)$	**if** $c = a$
$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}_{c^*}}(pk, c^*, st)$	**return** $m' := \perp$
return $[\![b' = b]\!]$	**else return** $m' := \mathsf{Dec}(sk, c)$

Fig. 3. Game IND-qCCA for PKE.

Saito, Xagawa and Yamakawa [20] introduced a new security notion named DS for dPKE. Here we give a modified version and we keep the name unchanged in this paper.

Definition 6 (DS, modified from [20]). *Let $\mathcal{D}_{\mathcal{M}}$ denote an efficiently sampleable distribution on a set $\mathcal{M}$. A deterministic public-key encryption 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 (DS) if there exists a PPT algorithm $\mathcal{S}$ that satisfies the followings.*

- *Disjointness:*

$$\mathsf{Disj}_{\mathsf{PKE},\mathcal{S}} \coloneqq \Pr[c^* \in \mathsf{Enc}(pk, \mathcal{M}) | (pk, sk) \leftarrow \mathsf{Gen}, c^* \leftarrow \mathcal{S}(pk)]$$

  is negligible.
- *Ciphertext-indistinguishability: For any PPT adversary $\mathcal{A}$,*

$$\mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE},\mathcal{D}_{\mathcal{M}},\mathcal{A},\mathcal{S}} \coloneqq$$

$$\left| \begin{array}{c} \Pr[1 \leftarrow \mathcal{A}(pk, c^*) | (pk, sk) \leftarrow \mathsf{Gen}, m^* \leftarrow \mathcal{D}_{\mathcal{M}}, c^* \coloneqq \mathsf{Enc}(pk, m^*)] \\ - \Pr[1 \leftarrow \mathcal{A}(pk, c^*) | (pk, sk) \leftarrow \mathsf{Gen}, c^* \leftarrow \mathcal{S}(pk)] \end{array} \right|$$

  is negligible.

Remark 2. In the original definition of DS, the first condition is "statistical disjointness":

$$\mathsf{Disj}_{\mathsf{PKE},\mathcal{S}} \coloneqq \max_{(pk,sk) \in \mathsf{Gen}(1^\lambda;\mathcal{R})} \Pr[c^* \in \mathsf{Enc}(pk, \mathcal{M}) | c^* \leftarrow \mathcal{S}(pk)]$$

is negligible, where λ is the security parameter and $\mathcal{R}$ denotes the randomness space for Gen. We relax this condition to "disjointness" as we find it is sufficient to prove those theorems we needed.

2.4 Key Encapsulation Mechanism

Definition 7 (KEM). *A key encapsulation mechanism (KEM) is defined over a key space $\mathcal{K}$, a ciphertext space $\mathcal{C}$, a public key space $\mathcal{PK}$ and a secret key space $\mathcal{SK}$. It consists of a triple of algorithms $\mathsf{KEM} = (\mathsf{Gene}, \mathsf{Enca}, \mathsf{Deca})$ defined as follows.*

- $\mathsf{Gene} \rightarrow (pk, sk)$ *is a randomized algorithm that returns a public key $pk \in \mathcal{PK}$ and a secret key $sk \in \mathcal{SK}$.*
- $\mathsf{Enca}(pk) \rightarrow (c, k)$ *is a randomized algorithm that takes as input a public key pk and outputs a ciphertext $c \in \mathcal{C}$ as well as a key $k \in \mathcal{K}$.*
- $\mathsf{Deca}(sk, c) \rightarrow k / \perp$ *is a deterministic algorithm that takes as input a secret key $sk \in \mathcal{SK}$ and a ciphertext $c \in \mathcal{C}$ and returns either a key $k \in \mathcal{K}$ or a failure symbol $\perp \notin \mathcal{K}$.*

Definition 8 (Correctness [12]). *A key encapsulation mechanism KEM is δ-correct if*

$$\Pr[\mathsf{Deca}(sk, c) \neq k | (pk, sk) \leftarrow \mathsf{Gene}, (c, k) \leftarrow \mathsf{Enca}(pk)] \leq \delta.$$

Let $\mathsf{KEM} = (\mathsf{Gene}, \mathsf{Enca}, \mathsf{Deca})$ be a key encapsulation mechanism with key space $\mathcal{K}$. Following the definition of IND-qCCA for PKE, the KEM version for it can be defined similarly. We say the KEM is IND-qCCA secure if $\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}}$ is negligible for any PPT adversary $\mathcal{A}$.

Definition 9 (IND-qCCA [22]). *The* IND-qCCA *game for* KEM *is defined in Fig. 4, and the* IND-qCCA *advantage of an adversary* $\mathcal{A}$ *against* KEM *is defined as* $\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} := |\Pr[\mathsf{IND\text{-}qCCA}^{\mathcal{A}}_{\mathsf{KEM}} \Rightarrow 1] - 1/2|$.

GAME $\mathsf{IND\text{-}qCCA}^{\mathcal{A}}_{\mathsf{KEM}}$	$\mathsf{Deca}_a(\sum_{c,k} \psi_{c,k} \lvert c,k\rangle)$
$(pk, sk) \leftarrow \mathsf{Gene}$	**return** $\sum_{c,k} \psi_{c,k} \lvert c, k \oplus f_a(c)\rangle$
$b \xleftarrow{\$} \{0,1\}$	
$(c^*, k_0^*) \leftarrow \mathsf{Enca}(pk)$	$f_a(c)$
$k_1^* \xleftarrow{\$} \mathcal{K}$	**if** $c = a$
$b' \leftarrow \mathcal{A}^{\mathsf{Deca}_{c^*}}(pk, c^*, k_b^*)$	**return** $k' := \perp$
return $[\![b' = b]\!]$	**else return** $k' := \mathsf{Deca}(sk, c)$

Fig. 4. Game IND-qCCA for KEM.

3 Tighter Proofs for the Transformation KC

In this section, we give a tighter security reduction for the transformation KC [20] that transforms OW-CPA secure dPKEs into DS secure dPKEs without the perfect correctness requirement of underlying PKEs.

Transformation KC. To a deterministic public-key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$, and a hash function $\mathsf{H} : \mathcal{M} \to \{0,1\}^n$, we associate $\mathsf{PKE}' := \mathsf{KC}[\mathsf{PKE}, \mathsf{H}]$. The algorithms of $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ are defined in Fig. 5.

$\underline{\mathsf{Gen}'}$	$\underline{\mathsf{Enc}'(pk, m)}$	$\underline{\mathsf{Dec}'(sk, (c,d))}$	$\underline{\mathcal{S}(pk)}$
$(pk, sk) \leftarrow \mathsf{Gen}$	$c := \mathsf{Enc}(pk, m)$	$m' := \mathsf{Dec}(sk, c)$	$m^* \leftarrow \mathcal{U}_{\mathcal{M}}$
return (pk, sk)	$d := \mathsf{H}(m)$	**if** $m' = \perp$ **or** $\mathsf{H}(m') \neq d$	$c^* := \mathsf{Enc}(pk, m^*)$
	return (c, d)	**return** $\perp$	$d^* \xleftarrow{\$} \{0,1\}^n$
		else return m'	**return** (c^*, d^*)

Fig. 5. $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}') := \mathsf{KC}[\mathsf{PKE}, \mathsf{H}]$ with simulator $\mathcal{S}$.

Before we prove the security of KC, we first review the transformation T introduced in [12].

Transformation T. To a public-key encryption scheme $\mathsf{PKE}_0 = (\mathsf{Gen}_0, \mathsf{Enc}_0, \mathsf{Dec}_0)$ with message space $\mathcal{M}$ and randomness space $\mathcal{R}$, and a hash function $\mathsf{G} : \mathcal{M} \to \mathcal{R}$, we associate $\mathsf{PKE} := \mathsf{T}[\mathsf{PKE}_0, \mathsf{G}]$. The algorithms of $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ are defined in Fig. 6.

$\underline{\mathsf{Gen}}$	$\underline{\mathsf{Enc}(pk, m)}$	$\underline{\mathsf{Dec}(sk, c)}$
$(pk, sk) \leftarrow \mathsf{Gen}_0$	$c := \mathsf{Enc}_0(pk, m; \mathsf{G}(m))$	$m' := \mathsf{Dec}_0(sk, c)$
return (pk, sk)	**return** c	**if** $m' = \perp$ **or** $\mathsf{Enc}_0(pk, m'; \mathsf{G}(m')) \neq c$
		return $\perp$
		else return m'

Fig. 6. $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}) := \mathsf{T}[\mathsf{PKE}_0, \mathsf{G}]$.

Next, we give a lemma related to the transformation T. It roughly speaks that there is a high probability the ciphertext corresponding to a randomly chosen message has only one preimage with regard to $\mathsf{PKE} := \mathsf{T}[\mathsf{PKE}_0, \mathsf{G}]$.

Lemma 4. *Let* $\mathsf{PKE}_0 = (\mathsf{Gen}_0, \mathsf{Enc}_0, \mathsf{Dec}_0)$ *be a* δ*-correct* rPKE *with message space* $\mathcal{M}$ *and randomness space* $\mathcal{R}$*. We define a set with respect to fixed* (pk, sk) *and* $\mathsf{G} \in \Omega_{\mathsf{G}}$:

$$S^{collision}_{(pk,sk),\mathsf{G}} := \{m \in \mathcal{M} | \exists m' \neq m, \mathsf{Enc}_0(pk, m'; \mathsf{G}(m')) = \mathsf{Enc}_0(pk, m; \mathsf{G}(m))\},$$

where Ω_{G} *denotes the set of all functions* $\mathsf{G} : \mathcal{M} \to \mathcal{R}$.

Then we have

$$\Pr[m \in S^{collision}_{(pk,sk),\mathsf{G}} | (pk, sk) \leftarrow \mathsf{Gen}_0, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}, m \xleftarrow{\$} \mathcal{M}] \leq 2\delta.$$

Proof. From the definition of δ-correct, we have

$$\mathop{\mathrm{E}}_{(pk,sk)\leftarrow\mathsf{Gen}_0} \left[\max_{m \in \mathcal{M}} \Pr[\mathsf{Dec}_0(sk, c) \neq m | c \leftarrow \mathsf{Enc}_0(pk, m)] \right] \leq \delta.$$

The inequality still holds when the m is chosen at random, i.e.,

$$\mathop{\mathrm{E}}_{(pk,sk)\leftarrow\mathsf{Gen}_0} \left[\mathop{\mathrm{E}}_{m \xleftarrow{\$} \mathcal{M}} \Pr[\mathsf{Dec}_0(sk, c) \neq m | c \leftarrow \mathsf{Enc}_0(pk, m)] \right] \leq \delta.$$

We represent above inequality in a different form with equivalent meaning:

$$\Pr[\mathsf{Dec}_0(sk, c) \neq m | (pk, sk) \leftarrow \mathsf{Gen}_0, m \xleftarrow{\$} \mathcal{M}, c \leftarrow \mathsf{Enc}_0(pk, m)] \leq \delta.$$

Then we make the randomness used by Enc_0 explicit:

$$\Pr[\mathsf{Dec}_0(sk, \mathsf{Enc}_0(pk, m; r)) \neq m | (pk, sk) \leftarrow \mathsf{Gen}_0, m \xleftarrow{\$} \mathcal{M}, r \xleftarrow{\$} \mathcal{R}] \leq \delta.$$

It equals that:

$$\Pr[\mathsf{Dec}_0(sk, \mathsf{Enc}_0(pk, m; \mathsf{G}(m))) \neq m | (pk, sk) \leftarrow \mathsf{Gen}_0, m \xleftarrow{\$} \mathcal{M}, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}] \leq \delta.$$

Here we define a set in which messages are incorrectly decrypted with respect to fixed (pk, sk) and G:

$$S^{error}_{(pk,sk),\mathsf{G}} := \{m \in \mathcal{M} | \mathsf{Dec}_0(sk, \mathsf{Enc}_0(pk, m; \mathsf{G}(m))) \neq m\}.$$

Finally, we have

$$\begin{aligned}
&\Pr[m \in S^{collision}_{(pk,sk),\mathsf{G}} | (pk, sk) \leftarrow \mathsf{Gen}_0, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}, m \xleftarrow{\$} \mathcal{M}] \\
&\leq 2 \Pr[m \in S^{collision}_{(pk,sk),\mathsf{G}} \cap S^{error}_{(pk,sk),\mathsf{G}} | (pk, sk) \leftarrow \mathsf{Gen}_0, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}, m \xleftarrow{\$} \mathcal{M}] \\
&\leq 2 \Pr[m \in S^{error}_{(pk,sk),\mathsf{G}} | (pk, sk) \leftarrow \mathsf{Gen}_0, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}, m \xleftarrow{\$} \mathcal{M}] \\
&= 2 \Pr[\mathsf{Dec}_0(sk, \mathsf{Enc}_0(pk, m; \mathsf{G}(m))) \neq m | (pk, sk) \leftarrow \mathsf{Gen}_0, m \xleftarrow{\$} \mathcal{M}, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}] \\
&\leq 2\delta,
\end{aligned}$$

where the first inequality follows from the fact that m is chosen randomly and $|S^{collision}_{(pk,sk),\mathsf{G}} \setminus S^{error}_{(pk,sk),\mathsf{G}}| \leq |S^{collision}_{(pk,sk),\mathsf{G}} \cap S^{error}_{(pk,sk),\mathsf{G}}|$ for fixed (pk, sk) and G. □

Now we are ready to prove the security of KC in the QROM. In particular, we prove it in two cases. The first case is that the underlying dPKE is derived from T, as opposed to a general δ-correct dPKE in the second case. In both cases, underlying PKEs don't need to be perfectly correct.

Previous proofs [17,20] use some variants of O2H lemma, but they all incur a quadratic loss of security. Kuchta et al. [18] recently introduced the MRM O2H lemma (Lemma 3) without the square-root advantage loss. We apply it to KC and we avoid the square-root advantage loss in the proof accordingly.

Theorem 1 (Security of KC in the QROM, Case 1). *Let* PKE *be a* dPKE *transformed from* PKE_0 *by* T*, i.e.,* $\mathsf{PKE} := \mathsf{T}[\mathsf{PKE}_0, \mathsf{G}]$. PKE_0 *is a* δ*-correct* rPKE *with message space* $\mathcal{M}$ *and randomness space* $\mathcal{R}$*. Let* $\mathsf{G} : \mathcal{M} \to \mathcal{R}$, $\mathsf{H} : \mathcal{M} \to \{0,1\}^n$ *be hash functions modeled as quantum random oracles.* $\mathsf{PKE}' := \mathsf{KC}[\mathsf{PKE}, \mathsf{H}]$ *and* $\mathcal{S}$ *is the algorithm defined in Fig. 5. Then we have* $\mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} \leq 2^{-n} + 2\delta$*. Moreover, for any adversary* $\mathcal{A}$ *against the* DS-IND *security of* PKE′ *issuing quantum queries to* H *with depth* d_{H}*, there exists an adversary* $\mathcal{B}$ *against the* OW-CPA *security of* PKE *such that*

$$\mathsf{Adv}^{\text{DS-IND}}_{\mathsf{PKE}',\mathcal{U}_{\mathcal{M}},\mathcal{A},\mathcal{S}} \leq 4d_{\mathsf{H}} \cdot (\mathsf{Adv}^{\text{OW-CPA}}_{\mathsf{PKE},\mathcal{B}} + 2\delta)$$

and $\mathsf{Time}(\mathcal{B}) \approx 2 \cdot \mathsf{Time}(\mathcal{A})$.

Proof. We first define two events:

$$\mathsf{Bad} := [m^* \in S^{collision}_{(pk,sk),\mathsf{G}} | (pk, sk) \leftarrow \mathsf{Gen}, \mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}, m^* \xleftarrow{\$} \mathcal{M}],$$

where $S^{collision}_{(pk,sk),\mathsf{G}}$ is defined in Lemma 4, and Lemma 4 says that $\Pr[\mathsf{Bad}] \leq 2\delta$ as Gen equals Gen_0;

$$\mathsf{Disj} \coloneqq [(c^*, d^*) \in \mathsf{Enc}'(pk, \mathcal{M}) | (pk, sk) \leftarrow \mathsf{Gen}', (c^*, d^*) \leftarrow \mathcal{S}(pk)].$$

Then, we have

$$\begin{aligned}
\mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} &= \Pr[\mathsf{Disj}] \\
&= \Pr[\mathsf{Disj} \wedge \overline{\mathsf{Bad}}] + \Pr[\mathsf{Disj} \wedge \mathsf{Bad}] \\
&\leq \Pr[\mathsf{Disj} \wedge \overline{\mathsf{Bad}}] + \Pr[\mathsf{Bad}] \\
&\leq 2^{-n} + 2\delta,
\end{aligned}$$

where the first equality follows from the definition of DS and the last inequality follows from the fact that if Bad doesn't happen, the only possibility that Disj happens is the second part d^* of the element returned by $\mathcal{S}$ collides with the unique value which is $\mathsf{H}(m^*)$. The probability of this is 2^{-n} as d^* is chosen uniformly at random.

To prove the rest of the theorem, we consider games in Fig. 7. From the definition of DS, we have

$$\mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{U}_{\mathcal{M}},\mathcal{A},\mathcal{S}} = |\Pr[G_0^{\mathcal{A}} \Rightarrow 1] - \Pr[G_1^{\mathcal{A}} \Rightarrow 1]|.$$

GAMES $G_0 - G_2$

$(pk, sk) \leftarrow \mathsf{Gen}$; $\mathsf{H} \xleftarrow{\$} \Omega_{\mathsf{H}}$
$\mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}$
$m^* \xleftarrow{\$} \mathcal{M}$
$c^* \coloneqq \mathsf{Enc}(pk, m^*) = \mathsf{Enc}_0(pk, m^*; \mathsf{G}(m^*))$
$d^* \coloneqq \mathsf{H}(m^*)$ $//G_0, G_2$
$d^* \xleftarrow{\$} \{0,1\}^n$ $//G_1$
$\mathsf{H}' \coloneqq \mathsf{H}$; $S_{c^*} \coloneqq \{m \in \mathcal{M} | \mathsf{Enc}(pk, m) = c^*\}$ $//G_2$
for each $m \in S_{c^*}$, $\mathsf{H}'(m) \xleftarrow{\$} \{0,1\}^n$ $//G_2$
$b \leftarrow \mathcal{A}^{\mathsf{H},\mathsf{G}}(pk, (c^*, d^*))$ $//G_0 - G_1$
$b \leftarrow \mathcal{A}^{\mathsf{H}',\mathsf{G}}(pk, (c^*, d^*))$ $//G_2$
return b

Fig. 7. Games $G_0 - G_2$ for the proof of Theorem 1.

Notice that H', d^* in game G_2 are randomly distributed as H, d^* in game G_1, and they are independent of each other and $\mathcal{A}$'s other view (G, pk, c^*) in both G_1 and G_2, that is, the environments of $\mathcal{A}$ in G_1 and G_2 have the same distribution. It follows that

$$\Pr[G_1^{\mathcal{A}} \Rightarrow 1] = \Pr[G_2^{\mathcal{A}} \Rightarrow 1].$$

The only difference between game G_0 and game G_2 is that $\mathcal{A}$ is interacted with H or H' respectively. Therefore, applying Lemma 3 with $X = \mathcal{M}, Y = \{0,1\}^n, G = \mathsf{H}, H = \mathsf{H}', S = S_{c^*}, z = (\mathsf{G}, pk, (c^*, d^*))$[3] and $\mathcal{A}$, we can construct algorithm $\mathcal{D}$, with run-time $\approx 2 \cdot \mathsf{Time}(\mathcal{A})$ and making oracle calls to H, H' and G in game G_3, such that

$$|\Pr[G_0^{\mathcal{A}} \Rightarrow 1] - \Pr[G_2^{\mathcal{A}} \Rightarrow 1]| \leq 4d_{\mathsf{H}} \cdot \Pr[T \cap S_{c^*} \neq \varnothing],$$

where T is the output of $\mathcal{D}$ and game G_3 is described in Fig. 8.

GAME G_3
$(pk, sk) \leftarrow \mathsf{Gen}$; $\mathsf{H} \xleftarrow{\$} \Omega_{\mathsf{H}}$
$\mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}$
$m^* \xleftarrow{\$} \mathcal{M}$
$c^* \coloneqq \mathsf{Enc}(pk, m^*) = \mathsf{Enc}_0(pk, m^*; \mathsf{G}(m^*))$
$d^* \coloneqq \mathsf{H}(m^*)$
$\mathsf{H}' \coloneqq \mathsf{H}$; $S_{c^*} \coloneqq \{m \in \mathcal{M} | \mathsf{Enc}(pk, m) = c^*\}$
for each $m \in S_{c^*}$, $\mathsf{H}'(m) \xleftarrow{\$} \{0,1\}^n$
$T \leftarrow \mathcal{D}^{\mathsf{H},\mathsf{H}',\mathsf{G}}(pk, (c^*, d^*))$
if $T \cap S_{c^*} \neq \varnothing$
  $m' \coloneqq$ any element $\in T \cap S_{c^*}$
else $m' \coloneqq \perp$
return $[\![m' = m^*]\!]$

Fig. 8. Game G_3 for the proof of Theorem 1.

The game G_3 actually can be seen as the $\mathsf{OW\text{-}CPA}$ game for PKE, in which an adversary $\mathcal{B}$ invokes the algorithm $\mathcal{D}$. More specifically, the $\mathsf{OW\text{-}CPA}$ game for PKE and the adversary $\mathcal{B}$ against PKE we construct are described in Fig. 9. We note that $\mathcal{B}$ cannot directly compute $\mathsf{H}(m^*)$ because m^* is unknown for $\mathcal{B}$, but $\mathcal{B}$ can choose a random value $d^* \in \{0,1\}^n$ as $\mathsf{H}(m^*)$ in advance and simulate H using it, i.e., $\mathcal{B}$ returns d^* if $\mathsf{Enc}(pk, m) = c^*$, else returns $\mathsf{H}(m)$, where m is $\mathcal{D}$'s query to H. Furthermore, if Bad doesn't happen, the set S_{c^*} has only one element, m^*, and the environments of $\mathcal{D}$ in game G_3 and game $\mathsf{OW\text{-}CPA}^{\mathcal{B}}_{\mathsf{PKE}}$ have the same distribution. In other words, $\mathcal{B}$ can simulate the environment for $\mathcal{D}$ as

[3] Like the note of [2, Theorem 1], if we want to consider an adversary $\mathcal{A}^{H,F}()$, we can instead write $\mathcal{A}^{H}(F)$ where F is a complete (exponential size) description of F since there is no assumption on the size of z. From another point of view, we can simply extend the Lemma 3 to cover this case explicitly by letting $\mathcal{D}$ forward $\mathcal{A}$'s queries to the additional oracles and send the replies back to $\mathcal{A}$.

in game G_3 perfectly in the case that Bad doesn't happen. Therefore, we have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{B}} &= \Pr[\mathsf{OW\text{-}CPA}^{\mathcal{B}}_{\mathsf{PKE}} \Rightarrow 1] \\ &= \Pr[\mathcal{B} \Rightarrow m^*] \\ &\geq \Pr[\mathcal{B} \Rightarrow m^* \wedge \overline{\mathsf{Bad}}] \\ &= \Pr[T \cap S_{c^*} \neq \varnothing \wedge \overline{\mathsf{Bad}}],\end{aligned}$$

where the final equality holds for the same reason that if Bad doesn't happen, the set S_{c^*} has only one element, m^*.

GAME $\mathsf{OW\text{-}CPA}^{\mathcal{B}}_{\mathsf{PKE}}$	$\mathcal{B}^{\mathsf{G}}(pk, c^*)$
$(pk, sk) \leftarrow \mathsf{Gen}$	$\mathsf{H}' \xleftarrow{\$} \Omega_{\mathsf{H}};\ d^* \xleftarrow{\$} \{0,1\}^n$
$\mathsf{G} \xleftarrow{\$} \Omega_{\mathsf{G}}$	$\mathsf{H} := \mathsf{H}';\ S_{c^*} := \{m \in \mathcal{M} \mid \mathsf{Enc}(pk, m) = c^*\}$
$m^* \xleftarrow{\$} \mathcal{M}$	**for each** $m \in S_{c^*},\ \mathsf{H}(m) := d^*$
$c^* := \mathsf{Enc}(pk, m^*)$	$T \leftarrow \mathcal{D}^{\mathsf{H},\mathsf{H}',\mathsf{G}}(pk, (c^*, d^*))$
$\quad = \mathsf{Enc}_0(pk, m^*; \mathsf{G}(m^*))$	**if** $T \cap S_{c^*} \neq \varnothing$
$m' \leftarrow \mathcal{B}^{\mathsf{G}}(pk, c^*)$	$\quad$ **return** any element $\in T \cap S_{c^*}$
return $[\![m' = m^*]\!]$	**else return** $\perp$

Fig. 9. Game $\mathsf{OW\text{-}CPA}^{\mathcal{B}}_{\mathsf{PKE}}$ for the proof of Theorem 1.

Combining above formulas with the following simple inequality:

$$\Pr[T \cap S_{c^*} \neq \varnothing] \leq \Pr[T \cap S_{c^*} \neq \varnothing \wedge \overline{\mathsf{Bad}}] + \Pr[\mathsf{Bad}],$$

we finally obtain

$$\begin{aligned}\mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{U}_{\mathcal{M}},\mathcal{A},\mathcal{S}} &= |\Pr[G_0^{\mathcal{A}} \Rightarrow 1] - \Pr[G_1^{\mathcal{A}} \Rightarrow 1]| \\ &= |\Pr[G_0^{\mathcal{A}} \Rightarrow 1] - \Pr[G_2^{\mathcal{A}} \Rightarrow 1]| \\ &\leq 4d_{\mathsf{H}} \cdot \Pr[T \cap S_{c^*} \neq \varnothing] \\ &\leq 4d_{\mathsf{H}} \cdot (\Pr[T \cap S_{c^*} \neq \varnothing \wedge \overline{\mathsf{Bad}}] + \Pr[\mathsf{Bad}]) \\ &\leq 4d_{\mathsf{H}} \cdot (\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{B}} + 2\delta).\end{aligned}$$

□

Theorem 2 (Security of KC in the QROM, Case 2). *Let* PKE *be a* δ*-correct* dPKE *with message space* $\mathcal{M}$*. Let* $\mathsf{H} : \mathcal{M} \to \{0,1\}^n$ *be a hash function modeled as a quantum random oracle.* $\mathsf{PKE}' := \mathsf{KC}[\mathsf{PKE}, \mathsf{H}]$ *and* $\mathcal{S}$ *is the algorithm defined in Fig. 5. Then we have* $\mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} \leq 2^{-n} + \delta$*. Moreover, for any adversary* $\mathcal{A}$ *against the* $\mathsf{DS\text{-}IND}$ *security of* PKE' *issuing quantum queries to* H *with depth* d_{H}*, there exists an adversary* $\mathcal{B}$ *against the* $\mathsf{OW\text{-}CPA}$ *security of* PKE *such that*

$$\mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{U}_{\mathcal{M}},\mathcal{A},\mathcal{S}} \leq 4d_{\mathsf{H}} \cdot (\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{B}} + \delta)$$

and $\mathsf{Time}(\mathcal{B}) \approx 2 \cdot \mathsf{Time}(\mathcal{A})$*.*

Proof. The proof is essentially the same as Theorem 1's proof, except for the definition of Bad:

$$\mathsf{Bad} := [\exists m \in \mathcal{M},\ \mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) \neq m | (pk, sk) \leftarrow \mathsf{Gen}].$$

From the fact that PKE is deterministic and the definition of δ-correct, we have

$$\Pr[\mathsf{Bad}] \leq \delta.$$

Then, we complete the proof. □

Remark 3. PKE′ remains δ-correct.

4 QCCA-Secure Generic KEM in the QROM

In this section, we prove that DS secure dPKEs can be converted to IND-qCCA secure KEMs by transformation SXY [20] in the QROM. In particular, we also consider two cases corresponding to the two cases in Sect. 3. The first case is that the underlying dPKE is derived from $\mathsf{KC} \circ \mathsf{T}$[4], as opposed to a general δ-correct dPKE in the second case. In both cases, underlying PKEs don't need to be perfectly correct. Note that the second case was proved in [22], we present it here as a lemma.

At the end, we combine results in this paper and get two IND-qCCA secure generic KEMs without quadratic security loss in the QROM. One is based on rPKEs and the other is based on dPKEs.

Transformation SXY. To a deterministic public-key encryption scheme $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$, and two hash functions $\mathsf{H}_1 : \mathcal{M} \to \mathcal{K}$, $\mathsf{H}_2 : \{0,1\}^l \times \mathcal{C} \to \mathcal{K}$, we associate $\mathsf{KEM} := \mathsf{SXY}[\mathsf{PKE}', \mathsf{H}_1, \mathsf{H}_2]$. The algorithms of $\mathsf{KEM} = (\mathsf{Gene}, \mathsf{Enca}, \mathsf{Deca})$ are defined in Fig. 10.

$\underline{\mathsf{Gene}}$	$\underline{\mathsf{Enca}(pk)}$	$\underline{\mathsf{Deca}((sk, s), c)}$
$(pk, sk) \leftarrow \mathsf{Gen}'$	$m \leftarrow \mathcal{D}_{\mathcal{M}}$	$m' := \mathsf{Dec}'(sk, c)$
$s \xleftarrow{\$} \{0,1\}^l$	$c := \mathsf{Enc}'(pk, m)$	**if** $m' = \perp$ **or** $\mathsf{Enc}'(pk, m') \neq c$
return $(pk, (sk, s))$	$k := \mathsf{H}_1(m)$	**return** $k' := \mathsf{H}_2(s, c)$
	return (c, k)	**else return** $k' := \mathsf{H}_1(m')$

Fig. 10. $\mathsf{KEM} = (\mathsf{Gene}, \mathsf{Enca}, \mathsf{Deca}) := \mathsf{SXY}[\mathsf{PKE}', \mathsf{H}_1, \mathsf{H}_2]$.

[4] T is the point and KC can be replaced by other suitable transformations.

Theorem 3 (IND-qCCA **Security of** SXY **in the QROM, Case 1).** *Let* PKE' *be a* dPKE *transformed from* PKE_0 *by* $\mathsf{KC} \circ \mathsf{T}$*, i.e.,* $\mathsf{PKE}' := \mathsf{KC}[\mathsf{T}[\mathsf{PKE}_0, \mathsf{G}], \mathsf{H}]$. PKE_0 *is a* δ*-correct* rPKE *with message space* $\mathcal{M}$*, ciphertext space* $\mathcal{C}$ *and randomness space* $\mathcal{R}$*. Let* $\mathsf{G} : \mathcal{M} \to \mathcal{R}$*,* $\mathsf{H} : \mathcal{M} \to \{0,1\}^n$*,* $\mathsf{H}_1 : \mathcal{M} \to \mathcal{K}$*,* $\mathsf{H}_2 : \{0,1\}^l \times \mathcal{C} \times \{0,1\}^n \to \mathcal{K}$ *be hash functions modeled as quantum random oracles. Suppose that* PKE' *is* $\mathcal{D}_{\mathcal{M}}$*-disjoint-simulatable with a simulator* $\mathcal{S}$*. Then for any adversary* $\mathcal{A}$ *against the* IND-qCCA *security of* $\mathsf{KEM} := \mathsf{SXY}[\mathsf{PKE}', \mathsf{H}_1, \mathsf{H}_2]$ *issuing* q_{G} *and* q_{H_2} *quantum queries to* G *and* H_2*, there exists an adversary* $\mathcal{B}$ *against the* DS-IND *security of* PKE' *such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} \leq \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}} + \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + (16q_{\mathsf{G}}^2 + 2) \cdot \delta$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Proof. We use a game-hopping proof. The proof is essentially the same as the following Lemma 5 [22]'s proof, except for two more games. We insert game $G_{0.5}$ and $G_{3.5}$ into G_0, G_1 and G_3, G_4 respectively. Besides, we replace the event $\overline{\mathsf{Acc}}$ with another event Bad. The overview of all games is given in Table 2.

Table 2. Summary of games for the proof of Theorem 3.

Game	H_1	c^*	k_0^*	k_1^*	Decryption of valid c	Decryption of invalid c	G/G'	justification
G_0	$\mathsf{H}_1(\cdot)$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_1(m^*)$	random	$\mathsf{H}_1(m)$	$\mathsf{H}_2(s, c)$	G	
$G_{0.5}$	$\mathsf{H}_1(\cdot)$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_1(m^*)$	random	$\mathsf{H}_1(m)$	$\mathsf{H}_2(s, c)$	G'	Lemma 2
G_1	$\mathsf{H}_1(\cdot)$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_1(m^*)$	random	$\mathsf{H}_1(m)$	$\mathsf{H}_q(c)$	G'	Lemma 1
$G_{1.5}$	$\mathsf{H}'_q(\mathsf{Enc}'(pk, \cdot))$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_1(m^*)$	random	$\mathsf{H}_1(m)$	$\mathsf{H}_q(c)$	G'	$\overline{\mathsf{Bad}}$
G_2	$\mathsf{H}_q(\mathsf{Enc}'(pk, \cdot))$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_1(m^*)$	random	$\mathsf{H}_1(m)$	$\mathsf{H}_q(c)$	G'	$\overline{\mathsf{Bad}}$
G_3	$\mathsf{H}_q(\mathsf{Enc}'(pk, \cdot))$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_q(c^*)$	random	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	G'	Conceptual
$G_{3.5}$	$\mathsf{H}_q(\mathsf{Enc}'(pk, \cdot))$	$\mathsf{Enc}'(pk, m^*)$	$\mathsf{H}_q(c^*)$	random	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	G	Lemma 2
G_4	$\mathsf{H}_q(\mathsf{Enc}'(pk, \cdot))$	$\mathcal{S}(pk)$	$\mathsf{H}_q(c^*)$	random	$\mathsf{H}_q(c)$	$\mathsf{H}_q(c)$	G	DS-IND

GAME G_0: This is the original game, $\mathsf{IND\text{-}qCCA}^{\mathcal{A}}_{\mathsf{KEM}}$.

Let G' be a random function such that $\mathsf{G}'(m)$ is sampled according to the uniform distribution over $\mathcal{R}^{good}_{(pk,sk),m} := \{r \in \mathcal{R} | \mathsf{Dec}_0(sk, \mathsf{Enc}_0(pk, m; r)) = m\}$. Let $\Omega_{\mathsf{G}'}$ be the set of all functions G'. Define $\delta_{(pk,sk),m} = \frac{|\mathcal{R} \setminus \mathcal{R}^{good}_{(pk,sk),m}|}{|\mathcal{R}|}$ as the fraction of bad randomness and $\delta_{(pk,sk)} = \max_{m \in \mathcal{M}} \delta_{(pk,sk),m}$. With this notation $\delta = \mathrm{E}[\delta_{(pk,sk)}]$, where the expectation is taken over $(pk, sk) \leftarrow \mathsf{Gen}_0$.

GAME $G_{0.5}$: This game is the same as G_0 except that we replace G by G' that uniformly samples from "good" randomness at random, i.e., $\mathsf{G}' \xleftarrow{\$} \Omega_{\mathsf{G}'}$.

GAME G_1: This game is the same as $G_{0.5}$ except that $\mathsf{H}_2(s, c)$ in the decapsulation oracle is replaced with $\mathsf{H}_q(c)$ where $\mathsf{H}_q : \mathcal{C} \times \{0,1\}^n \to \mathcal{K}$ is another random oracle. We remark that $\mathcal{A}$ is not given direct access to H_q.

GAME $G_{1.5}$: This game is the same as G_1 except that the random oracle $\mathsf{H}_1(\cdot)$ is simulated by $\mathsf{H}'_q(\mathsf{Enc}'(pk, \cdot))$ where H'_q is yet another random oracle. We

remark that the decapsulation oracle and generation of k_0^* also use $\mathsf{H}'_q(\mathsf{Enc}'(pk,\cdot))$ as $\mathsf{H}_1(\cdot)$ and that $\mathcal{A}$ is not given direct access to H'_q.

GAME G_2: This game is the same as $G_{1.5}$ except that the random oracle $\mathsf{H}_1(\cdot)$ is simulated by $\mathsf{H}_q(\mathsf{Enc}'(pk,\cdot))$ instead of $\mathsf{H}'_q(\mathsf{Enc}'(pk,\cdot))$. We remark that the decapsulation oracle and generation of k_0^* also use $\mathsf{H}_q(\mathsf{Enc}'(pk,\cdot))$ as $\mathsf{H}_1(\cdot)$.

GAME G_3: This game is the same as G_2 except that k_0^* is set as $\mathsf{H}_q(c^*)$ and the decapsulation oracle always returns $\mathsf{H}_q(c)$ as long as $c \neq c^*$. We denote the modified decapsulation oracle by Deca'.

GAME $G_{3.5}$: This game is the same as G_3 except that we switch G' back to the ideal random oracle G.

GAME G_4: This game is the same as $G_{3.5}$ except that c^* is set as $\mathcal{S}(pk)$.

The above completes the descriptions of games. We clearly have

$$\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} = |\Pr[G_0 \Rightarrow 1] - 1/2|$$

by the definition. We bound this by the following claims.

Claim 1. *We have*

$$|\Pr[G_0 \Rightarrow 1] - \Pr[G_{0.5} \Rightarrow 1]| \leq 8q_{\mathsf{G}}^2\delta,$$

$$|\Pr[G_3 \Rightarrow 1] - \Pr[G_{3.5} \Rightarrow 1]| \leq 8q_{\mathsf{G}}^2\delta.$$

Proof. Following the same analysis as in the proof of [15, Theorem 1], we can show that the distinguishing problem between G_0 and $G_{0.5}$ is essentially the distinguishing problem between G and G', which can be converted into a distinguishing problem between F_1 and F_2, where F_1 is a function such that $\mathsf{F}_1(m)$ is sampled according to Bernoulli distribution $B_{\delta_{(pk,sk),m}}$, i.e., $\Pr[\mathsf{F}_1(m) = 1] = \delta_{(pk,sk),m}$ and $\Pr[\mathsf{F}_1(m) = 0] = 1-\delta_{(pk,sk),m}$, and F_2 is a constant function that always outputs 0 for any input. Thus, conditioned on a fixed (pk, sk) we obtain by Lemma 2, $|\Pr[G_0 \Rightarrow 1|(pk,sk)] - \Pr[G_{0.5} \Rightarrow 1|(pk,sk)]| \leq 8q_{\mathsf{G}}^2\delta_{(pk,sk)}$. By averaging over $(pk, sk) \leftarrow \mathsf{Gen}_0$ we finally obtain

$$|\Pr[G_0 \Rightarrow 1] - \Pr[G_{0.5} \Rightarrow 1]| \leq 8q_{\mathsf{G}}^2\mathrm{E}[\delta_{(pk,sk)}] = 8q_{\mathsf{G}}^2\delta.$$

In the same way, we have

$$|\Pr[G_3 \Rightarrow 1] - \Pr[G_{3.5} \Rightarrow 1]| \leq 8q_{\mathsf{G}}^2\delta.$$

□

Claim 2. *We have*

$$|\Pr[G_{0.5} \Rightarrow 1] - \Pr[G_1 \Rightarrow 1]| \leq q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}}.$$

Proof. This is obvious from Lemma 1. □

Claim 3. *We define an event:*

$$\mathsf{Bad} := [\exists m \in \mathcal{M}, \mathcal{R}^{good}_{(pk,sk),m} = \varnothing | (pk, sk) \leftarrow \mathsf{Gen_0}].$$

Then we have $\Pr[\mathsf{Bad}] \leq \delta$ *and*

$$|\Pr[G_1 \Rightarrow 1] - 1/2| \leq |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta.$$

Proof. By the definition, we have

$$\begin{aligned}
&\Pr[\mathsf{Bad}] \\
&= \Pr[\exists m \in \mathcal{M}, \mathcal{R}^{good}_{(pk,sk),m} = \varnothing | (pk, sk) \leftarrow \mathsf{Gen_0}] \\
&= \Pr[\exists m \in \mathcal{M}, \delta_{(pk,sk),m} = 1 | (pk, sk) \leftarrow \mathsf{Gen_0}] \\
&= \Pr[\delta_{(pk,sk)} = 1 | (pk, sk) \leftarrow \mathsf{Gen_0}] \\
&\leq \mathrm{E}[\delta_{(pk,sk)}] \\
&= \delta.
\end{aligned}$$

Then we have

$$\begin{aligned}
&|\Pr[G_1 \Rightarrow 1] - 1/2| \\
&= |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] + \Pr[G_1 \Rightarrow 1 \wedge \mathsf{Bad}] - 1/2| \\
&\leq |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \Pr[G_1 \Rightarrow 1 \wedge \mathsf{Bad}] \\
&\leq |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \Pr[\mathsf{Bad}] \\
&\leq |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta
\end{aligned}$$

as we wanted. □

Claim 4. *We have*

$$\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] = \Pr[G_{1.5} \Rightarrow 1 \wedge \overline{\mathsf{Bad}}].$$

Proof. From the definition of G', if Bad doesn't happen, any message can be decrypted correctly for the PKE', i.e., $\mathsf{Dec}'(sk, \mathsf{Enc}'(pk, m)) = m$ for all $m \in \mathcal{M}$. Therefore, $\mathsf{Enc}'(pk, \cdot)$ is injective. And if $\mathsf{H}'_q(\cdot)$ is a random function, then $\mathsf{H}'_q(\mathsf{Enc}'(pk, \cdot))$ 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 $\mathsf{H_1}(\cdot)$ with $\mathsf{H}'_q(\mathsf{Enc}'(pk, \cdot))$. □

Claim 5. *We have*

$$\Pr[G_{1.5} \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] = \Pr[G_2 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}].$$

Proof. We say that a ciphertext c is valid if we have $\mathsf{Enc}'(pk, \mathsf{Dec}'(sk, c)) = c$ and invalid otherwise. We remark that H_q is used only for decrypting an invalid ciphertext c as $\mathsf{H}_q(c)$ in $G_{1.5}$. This means that a value of $\mathsf{H}_q(c)$ for a valid c is not used at all in $G_{1.5}$.

On the other hand, any output of $\mathsf{Enc}'(pk,\cdot)$ is valid if Bad doesn't happen. Since H'_q is only used for evaluating an output of $\mathsf{Enc}'(pk,\cdot)$, a value of $\mathsf{H}'_q(c)$ for an invalid c is not used at all in $G_{1.5}$.

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. □

Claim 6. *We have*

$$\Pr[G_2 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] = \Pr[G_3 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}].$$

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

Claim 7. *We have*

$$|\Pr[G_3 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| \leq |\Pr[G_3 \Rightarrow 1] - 1/2| + \delta.$$

Proof. We have

$$\begin{aligned}
&|\Pr[G_3 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| \\
&= |\Pr[G_3 \Rightarrow 1] - \Pr[G_3 \Rightarrow 1 \wedge \mathsf{Bad}] - 1/2| \\
&\leq |\Pr[G_3 \Rightarrow 1] - 1/2| + \Pr[G_3 \Rightarrow 1 \wedge \mathsf{Bad}] \\
&\leq |\Pr[G_3 \Rightarrow 1] - 1/2| + \Pr[\mathsf{Bad}] \\
&\leq |\Pr[G_3 \Rightarrow 1] - 1/2| + \delta.
\end{aligned}$$

□

Claim 8. *There exists a quantum adversary $\mathcal{B}$ such that*

$$|\Pr[G_{3.5} \Rightarrow 1] - \Pr[G_4 \Rightarrow 1]| = \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}}$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Proof. We construct an adversary $\mathcal{B}$, which is allowed to access two random oracles H_q and H_2, against the disjoint simulatability as follows.

$\mathcal{B}^{\mathsf{H}_q,\mathsf{H}_2}(pk,c^*)$: It picks $b \leftarrow \{0,1\}$, sets $k_0^* := \mathsf{H}_q(c^*)$ and $k_1^* \xleftarrow{\$} \mathcal{K}$, and invokes $b' \leftarrow \mathcal{A}^{\mathsf{H}_1,\mathsf{H}_2,\mathsf{Deca}'}(pk,c^*,k_b^*)$ where $\mathcal{A}$'s oracles are simulated as follows:

- $\mathsf{H}_1(\cdot)$ is simulated by $\mathsf{H}_q(\mathsf{Enc}'(pk,\cdot))$.
- H_2 can be simulated because $\mathcal{B}$ has access to an oracle H_2.
- Deca' is simulated by filtering c^* and using $\mathsf{H}_q(\cdot)$, that is, on input $\sum_{c,k}\psi_{c,k}|c,k\rangle$, $\mathcal{B}$ returns $\sum_{c\neq c^*,k}\psi_{c,k}|c,k\oplus\mathsf{H}_q(c)\rangle + \sum_k \psi_{c^*,k}|c^*,k\oplus\perp\rangle$.

Finally, $\mathcal{B}$ returns $[\![b'=b]\!]$.

This completes the description of $\mathcal{B}$. It is easy to see that $\mathcal{B}$ perfectly simulates $G_{3.5}$ if $c^* = \mathsf{Enc}'(pk,m^*)$ and G_4 if $c^* = \mathcal{S}(pk)$. Therefore, we have

$$|\Pr[G_{3.5} \Rightarrow 1] - \Pr[G_4 \Rightarrow 1]| = \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}}$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$. □

Claim 9. *We have*

$$|\Pr[G_4 \Rightarrow 1] - 1/2| \leq \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}}.$$

Proof. Let Bad' denote the event that c^* is in $\mathsf{Enc}'(pk, \mathcal{M})$ in G_4. Then we have

$$\Pr[\mathsf{Bad}'] = \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}}.$$

When Bad' does not occur, i.e., $c^* \notin \mathsf{Enc}'(pk, \mathcal{M})$, $\mathcal{A}$ obtains no information about $k_0^* = \mathsf{H}_q(c^*)$. This is because queries to H_1 only reveal $\mathsf{H}_q(c)$ for $c \in \mathsf{Enc}'(pk, \mathcal{M})$, and $\mathsf{Deca}'(c)$ returns $\perp$ if $c = c^*$. Therefore, we have

$$\Pr[G_4 \Rightarrow 1|\overline{\mathsf{Bad}'}] = 1/2.$$

Combining the above, we have

$$\begin{aligned}
&|\Pr[G_4 \Rightarrow 1] - 1/2| \\
&= |\Pr[\mathsf{Bad}'] \cdot (\Pr[G_4 \Rightarrow 1|\mathsf{Bad}'] - 1/2) + \Pr[\overline{\mathsf{Bad}'}] \cdot (\Pr[G_4 \Rightarrow 1|\overline{\mathsf{Bad}'}] - 1/2)| \\
&\leq \Pr[\mathsf{Bad}'] + |\Pr[G_4 \Rightarrow 1|\overline{\mathsf{Bad}'}] - 1/2| \\
&= \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}}
\end{aligned}$$

as we wanted. □

Combining all claims above, we obtain the following inequality:

$$\begin{aligned}
&\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} \\
&= |\Pr[G_0 \Rightarrow 1] - 1/2| \\
&\leq |\Pr[G_{0.5} \Rightarrow 1] - 1/2| + 8q_{\mathsf{G}}^2\delta \\
&\leq |\Pr[G_1 \Rightarrow 1] - 1/2| + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&\leq |\Pr[G_1 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&= |\Pr[G_{1.5} \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&= |\Pr[G_2 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&= |\Pr[G_3 \Rightarrow 1 \wedge \overline{\mathsf{Bad}}] - 1/2| + \delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&\leq |\Pr[G_3 \Rightarrow 1] - 1/2| + 2\delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 8q_{\mathsf{G}}^2\delta \\
&\leq |\Pr[G_{3.5} \Rightarrow 1] - 1/2| + 2\delta + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 16q_{\mathsf{G}}^2\delta \\
&\leq |\Pr[G_4 \Rightarrow 1] - 1/2| + \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}} + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + (16q_{\mathsf{G}}^2 + 2) \cdot \delta \\
&\leq \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}} + \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + (16q_{\mathsf{G}}^2 + 2) \cdot \delta.
\end{aligned}$$

□

Lemma 5 (IND-qCCA Security of SXY in the QROM, Case 2 [22, Theorem 4.1]**).** *Let* PKE' *be a* δ*-correct* dPKE *with message space* $\mathcal{M}$ *and ciphertext*

space $\mathcal{C}$. *Let* $\mathsf{H}_1 : \mathcal{M} \to \mathcal{K}$, $\mathsf{H}_2 : \{0,1\}^l \times \mathcal{C} \to \mathcal{K}$ *be hash functions modeled as quantum random oracles. Suppose that* PKE' *is* $\mathcal{D}_{\mathcal{M}}$*-disjoint-simulatable with a simulator* $\mathcal{S}$. *Then for any adversary* $\mathcal{A}$ *against the* IND-qCCA *security of* $\mathsf{KEM} := \mathsf{SXY}[\mathsf{PKE}', \mathsf{H}_1, \mathsf{H}_2]$ *issuing* q_{H_2} *quantum queries to* H_2, *there exists an adversary* $\mathcal{B}$ *against the* DS-IND *security of* PKE' *such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} \leq \mathsf{Adv}^{\mathsf{DS\text{-}IND}}_{\mathsf{PKE}',\mathcal{D}_{\mathcal{M}},\mathcal{B},\mathcal{S}} + \mathsf{Disj}_{\mathsf{PKE}',\mathcal{S}} + q_{\mathsf{H}_2} \cdot 2^{\frac{-l+1}{2}} + 2\delta$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Remark 4. Lemma 5 still holds with our modified definition of DS. The only thing that needs to be changed is "$\Pr[\mathsf{Bad}] \leq \mathsf{Disj}_{\mathsf{PKE}_1,\mathcal{S}}$" in [22, Lemma 4.8], which should be replaced with "$\Pr[\mathsf{Bad}] = \mathsf{Disj}_{\mathsf{PKE}_1,\mathcal{S}}$" as $(ek, dk) \leftarrow \mathsf{Gen}_1$ exactly in the proof.

Remark 5. KEM remains δ-correct.

We also need the following lemma about the security of transformation T. It is a version without the square-root advantage loss at the cost of stronger security requirement of the underlying PKE.

Lemma 6 (Security of T in the QROM [5, Theorem 1]**).** *Let* PKE_0 *be a* rPKE *with messages space* $\mathcal{M}$ *and random space* $\mathcal{R}$. *Let* $\mathsf{G} : \mathcal{M} \to \mathcal{R}$ *be a hash function modeled as a quantum random oracle. Then for any adversary* $\mathcal{A}$ *against the* OW-CPA *security of* $\mathsf{PKE} := \mathsf{T}[\mathsf{PKE}_0, \mathsf{G}]$ *issuing* q_{G} *quantum queries to* G *with depth* d_{G}, *there exists an adversary* $\mathcal{B}$ *against the* IND-CPA *security of* PKE_0 *such that*

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}} \leq (d_{\mathsf{G}} + 2) \cdot \left(\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}_0,\mathcal{B}} + \frac{8(q_{\mathsf{G}} + 1)}{|\mathcal{M}|} \right)$$

and $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$.

Finally, we can get the security results of the two KEMs. For simplicity, we assume the number of parallel queries is n_p for all oracle algorithms. And we use $\mathcal{A}^{\mathsf{P}}$ in the following proofs to denote the adversary against the scheme P.

Combining Lemma 6 with Theorem 1 and Theorem 3, we obtain the following result for the IND-qCCA security of $\mathsf{KEM} := \mathsf{SXY} \circ \mathsf{KC} \circ \mathsf{T}$ from the IND-CPA security of a δ-correct rPKE in the QROM.

Corollary 1 (IND-qCCA Security of $\mathsf{SXY} \circ \mathsf{KC} \circ \mathsf{T}$ **in the QROM).** *Let* PKE_0 *be a* δ*-correct* rPKE *with message space* $\mathcal{M}$, *ciphertext space* $\mathcal{C}$ *and randomness space* $\mathcal{R}$. *Let* $\mathsf{G} : \mathcal{M} \to \mathcal{R}$, $\mathsf{H} : \mathcal{M} \to \{0,1\}^n$, $\mathsf{H}_1 : \mathcal{M} \to \mathcal{K}$, $\mathsf{H}_2 : \{0,1\}^l \times \mathcal{C} \times \{0,1\}^n \to \mathcal{K}$ *be hash functions modeled as quantum random oracles. Then for any adversary* $\mathcal{A}$ *against the* IND-qCCA *security of* $\mathsf{KEM} := \mathsf{SXY}[\mathsf{KC}[\mathsf{T}[\mathsf{PKE}_0, \mathsf{G}], \mathsf{H}], \mathsf{H}_1, \mathsf{H}_2]$ *issuing* q_{G}, q_{H}, q_{H_1} *and* q_{H_2} *quantum queries to* G, H, H_1 *and* H_2 *with*

depth d_{G}, d_{H}, d_{H_1} *and* d_{H_2}, *there exists an adversary* $\mathcal{B}$ *against the* IND-CPA *security of* PKE_0 *such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}} \leq 4d'_{\mathsf{H}}(d'_{\mathsf{G}}+2)\cdot\left(\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}_0,\mathcal{B}}+\frac{8(q'_{\mathsf{G}}+1)}{|\mathcal{M}|}\right) + (16q_{\mathsf{G}}^2+8d'_{\mathsf{H}}+4)\cdot\delta+q_{\mathsf{H}_2}\cdot 2^{\frac{-l+1}{2}}+2^{-n}$$

and $\mathsf{Time}(\mathcal{B})\approx 2\cdot\mathsf{Time}(\mathcal{A})$, *where* $d'_{\mathsf{H}}:=d_{\mathsf{H}}+d_{\mathsf{H}_1}$, $d'_{\mathsf{G}}:=2(d_{\mathsf{G}}+d_{\mathsf{H}}+2d_{\mathsf{H}_1}+1)$ *and* $q'_{\mathsf{G}}:=2(q_{\mathsf{G}}+q_{\mathsf{H}}+2q_{\mathsf{H}_1}+n_p)$.

Proof. From the construction of $\mathcal{A}^{\mathsf{PKE}'}$ in the proof of Theorem 3, we can know that $\mathcal{A}^{\mathsf{PKE}'}$ issues $q_{\mathsf{G}}+q_{\mathsf{H}_1}$, $q_{\mathsf{H}}+q_{\mathsf{H}_1}$ queries to G, H with depth $d_{\mathsf{G}}+d_{\mathsf{H}_1}$, $d_{\mathsf{H}}+d_{\mathsf{H}_1}$. Furthermore, from the construction of $\mathcal{A}^{\mathsf{PKE}}$ in the proof of Theorem 1 and the construction of $\mathcal{D}$ in the proof of Lemma 3, we can know that $\mathcal{A}^{\mathsf{PKE}}$ issues at most $(q_{\mathsf{G}}+q_{\mathsf{H}_1})\times 2+(q_{\mathsf{H}}+q_{\mathsf{H}_1})\times 2+2n_p$ queries to G with depth $(d_{\mathsf{G}}+d_{\mathsf{H}_1})\times 2+(d_{\mathsf{H}}+d_{\mathsf{H}_1})\times 2+2$, where the first part comes from $\mathcal{D}$'s twice invocations to $\mathcal{A}^{\mathsf{PKE}'}$, the second part comes from $\mathcal{D}$'s queries to H and H', and the third part comes from $\mathcal{A}^{\mathsf{PKE}}$'s testing of the set T returned by $\mathcal{D}$. □

Combining Theorem 2 with Lemma 5, we obtain the following result for the IND-qCCA security of $\mathsf{KEM}:=\mathsf{SXY}\circ\mathsf{KC}$ from the OW-CPA security of a δ-correct dPKE in the QROM.

Corollary 2 (IND-qCCA Security of $\mathsf{SXY}\circ\mathsf{KC}$ in the QROM). *Let* PKE *be a* δ*-correct* dPKE *with message space* $\mathcal{M}$ *and ciphertext space* $\mathcal{C}$. *Let* $\mathsf{H}:\mathcal{M}\to\{0,1\}^n$, $\mathsf{H}_1:\mathcal{M}\to\mathcal{K}$, $\mathsf{H}_2:\{0,1\}^l\times\mathcal{C}\times\{0,1\}^n\to\mathcal{K}$ *be hash functions modeled as quantum random oracles. Then for any adversary* $\mathcal{A}$ *against the* IND-qCCA *security of* $\mathsf{KEM}:=\mathsf{SXY}[\mathsf{KC}[\mathsf{PKE},\mathsf{H}],\mathsf{H}_1,\mathsf{H}_2]$ *issuing* q_{H}, q_{H_1} *and* q_{H_2} *quantum queries to* H, H_1 *and* H_2 *with depth* d_{H}, d_{H_1} *and* d_{H_2}, *there exists an adversary* $\mathcal{B}$ *against the* OW-CPA *security of* PKE *such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}qCCA}}_{\mathsf{KEM},\mathcal{A}}\leq 4d'_{\mathsf{H}}\cdot\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},\mathcal{B}}+(4d'_{\mathsf{H}}+3)\cdot\delta+q_{\mathsf{H}_2}\cdot 2^{\frac{-l+1}{2}}+2^{-n}$$

and $\mathsf{Time}(\mathcal{B})\approx 2\cdot\mathsf{Time}(\mathcal{A})$, *where* $d'_{\mathsf{H}}:=d_{\mathsf{H}}+d_{\mathsf{H}_1}$.

Proof. From the construction of $\mathcal{A}^{\mathsf{PKE}'}$ in the proof of Lemma 5, we can know that $\mathcal{A}^{\mathsf{PKE}'}$ issues $q_{\mathsf{H}}+q_{\mathsf{H}_1}$ queries to H with depth $d_{\mathsf{H}}+d_{\mathsf{H}_1}$. □

Acknowledgements. We would like to thank the anonymous reviewers for pointing out proof gaps in a previous version of this paper and for their helpful suggestions. The authors are supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704702), the National Natural Science Foundation of China (Grant No. 61832012) and the National Cryptography Development Fund (Grant No. MMJJ20180210).

References

1. Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: the hardness of quantum rewinding. In: 2014 IEEE 55th Annual Symposium on Foundations of Computer Science, pp. 474–483, October 2014. https://doi.org/10.1109/FOCS.2014.57
2. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. LNCS, vol. 11693, pp. 269–295. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26951-7_10
3. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM **48**(4), 778–797 (2001). https://doi.org/10.1145/502090.502097
4. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 62–73. CCS '93, Association for Computing Machinery, New York (1993). https://doi.org/10.1145/168588.168596
5. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019. LNCS, vol. 11892, pp. 61–90. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36033-7_3
6. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random Oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_3
7. Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 361–379. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_21
8. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. **33**(1), 167–226 (2004). https://doi.org/10.1137/S0097539702403773
9. Dent, A.W.: A designer's guide to KEMs. In: Paterson, K.G. (ed.) Cryptography and Coding 2003. LNCS, vol. 2898, pp. 133–151. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40974-8_12
10. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_34
11. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. J. Cryptology **26**(1), 80–101 (Jan 2013). https://doi.org/10.1007/s00145-011-9114-1
12. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10677, pp. 341–371. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70500-2_12
13. 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.) PKC 2020. LNCS, vol. 12111, pp. 389–422. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45388-6_14

14. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49384-7_15
15. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random Oracle model, revisited. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10993, pp. 96–125. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96878-0_4
16. Jiang, H., Zhang, Z., Ma, Z.: Key encapsulation mechanism with explicit rejection in the quantum random Oracle model. In: Lin, D., Sako, K. (eds.) PKC 2019. LNCS, vol. 11443, pp. 618–645. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17259-6_21
17. 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.) PQCrypto 2019. LNCS, vol. 11505, pp. 227–248. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_13
18. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.-F.: Measure-rewind-measure: tighter quantum random Oracle model proofs for one-way to hiding and CCA Security. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 703–728. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_24
19. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th edn. Cambridge University Press, USA (2011)
20. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random Oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10822, pp. 520–551. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_17
21. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 129–146. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_8
22. Xagawa, K., Yamakawa, T.: (Tightly) QCCA-secure key-encapsulation mechanism in the quantum random Oracle model. In: Ding, J., Steinwandt, R. (eds.) PQCrypto 2019. LNCS, vol. 11505, pp. 249–268. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_14